# SANS GIAC Firewalls, Perimeter Protection, and VPNs
# GCFW Practical Assignment Version 1.5e

SANSFire Security Conference 2001, Washington D.C.

Submitted by:
Doreen Nozawa
October 10, 2001

Contents Page

**Assignment 1: Security Architecture for GIAC Enterprises**
Practical Assignment Overview
Network Traffic Profile
- Suppliers 3
- Partners 3
- Customers 4
- Internal Users 4

Infrastructure Design 4
- Addressing Requirements 4
- Network Diagram

**Assignment 2: Security Policy for GIAC Enterprises**
Corporate Security Policy Overview 6
Infrastructure Devices
- Border Router 6
- Primary Firewall 9
- VPN 12
- Internal Firewall (Secure Network) 15
- Internal Firewall (Fortune Network) 16
- Service Network Router 17
- Service Network Switch 19

**Assignment 3: Audit Your Security Architecture**
Plan the Assessment 20
Implment the Assessment 21
Perimeter Analysis 21

**Assignment 4: Design Under Fire**
Attacking the Border Router 25
Attacking the Firewall 27

References 29

## Practical Assignment Overview

Focus of this project is to define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. The architecture plan must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Diagrams and explanatory text is required to define how perimeter technologies have been implemented in the security architecture. The practical is presented in the following four parts:

- Assignment 1 - Security Architecture
- Assignment 2 - Security Policy
- Assignment 3 - Audit your Security Architecture
- Assignment 4 - Design under fire

## ASSIGNMENT 1: SECURITY ARCHITECTURE

### Network Traffic Profiles

Suppliers

Suppliers provide GIAC with Fortune Cookie sayings via a VPN tunnel. As this information is to become the company's 'crown jewels' an IPSEC tunnel is used to provide for a secure, encrypted data flow. Suppliers are able to pass their sayings to the secured databases located on the Production network behind the external firewall. The sayings are then screened, the transactional information is recorded and transferred to the administrative segment of the corporate network, and then transferred to the Fortune Cookie LAN to be encrypted and stored. Suppliers do not do not have direct access to the Fortune Cookie LAN where the sayings are stored.

Partners - Extranet Traffic
Partners are provided access to the internal network via a VPN tunnel. Partners are responsible for the purchase and re-sale of GIAC cookie sayings; hence, they will be provided access to the partner database behind the Fortune Cookie firewall, but they will not have direct access to the highly sensitive Fortune Cookie database Partners will access the application servers and databases on the Partner network. Web-proxy, mail, and nameserver services for the partner LAN are provided by the internal devices in the corporate network.

Customers

- General HTTP (80) web surfing traffic
- Secure HTTPS (443) connections for e-commerce transactions

General web surfing traffic via HTTP is allowed to access the external web servers located on the external service network. Customers who wish to purchase fortune cookie sayings can access the secured network via HTTPS(443) to submit orders and view transaction history and billing information. Usernames and passwords are stored on the web on the same segment, behind a Linux (kernal 2.4) Firewall running ipchains and hardened with Bastille Linux. Stored passwords will be encrypted using GnuPG 1.0.6 and stored on this segment.

Internal Users

Outbound internet traffic is statefully inspected by the primary firewall; hence only connections initiated by internal users (ie. general web surfing traffic, ftp, https, etc.) is allowed. Filters exist to restrict access to the Fortune Cookie LAN to the appropriate users that have a valid business need to access the sensitive data stored on these servers. Internal services, web-proxy, mail, DNS, LDAP servers are accessible to internal users. Network support personnel and mobile users will have remote access to the Corporate Network via a VPN tunnel to the corporate network.

**Infrastructure Design**

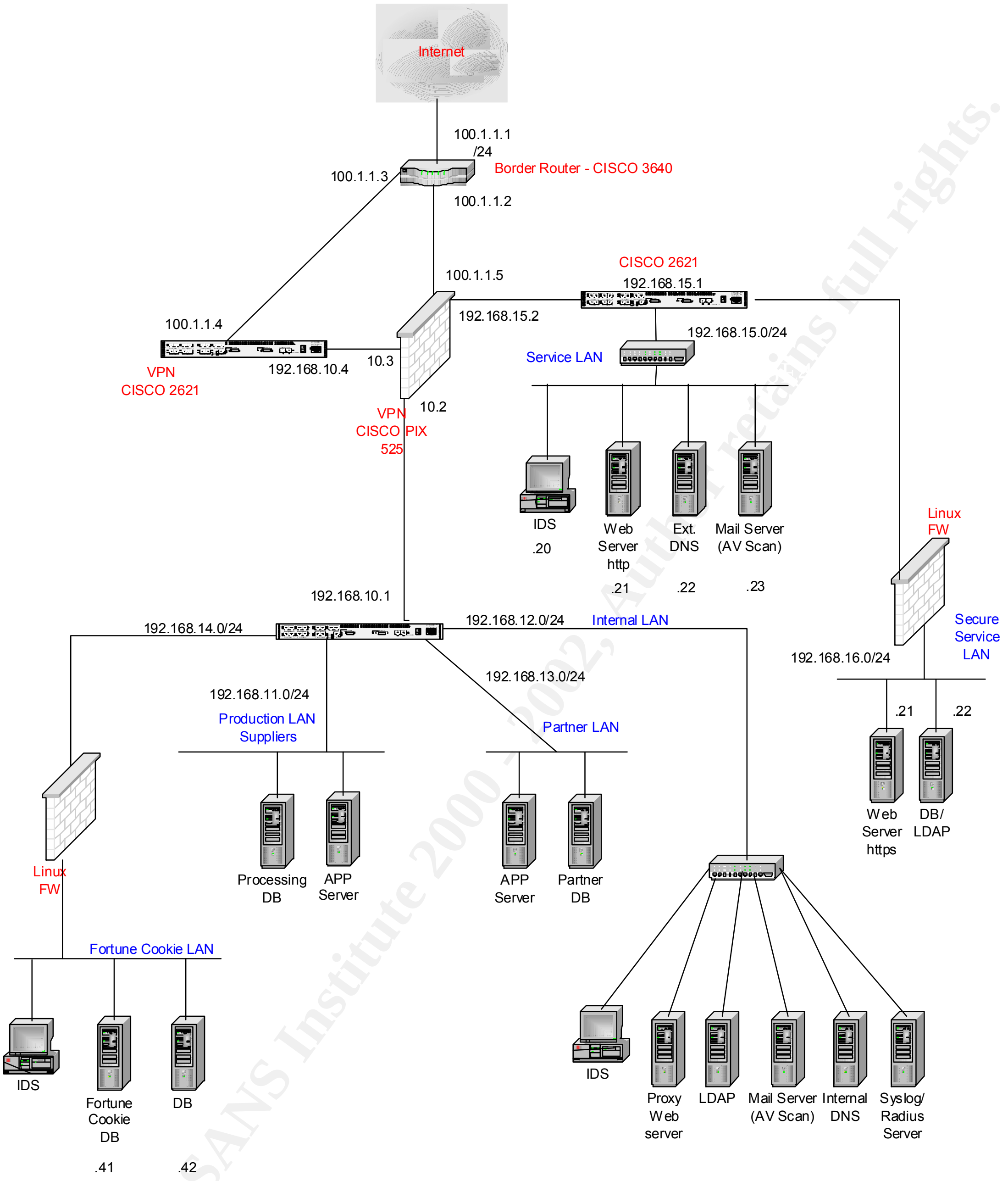
Addressing Requirements:

| | |
|---|---|
| 100.1.1.0/24 | Public IP |
| 192.168.10.0/24 | Management subnet |
| 192.168.11.0/24 | Production LAN |
| 192.168.12.0/24 | Corporate LAN |
| 192.168.13.0/24 | Partner LAN |
| 192.168.14.0/24 | Fortune Cookie LAN |
| 192.168.15.0/24 | Service Network – Web |
| 192.168.16.0/24 | Secure Service Network |

Network Diagram Overview

Primary internet gateway is the CISCO 3640 Border Router. A CISCO PIX 525 Firewall provides access to the external service network. Split horizon is achieved through a complete separation of external services from internal services. The most protected segment is the Fortune Cookie LAN on which the actual sayings are stored. As recommended by security professionals, a variety of firewalls (CISCO IOS, PIX, and Linux – ipchains) are used in the network.

GIAC Network Diagram



## Assignment 2: Security Policy for GIAC Enterprises

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPsec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPsec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

| **Firewall/Border Router Filters (General Overview)** | | | | |
|---|---|---|---|---|
| **Permit/ Deny** | **Source** | **Destination** | **Port/protocol** | **Policy** |
| permit | any | mail server (.23) | 25 (tcp) | service network |
| permit | any | dns server (.22) | 53 (udp) | service network |
| permit | any | web server (.21) | 80 (tcp) | service network |
| permit | any | https server | 443 (tcp) | secure service network |
| permit | vpn | internal .11,.12,.13 | 50(esp),51 (ah),500(udp) | vpn tunnel (fom .11,.12,.13 subnets only) |
| permit | internal .11,.12,.13 | vpn | 50(esp),51 (ah),500(udp) | vpn tunnel (to .11,.12,.13 subnets only) |
| permit | internal | any | any | outbound internal user traffic (includes internal services) |
| permit | any | internal network | >1023 (tcp,udp) | return traffic to internally initiated connections |
| permit | 4 internal hosts | secure network | 443, 1234, 1235 | support/admin connection with secure network |
| deny | any | any | any | default deny statement |
| **Fortune Cookie Lan Filters (General Overview)** | | | | |
| permit | 192.168.12.30 | 192.168.14.41 | 2234 | authentication port for internal host to Cookie DB |
| permit | 192.168.12.31 | 192.168.14.42 | 2234 | authentication port for internal host to Cookie DB |
| permit | 192.168.12.30 | 192.168.14.41 | 2235 | data connection between Internal hosts & Cookie DB |
| permit | 192.168.12.31 | 192.168.14.42 | 2235 | data connection between Internal hosts & Cookie DB |
| permit | 192.168.12.30 | 192.168.14.41 | icmp | ping from internal hosts |
| permit | 192.168.12.31 | 192.168.14.42 | icmp | ping from internal hosts |
| deny | any | any | any | default deny statement |

## Border Router - CISCO 3640 (IOS 12.2.5 ENTERPRISE PLUS IPSEC 3DES)

A Cisco 3640 router was selected for the Border Router. It will server as the packet filtering router for the GIAC network and enforce the security policy related to internet access for internal and external users to the GIAC network. Standard ingress and egress filtering is implemented to block private addresses, multicasts, spoofed ip addresses, and broadcast from entering the GIAC network.

Descriptive, named access-lists will be applied to the appropriate interfaces, as a means to easily identify the data flows for which the rule sets are defined. Filters will be reviewed and tested by issuing commands that either are permitted or denied by the applied access lists and then reviewing the log entries the 'show access-lists' command, to verify the filters are functioning as intended.

Ingress and egress filtering will be implemented on the Border Router to prevent spoofed IP packets from entering or leaving the network. For example, a packet with a

source address of 10.1.1.1 would never be a legitimate packet coming from the internet; hence, it should be promptly discarded at the Border Router's external interface.
Standard Security Base Configuration for all routers and switches in the GIAC network (some of these are part of the default configuration, but should be reviewed that they are present in the configuration):

```
service password-encryption
no ip direct-broadcast
no ip source-route
no tcp-small-servers
no udp-small-servers
no ip finger
no service pad
no cdp run
no ip http server
no snmp
no ip proxy arp

!set banner motd
banner ^ Authorized access only. Violators will be prosecuted! ^C

!other options (user preference to turn off the annoying options):
no ip domain-lookup
no logging console
```

**From_Internet** access-list details:

```
 !  Deny RFC#1918 addresses
 access-list From_Internet deny   ip 0.0.0.0 0.255.255.255 any log
 access-list From_Internet deny   ip 10.0.0.0 0.255.255.255 any log
 access-list From_Internet deny   ip 127.0.0.0 0.255.255.255 any log
 access-list From_Internet deny   ip 172.16.0.0 0.15.255.255 any log
 access-list From_Internet deny   ip 192.168.0.0 0.0.255.255 any log

 !  disallow multi-cast
 access-list Internet_in deny   ip 224.0.0.0 31.255.255.255 any log
 !  disallow broadcast
 access-list From_Internet deny   ip host 255.255.255.255 any log

!Deny spoofed packets:
access-list From_Internet deny ip 100.1.1.0 0.0.0.255 any  log

!Deny attempts to tftp to Border Router
access-list From_Internet deny udp any any eq 69 log

! Allow traffic to service network
```

```
access-list From_Internet  permit tcp any 100.1.1.21 eq www
access-list From_Internet  permit udp any 100.1.1.22 eq nameserver
access-list From_Internet  permit tcp any 100.1.1.23 eq smtp
access-list From_Internet  permit tcp any 100.1.1.24 eq 443

!Allow return tcp and udp traffic
access-list From_Internet  permit tcp any any gt 1023 established
access-list From_Internet  permit udp any any gt 1023

!Permit VPN traffic/IPSec protocols
access-list From_Internet  permit udp any any eq isakmp log
access-list From_Internet  permit esp any any
access-list From_Internet  permit ahp any any

!Deny everything else
access-list From_Internet  deny   ip any any log

interface Serial0
 description From Internet
 ip address 100.1.1.1 255.255.255.240
 no ip directed-broadcast
 no ip mroute-cache
 ip access-group From_Internet in
```

Packet filtering for inbound traffic from the internet to the GIAC network is filtered on Serial 0. Packet filtering for outbound traffic from the GIAC network is filtered on the Ethernet 1 interface attached to the External Firewall, though which all outgoing traffic must pass. (This is a well known technique to save CPU cycles- if the access list were placed on the serial interface, not the Ethernet 1 interface, the packet would have to go through the E1 interface and the routing process before it is evaluated by the ACL).

**Outbound traffic – To Internet**

```
!Allow out-bound traffic with a valid source GIAC ip only and log the MAC address of
violations via the 'log-input' command
access-list To_Internet  permit ip 100.1.1.0  0.0.0.255 any

!Deny everything else
access-list To_Internet  deny   ip any any log-input

!Apply To_Internet ACL to Ethernet interface 1
interface Ethernet 1
 description To_ Internet
 ip address 100.1.1.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 ip access-group To_Internet out
```

### E0 Interface to VPN

```
 ! IPsec protocols for traffic from Internet going to VPN
 access-list To_VPN  permit esp any host 100.1.1.4 log
 access-list To_VPN  permit ahp any  host 100.1.1.4 log
 access-list To_VPN  permit udp any host 100.1.1.4 eq isakmp log

! Permit return traffic to VPN
 access-list To_VPN  permit tcp any host 100.1.1.4 established

 ! Deny and log everything else
 access-list To_VPN  deny   ip any any log

! VPN Outbound traffic – permit connection going out to the internet from the VPN:
access-list From_VPN  permit ip host 100.1.1.4  any

! Deny and log everything else
access-list From_VPN  deny ip any any log
 !
Interface Ethernet 0
description VPN Connection
 ip address 100.1.1.3 255.255.255.240
 no ip directed-broadcast
ip access-group To_VPN out
ip access-group From_VPN in
```

TIP: Access lists are order-dependent. Incorrect order of the statements could severely impact network connectivity. Filter reviews and testing prior to implementation is a must. Access lists changes could also impact the current connection and should be done with caution, preferably at the console. To maintain the order of the statements, a text file should be created, starting with a no ip access-list [number or name] command. After implementation, generate permissible and deniable traffic and verify via the show access-lists <ACL number or name> command to verify counters. Also verify any entries tagged with the log option are, in fact, logging properly.

### External Firewall – CISCO PIX 525

The Cisco PIX 525 firewall will be the main firewall that filters the brunt of the network traffic as it enters and exits the network. It is capable of providing service for large organizations that have high traffic demands and will provide the required scalability for the growing GIAC Enterprises. Specific details the PIX 525 can be obtained from the following CISCO site: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/.

The DMZ's protected by this firewall and their respective security levels are summarized in diagram 2-1 below:

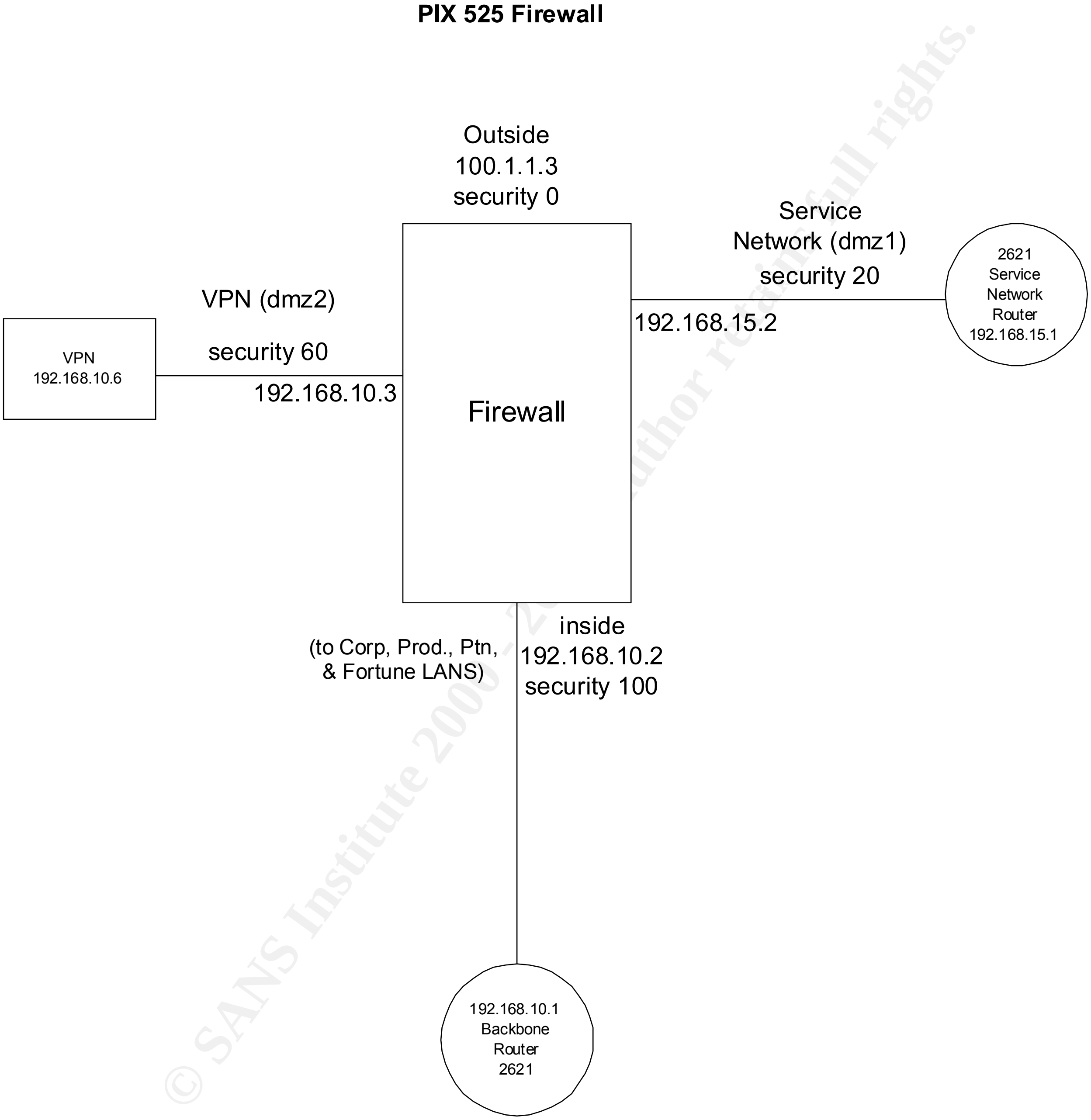


**diagram 2-1**

For the service network, this device will be configured to allow HTTP (port 80), HTTPS (port 443), SMTP (port 25) and DNS (port 53) to specific server addresses. This device will also be providing the NAT (network address translation) function for the GIAC web site network. NAT provides an additional layer of security as the private IP addresses of the service network devices are not known to the public.

TIP: CISCO PIX access lists are not defined using the same command syntax as CISCO router IOS. For example key word "nameserver" which is IOS syntax is "domain" in PIX syntax. More importantly, zeros indicate wildcards for the PIX network mask, whereas IOS masks require the wildcards bits to be 1. Specifying the wrong mask may negate the intended security restrictions of the access-list, creating an unwanted hole in the filter process. Note the difference in the following subnet mask definitions:

| Subnet Mask | PIX | IOS |
|---|---|---|
| Class A (match 1st octect) | 255.0.0.0 | 0.255.255.255 |
| Class B (match 1st, 2st octect) | 255.255.0.0 | 0.0.255.255 |
| Class C(match 1st, 2st, 3rd octect) | 255.255.255.0 | 0.0.0.255 |

For those unfamiliar with the PIX Firewall, it is important to briefly describe which commands are needed to permit connectivity between DMZs with different security levels defined. Higher to lower connections require the 'nat' and 'global' commands. Lower to higher connections require the 'static' and 'access-list' commands.

For example:

Higher to Lower (lets corp users security = 100 access ext. service LAN security =20 )

```
nat (inside) dmz1 1 0 0
global (dmz2) 1  192.168.15.1-192.168.15.254
```

Lower to Higher (lets vpn users security = 40 access production LAN security =80 )
format is (higher, lower) lower, higher

```
static (inside, dmz2) 192.168.10.6 192.168.10.3 netmask 255.255.255.255
access-list vpn_in permit ip any 192.168.14.0 255.255.255.0
```

In the following configuration, only the basic access control portions of the configuration process are covered (static routing and miscellaneous configuration details are intentionally omitted- see configuration guide at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm for details).

TIP The same NAT ID number can be used if the the general rule is to allow higher security users are to have access to ALL lower security dmz's. For the GIAC network, this is not appropriate as dmz2(vpn) is not going to need access to dmz1(service network), and should only access one of three subnets on the inside, internal network (partner, production, or internal).

```
nameif Ethernet0 outside security0
nameif Ethernet1 inside security 100
nameif Ethernet2 dmz1 security 20 (service network)
nameif Ethernet3 dmz2 security 60 (vpn network)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
ip address outside 100.1.1.5 255.255.255.0
ip address dmz1 192.168.15.2
ip address dmz2 192.168.10.3
ip address inside 192.168.10.2
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname extfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol domain 53
fixup protocol 443
fixup protocol 50
fixup protocol 51
fixup protocol 50
fixup protocol 500
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
names
pager lines 24
no logging timestamp
logging console debugging
logging monitor errors
logging buffered errors
no logging trap
logging facility 20
arp timeout 14400
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 100.1.1.2
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
no snmp-server community public
no snmp-server enable traps
mtu outside 1500
mtu inside 1500
mtu dmz1 1500
mtu dmz2 1500
!Let internal users have access to service net,vpn, and ext
nat (inside) 10 0 0
!Let service network have access to the outside
nat (dmz1)    2 0 0
!Let vpn users have access to .11,.12,.13 internal networks
static(inside,dmz2) 192.168.10.3 192.168.10.2
access-list vpn_net permit tcp any 192.168.11.0 255.255.252.0
access-list vpn_net permit esp any 192.168.11.0 255.255.252.0
access-list vpn_net permit ah any 192.168.11.0 255.255.252.0
access-list vpn_net permit udp any 192.168.11.0 255.255.252.0 eq isakmp
access-group vpn_net in inside
```

## VPN - CISCO 2621 (IOS 12.2.5 ENTERPRISE PLUS IPSEC 3DES)

Before any communication takes place between a supplier or partner and the GIAC network, the user must be authenticated via IKE (Internet Key Exchange) with an RSA signature (each peer authenticates with the VPN device by sending a certificate issued and validated by the CA.). To minimize the administrative burden of pre-shared keys, an external Certificate Authority (CA) (ie.: Verisign) will be used to issue RSA public keys for the participating devices.

To provide an additional layer of security, the VPN termination function is not combined with the PIX firewall. Although a VPN 3030 Concentrator was requested, management is concerned with costs at a minimum, so a CISCO 2621 that is no longer in use due to the recent merger between the two companies will have to suffice. This is a viable alternative that will enhance the various layers of security implemented within the GIAC network. The device will run ENTERPRISE PLUS IPSEC 3DES version 12.2.5 and serve as the VPN termination point. The primary assumptions are as follows:

1. VPN software has been properly configured on the client
2. Suppliers require access information stored on the Processing LAN
3. Partners require access information stored on the Partner LAN
4. Primary means of access is through the Internet- no dedicated connections exist

Suppliers and Providers are not provided direct access to the Fortune Cookie LAN. VPN clients will be a mixture of mobile users who access the GIAC network: suppliers who access the Production (.11) network, mobile users who access the Internal (.12) network, and partners who access the Partner (.13) network. Since there are no specific peers for which we can define static crypto maps, dynamic crypto maps will be implemented. With this remote access arrangement, strong (128-bit) authentication is an absolute must. As a majority of the connections will be made from external peers and mobile users, dynamic crypto maps will be used. In addition, network devices require authentication via a Radius authentication server. IKE will be used to negotiate security associations to accommodate mobile VPN clients that will receive dynamic IP addresses, and for remote peers- suppliers and partners, for whom the peer address is not always known.

TIPs from CISCO:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/ipsec.htm#95829

“If you must use the ‘any’ keyword in a permit statement, you must preface that statement with a series of deny statements to filter out any traffic (that would otherwise fall within that permit statement) that you do not want to be protected.)…Since it is possible for multicast and broadcast traffic to be permitted, an access-list should include deny entries for those addresses ranges…. Access lists should also include deny entries for traffic that is not IPSec protected… Must apply the crypto map to all interfaces over which IPSec data will flow. For data encryption, esp is selected. For authentication of the IP header as well, ah is selected. You must create a separate crypto map entry for each crypto access list… Note: Only the transform-set field is REQUIRED to be configured within each dynamic crypto map entry.”

Minimum VPN configuration:

```
!Filter  broadcast and multicast
Access-list 101 deny   ip 224.0.0.0 31.255.255.255 any
 !  disallow broadcast
Access-list 101 deny   ip host 255.255.255.255 any

!Filter traffic to external service network
Access-list 101 deny ip any host 100.1.1.6 0.0.0.255 any

!Create an access list to identify and restrict VPN traffic (Supplier)
!Traffic going to Production LAN
Access-list  vpn111 permit ip any 192.168.11.0  0.0.0.255

!Create an access list to identify and restrict VPN traffic (Internal Users)
!Access to management subnet
Access-list vpn112 permit ip any 192.168.12.0  0.0.0.255

!Create an access list to identify and restrict VPN traffic (Partner)
!Traffic going to Partner LAN
Access-list vpn113 permit ip any 192.168.13.0  0.0.0.255

!Allow IPSec protocols
Access-list 101 permit esp any any
Access-list 101 permit ahp any any
Access-list 101 permit udp any any eq isakmp

! Allow all VPN traffic to the VPN public interface address
Access-list 101 permit ip any host 100.1.1.4

! Allow traffic from VPN going out to the internet
Access-list 101 permit ip host 100.1.1.4 any

!Default deny statement
Access-list 101 deny ip any any

!Set Certificate Authority server, authenticate, and request certificate
crypto ca identity CA.server.com
crypto ca authenticate CA.server.com
crypto ca enroll

!Define crypto policy
crypto isakmp policy 1
```

```
 authentication  rsa-sig
 encr 3des
 hash md5

#Configure crypto map for IPSec ISAKMP
crypto map vpn_Static 10 ipsec-isakmp

#Configure a transform-set that defines the protocols and algorithms to be used by the
VPN tunnel (just one set is defined for simplicity)
crypto ipsec transform-set vpn_set ah-sha-hmac esp-des

#Assign the transform set to dynamic crypto map
crypto dynamic-map vpn11_map 11 set transform-set vpn_set
crypto dynamic-map vpn12_map 12 set transform-set vpn_set
crypto dynamic-map vpn13_map 13 set transform-set vpn_set

#Apply access list to dynamic crypto map
crypto dynamic-map vpn11 11 match address vpn111
crypto dynamic-map vpn12 12 match address vpn112
crypto dynamic-map vpn13 13 match address vpn113

#Associate the dynamic map with the static crypto map
crypto map vpn_Static vpn11 200 ipsec-isakmp dynamic vpn11
crypto map vpn_Static vpn12 201 ipsec-isakmp dynamic vpn12
crypto map vpn_Static vpn13 202 ipsec-isakmp dynamic vpn13

#Apply crypto map to interface e0 (connection to Border Router)
interface e0
  ip address 100.1.1.4 255.255.255.0
  ip access-group 101 in
  ip access-group vpn111 in
  ip access-group vpn112 in
  ip access-group vpn113 in
  crypto map vpn11
  crypto map vpn12
  crypto map vpn13
```

**Interface e1 – connection to PIX firewall**

```
!Traffic going to/from the internal networks (.11-.13) via VPN tunnel to the internet
access-list VPN_pix  permit ip 192.168.11.0 0.0.252.255 any
access-list VPN_pix permit ip host 100.1.1.4 192.168.11.0 0.0.252.255 any

! Deny and log everything else
 access-list VPN_pix  deny   ip any any log
```

```
interface e1
  ip address 192.168.10.4 255.255.255..0
  ip access-group VPN_pix in
  ip access-group VPN_pix out
```

**Secure Network Firewall – Linux 2.4 (Bastille)**

TIP: Securing Linux
All Linux servers should be hardened – disable Loadable Kernal Modules, get rid of relic items such as tip, and turn off unnecessary ports and deamons (ie: ntp on those machines that do not require time updates), etc. While all of this can be done manually, Bastille Linux hardening scripts will be used to do most of the preliminary, hardening work.

Ipchains will be used to add to the complexity of the security infrastructure of the GIAC network. Rules defined on this firewall will allow packets to the https server via a secure connection on https port 443. Behind this firewall, customer information (usernames, passwords, billing information,etc.), is stored on the customer database. Information is encrypted using GnuP 1.06. To process customer inquiries and purchases, the HTTPS server will have access information stored on the customer database. Additionally, access from select network support and administrative hosts to the customer database is also allowed. Internal hosts permitted access to sensitive data, such as the customer database, are under restricted access and require strong authentication. Default is set to deny, all other allowed traffic must be explicitly configured as follows:

```
#default policy to deny
ipchains –P input DENY
ipchains –P output DENY
ipchains –P forward DENY

#allow customers and internal users to initiate connection to https server, port 443 on ethernet0 interface
ipchains –A input –p tcp –y –i eth0  –s 0/0 –d 192.168.16.21  443 –j ACCEPT

#allow response traffic from https server, syn flag not set, to any ephemeral port
ipchains –A output –p tcp  !-y –i eth0  –s 192.168.16.21–d 0/0  1024:65535 –j ACCEPT

#allow specific internal hosts to access customer database (port 1234 used for authentication)
#Ethernet 1, protocol tcp source 12.3x, syn bit set, destination https server, port 1234
ipchains –A input –p tcp –y –i eth1 –s 192.168.12.30 –d 192.168.16.22  1234 –j ACCEPT
ipchains –A input –p tcp –y –i eth1 –s 192.168.12.31 –d 192.168.16.22  1234 –j ACCEPT
ipchains –A input –p tcp –y –i eth1 –s 192.168.12.32 –d 192.168.16.22  1234 –j ACCEPT
ipchains –A input –p tcp –y –i eth1 –s 192.168.12.33 –d 192.168.16.22  1234 –j ACCEPT

#allow customer database info to be sent to specific internal hosts (port 1235 used for data connection)
#Ethernet 1, protocol tcp source 12.3x, syn bit not set, destination internal hosts, port 1235
ipchains –A output –p tcp  !-y  –i eth1 –s 192.168.12.22  –d 192.168.16.30  1235 –j ACCEPT
ipchains –A output –p tcp  !-y  –i eth1 –s 192.168.12.22  –d 192.168.16.31  1235 –j ACCEPT
ipchains –A output –p tcp  !-y  –i eth1 –s 192.168.12.22  –d 192.168.16.32  1235 –j ACCEPT
ipchains –A output –p tcp  !-y  –i eth1 –s 192.168.12.22  –d 192.168.16.33  1235 –j ACCEPT

#network support access (pings from hosts.30/.31 to https/customerDB .21/.22)
```

```
ipchains –A input –p icmp –i eth1  –s 192.168.12.30 –d 192.168.16.21  –j ACCEPT
ipchains –A input –p icmp –i eth1  –s 192.168.12.30 –d 192.168.16.22  –j ACCEPT
ipchains –A input –p icmp –i eth1  –s 192.168.12.31 –d 192.168.16.21  –j ACCEPT
ipchains –A input –p icmp –i eth1  –s 192.168.12.31 –d 192.168.16.22  –j ACCEPT

ipchains –A output –p icmp  –i eth1 –s 192.168.16.21  –d 192.168.12.30   –j ACCEPT
ipchains –A output –p icmp  –i eth1 –s 192.168.16.21  –d 192.168.12.31   –j ACCEPT
ipchains –A output –p icmp  –i eth1 –s 192.168.16.22  –d 192.168.12.30   –j ACCEPT
ipchains –A output –p icmp  –i eth1 –s 192.168.16.22  –d 192.168.12.21   –j ACCEPT
#discard syn packets received on Ethernet 0 that do not have a valid destination port for https & database
ipchains –A input –p tcp –y –i eth0  –s 0/0 –d 192.168.16.21 ! 443 –j DENY
ipchains –A input –p tcp –y –i eth1  –s 0/0 –d 192.168.16.22 ! 1234:1235 –j DENY

#discard outbound packets with invalid destination port for https & database
ipchains –A output –p tcp  !-y –i eth0  –s 192.168.16.21–d 0/0 ! 1024:65535 –j DENY
ipchains –A output –p tcp  !-y –i eth1  –s 192.168.16.22–d 0/0 ! 1234:1235 –j DENY
```

### Fortune Cookie Firewall – Linux 2.4 (Bastille)

Ipchains filters on the Fortune Cookie firewall only allow connections from select network support and admin hosts (.30 for network support .33 for admin access), deny everything else. Internal hosts permitted access to Fortune Cookie data, are under restricted access and require strong authentication (via port 2234). Data flows will occur via port 2235, and only to the authorized devices noted below. The default policy is set to deny, all other allowed traffic must be explicitly configured as follows:

```
#default policy to deny
ipchains –P input DENY
ipchains –P output DENY
ipchains –P forward DENY

#allow specific internal hosts to Cookie database (port 2234 used for authentication)
#Ethernet 1, protocol tcp source 12.30 or 12.31, syn bit set, destination https server, port 2234
ipchains –A input –p tcp –y –i eth0 –s  192.168.12.30 –d 192.168.14.41 2234 –j ACCEPT
ipchains –A input –p tcp –y –i eth0 –s  192.168.12.33 –d 192.168.14.42 2234 –j ACCEPT

#allow customer database info to be sent to specific internal hosts (port 2235 used for data connection)
#Ethernet 1, protocol tcp source 12.3x, syn bit not set, destination internal hosts, port 2235
ipchains –A output –p tcp  !-y  –i eth1 –s 192.168.14.40 !-y –d 192.168.12.30  2235 –j ACCEPT
ipchains –A output –p tcp  !-y  –i eth1 –s 192.168.14.41 !-y –d 192.168.12.33  2235 –j ACCEPT

#network support access (allow pings between network support devices 12.30,31 and CookieDatabases
14.41,42)
ipchains –A input –p icmp –i eth1 –s 192.168.12.30 –d 192.168.14.41  –j ACCEPT
ipchains –A input –p icmp –i eth1 –s 192.168.12.30 –d 192.168.14.42  –j ACCEPT
ipchains –A input –p icmp –i eth1 –s 192.168.12.33 –d 192.168.14.41  –j ACCEPT
ipchains –A input –p icmp –i eth1 –s 192.168.12.33 –d 192.168.14.42  –j ACCEPT
```

### Service Network Router CISCO 2621

A Router is needed on the service network to provide an inter-vlan routing function for the service network. Each external server will reside on a separate vlan, which reduces the risk of all servers being attacked in the event that one is compromised. Likewise, the Service Network Router will serve as another barrier between the exposed service network and secure network over which customer transactions occur; it must also permit customers to connect via a secure connection (443):

```
!Allow Secure network connectivity to default gateway (service router)
access-list Secure_Net permit  ip 192.168.16.0 0.0.0.255 host 192.168.15.1

!Allow connectivity with internal .12 network
access-list Secure_Net permit ip 192.168.12.0 255.255.255.0 any
access-list Secure_Net permit ip 192.168.16.0 255.255.255.0 192.168.12.0 255.255.255.0 any

!Allow SSH (443) connections to HTTPS server and return traffic
access-list Secure_Net permit tcp any 192.168.16.21 eq 443
access-list Secure_Net permit tcp 192.168.16.21 any gt 1023 established

!Deny traffic between service and secure networks
access-list Secure_Net deny ip 192.168.15.0 0.0.0.255 192.168.16 0.0.0.255 any
access-list Secure_Net deny ip 192.168.16.0 0.0.0.255 192.168.15.0 0.0.0.255 any
access-list Secure_Net deny ip any any
```

Apply these rules to the .16 interface

```
interface vlan16
  ip address 192.168.16.1 255.255.255.0
  access-group Secure_Net in
  access-group Secure_Net out
```

**Service Network Switch CISCO 2912XL**

For the service switch, all ports not in use will be disabled. As mentioned above, each server will reside on a separate vlan as follows:

```
interface FastEthernet0/1
 description www
 switchport access vlan 21
!
interface FastEthernet0/2
 description dns
 switchport access vlan 22
!
interface FastEthernet0/3
 description mail
 switchport access vlan 23
```

## Assignment 3: Audit Your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

### 1. Plan the Assessment

GIAC is not a global organization; hence, off-shift hours have been selected to do the penetration and vulnerability scanning since these tools place additional demands on network bandwidth. While a zero-knowledge, third party penetration test would provide an excellent snap-shot of the GIAC network's security posture, it is costly. Therefore, the network support team has been charged with the responsibility of researching the available tools and utilizing these tools to conduct the necessary testing and scans to provide a comprehensive overview of the security architecture. The technical review and documentation procedures for the initial security review of GIAC Enterprises will include the following:

1. Vulnerability mapping – review of published vulnerabilities to ensure proper level of code is implemented.
2. Internet and DMZ scanning – review scan results to ensure no unnecessary ports are left open (including fragmentation testing).
3. Icmp testing – ensure border devices and external firewall are properly protected against icmp scans.
4. Documentation of vulnerabilities found and corrective action.

The primary goal of the assessment is to identify any vulnerability at the Border Router or the External Firewall, as this would contribute to a serious exposure. The access control points throughout the network- internal firewalls and service network servers, will also be scanned for unnecessary ports/services open. A review and documentation of the level of code for each device is also performed during this assessment as part of the vulnerability mapping process. All vulnerabilities are to be documented and promptly fixed. Any vulnerabilities found on the External Firewall or Border Router will be summarized in this report.

**2. Implement the Assessment**

The primary objective is to test the strength of the external Firewall. In addition to the firewall, the all other packet filtering devices should be scanned accordingly (although not detailed in this report). For example, access-list testing (ingress and egress filters) are performed by generating illogical or prohibited traffic and observing the detailed results in the logging entries. Port scans can also be utilized to identify any unnecessary, open ports. Icmpquery tests will performed against the Border Router and External Firewall. The Firewall security policy to be tested will include the following:

1. Vulnerability mapping for the latest Cisco advisories.
2. Internet and DMZ scanning: nmap scans
   -sS for "half-open" SYN scan used to test the interfaces/ports:
   -sU for UDP scans against the same ports on the External Firewall:
   -f -sF (Stealth Fin) for fragment testing using a –sF (Stealth Fin) mode to see if the IDS senors detect frag scans.
3. Icmp testing – Icmpquery tool used to run tests against Border Router and External Firewall
4. Documentation of vulnerabilities found and corrective action- see the following section for detailed results and configuration changes.

**3. Perimeter Analysis – Findings and Reccomendations**

1. Recent Cisco advisory concerning the PIX Firewall 6.0 code requires upgrade to 6.1.

Cisco Secure PIX Firewall SMTP Filtering Vulnerability
Summary
=======
The Cisco Secure PIX firewall feature "mailguard" which limits SMTP
commands to a specified minimum set of commands can be bypassed.
This vulnerability can be exploited to bypass SMTP command filtering.
This vulnerability has been assigned Cisco bug ID CSCdu47003.
The complete notice will be available at:

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

Tip: Be sure to receive vulnerability notices. DO NOT rely only on network support to manually check Bugtraq, CERT, etc, everyday- have the notices emailed to the support staff and procedures to implement HIGH risk vulnerabilities on internet access points immediately.

2. Internet scanning results (see Summary of Results on page 23).
   Ports required to be open were not. Corrections made to configuration to allow ftp access at Border Router and port 1234/5 through Firewall.

3. ICMP Testsing:

Based on the results of Icmpquery tests performed, no responses were sent by the Firewall; however, the Border Router had 4 minor vulnerabilities- responses to time-stamp/mask requests or timestamp/mask replies were not prohibited.

```
network1# icmpquery --t 100.1.1.1
                 t 100.1.1.1
   100.1.1.1
   100.1.1.1: 11:36:19
               : 11:36:19
network1# icmpquery --m 100.1.1.1
                  m 100.1.1.1
   100.1.1.1
   100.1.1.1: 0xFFFFFFE0
               : 0xFFFFFFE0
```

These issues were fixed with the following configuration for the inbound and outbound access lists:

```
!Disallow icmp timestamp and mask requests
access-list From_Internet  deny   icmp any any timestamp-requests
access-list From_Internet  deny   icmp any any mask-requests

!Disallow icmp time and mask replies
access-list To_Internet  deny   icmp any any timestamp-reply
access-list To_Internet  deny   icmp any any mask-reply
```

Additional testing included:

Test the external nameserver for gratuitous arps and unauthorized zone transfers: WHOIS lookup lists the external nameserver, master.giac.com. Zone transfers were attempted and failed. Verified named.conf file listed no unauthorized nameservers to pull zone transfers. Verified that the gratuitious arp function was in fact disabled.

Testing for default passwords:
Performed manually as there are a limited number of devices to test, and results were as expected – no default "null" passwords were in use. For a listing of default out-of the-box passwords, see: www.securityparadigm.com/defaultpw.htm

4. Vulnerabiliites documented in this report have been corrective as of the report date. Additional testing details will be made available to management upon request. Subsequent procedures for preliminary testing prior to implementing devices into the production environment will include the aforementioned testing procedures.

## Summary of Scan Results

p = pass D=discrepancy f= failed

| command | | target ip | description | results | corrective |
|---|---|---|---|---|---|
| | | | | external | action |
| nmap -sS | -p 1-65535 | 100.1.1.1 | border-internet | D open 25,50,51,80,443 | ftp |
| nmap -sU | -p 1-65535 | 100.1.1.1 | border-internet | D - open 53,500 | ftp |
| nmap -sF | | 100.1.1.1 | border-internet | p | |
| nmap -sS | -p 1-65535 | 100.1.1.2 | border-pix | D 24,53,80,443,gt1023 | ftp |
| nmap -sU | -p 1-65535 | 100.1.1.2 | border-pix | D 53 gt 1023 | ftp |
| nmap -sF | | 100.1.1.2 | border-vpn | p | |
| nmap -sS | -p 1-65535 | 100.1.1.3 | border-vpn | p - open 50,51 | |
| nmap -sU | -p 1-65535 | 100.1.1.3 | border-vpn | p - open 53,500 | |
| nmap -sF | | 100.1.1.3 | border-vpn | p | |
| nmap -sS | -p 1-65535 | 192.168.15.2 | pix - service dmz | D open 21,25,80,443 | 1234/5 |
| nmap -sU | -p 1-65535 | 192.168.15.2 | pix - service dmz | p open 53 | |
| nmap -sF | | 192.168.15.2 | pix - service dmz | p | |
| nmap -sS | -p 1-65535 | 192.168.10.3 | pix - vpn | p - open 50,51 | |
| nmap -sU | -p 1-65535 | 192.168.10.3 | pix - vpn | p - open 500 | |
| nmap -sF | | 192.168.10.3 | pix - vpn | p | |
| nmap -sS | -p 1-65535 | 192.168.10.2 | pix- internal | p | |
| nmap -sU | -p 1-65535 | 192.168.10.2 | pix- internal | p | |
| nmap -sF | | 192.168.10.2 | pix- internal | p | |
| nmap -sS | -p 1-65535 | 100.1.1.21 | www | p - open 80 | |
| nmap -sU | -p 1-65535 | 100.1.1.21 | www | p | |
| nmap -sF | | 100.1.1.21 | www | p | |
| nmap -sS | -p 1-65535 | 100.1.1.22 | dns | p | |
| nmap -sU | -p 1-65535 | 100.1.1.22 | dns | p - open 53 | |
| nmap -sF | | 100.1.1.22 | dns | p | |
| nmap -sS | -p 1-65535 | 100.1.1.23 | smtp | p - open 25 | |
| nmap -sU | -p 1-65535 | 100.1.1.23 | smtp | p | |
| nmap -sF | | 100.1.1.23 | smtp | p | |
| nmap -sS | -p 1-65535 | 100.1.1.24 | https | o - open 443 only | |
| nmap -sU | -p 1-65535 | 100.1.1.24 | https | p | |
| nmap -sF | | 100.1.1.24 | https | p | |
| nmap -sS | -p 1-65535 | 100.1.1.4 | vpn | p - open 50,51 | |
| nmap -sU | -p 1-65535 | 100.1.1.4 | vpn | p - open 53,500 | |
| nmap -sF | | 100.1.1.4 | vpn | p | |
| nmap -sS | -p 1-65535 | 192.168.10.4 | vpn-pix | p - open 50,51 | |
| nmap -sU | -p 1-65535 | 192.168.10.4 | vpn-pix | p - open 53,500 | |
| nmap -sF | | 192.168.10.4 | vpn-pix | p | |
| icmpquery m | -p 1-65535 | 100.1.1.1 | border-internet | f | deny mask req/reply |
| icmpquery t | -p 1-65535 | 100.1.1.1 | border-internet | f | deny time.req/reply |
| icmpquery m | -p 1-65535 | 100.1.1.2 | border-pix | p | |
| icmpquery t | -p 1-65535 | 100.1.1.2 | border-pix | p | |
| icmpquery m | -p 1-65535 | 100.1.1.3 | pix | p | |
| icmpquery t | -p 1-65535 | 100.1.1.3 | pix | p | |

## Assignment 4: Design Under Fire

### Assignment 4 - Design Under Fire (25 Points)

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

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.

2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.

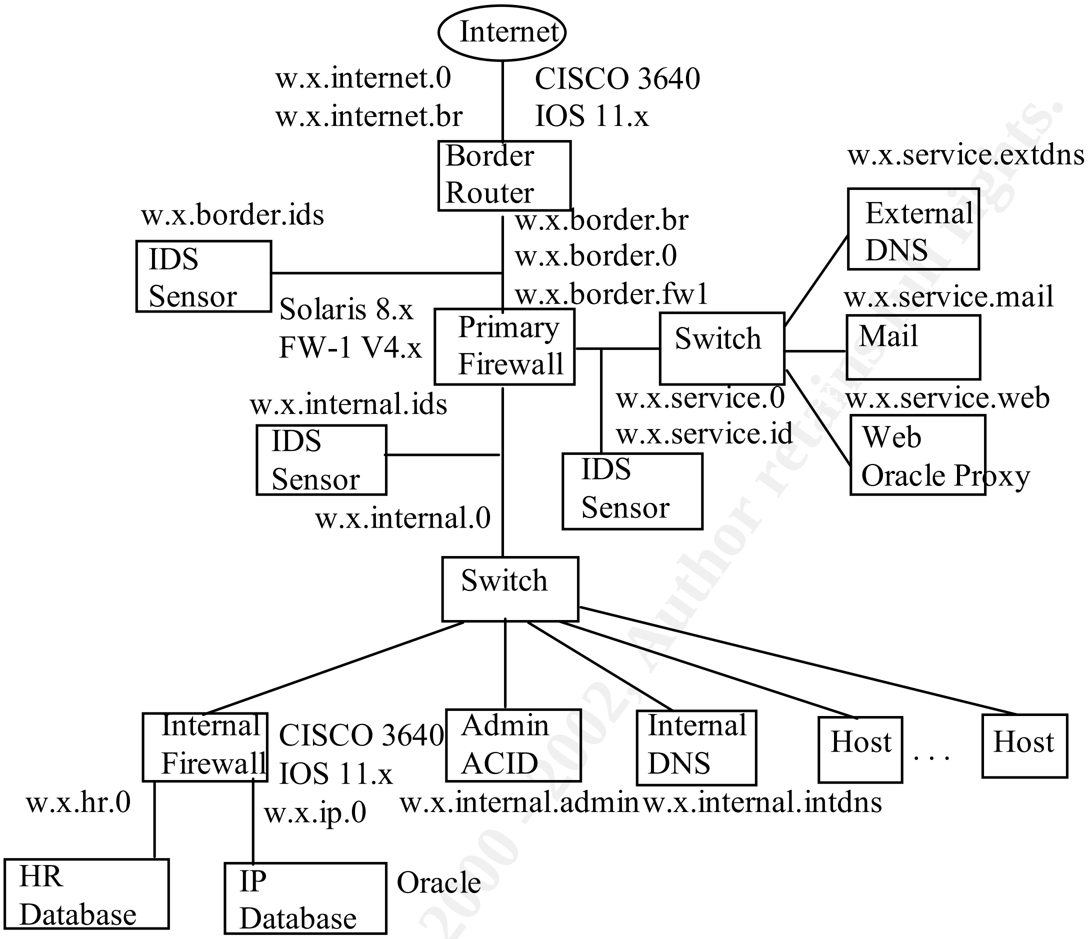
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

### Attacking the Border Router

Since the selected design has a significant vulnerability at the entrance to the network, the Border Router was selected for the first point of attack. Circumventing the Border Router to gain access to the firewall is a likely scenario in this particular case study. The reviewed assignment was the most recent assignment from the prior class, submitted June 2001. I am surprised at the author’s use of IOS v11.x on the Border Router, as known vulnerabilities for this particular level of code have existed since 1998. (Note: The network diagram specifies a CISCO 3640 router, while the details of the report indicate that the Border Router is a CISCO 4000 router running IOS 11.x. )

**Case Study Network Diagram**



" ***Border Router (CISCO 4000, IOS 11.x)***

*The border router is the interface between GIAC Enterprises intranet and the internet. Its function is to properly provide ingress an egress packet routing of network traffic. The router's security role is to help enforce /implement GIAC's security policy. This router's security benefit is two fold. First, it protects GIAC Enterprises from the internet "noise" that is easily detected and efficiently dropped. Typically this noise consists of network mapping, port scanning, operating system (OS) fingerprinting, or simple protocol based attacks. Secondly, border filtering has the additional benefit of offloading the primary firewall, increasing its throughput and performance. The border router Access Control Lists (ACLs) should filter the following:…"*

Again, a fundamental flaw in this design that this router is running 11.x code (note that it could be running any version of IOS 11). The assumptions, therefore, are that any of the known vulnerabilities related to the "IOS v11.x" code versions are applicable. Here are just a few of the potential implications of running such outdated code (obtained from the CISCO web-site):

1. *Cisco IOS Remote Router Crash (August 1998) affected versions*

** 11.3(1), 11.3(1)ED, 11.3(1)T*
** 11.2(10), 11.2(9)P, 11.2(9)XA, 11.2(10)BC*
** 11.1(15)CA, 11.1(16), 11.1(16)IA, 11.1(16)AA, 11.1(17)CC, 11.1(17)CT*
** 11.0(20.3)*

*Summary*
*=======*
*An error in Cisco IOS software makes it possible for untrusted,unauthenticated users who can gain access to the login prompt of a router orother Cisco IOS device, via any means, to cause that device to crash and reload.*

*This applies only to devices running classic Cisco IOS software. This includes most Cisco routers with model numbers greater than or equal to 1000, but does not include the 7xx series, the Catalyst LAN switches, WAN switching products in the IGX or BPX lines, the AXIS shelf, early models of the LS1010 or LS2020 ATM switches, or any host-based software.*

*2. Cisco IOS Syslog Crash affected versions 11.3AA; 11.3DB; or any 12.0x (February 1999)*
*Summary*
*=======*
*Certain versions of Cisco IOS software may crash or hang when they receive invalid user datagram protocol (UDP) packets sent to their "syslog" ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such crashes and hangs. This fact has been announced on public Internet mailing lists which are widely read both by security professionals and by security "crackers", and should be considered public information.*

*3. Cisco IOS Software TELNET Option Handling Vulnerability affected versions 11.3AA; 12.0(2) through 12.0(Z ) (August 2000)*
*Summary*
*=======*

*A defect in multiple Cisco IOS software versions will cause a Cisco router to reload unexpectedly when the router is tested for security vulnerabilities by security scanning software programs. The defect can be exploited repeatedly to produce a consistent denial of service (DoS) attack.*

***Customers using the affected Cisco IOS software releases are urged to upgrade as soon as possible to later versions that are not vulnerable to this defect.***

The Border Router filters may mitigate some of the aforementioned exposures, however, a simple code upgrade would patch these known vulnerabilities. Running vulnerable code on the primary Internet gateway lacks any prudence.

A review of the router’s filters reveals a suspicious item in the Border Router configuration allows echo requests and replies, to the partner network, yet there is no stateful inspection required, going in or out of the ICMP packets. Although the author does limit such stimuli and responses to the partner network, without stateful inspection, there is no matching of ICMP requests and replies; hence another exposure for trouble. Albeit the hacker will have to spoof the partner’s IP, but once that has been accomplished, the Border Router will let them right in and could potentially be used to assist in the flooding the partner’s network with ICMP packets as well. Several ICMP-based attacks could be implemented. Here’s a listing from the IRChelp website: http://www.irchelp.org/irchelp/nuke/info.html

1.SMB
2.bonk
3.land
4.teardrop
5.click
6.ssping
7.WinNuke
8.ICMP Flood
9.smurf

Futhermore, if an attacker were able to compromise any of the devices on the service network, a simple tool called nmap could be used to bring down the Border Router, as that is one of the primary flaws in its version of IOS. If 50 compromised systems (internal or external) targeted this Border Router, a successful Denial of Service attack would result.

### Attacking the Firewall

The attacker, who was allowed in via a spoofed partner IP address, also has access to the Checkpoint Firewall, as defined Border Router's filters. Like the Border Router, the firewall is too running vulnerable code "V4.x". Again, the information relative to the project due date should be noted (the release date of the alert is June 2000, and the project was submitted in June 2001). This version has a significant vulnerability for denial-of-service attacks, as noted by the following advisory:

http://www.cert.org/vul_notes/VN-2000-02.html

*CERT® Vulnerability Note VN-2000-02*

*IP Fragmentation Denial-of-Service Vulnerability in FireWall-1*
*Original release date: June 16, 2000*
*Last revised: September 12, 2000*

*Description*

*A denial-of-service vulnerability has been discovered in the FireWall-1 product from Check Point Software Technologies. Check Point has tested versions 4.0 and 4.1 of the product and has confirmed that both are affected…This vulnerability can be exploited by sending a stream of large IP fragments to the firewall. As the fragments arrive, the mechanism used to log IP fragmentation anomalies can monopolize the CPU on the host machine and prevent further traffic from passing through the firewall.*

*Impact*

*An attacker who exploits this vulnerability can monopolize the CPU of a FireWall-1 firewall, rendering it incapable of processing any incoming or outgoing traffic. Attackers are not able to pass packets or fragments that would be filtered out under normal circumstances, nor are they able to gain privileged access to the firewall or its host system.*

Any fragmentation tool of choice could be used. Hping (obtained from http://www.hping.org/) can be used to, first, find the Firewall, and then bombard it with large IP fragments, causing it to cease functioning. A nice 'howto' guide itemizes the steps one should take to perform rudimentary OS fingerprinting: http://www.kyuzz.org/antirez/hping2/docs/HPING2-HOWTO.txt

Important switches to use when using hping include:

```
-f --frag
              Split packets in more fragments, this may be useful in order to test IP stacks fragmentation
              performance and to test if some packet filter is so weak that can be passed using tiny
              fragments (anachronistic). Default 'virtual mtu' is 16 bytes. see also --mtu option.
```

```
-m --mtu mtu value
                    Set different 'virtual mtu' than 16 when fragmentation is enabled. If packets size is greater
                    that 'virtual mtu' fragmentation is automatically turned on.
```

The devastating fragments coming from the example of 50 compromised hosts would look something like this hping command sending an over-sized packet to the Checkpoint Firewall to complete the DOS:

```
#hping 10.20.20.1 –f  -m 70000
```

(for clarity bogus numbers replace the "w.x.border.fw1" IP address listed in the diagram on page 24)

As the vulnerable Firewall is unable to process unusually large fragments, this process is repeated until the mission has been accomplished.

If the Checkpoint FW-1 device was properly patched and configured to drop icmp fragments this event would not have been successful. To give some credit to the author, the most obvious potential damage that could be inflicted is a denial-of-service type of attack on the Border Router- the 'crown jewels' are in tact, but now **no one** can access the network.

## References

Held, G. & Hundley, K. Cisco Security Architectures. 1999.

Information Security Magazine. Part 3 Penetration Testing Exposed. September 2000. p 90.

## URL References

CERT
http://www.cert.org/vul_notes/VN-2000-02.html

Cisco Public Advisories
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml

Cisco Configuration Guide for the Cisco Secure Pix Firewall Version 6.1
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/index.htm

Cisco PIX 525 Product Documentation
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/.

Configuring IPSec
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/ipsec.htm#95829

Gale Slentz's practical assignment:
http://www.sans.org/y2k/practical/Gale_Slentz_GCFW.doc

Hping
http://www.hping.org/) can be used to, first, find the Firewall, and then bombard it with

IRCHelp. ICMP Based Attacks.
http://www.irchelp.org/irchelp/nuke/info.html

OS Fingerprinting Howto
http://www.kyuzz.org/antirez/hping2/docs/HPING2-HOWTO.txt

Testing for Default Passwords
www.securityparadigm.com/defaultpw.htm