Global Information Assurance Certification Paper

Firewalls, Perimeter Protection and VPNs
GCFW Practical Assignment

Davey Rance

Sans Sydney 2001

Version 1.5d

April 2001

Assignment 1 - Security Architecture 3
Customer Access 3
Supplier Access 3
Partners Access 3
Proposed Network Diagram 4
Hard Ware 4
Border Router 4
External Firewall 5
Internal Firewall 5
DNS Server 5
Public Web Server 5
Mail Relay Server 6
IDS Servers 6
ISA Server 6
Assignment 2 – Security Policy 7
Border Router 8
Security Description 8
Firewall External 13
Security Description 13
Security Policy 13
Firewall Internal 17
Security Description 17
Security Policy 18
VPN 19
Assignment 3 21
Audit Your System Architecture 21
Plan the Assessment 21
Implement the Assessment 22
Recommendations 24
Assignment 4 26
Design Under Fire 26
Target Network 26
An attack Against the Firewall 27
Denial of Service Attack 28
Compromise an Internal System 29
Resources 30

Assignment 1 - Security Architecture

"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. Your architecture must specify filter routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defence component. Produce a diagram or set of diagrams with explanatory text that defines how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (The companies that purchase bulk online fortunes).
- Suppliers (The authors of fortune cookie sayings that connect to supply fortunes).
- Partners (The international Partners that Translate and resell fortunes)."

Customer Access

As customers may not always want to access the bulk fortunes from their office, an alternate connection method is available.

1 Via a SSL connection to the Customers Web Site from a trusted IP address.
2 Via a VPN connection from their office to the Customers Web Site.

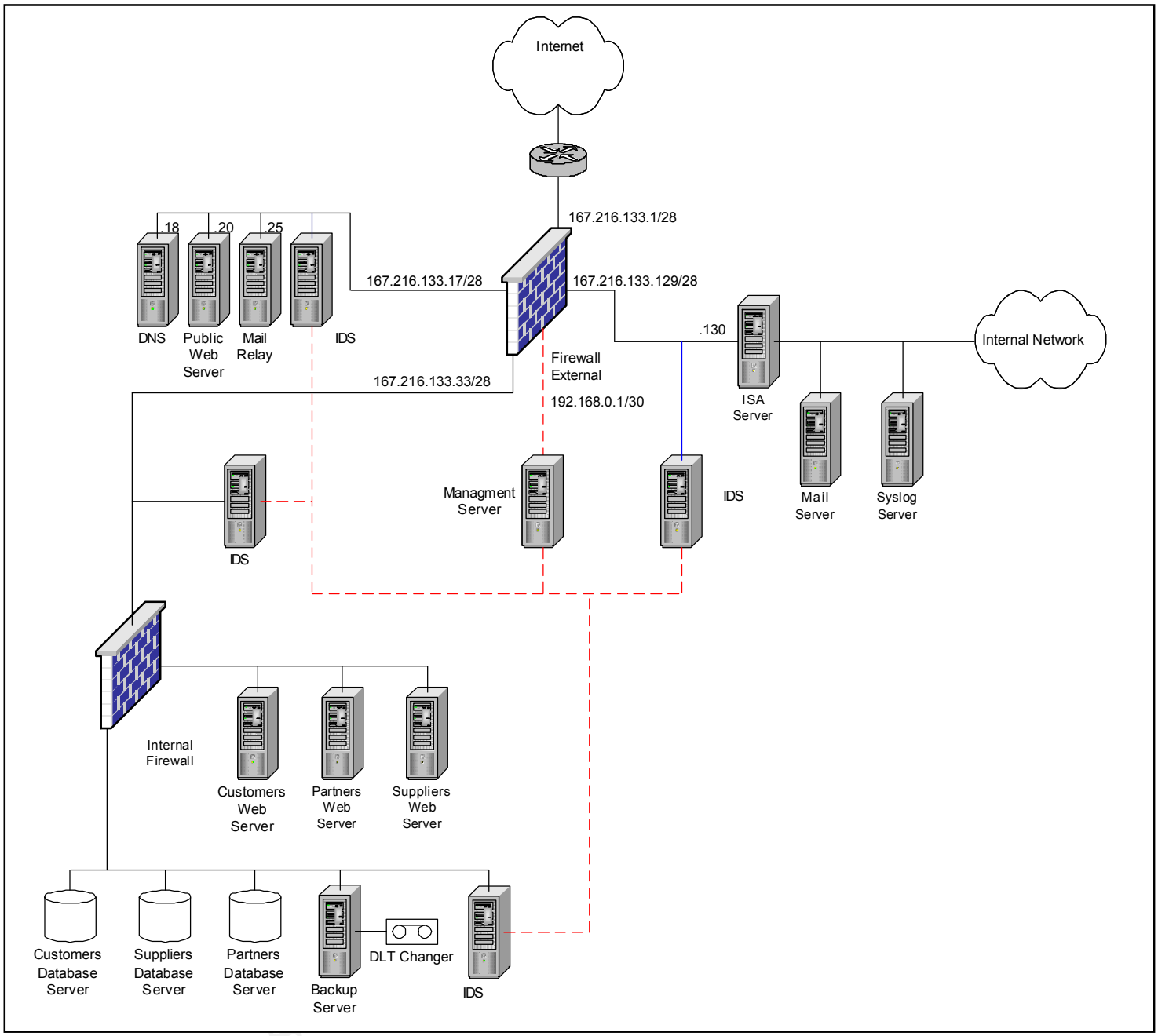
Supplier Access

As the suppliers of the fortune are keen to protect their intellectual property they don't mind having the additional hassle of having to use a VPN client when they up load the fortunes. As a result, all access for the suppliers will be via a VPN connection to the External Firewall. There it will be terminated and all traffic from the VPN will then be routed to the Internal Firewall. On arrival it will then be routed to the Suppliers Web Server.

Partners Access

The Partners have special needs to access the fortunes. They need to be able to translate the fortunes and have direct VPN access to the Partners Web Server and access to the Partners Database Server. This allows the use of custom front ends to the database if required.

Proposed Network Diagram



Hard Ware

Border Router

Cisco 3640 running IOS version 12.1.03

The Border router's main function is to route packets to and from the Internet and the internal networks. It will also provide a base security filter including ingress and egress. The connection to the Internet is via a 2 Mbit serial link.

External Firewall

Cisco PIX 525 Running IOS version 5.3(1)
IPSec Hardware VPN Accelerator Card (VAC)
4 Port network card

The External Firewall will terminate the VPN connections for incoming customers, partners and suppliers. Implementing the main security policy as defined by GIAC and protecting the internal firewall and servers from DOS attacks where possible. The security policy of the firewall will be to DENY everything with the exception of specific ports and IP addresses that allow users to access servers.

Internal Firewall

Linux, Kernel 2.4.2
Net Filter 1.2.

The main function of the Internal Firewall is to do finer filtering on incoming and outgoing connections for the customer, partners and suppliers web servers. The servers will have each have access to their corresponding database server. They will be able to return query's via the VPN.

The partners main access is intended to be via the partners web site but additional access if required to their database server can be easily configured through the firewall.

DNS Server

Windows 2000 Service Pack 1
Microsoft DNS server

The DNS server will have all appropriate patches and hot-fixes applied to it. All unneeded services will be disabled or deleted. The server will have the following additional services running on it:

SSH - to allow removal of the event logs,
Domain Time II - to make sure that the system time is the same as the network timeserver to make log analysis possible.

Secondary DNS Services will be hosted by the ISP. Zone transfers will only be allowed between configured hosts. DNS will be using Split Horizons so the only hosts that will be listed on the Server will be the Mail Relay Server, Public, Customer, Partners, and Supplier Web Servers. A private DNS server, in the internal network, will do all internal DNS resolution.

Public Web Server

Windows 2000 Service Pack 1
IIS 5

The Web server will run IIS 5 with all appropriate patches and hot fixes applied to it. All unneeded services will be disabled or deleted. The server will have the following additional services running on it:

SSH - to allow removal of the event logs,

Domain Time II - to make sure that the system time is the same as the network timeserver to make log analysis possible.

IIS will have the default web site removed and all vendor supplied sample pages removed. All application mappings will be removed except *.asp. This removes the common HTR problem that is associated with IIS web sites.

Mail Relay Server

Windows 2000 Service Pack 1
MimeSweeper 4.2

The Relay server will run Content Technology's MimeSweeper Version 4.2. This mail relay package allows content filtering and virus scanning. All operating system hot fixes and patches have been applied. The server will have the following additional services running on it:

SSH - to allow removal of the event logs,
Domain Time II - to make sure that the system time is the same as the network timeserver to make log analysis possible.

The display banner of the SMTP server has been changed, this makes it harder to discover the SMTP server being communicated with. The configuration of MimeSweeper is beyond this document but the following minimal rules will be enforced:

- Block all incoming *.vbs files,
- Block all messages that have conflicting mime types,
- Block all encrypted messages,
- Scan every message with two virus scanners,
- Block HTML messages that have any script tags (Removing threats of VBscript and Jscript attacks),
- Deny relaying from any external mail server.

IDS Servers

Windows 2000 Service Pack 1
SNORT

Currently SNORT is running on Windows 2000 Servers. All IDS servers are multi homed with one NIC on the wire to be monitored and one in a management network. The NIC on the wire to be monitored will have no IP address assigned to it (it will be running in promiscuous mode). The second NIC will be on the management LAN. All traffic passing on the wire will have the first 60 Bytes logged. The logs will be checked and archived each day using grep.

ISA Server

Windows 2000 Service Pack 1
Microsoft ISA Server 1

Again all appropriate hot fixes and service packs have been applied. The Proxy server for all internal network access is via Microsoft ISA Server. This application level proxy server has a client that will be installed on hosts through out the internal network. The proxy server allows logging of all internal access to the Internet. The configuration of ISA is beyond the scope of this document.

Assignment 2 – Security Policy

"Based on the security architecture that you defined in Assignment 1, provide 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 ACL's, 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 in E-Business with customers, suppliers and partners – you MAY NOT simply block everything!

(Special note VPN's: 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:

The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.

Any relevant information about he behaviour of the service or protocol on the network.

The syntax of the ACL, filter, rule, etc

A description of each of the parts of the filter.

An explanation of how to apply the filter.

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.)

Explain how to test the ACL/filter/rule.

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

Border Router

Security Description

The security applied to the border router is very limited. The router is fastest at routing and not being a firewall. As a result the border router has an ingress filter applied to block invalid IP address from coming in to the network as well as an egress filter to make sure that data leaving the network is only from hosts on the network.

Any extra services that are running on the router are disabled.
Good neighbor settings are also applied.

Security policy

- **Make sure that router its self is secure**

```
enable secret                ! Uses MD5 hashing on the enable password
service password-encryption  ! Makes sure that all service passwords are encrypted
```

Applying these commands means that passwords are no longer in plain text when a show running is executed.

- **Disable unneeded services**

```
no service udp-small-servers  ! Disable the misc UDP services that may be running
no service tcp-small-servers  ! Disable the misc TCP services that may be running
no ntp enable                 ! Disable the ntp time server
no service finger             ! Disable the finger server
no service pad
no bootp server               ! Disable the bootp server
no snmp-server location       ! Remove the SNMP location
no snmp-server contact        ! Remove the SNMP contact person information
no snmp-server community      ! Remove the SNMP community
no snmp-server enable traps   ! Stop the router from sending out SNMP traps
no cdp run                    ! Disable the Cisco Discovery Protocol
no ip http server             ! Make sure that the web server is disabled ( in some IOS's
                              enabled is default)
no service DHCP               ! Disable the DHCP service
no ip classless               ! Make sure that only configured subnets can forward data
no ip domain-lookup           ! Disable the router from doing DNS queries
```

The UDP and TCP small services are a range of small services that include finger, bootp, echo, chargen, discard and daytime. These are all disabled to reduce the chances of new exploits in these services.

- **Good neighbor**

```
no ip directed-broadcast      ! Makes it so the router can't be used for "smurf" attacks
no ip source route            ! Prevent source routed packets from entering the network
```

```
no ip unreachables          ! No ip unreachable messages to be returned
no ip redirects             ! Stops packets that may have a different return route
```

This sets up a few options to reduce the chances of being used in a "traffic amplification" attack. Preventing source routed packets means that any packet that has a different route for return can't be used to launch a attack or bypass any manual routing commands that might be in place.

- **Ingress Filter**

```
access-list 1 deny 127.0.0.0 0.255.255.255      ! Deny the loopback address range
access-list 1 deny 167.216.133.0 0.0.0.255      ! Deny any packets coming in with a source of
                                                our network
access-list 1 deny host 0.0.0.0                 ! Deny all packets coming from a invalid host
access-list 1 permit any                        ! Permit any other traffic
access-list 1 deny any                          ! Explicit deny is just listed to remind that it is
                                                there
```

The basic ingress filter is using a standard access list. These are very fast but can only define source address so they have limited use.

Syntax for a standard access list.

```
access-list  access-list-number {Permit | Deny} source [source-wildcard] any
```

The order of the rules is very important. The rules are processed from top down and once a packet has found a match no other testing is done, as in following example:

A packet from host 192.169.15.1

```
access-list 1 deny 192.169.15.0 0.0.0.255    ! Deny any traffic from the 192.169.15.0 network
access-list 1 permit 192.169.15.1            ! Allow traffic from host 192.169.15.1
```

The packets from the host would never get through as the network address would be matched first, then the deny applied. For this to work as required the following ACL would need to be used:

```
access-list 1 permit 192.169.15.1            ! Allow traffic from host 192.169.15.1
access-list 1 deny 192.169.15.0 0.0.0.255    ! Deny any traffic from the 192.169.15.0 network
```

The addresses listed in the ingress filter should never appear on the Internet. If they do, they have been more than likely been created for misuse. The loopback address range is used for local loopbacks on each machine. They should be non-routed and as such never seen. There should be never any incoming packets from the Internet having a source IP address in the range of the network's public address. If so, then some one has been spoofing the IP address.

To test the ingress filter a tool like Nmap can be used to spoof the IP address of one of Mail Relay Server. Using the show access-list command it would be seen that the number of matches increasing. It will be very difficult to test the loopback address range and the 0.0.0.0 host as these should be blocked at every step along the way.

The address 0.0.0.0 should never be present on the public network, it is an invalid address and should be blocked.

All other incoming traffic will be permitted. Any other filtering required will be done by the firewall.

The "deny any" has been listed to remind the user that it is implicit in every standard access list.

The access list then needs to be applied to the serial port.

To apply access-list 1 to all incoming traffic on the external interface.

From config mode enter the following lines:

```
Router(config)# interface serial 0/0          ! Select the correct serial interface
Router(config-int)# access-group 1 in         ! Apply the filter to all incoming traffic
Router(config-int)# exit
```

NB: Some other IP addresses need to be blocked and will be dealt with by a rule slightly later in the configuration.

- **Basic Egress Filter**

```
! named extended access list
Router(conrfig)ip access-list extended EgressFilterOut

! allow access from the Proxy server to any host
Router(config-nacl-ext)# permit ip host 167.216.133.130 any any

! allow access from the DMZ network
Router(config-nacl-ext)# permit ip 167.216.133.16 0.0.0.240 any any

! allow access from the Services network
Router(config-nacl-ext)# permit ip 167.216.133.32 0.0.0.240 any any

! deny any other host that trys to send data.
Router(config-nacl-ext)# deny any any
```

The basic egress filter has been applied using a named extended access-list. This allows much greater configuration.

Syntax for Extended Access list
Access-list access-list-number {Permit | Deny} {Protocol | Protocol-keyword} {Source source-wildcard | any} [protocol-specific-options] [protocol-specific-options] [log]

The filter applied uses a named extended access-list, which removes the restrictions of only 100 access lists. Therefore a meaningful name can be used rather than a number.

Syntax for Extended Named Access list
Router(config)# ip access-list extended name
Router(config-nacl-ext)# [Permit | Deny] protocol source source-wildcard destination destination-wildcard operator port-number

It can be seen that options for the extended access list are far greater than the standard. This makes it possible to filter on port numbers.

Currently the egress filter is very simple, just allowing return access from the specified networks. The reason for this is, the firewall is more suited to ensure only the required servers can respond on specific ports. This also simplifies management of the router and network. If the extra security of having the servers checked at both the firewall and the router is required then the following rules would be added for each server changing the ports as needed:

```
! allow the mail relay server to be able to send mail and do dns lookups.
Router(config-nacl-ext)# permit ip host 167.216.133.25 any eq SMTP
Router(config-nacl-ext)# permit ip host 167.216.133.25 any eq DNS
```

Once the rules have been selected they will then be applied to the serial port.

```
Router(config)# interface serial 0/0                    ! select the correct serial interface
Router(config-int)# access-group EgressFilterOut out    ! apply the named access list
```

To test the egress filter connect a test machine after the firewall and assign an IP address to it. It should not be possible to cerate a valid connection to a host on the Internet.

- **Block all other invalid IP addresses**

```
ip route 10.0.0.0 255.0.0.0 null 0          ! Route all class A private addresses to NULL
ip route 172.16.0.0 255.16.0.0 null 0       ! Route all class B private addresses to NULL
ip route 192.168.0.0 255.255.0.0 null 0     ! Route all class C private addresses to NULL
ip route 224.0.0.0 16.0.0.0 null 0          ! Route all multi cast addresses to NULL
```

As part of the ingress filter all invalid IP addresses will be blocked. But using access lists for blocking IP address ranges is a waste of CPU and memory. If the addresses should be not allowed either incoming or outgoing, and logging is not required then the best way to remove these packets is via a static route.

When a packet enters a router the first thing that is checked is the routing table and then ACL. So if the packet gets routed to an interface that just drops it, much less processing is required. The interface for doing this is NULL 0.

These static routes apply to all traffic. They will be applied before dynamically learnt routes because the cost of a static route is administratively lower. If the router is doing NAT and the private address range was one of the above, then all packets would all be routed to NULL 0 therefore not returning to the network.

These filters are hard to test, as the packets should be blocked on every border router on the Internet. If the "debug ip packet" command is used, then some traffic sent to the router with a source address in the network ranges it is displayed on the console and routed to the null 0 interface.

- **Default Route**

  ip route 0.0.0.0 255.255.255.255 serial 0/0 ! set the static route for all unknown data

This route means that all traffic with a destination port that the router does not know, gets routed out serial port 0/0

As this is a static route there is no chance of route poisoning, internal routing protocols will not redistribute over static routes by default so internal network topology won't be given away.

- **Display Warning Banner**

  Banner motd ^
  Authorized access only ^

Display of a warning banner informs other users that only authorized people should access. If a more comprehensive banner is required text can be inserted, the ^ character marks the end.

- **Disable Telnet**

```
Router(config)# access-list 10 deny any      ! Set the access list for console access
Router(config)# line vty 0 4                 ! Set which vtys this will apply to
Router(config-line)# access-group 10 in      ! Deny all access to the router using telnet
Router(config-line)# access-group 10 out     ! Make sure that the router can't telnet out
```

Disabling telnet on the router is both a security gain and a security risk. Telnet access to and from a router is in plain text, it is very easily sniffed, meaning it is very easy to get the router passwords and change the security of the router. While the access list can be set up to allow access only from only selected IP addresses this is still not foolproof.

If telnet access is disabled, the only way to configure the router is via the console port (the web interface was disabled in the beginning of the security policy). If the console port is connected to a modem this introduces new security risks. The preferred way to access the router would be via SSH to a machine physically close to the router and have the console port connected to this. The ideal machine would be one of the IDS machines. This means that all access to the machine would be encrypted using SSH and access to the router is directly via a serial port thus no passwords would be transmitted over the network as clear text.

"**Gotcha**" If configuration of ACLs is done via telnet, make sure that ACL is not applied that will deny the telnet connection. To reduce the effects of this make sure the running configuration of the router has been saved before changing any ACLs. If telnet access is lost reset the router to return to the last known good configuration.

Test the telnet restrictions by trying to telnet to the router, no connection should be made.

Firewall External

Security Description

The external firewall restricts access to and from specific hosts and network services.

Security Policy

- **Secure the Firewall**

```
Floodguard 1                        ! Allows faster reclaim of uauth resources if they are all
                                      consumed
sysopt connection enforcessubnet    ! Blocks against spoofing
sysopt noproxyarp Outside
sysopt security fragguard           ! Protect against fragmented packet attacks
no snmp-server
```

floodguard: if the firewall finds the user authentication subsystem has run out of resources it will actively reclaim them.

enforcessubnet: tells the fire wall not to pass packets that have been spoofed. E.g. if a packet arrives on the Outside interface but has a source address of DMZ the packet is dropped.

noproxyarp: means the PIX will not proxy ARP addresses on the interface specified. This reduces the chance of ARP poisoning.

fragguard: means that the firewall will limit the number of fragmented packets to 100 fragmented packets per interface per second, and each non-initial IP fragment is required to be associated with an already seen valid initial IP fragment. These two rules enable the PIX to reduce the chances of a IP fragmentation attack like "teardrop" or "land" but it breaks normal IP conventions.

no snmp-server: turns off the SNMP server in the firewall. This is a trade off between security and management. The SNMP service can have security problems, the write and read community strings are not changed by default on many devices. This may lead to unauthorized access or discovery of firewall settings. To check that the SNMP server is disabled try to connect with a SNMP client like snmputil.exe from the NT Resource kit.

- **Configure Logging**

```
logging host Inside 167.216.133.130 ! Set the syslog server host ip address
logging on                          ! Set logging to be enabled
logging Buffered errors             ! Local buffing of severe syslog and error messages
logging trap Notifications          ! Send trap and server syslog messages to syslog server
```

Set the syslog server address for logging important events to. This is on the inside interface and has the IP address of the ISA server. The syslog server is a host on the internal network and using the ISA client port 514 from syslog server is mapped to the external interface on the ISA server port 514.

Buffering server errors to the local buffer on the firewall means that if debugging is currently being done at the console, messages will be displayed there as well as being sent to the syslog server.

Check the syslog server to make sure that the syslog messages are being received as expected.

"**Gotcha**" If logging to the console is enabled this degrades firewall performance. This is acceptable for testing but not recommended for production systems.

- **Apply Protocol Fixes**

```
fixup protocol smtp 25          ! Only a subset of SMTP commands are allowed
fixup protocol http 80          ! Only valid http commands are used
fixup protocol ftp 21
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
fixup protocol sip 5060
```

The fixup command enables the firewall's application protocol feature

smtp 25: This limits the commands that can be used to connect to the mail server to only the following: HELO, MAIL, RCPT, DATA, RSET, NOOP and QUIT
http 80: Allows the use of filter url if required.
ftp 21: Tracks the port usage in the data stream so active ftp may be used for outgoing client connections.

To test the smtp fixup telnet to port 25 on the mail server, try one of the restricted mail commands. The response from the firewall will be "500 command unrecognized".

The remaining protocols listed above have protocol specific port requirements and may change in mid stream that is why the application proxy service is required. If the protocol does not have the "fixup" applied, the firewall will block the traffic.

- **Name the Interfaces**

```
nameif ethernet0 Outside security 0
nameif ethernet1 Inside security 100
nameif ethernet2 DMZ security 30
nameif ethernet3 Service security 50
nameif ethernet4 Manage security 70
```

Defines the name and security level that is assigned to each physical interface.

Syntax
nameif hardware_id if_name security_level

When defining security levels it should be noted that access from a higher security to a lower security level, global and static commands must be present. For access from a lower security level to a higher level, static and access-list commands must be present.

- **Assign IP Addresses to the Interfaces**

```
ip address Outside 167.216.133.1 255.255.255.240
ip address Inside 167.216.133.129 255.255.255.240
ip address DMZ 167.216.133.17 255.255.255.240
ip address Service 167.216.133.33 255.255.240
ip address Manage 192.168.0.1 255.255.255.252
```

Assign names and IP addresses to the interfaces that have been used. Each interface is on a different subnet to avoid routing problems.

Syntax
ip addresses interface_name IP_address [subnet_mask]

- **Configure NAT**

```
nat (Inside) 0 167.216.133.128 255.255.255.240
nat (DMZ) 0 167.216.133.16 255.255.255.240
nat (Service) 0 167.216.133.32 255.255.255.240
nat (Manage) 0 192.168.0.1 255.255.255.252
```

As a routable address space has been used, NAT needs to be disabled for each interface.

Syntax
nat [(if_name)] 0 local_ip [netmask[max_cons[em_limit]]][norandomseq]

- **Configure Statics**

```
static (DMZ,Outside) 167.216.133.18 167.216.133.18      ! DNS Server
static (DMZ,Outside) 167.216.133.20 167.216.133.20      ! Web Server
static (DMZ,Outside) 167.216.133.25 167.216.133.25      ! Mail Relay
static (Inside,DMZ) 167.216.133.130 167.216.133.130     ! Internal network
static (Service,Outside) 167.216.133.40 167.216.133.40  ! Customers Web Server
```

Statics allow access to an interface from one with a lower security setting, e.g. to allow some one, on the Internet, access to a machine in the DMZ a static has to be set up.

Syntax
Static [(internal_if_name,external_if_name)] global_ip local_ip [netmask network_mask] [max_cons[em_limit]][norondomseq]]

- **Access Lists for Interface Access**

```
! Allow public access to the DNS Server from any IP address
access-list acl_Outside permit UDP any host 167.216.133.18 eq domain
! Allow secure access to the Public Web Server from any IP address
```

```
access-list acl_Outside permit TCP any host 167.216.133.20 eq www
! Allow public access to the Web Server from any IP address
access-list acl_Outside permit tcp any host 167.216.133.20 eq 443
! Allow public access to the Mail Relay Server from any IP address
access-list acl_Outside permit tcp any host 167.216.133.25 eq smtp
! Allow secure access to the Customers Web Server from any IP address
access-list acl_Outside permit tcp any host 167.216.133.40 eq 443


! Allow a host on the DMZ to use NTP off the ISA Server
access-list acl_DMZ permit tcp 167.216.133.16 255.255.255.240 host 167.216.133.130 eq 37
! Allow a host on the DMZ to report syslog messages to the ISA Server
access-list acl_DMZ permit UDP 167.216.133.16 255.255.255.240 host 167.216.133.130 eq
514
! Allow SQL logging from the MimeSweeper Host to the ISA Server
access-list acl_DMZ permit tcp hostt 167.216.133.25 host 167.216.133.130 eq 1443
```

The access-list defines how users can access server addresses: E.g. IP address, and port.

```
Syntax
Access-list acl_name [deny | permit ] protocol src_addr src_mask operator port dest_addr
dest_mask operator port
```

The access-list creates a "virtual tunnel" so that a lower security interface can see the resources on a higher security interface.

The access-list then needs to be applied to the lower security interface.

```
! Apply the access-list acl_Outside to the outside interface
access-group acl_Outside in interface Outside

! Apply the access-list acl_DMZ to the DMZ Interface
access-group acl_DMZ in interface DMZ
```

To test the above access-lists NmapNT can be used to scan each destination host or network. The nmapnt responses should show only the ports that are expected open. The scans that should be executed are at least TCP SYN scan –sS and UDP scan –sU.

The following access-list entries tighten security even more:

```
! Allow the mail relay server to create outgoing SMTP connections
access-list acl_DMZ permit tcp host 167.216.133.25 any eq smtp
! Allow the mail relay server to do DNS lookups
access-list acl_DMZ permit tcp host 167.216.133.25 any eq domain
! Deny any other hosts in the DMZ network from creating an outgoing connection
access-list acl_DMZ deny any any


! Allow the ISA server full access
access-list acl_Inside permit tcp host 167.216.133.130 any any
! Deny any other hosts in the Inside network from creating an outgoing connection
access-list acl_Inside deny any any
```

```
! Allow the Management server to create a SMTP connection to the mail relay server
access-list acl_Manage permit tcp host 192.168.0.2 host 167.216.133.25 eq smtp
! Deny any other network access from the Management network
access-list acl_Manage deny any any


! Deny any hosts on the Service network from creating any outgoing connections
access-list acl_Service deny any any

! Permit incoming icmp unreachable messages
access-list acl_Outside permit icmp any 167.216.133.0 255.255.255.0 unreachable
! Deny all other incoming icmp.
access-list acl_Outside deny icmp any 167.216.133.0 255.255.255.0 any
! Deny outgoing echo-reply, time-exceeded and unreachable messages.
access-list acl_Outside deny icmp 167.216.133.0 255.255.255.0 any echo-reply
access-list acl_Outside deny icmp 167.216.133.0 255.255.255.0 any time-exceeded
access-list acl_Outside deny icmp 167.216.133.0 255.255.255.0 any unreachable
! Permit echo-request from the network
access-list acl_Outside permit icmp 167.216.133.0 255.255.255.0 any echo-request
```

"Gotcha" by disabling all icmp messages from the Internet there might be communication problems with some sites. If a packet is too big icmp is used to communicate this back to the sending host.

The above access-lists need to be applied to the appropriate interface as below.

```
! Apply the access-list acl_Inside to the Inside interface
access-group acl_Inside in interface Inside

! Apply the access-list acl_Manage to the Management interface
access-group acl_Manage in interface Manage

! Apply the access-list acl_Service to the services interface
access-group acl_Service in interface Service
```

Again these rules can be tested using NmapNT.

Firewall Internal

Security Description

The internal firewall performs filtering on packets that have been terminated in the VPN. Only port 80 is open to all Web Servers with port 443 open on the Customers Web Server.

Only a brief rule set has been supplied here as the main focus of this paper was the external defenses. If more information is required the following sources have excellent information:

The Netfiter home page http://netfilter.kernelnotes.org/
A reasonable site with a good list of howto http://my.netfilter.se/

Another good site is http://www.telematik.informatik.uni-karlsruhe.de/lehre/seminare/LinuxSem/downloads/netfilter/iptables-HOWTO-3.html

Use a web search engine looking for the key words of IPtables or Netfilter.

Security Policy

- **Set Default Actions**

  IPTables –p Input DROP
  IPTables –p Output DROP
  IPTables –P Forward DROP

Set the default actions to drop any packet that enters the firewall. Then access will be granted to each data stream that we require.

- **Block invalid packets**

  # Block XMAS packets
  iptables -A Input -p tcp --tcp-flags ALL ALL -j DROP
  iptables -A Forward -p tcp --tcp-flags ALL ALL -j DROP
  # Block NULL packets
  iptables -A Input -p tcp --tcp-flags ALL NONE -j DROP
  iptables -A Forward -p tcp --tcp-flags ALL NONE -j DROP

- **Allow HTTP traffic to cross the firewall**

  $Customer_Web = 167.216.133.48
  $Parters_Web=167.216.133.49
  $Suppliers_Web=167.216.133.50
  # Define names for the addresses
  iptables -t nat -A Forward -i eth0 -d 167.216.133.35 -dport 80 -j DNAT --to $Customer_Web
  # Forward any traffic destined for the Customer Web Server port 80 to the true IP address.
  iptables -t nat -A Forward -i eth0 -d 167.216.133.40 -dport 443 -j DNAT --to $Customer_Web
  # Forward any SSL traffic destined for the Customer Web Server to the true IP address.
  iptables -t nat -A Forward -i eth0 -d 167.216.133.36 -dport 80 -j DNAT --to $Partners_Web
  # Forward any traffic destined for the Partners Web Server port 80 to the true IP address.
  iptables -t nat -A Forward -i eth0 -d 167.216.133.35 -dport 80 -j DNAT --to $Supplier_Web
  # Forward any traffic destined for the Supplier Web Server port 80 to the true IP address.

- **Allow Database access from the WebServers**

  $Customer_Database = 167.216.133.66
  $Parters_Database=167.216.133.67
  $Suppliers_Database=167.216.133.68
  # Define names for the addresses
  iptables -t nat -A Forward -i eth1 -d $Customer_Web -dport 80 -j DNAT --to $Customer_Database
  # Forward any databese traffic from the Customer Web Server to the database server.
  iptables -t nat -A Forward -i eth1 -d $Partners_Web -dport 80 -j DNAT --to $Partners_Database

```
# Forward any databese traffic from the Partners Web Server to the database server
iptables -t nat -A Forward -i eth1 -d Supplier_Web -dport 80 -j DNAT --to $Suppliers_Database
# Forward any databese traffic from the Suppliers Web Server to the database server
```

If further increases in security are required it multiple Ethernet cards can be installed in the firewall giving each Web Server its own subnet. This means that if any system is compromised that no other traffic could be intercepted.

VPN

A VPN is used to encrypt data between Customer, Partner and Supplier Web Servers and the end users. The VPN is terminated on the PIX firewall using a hardware accelerator card. ESP will be used as the security protocol, ESP encrypts both the original data payload and the TCP header to provide both authentication and data integrity. AH only protects the TCP header, this provides packet source integrity but not data integrity. A disadvantage with AH is, if the TCP header gets changed in any way e.g. by NAT the packet will be rejected.

Key exchange will be done using Internet Key Exchange.

To enable VPN access the following commands are entered from config mode:

```
access-list Secure-Out permit ip [Suppliers Firewall] [Network mask] host 167.216.133.34
access-list Secure-Out permit ip [Customers Firewall] [Network mask] host 167.216.133.35
access-list Secure-Out permit ip [Partners Firewall] [Network mask] host 167.216.133.36
```

Creates an access-list that sets which traffic will be encrypted.

```
crypto ipsec transform-set Suppliers esp-3des esp-md5-hmac
crypto ipsec transform-set Customers esp-3des esp-md5-hmac
crypto ipsec transform-set Partners esp-3des esp-md5-hmac
```

Sets the type of encryption to use for each link. Both authentication and encryption have been selected.

```
crypto map Secure-Out 10 ipsec-isakmp
crypto map Secure-Out 10 match address Secure-Out
crypto map Secure-Out 10 set peer [Suppliers Firewall] [Customers Firewall] [Partners
Firewall]
```

Create the crypto map and assign a number to it. ISAKMP is used to exchange key and encryption algorithms. Set the peers for the encryption e.g. the VPN termination device.

```
crypto map Secure-Out 10 set transform-set Suppliers Customers Partners
```

Apply the transform-sets to be used.

```
isakmp enable Outside
```

Enables isakmp negotiation on the Outside interface.

```
isakmp key Suppliers3ecretPassw0rd address [Supplier Firewall]
isakmp key Customers3ecretPassw0rd address [Customers Firewall]
isakmp key Partners3ecretPassw0rd address [Partners Firewall]
```

Define peer passwords.

isakmp identity address
The IP address will be used for the isakmp indentity.

isakmp policy 10 Authentication pre-share
isakmp policy 10 encryption 3 des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 7200
Authentication pre-share uses the passwords defined above. This enables a slightly more secure tunnel. 3 des encryption is to be used inside the IKE policy. Sha is the hash algorithm to be used inside the IKE policy. Defining the group to 1 means that 768 bit Diffie-Hellman goup will be used. The lifetime of the IKE security policy is 2 hours.

crypto map Secure-Out interface Outside
Apply the map to the outside interface.

sysopt connection permit-ipsec
Enable ipsec communication.

To test ipsec communication execute the following show commands:

show access-list
Lists the access-list command statements in the configuration and has a hit counter that shows how many times each list has been matched

show crypto ipsec sa
Lists:
The crypto tag that the firewall has used,
Local and remote address/mask/protocol/port,
Of encrypted packets in and out,
Transform settings and statistics,
Remaining key lifetime.

Assignment 3

Audit Your System 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:

- 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.
- 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.
- 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."

Plan the Assessment

The objective of the assessment is to ensure the perimeter of the network is secure, including both the border router and the primary firewall.

Given that the audit is limited to the border router and primary firewall, approximately 48 to 60 hours would be required to audit the system and prepare a report. The cost for the auditor is $125 per hour plus travel expenses. Estimated cost is between $6000 and $7500 + travel expenses.

An accurate network diagram will be requested showing external access points and a copy of the current security policy.

- **External Network Scan and Probe Test**

After discussion with GIAC management and written permission is granted a penetration test and port scan can commence. The scan has been scheduled for a Sunday afternoon between 1 pm and 7 pm. This is a low traffic time, which will inconvenience very few people and minimize risks to the network and customers. GIAC help desk staff will be informed of the scan and which hosts are to be tested. An emergency contact number has been supplied to the duty senior help desk administrator. Should the scanning produce any serious problems staff can be contacted and the scan stopped.

Test the external operation of the filtering at the border router. The scan of the network would comprise of the following steps:

Connect to the router using the default SNMP community strings,
Port scan of the network,
icmp tests.

- **On Site Information Gathering**

On site meeting with IT management is essential to gain an understanding of what they think firewall and security polices are. A meeting with the Network Team who look after the perimeter network on day-to-day basis would be conducted to check consistency between the documented security policy and the implemented policy.

A site inspection would be conducted to make sure that the router is physically secure and no passwords are taped to the outside of the routers or other network equipment.

A copy of the security policy will be requested to confirm that the copy shipped with the request for audit is the same as currently being used.

A copy of the current configuration on the border router and firewall would also be requested.

- **Policy Verification**

Testing would then start to check that the listed security policies are in place and behaving as expected.

Then all the firewall rules would be tested individually to make sure that each rule is doing the job intended.

An internal port scan would then commence to check that no extra services are available.

- **Summary Report**

A summary report will be prepared detailing the following:

Methods used in the assessment
Hosts and networks scanned
Utilities used
Any policy breaches and possible solutions
Identifying any other issues.

Implement the Assessment

The external scan would start by checking if the default SNMP community strings are still enabled on the border router and firewall.

The tool used for this is snmputil.exe supplied in the NT Resource kit.

Syntax
snmputil {{get | getnext | walk} agent community oid [oid] | trap}

If the default strings have been disabled, the following output would be expected:

```
C:\>snmputil get border public system.sysDescr.0
error on SnmpMgrRequest 8

C:\>snmputil get border private system.sysDescr.0
```

```
error on SnmpMgrRequest 8
```

If the default strings are enabled the following output would be expected:

```
C:\>snmputil get border public system.sysDescr.0
Variable = system.sysDescr.0
Value    = Cisco Internetwork Operating System Software ..IOS (tm) 3640 ….

C:\>snmputil get border private system.sysDescr.0
Variable = system.sysDescr.0
Value    = Cisco Internetwork Operating System Software ..IOS (tm) 3640 ….
```

NB: On some routers the snmputil returns the value as a string in hex, in this instance the output would look something like this:

```
C:\>snmputil get border public system.sysDescr.0
Variable = system.sysDescr.0
Value    = String
<0x43><0x69><0x73><0x63><0x6f><0x20><0x49><0x6e><0x74><0x65><0x72><0x6e><0
x65>
<0x74><0x77><0x6f><0x72><0x6b><0x20><0x4f><0x70><0x65><0x72><0x61><0x74><0
x69>
```

The next step would be to conduct an external port scan of the network. Using nmapNT available from http://www.eEye.com.

The command used was:

NmapNT –v –sS –p0 167.216.133.1-254

Scanning the whole 167.216.133.X subnet Will pick up any hosts that can be seen from the Internet. The –sS sets scan type to use the TCP SYN. –v displays the output in verbose mode. –P means that the target is not pinged to check if it is up before the scan starts.

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Initiating SYN half-open stealth scan against 167.216.133.20
Adding TCP port 80  (state open).
Adding TCP port 443 (state open).
The SYN scan took 180 seconds to scan 1523 ports.
Interesting ports on 167.216.133.20:
Port       State       Service
80/tcp     filtered    http
443/tcp    open        https

Initiating SYN half-open stealth scan against 167.216.133.25
Adding TCP port 25  (state open).
```

```
The SYN scan took 184 seconds to scan 1523 ports.
Interesting ports on 167.216.133.25:
Port       State      Service
25/tcp     open       smtp

Initiating SYN half-open stealth scan against 167.216.133.40
Adding TCP port 443  (state open).
The SYN scan took 190 seconds to scan 1523 ports.
Interesting ports on 167.216.133.40:
Port       State      Service
443/tcp    open       https
```

The above scan shows that only the expected services were available from the Internet. The DNS server does not show up here as the port is only enabled for UDP.

The next scan would be almost the same but scanning for UDP ports using the –sU switch.

The output from this scan only shows DNS server

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Initiating FIN,NULL, UDP, or Xmas stealth scan against 167.216.133.18
The UDP or stealth FIN/NULL/XMAS scan took 200 seconds to scan 1523 ports.
Interesting ports on 167.216.133.18:
Port       State      Service
53/udp     open       domain
```

Checking the logs on the firewall shows the packets being blocked.

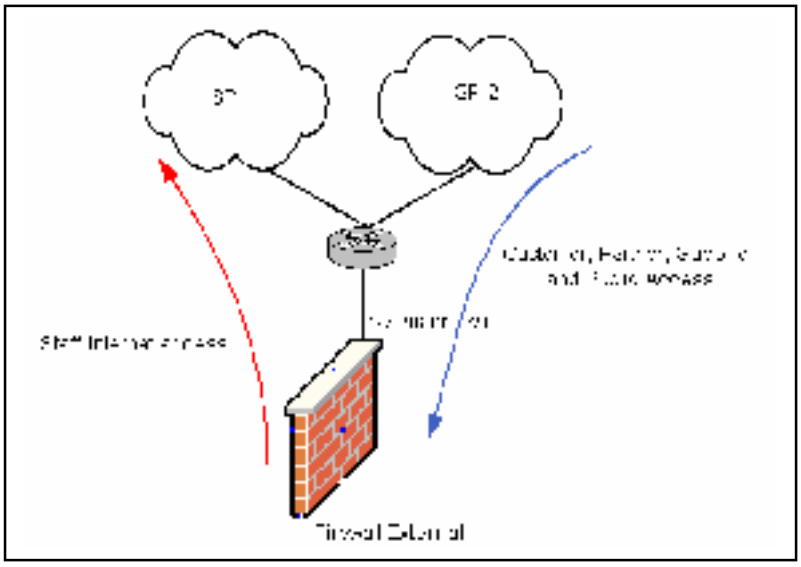
> %Firewall-2-106001: Inbound TCP connection denied from 210.54.17.127:1325 to 167.216.133.18:25 S on interface Outside

Once the external check has been done internal testing will follow the same format. Start by reviewing the access-lists and firewall polices, and checking each rule by using nmap to confirm the filter works.

Recommendations

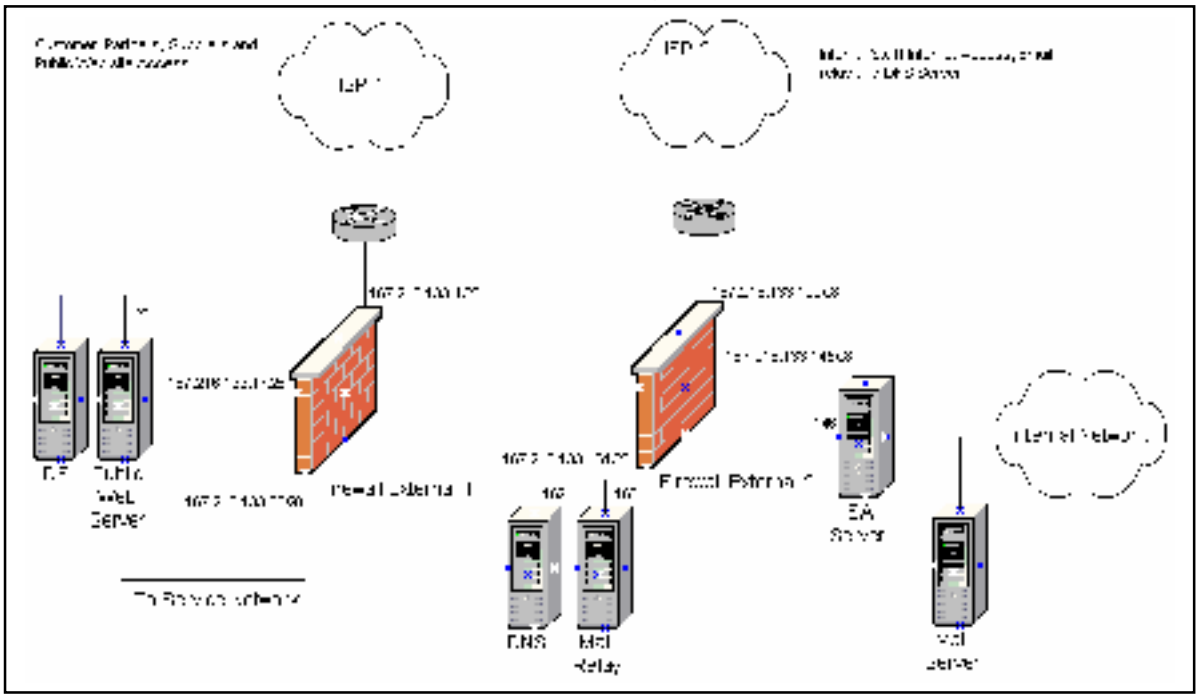
During the audit it was noted that all Internet access for the GIAC networks was through a single Internet connection with no QOS services. This means that if a GIAC staff member is downloading a large data file from the Internet or a very large email is received, customer service would be affected.

One solution would be to install a second Internet connection to the router, then would mean that staff Internet usage would have no effect on customer access. If a second ISP was used for this connection, diverse paths would be available increasing reliability.



Another possible solution would be installing a packet-shaping device like the packeteer from http://www.packeteer.com/. This allows administrator's control over the actual traffic profile on the connection. Then customer performance could be guaranteed.

A third possible solution is to separate the customer network from the GIAC network even further, providing a separate firewall and router for staff Internet access, DNS and Mail relay, with a connection between the firewalls to allow internal access to the databases.



On the border router the log keyword should be applied to all incoming access-lists. This means all access-list matches will create a syslog entry.

On the border router the access-lists could be changed to Reflexive access-lists. This uses a state table to control traffic flow.

Assignment 4

Design Under Fire

"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:

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.

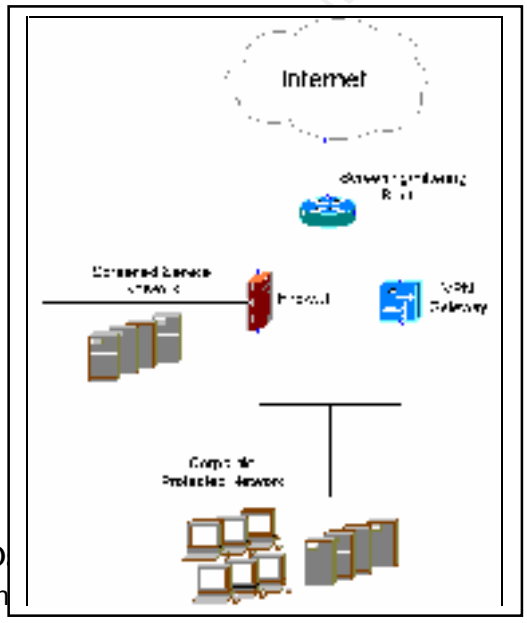
A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP or ICMP floods. Describe the countermeasures that can be put in place to mitigate the attack that you chose.

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."

Target Network

The network to be targeted for the attack, is the one submitted by Colin Stuckless.



The URL for Colin's Document is http://www.sans.org/y2k/practical/Colin_Stuckless.doc

The hardware and software listed bellow were defined by Colin.

"A Cisco 3640 acts as our filtering/screening firewall. While not representing the core of our security platform, the screening router plays an important role in being a front line defense mechanism. We configure the screening router to immediately discard traffic that has no legitimate purpose coming into our network.

A Cisco PIX firewall is the key component of this architecture. It is configure with three network interfaces, one for the external network (we'll call it the dmz interface), one for our semi-secure service network (service) and one for our internal network representing our secured corporate LAN (internal).

For VPN connectivity, I've separated this function from the firewall. While this represents an increase in cost, it also gives additional flexibility for vendor choice, change management, and maintenance. I feel these advantages outweigh the additional costs incurred for this type of solution. The VPN gateway device is a RedCreek 5100, which utilizes IPSec as a secure means of connecting GIAC Enterprises' remote offices and partners over the Internet.

The services network is a mixture of Solaris and NT servers providing HTTP and HTTPS, DNS, SMTP and FTP services. Intrusion detection runs on the router and a server based IDS is installed on the screened subnet. A combination Unix syslog and NT event log server is also located on the service network to aggregate logs from the other service network servers."

An attack Against the Firewall

The core security of the network is designed around a single PIX firewall version 5.0

A check for known exploits on Cisco PIX firewalls was conducted.

The following list of exploits was discovered:

Cisco Secure PIX Firewall Mailguard Vulnerability
Updated October 5, 2000
September 27, 2000

Cisco Secure PIX Firewall TCP Reset Vulnerability
July 11, 2000

Cisco Secure PIX Firewall FTP Vulnerability
March 16, 2000

Updated May 19, 2000
Field Notice: Cisco PIX and CBAC Fragmentation Attack
September 11, 1998

Field Notice: Cisco PIX Firewall Manager File Exposure
September 2, 1998

Field Notice: CRM Temporary File Vulnerability
August 13, 1998

Field Notice: PIX Private Link Key Processing and Cryptography Issues
Revision: June 16, 1998
June 3, 1998

On checking which versions of the firewall were vulnerable to each exploit the following were chosen.

Cisco Secure PIX Firewall TCP Reset Vulnerability
Cisco Secure PIX Firewall Mailguard Vulnerability
Cisco Secure PIX Firewall FTP Vulnerability

The first vulnerability while very important is rather hard to exploit remotely and of little use if an exploit was executed. The exploit and conditions needed are listed bellow:

> The PIX is unable to distinguish between a forged TCP RST packet and a genuine TCP RST packet. This means it is possible to close any TCP/IP connection established through the PIX.
>
> The attacker needs to know the source and destination IP address and ports of the connection that is going to be attacked. The addresses while easily acquired when on a local network, would be much harder to gain from a remote network.

If the exploit was executed remotely without knowledge of the port addresses the best the attacker could hope for would be to disconnect any valid TCP sessions that are open.

NB: If this attack was combined with a compromised system on either the ISP, partners, suppliers, or customers site, it might be possible to stop all communication with the network.

The second and third vulnerabilities are not directly related to the firewall.

Denial of Service Attack

The aim of the DOS attack is to stop services being supplied to customers. This attack while not directly damaging to hosts or systems, if executed for an extended period of time and News Media notified about the attack, can be very damaging for the public image of the company.

On checking the ACLs on the border router it has been noted that the following rules exist:

```
access-list 100 permit tcp any any
access-list 100 permit udp any any
```

These rules permit any TCP and UDP traffic that has not been explicitly denied in prior rules.

The simplest attack is a TCP SYN attack. This proceeds to "bombard" the victim with so many TCP requests the host can not reply to legitimate traffic.

From each compromised host a SYN attack would be commenced using npmap –sS

This attack is very hard to protect against as the sending a SYN packet is the first step in creating a TCP connection. To help to protect against this attack Cisco have provided the following features:

> PIX – Flood defender if the firewall finds that is running out of resources then it will actively reclaim TCP user resources.
>
> Router – TCP Intercept this allows the router to be a "man in the middle" with the destination host for creating connections. The router receives a connection request from a client, then it sends back a reply accepting the connection. If the connection is then created the router contacts the Server and creates another connection, then "stitches" the two together. This will increase latency but the added security might be worth it.

Compromise an Internal System

The attack utilizes the ftp vulnerability.

The first step when executing this exploit is to determine the version of the FTP server being attacked. While this is not directly related to executing the primary exploit it will make exploiting the host much simpler.

By opening a ftp client and connecting to the server the following splash was displayed:

```
ftp> open 3.3.3.4
Connected to 3.3.3.4.
220 3.3.3.4 Microsoft FTP Service (Version 4.0).
331 Anonymous access allowed, send identity (e-mail name) as password.
230 Anonymous user logged in.
```

The following Bugtraq article shows the exploit in more detail. Cisco FTP exploit.

The code for the utility used to execute the exploit is available from ftp-ozone.

The attack fools the PIX to open an incoming port to the FTP server. This port then bypasses incoming security ACLs as the PIX assumes that the FTP server created it.

Once the PIX has opened the port then any a scan for additional vulnerabilities can be executed.
If the FTP server returns an error code in response to a invalid command,
e.g. 227 (3,3,3,4,0,139)

A connection to the NBT service will possible gaining access to shares.

Then using brute force attack on the administrator account and password a full system compromise can be executed.

Resources

The following resources have been used for information in this assignment.

http://www.sans.org
http://www.cisco.com
http://www.windowsitsecurity.com/
http://www.microsoft.com/security
http://www.securityfocus.com
http://www.cert.org
http://www.ntbugtraq.com
http://netfilter.kernelnotes.org/

Sans Darling Harbour 2001 Firewalls, Perimeter Protection and Virtual Private Networks notes.