



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Enterprises

On Line Fortune Cookies



by
Nicholas Cop
17/08/2001

GIAC Training & Certification
Firewalls, Perimeter Protection and VPNs
Version 1.5d

Assumptions	3
Assignment 1 - Security Architecture (25 Points)	4
Logical Diagram	5
Dialup Network	6
Network Architecture	7
Physical Security	7
Internet Router(s)	7
VPN Router(s)	7
PIX(es)	8
Switch(es)	8
Host Protection and Miscellaneous Devices	8
Fortune Cookie Access	10
Partners	10
Suppliers	10
Customers	11
Remote GIAC Staff	11
Network Management	11
External Network	11
Internal Network	12
Protected Network	12
Secure Network	13
Assignment 2 - Security Policy (25 Points)	14
Internet Router(s)	15
VPN Router(s)	23
PIX(es)	31
Assignment 3 - Audit Your Security Architecture (25 Points)	37
Pre-Assessment	37
Plan the Assessment	38
Technical Approach	38
Schedule and Risks	38
Costs and Effort Level	39
Audit Diagram	40
Audit Implementation	41
Audit 1 (Internet)	42
Audit 2 (Internet LAN)	44
Audit 3 (VPN LAN)	44
Audit 4 (External Management LAN)	45
Audit 5 (DMZ LAN)	46
Audit 6 (Common LAN)	47
Audit 7 (Internal LAN)	47
Audit 8 & 9	48
Scan Results	49
Validation of Security Policy	51
VPN Validation	57
Alternate Architectures	67
Alternate 2	68
Alternate 3	69
Assignment 4 - Design Under Fire (25 Points)	70
Security Architecture	71
Security Policy	72

Assumptions

1. A complete business analysis of all current and projected traffic requirements has been completed.
2. Suggested infrastructure is in accordance with the associated business analysis and will be sufficient to meet future growth expectations of GIAC Enterprises.
3. Global security policy/manual has been drafted and will be implemented on physical hardware/software.
4. Security audit procedure document has been created and permissions have been signed by authorising officers and verified by auditing team leader.
5. A risk analysis has been carried out of physical infrastructure that includes any services/products that utilise the physical equipment.
6. Redundancies and failover equipment are not included in technical configurations.

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 1 - Security Architecture (25 Points)

Define 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 filtering 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 define how to use perimeter technologies to implement your security architecture.

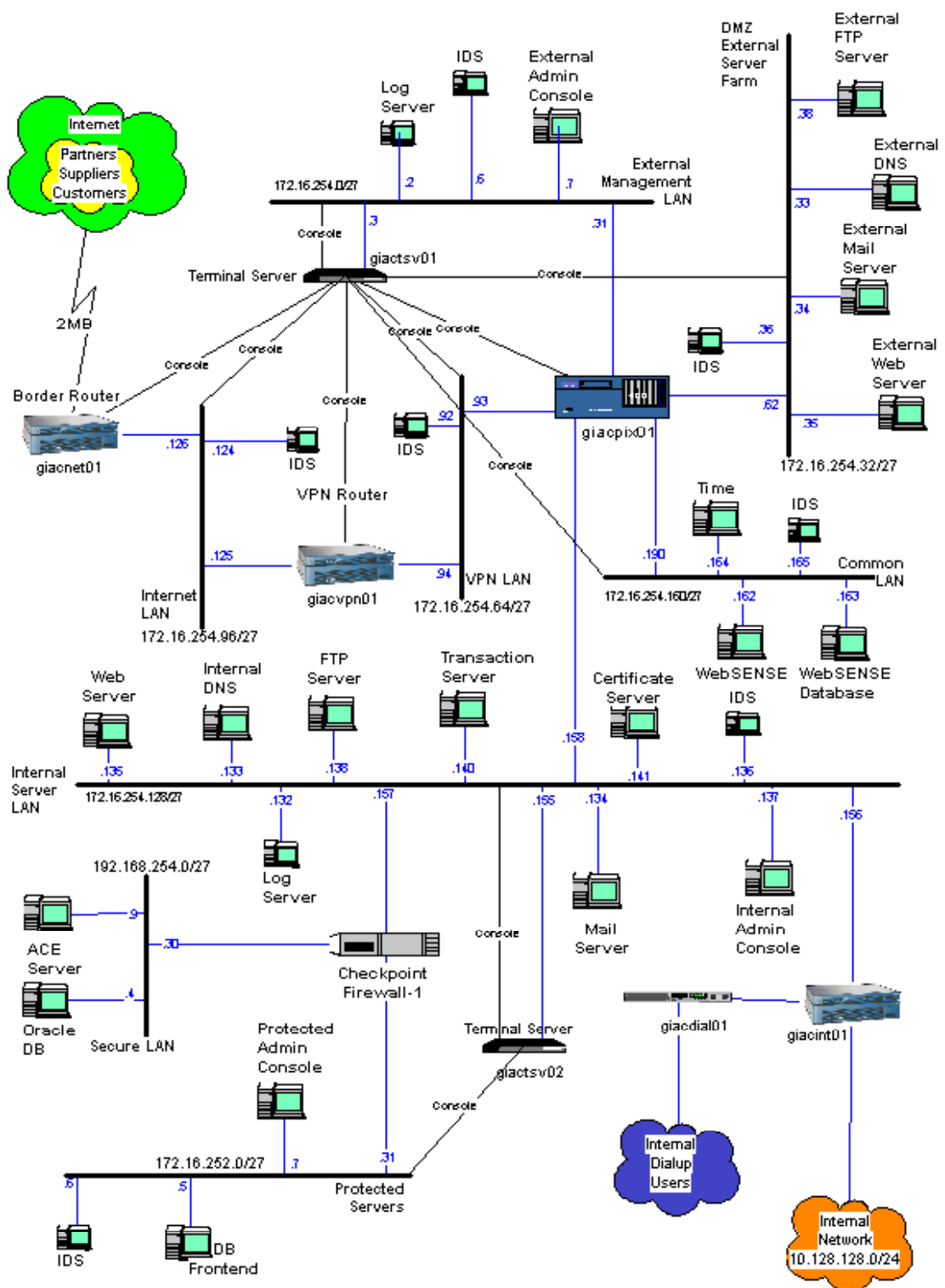
You must consider and define access for:

- 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).

© SANS Institute 2000 - 2005, Author retains full rights.

Logical Diagram

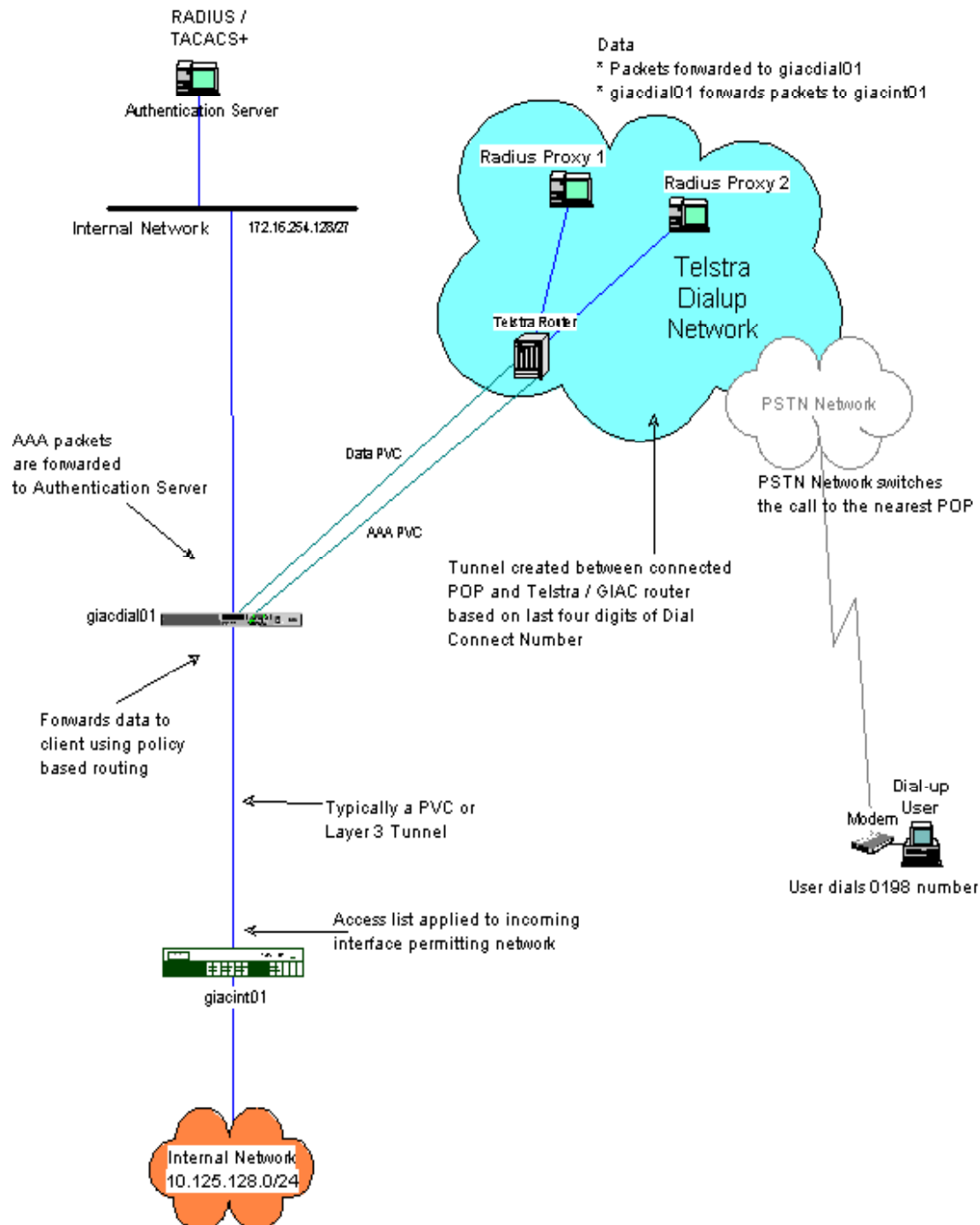
LOGICAL VIEW - GIAC Enterprises



Dialup Network

Authentication

- * Initial call sent to Telstra router based on last four digits
- * Telstra radius proxies recognise as GIAC authentication (last 4 digits)
- * Packets forwarded to Authentication Server
- * Authentication Server authenticate user



Network Architecture

The defence in depth of this network will use border routers, separate VPN routers that terminate IPSEC tunnels, PIX firewalls and secured switches. Further layers of defence will be noted when discussing how data will be accessed deeper to the Internal network.

Physical Security

All perimeter equipment will have physical access restrictions. Either a separate computer room or some sort of sectioned off area that can't be accessed by non-authorised staff. In addition, access logs to sensitive areas should be generated and reviewed by security staff. If such an area does not exist within GIAC then off site equipment warehousing may be considered. This scenario makes management and maintenance difficult. I believe that swipe card access is sufficient for GIAC needs, with authorised personnel access only and access monitoring.

The diagrams above shows a logical network topology omitting redundancies and backups.

Internet Router(s)

The Internet router is a 3640 running Cisco Firewall IOS which utilises both CBAC (Context-Based Access Lists) and software IDS (Intrusion Detection System). Internet access will be via a 2MB pipe to one ISP with a backup 2MB pipe to a separate ISP. BGP will be sent to the Internet but the full Internet routing table will not propagate back to the Internet router. GIAC does not need the Internet routing table (it takes up unnecessary memory and processing). The Internet routing table will be blocked at the ISP to reduce traffic on the link for cheaper access fees and also at the GIAC Internet router (just in case the ISP makes a rare mistake and lets the routing table through and crashes our router☺)

Cisco Firewall IOS was chosen because it provides addition functionality to standard IOS features.

CBAC (part of the F/W IOS) and has the added benefit of stateful inspection and multi-channel protocol analysis (eg FTP, SQLNet* that are relevant to this [proposed] architecture)

A built in Intrusion Detection System in the F/W IOS provides additional logging and will also provide some signature analysis and attack prevention based on these signatures.

Specifications:

Make	Cisco
Model	Cisco 3600 4-slot Modular Router-AC
IOS	IP/FW/IDS c3640-io3-mz.122-1a.T.bin (has to be .T if future use requires SSH)
Memory	2x16 MB Flash and 128 MB RAM
Card(s)	2 x WIC-1T - 1Port Serial WAN Interface Card 2 x NM-2E2W - 2Ethernet 2 WAN Card Slot Network Module

VPN Router(s)

The VPN router is a 3640 running 3DES software and a VPN accelerator card.

All IPSEC encryption will be done at this router. The reason that the VPN end-point is not on the PIX or past the PIX on the DMZ is to separate specific functions and lessen the load on the PIX so it can process traffic in the clear.

Placing another router on an inside LAN of the perimeter network adds the functionality to enable Partners, Suppliers and Customers to add backup routers using Frame or ISDN and create private networks that lessen the chance of data compromise. Some of these Partners, Suppliers and Customers may wish to completely isolate their own VPN traffic from all others and this provides another measure of function separation and being compromised.

The accelerator card was added as increase encryption speeds.

Make	Cisco
Model	Cisco 3600 4-slot Modular Router-AC
IOS	IP PLUS IPSEC 3DES c3640-ik9s-mz.122-1a.T.bin (.T for future SSH use)
Memory	2x16 MB Flash and 128 MB RAM
Card(s)	2 x NM-2E2W - 2Ethernet 2 WAN Card Slot Network Module 1 x NM-VPN/MP - DES/3DES VPN Encryption Module for 3620/3640

PIX(es)

Make	Cisco
Model	PIX 525UR Bundle (Chassis, unrestricted SW, 2 FE ports)
IOS	pix601.bin - PIX-VPN-3DES - PIX 3DES S/W License Without Client Software
Memory	8MB Flash and 64MB RAM
Card(s)	PIX-4FE PIX Four-port 10/100-Ethernet interface

The PIX will have up to 6 ports to provide necessary architecture for GIAC Enterprises. Alternate Architecture 3 (p68) will require IPSEC which is why I have added the software above.

Switch(es)

Make	Cisco
Model	WS-C2924-XL-EN 24-port 10/100 Switch (Enterprise Edition)
IOS	c2900XL-c3h2s-mz.120-5.3.WC.1.bin

Host Protection and Miscellaneous Devices

Within the context of the overall system architecture, security of individual hosts is treated as stand-alone and insecure. You don't need to purchase the latest and greatest super secure platform & OS if all you need is an internal log server that is already behind the existing secure environment. Keep in mind the complete network architecture if you decide to use Red Hat 7.1 on an x86 for a log server, then you should secure this device as much as possible (within the given environment) by disabling unneeded services, using ipchains or iptables, applying latest patches, installing monitoring software, physically securing the device, logging to a backup server...etc

These devices below will run on one type of operating system except for the syslog server. This is to simplify the management. The syslog servers run on Linux which is similar enough to Unix to be able to be managed by the same staff. If we chose to use all different platforms and operating systems, the difficulty in getting staff to manage all these devices would be very difficult.

DNS

GIAC Enterprises will be using a split DNS. The External DNS will only know how to resolve names that deal with the external sites (such as e-mail forwarding, web servers) The Internal DNS has all the information (names) that are needed to be resolved with the GIAC network. The DNS will use BIND9.1.2 and be run on Sun Solaris v8

Admin Console, Mail & FTP Server(s)

Servers will run on Sun Solaris v8

Web Server(s)

All Web Servers will run Apache v2.0 on Sun Solaris v8

Syslog Server(s)

RedHat Linux 7.1 with Kernal 2.4 for all syslog servers

Authentication Servers

- The Authentication server software used is CISCO's CiscoSecure product
- Provides support for both RADIUS and TACACS+.
- Dual redundant servers.

These host devices are in addition to the current perimeter devices

- Load Balancers – ([SonicWALL PRO-VX](#), [Zeus Load Balancer](#), [SysMaster](#))
- Database Oracle v8I (with latest patch)

--5 July 2001 Oracle Patches High Risk Security Hole in 8i

Oracle acknowledged a buffer overflow problem in the "listener" component of its database. The attacker who uses the vulnerability can read or change any information in the database. Oracle issued a patch. <http://news.cnet.com/news/0-1003-200-6469566.html?tag=owv>

The following will be applied to all the mentioned devices above.

- Latest relevant OS and patches are applied
- Anti-virus software is on relevant devices
- Unnecessary services are disabled
- Monitoring software is on relevant devices (such as [Tripwire](#))

DialConnect Component

- Telstra product offering a national dialup access service. Client requires either a NFR connection or a DialConnect interface connection into Telstra. 2 PVC's are usually established, one for authentication and one for data.
- Uses one national number - 0198 xxx xxx
- Supports PPP dialin only - PSTN and ISDN
- Local call charge for PSTN dialin user. Cost to the Host Service Provider (HSP) depends on where the user dials in from and where the HSP is. HSP in this case is GIAC and the NFR connection to DialConnect is in Brisbane
- Uses a RADIUS Proxy - forwards RADIUS messages to the customer's own RADIUS Authentication server.
- IP address pools are preallocated with DialConnect :
- Dedicated IP addresses can be implemented via the authentication server.
- All data traffic goes through the "giacdial01" router, which is then policy routed to the client based on the user's source IP address. See DialConnect diagram for more details.
- Access-lists are usually applied at the next hop router from the dialconhg router.

DialConnect Users

- The domain part is optional.
- Password users are CHAP users.
- SecureID users must configure dialup software to bring up terminal window after dialling.

Fortune Cookie Access

I will present a **logical** view of the topology and briefly mention in the Security Architecture section, what redundancies and failover techniques will be applied to the routers and firewalls. I will not go into host based redundancies where they do not impact on perimeter protection as that is outside the scope of this assignment. (but obviously host redundancies exist)

The fortune cookie data will be accessed in the following manner:

Partners

International partners that translate and resell fortunes

1. Partners will access the External Web Server with HTTP. This server will be used for front-end access only and will hold public information.
2. Partners will use a SecureID card to access their individual accounts. The token will authenticate to an Internal ACE/Server (RADIUS/TACACS+)
3. Once authenticated, Partners will gain admittance to the Transaction Server web interface with SSL (HTTPS). This server will be the central point for ordering fortune cookies and administering individual account details.
4. The Transaction Server will then interact with the Front End D.B. Server (FEDB) of the Oracle Database (ODB).
5. When orders have been placed and checked against relevant criteria (ie order must fall within acceptable parameters), the FEDB will issue commands to the FTP Server to send the bulk data of fortune cookies via the External FTP Server. The data will be encrypted to the Partner's site using IPSEC. The encryption level will be Partner dependant using the maximum level of 3DES plus ESP plus AH.
6. If export restrictions curtail the use of certain encryption methods, then the data can also be sent using secure FTP from the External FTP Server. Partners may wish to combine the use of IPSEC and S/FTP if they feel that their fortune cookies are a matter national secrecy☺

Suppliers

Authors of fortune cookie sayings that connect to supply fortunes

1. Suppliers will access the External Web Server with HTTP. This server will be used for front-end access only and will hold public information.
2. Suppliers will use a SecureID card to access their individual accounts. The token will authenticate to an Internal ACE/Server (RADIUS/TACACS+)
3. Once authenticated, Suppliers will gain admittance to the Transaction Server web interface with SSL (HTTPS). This server will be the central point for delivering fortune cookies and administering individual account details.
4. The Transaction Server will then interact with the Front End D.B. Server (FEDB) of the Oracle Database (ODB).
5. When orders have been received and checked against relevant criteria (ie order must fall with acceptable parameters), the Transaction Server will issue a receipt to the Supplier using SSL (HTTPS)
6. The Supplier can now use this unique receipt number to access the Transaction Server for FTP of the fortune cookies to the External FTP Server. The data will be encrypted to the Supplier's site using IPSEC. The encryption level will be at a level determined by GIAC Enterprises (eg 3DES and ESP).
7. If export restrictions curtail the use of certain encryption methods, then the data can also be delivered using secure FTP to the External FTP Server. GIAC will not be combining the use of

S/FTP encapsulated in IPSEC as it does not consider fortune cookies as a matter of national secrecy☺

Customers

Companies that purchase bulk online fortunes.

1. Customers will access the External Web Server with HTTP. This server will be used for front-end access only and will hold public information.
2. Customers will use a SecureID card to access their individual accounts. The token will authenticate to an Internal ACE/Server (RADIUS/TACACS+)
3. Dynamic crypto mapping has been established on the VPN termination point to cater for host-to-gateway access such as Customers who have smaller fortune cookie requirements.
4. Once authenticated, Customers will gain admittance to the Transaction Server web interface with SSL (HTTPS). This server will be the central point for ordering fortune cookies and administering individual account details.
5. The Transaction Server will then interact with the Front End D.B. Server (FEDB) of the Oracle Database (ODB).
6. When orders have been placed and checked against relevant criteria (ie order must fall with acceptable parameters), the FEDB will issue commands to the FTP Server to send the bulk data of fortune cookies via the External FTP Server. The data will be encrypted to the Customer's site using IPSEC. The encryption level will be Customer dependant using the maximum level of 3DES plus ESP plus AH.
7. If export restrictions curtail the use of certain encryption methods, then the data can also be sent using secure FTP from the External FTP Server. Customers may wish to combine the use of IPSEC and S/FTP.

Remote GIAC Staff

1. Remote GIAC staff will utilise a private VPDN that incorporates a local ISP architecture. This will serve as an alternate to Internet connectivity.
2. Staff will dial a local ISP number that will use Layer 2 Tunnelling Protocol (L2TP) to connect to an Internal Cisco 2600 router.
3. Authentication will be SecureID tokens.
4. Remote GIAC staff will have whatever access they have when on site as Internal connectivity is determined by individual authentication. (ie staff will be part of an Internal LAN when dial-in access is used)

Network Management

Four logical classifications of network management exist in the GIAC Network.

External Network

Includes all devices on the DMZ (172.16.254.32/27), Common (172.16.254.160/27), external networks up to the inside of the Internet router (172.16.254.96/27 & 172.16.254.62/27) and the External Management LAN (172.16.254.0/27).

1. Management of non-Cisco external devices on the perimeter network will require an SSH (v2 only) connection to the External Admin Console on the External Management LAN.
2. Access to the External Admin Console will be limited to authorised personnel that will be configured on the ACS Server.

3. SSH (v2 only) will be used to connect from the External Admin Console to individual non-Cisco hosts.
4. All Cisco equipment will be accessed via a secured Terminal Server that can only be reached from the External Admin Console on the External Management LAN using SSH (v1 only).
5. The Cisco Terminal Servers will be the only way to access any Cisco equipment.
6. All Cisco equipment will need SecureID to gain access to the console port.
7. Email/paging/logging services created to check time/frequency of login attempts to all perimeter devices.
8. No SNMP service on perimeter network as equipment heartbeat is checked by scripts from the External Admin Console.
9. Switches will not have IP addresses.
10. Cold switch standby to provide for single points of failure.

Internal Network

Includes all devices on the Internal LAN (172.16.254.128/27) and also the Internal GIAC Network (10.128.128.0/24)

1. Management of non-Cisco external devices on the Internal network will require an SSH (v2 only) connection to the Internal Admin Console on the Internal Server LAN.
2. Access to the Internal Admin Console will be limited to authorised personnel that will be configured on the ACS Server.
3. SSH (v2 only) will be used to connect from the Internal Admin Console to individual non-Cisco hosts.
4. All Cisco equipment will be accessed via a secured Terminal Server that can only be reached from the Internal Admin Console on the Internal Server LAN using SSH (v1 only).
5. The Cisco Terminal Servers will be used to access any Cisco equipment in addition to administrators being able to use SecureID to log onto any Internal Cisco device from the Internal Admin Console. (SSH will not be used to access Cisco equipment)
6. All Cisco equipment will need SecureID to gain access to the console port.
7. Email/paging/logging services created to check time/frequency of login attempts to all Internal devices.
8. SNMP will be active on the Internal network from the Internal Admin Console which will also function as some sort of polling device using HP OpenView.
9. Switches will have IP addresses and be polled by HP OpenView
10. Cold switch standby to provide for single points of failure.

Protected Network

Includes any device on the DMZ (172.17.254.0/27) of the CheckPoint Firewall (do not confuse this with the DMZ of the PIX firewall, they are separate)

This network is the front end to the Secure Network.

1. Management of non-Cisco devices on the Protected network will require an SSH (v2 only) connection to the Protected Admin Console on the Protected Server LAN.
2. Access to the Protected Admin Console will be limited to authorised personnel that will be configured on the ACS Server.
3. SSH (v2 only) will be used to connect from the Protected Admin Console to individual non-Cisco hosts.
4. The Cisco Terminal Servers will be used to access any Cisco equipment in addition to

- administrators being able to use SecureID to log onto any Protected Cisco device from the Protected Admin Console. (SSH will not be used to access Cisco equipment)
5. All Cisco equipment will need SecureID to gain access to the console port.
 6. Email/paging/logging services created to check time/frequency of login attempts to all Protected devices.
 7. No SNMP service on perimeter network as equipment heartbeat is checked by scripts from the Protected Admin Console.
 8. Switches will not have IP addresses.
 9. Cold switch standby to provide for single points of failure.

Secure Network

Includes any device on the inside of the CheckPoint Firewall (again, do not confuse this with the Inside of the PIX firewall, they are separate)

This network will be considered the most secure.

1. Access to ANY device on the Secure LAN will only be allowed from on site (ie no remote access of any kind).
2. Email/paging/logging services created to check time/frequency of login attempts to all Secure devices.
3. No SNMP service on perimeter network as equipment heartbeat is checked by scripts from the ACS Server.
4. Switches will not have IP addresses.
5. Cold switch standby to provide for single points of failure.

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 2 - Security Policy (25 Points)

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 defence in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall rule set, 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 behaviour 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.
8. Be certain to point out any tips, tricks, or "gotchas".

Internet Router(s)

Cisco has made changes to later releases of IOS to incorporate some default security configurations.

The list of default configurations is quite long so I will not add them.

Please note when reading the configs that my comments are in bold.

Many of the configs on the Internet router are duplicated on the VPN router. This provides easier management with a slight impact on security. If we were really pedantic we would use another device from a different vendor but the difficulty to manage these disparate devices would be very high. The usual standard services will be disabled and CBAC will not be utilised here. Instead, regular ACLs will be sufficient to secure this device. I did not use reflexive ACLs on the VPN Router(s) even though they are more secure than extended ACLs because of the limiting functionality of only being able to secure single channel protocols. Thus with Reflexive ACLs, only passive FTP can be used and we would run into future problems with other multi channel protocols such as SQLNet

As stated, I have elected not to group the related commands of the VPN and Internet Routers because I find it easier to view a config in its entirety rather than in pieces. This does create more reading to go through but in the long run it is easier to use as reference material when the configs are separate.

As the access lists are designed on the premise of an explicit permit of known traffic followed by a generic deny for all unknown traffic, many of the addresses/ports in the list are grouped into the end deny statement of the ACLs.

The design of the Internet & VPN Router(s) is based on the following the following suggested list from:

How To Eliminate The Ten Most Critical Internet Security Threats
The Experts' Consensus
Version 1.33 June 25, 2001
Copyright 2000 - 2001, The SANS Institute
<http://www.sans.org/topten.htm> (21/07/2001)

Appendix B: Perimeter Protection For An Added Layer of Defence In Depth

1. Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses, private (RFC1918 and network 127) and IANA reserved addresses. Also block source routed packets.
2. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
3. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
4. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 -- earlier ports plus 445(tcp and udp)
5. X Windows -- 6000/tcp through 6255/tcp
6. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
7. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
8. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
9. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

10. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
11. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

Allow detailed timestamps on the logs to match other devices and provide an accurate picture of when events occur

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime show-timezone
```

```
!
!
```

stop information being gained from the router

```
no ip finger
```

```
!
!
```

encrypt visible passwords on the router with the Vigenere cipher. NB this cipher is easily broken. This is mainly so people looking over your shoulder don't see the password when you display configs

```
service password-encryption
```

```
!
!
```

```
hostname giacnet01
```

log to router buffer at debugging (maximum) level

```
logging buffered 8192 debugging
```

```
!
```

use the inside interface as the source of logging to the syslog servers.

```
logging source-interface Ethernet0/0
```

```
!
```

the two log servers addresses that will receive all logging information

```
logging 172.16.254.2
```

```
logging 172.16.254.132
```

```
!
```

Highest debugging level is set initially

```
logging trap debugging
```

```
!
```

hashed MD5 secret password of the router

```
enable secret 5 $1$e4Wc$XJLwiIMbVeVcobhTT2ykV1
```

```
!
```

add a timezone to make the logs easier to read and match against other hardware

```
clock timezone AEST 10
```

```
ip subnet-zero
```

```
!
```

Stop IP packets that carry a source route option.

Without this option the sender of an IP datagram can control the route that the datagram will take.

reply packet can also be influenced with source route

```
no ip source-route
```

```
!
```

cef is enabled so the router can check the source address of packets against the interface they

entered.

this only works for symmetric routing so meshed networks should not have this command

ip cef

!

we are not using domain names so we disable it.

also if you misspell a command, the router searches for a matching address and this gets annoying

no ip domain-lookup

!

disable services that are not used

no ip bootp server

!

Add CBAC audit trail for logging

ip inspect audit-trail

!

DNS maximum lookup uptime

ip inspect dns-timeout 7

!

Global timeouts will be as default except for the following

Note that auditing is fully qualified on each service in case the global audit entry is removed

Inspect HTTP traffic

ip inspect name allow http alert on audit-trail on timeout 300

!

ftp will have a large timeout in the event of large downloads

ip inspect name allow ftp alert on audit-trail on timeout 3600

!

the tcp & udp timeout should be installed as a catchall traffic net

ip inspect name allow tcp alert on audit-trail on timeout 900

ip inspect name allow udp alert on audit-trail on timeout 15

!

Inspect mail

note that CBAC allows the EXPN and VRFY commands on SMTP connections. These 2 commands are considered by some to be insecure, so a mail sweeper may be added. (qv Alternate Architecture 3 page 68)

ip inspect name allow smtp alert on audit-trail on timeout 900

!

Enable the Cisco IOS IDS to log

ip audit notify log

!

set spamming threshold for email

ip audit smtp spam 100

!

what to do when attack signature is detected

will detect [information signatures](#) from access-list 99 and send an alarm to the syslog server

ip audit name internet_lan info list 99 action alarm

!

will detect [attack signatures](#) from access-list 99

Then send alarm to syslog server drop the packet and reset TCP connection

ip audit name internet_lan attack list 99 action alarm drop reset

!

!

!

interface Ethernet0/0

```

description Inside to VPN router giacvpn02
ip address 172.16.254.126 255.255.255.224
access-list from the inside network going to the outside
ip access-group private_to_public in
stop the router from being used to influence traffic paths
no ip redirects
don't send out ICMP unreachable
no ip unreachable
enable CBAC on this interface to check matched protocols and addresses
ip inspect allow in
enable IDS on the interface
ip audit internet_lan in
no ip mroute-cache
don't respond to ARP requests from unknown devices that are not on the same LAN as the router
no ip proxy-arp
disable CDP from functioning and sending out information about this device
no cdp enable
!
this interface is in BACKUP mode is it technically down until the PRIMARY goes down
interface Serial0/0
description BACKUP Connection to Internet
ip address 160.1.1.1 255.255.255.252
ip access-group public_to_private in
ip verify unicast reverse-path
no ip proxy-arp
no ip redirects
no ip unreachable
ip inspect allow in
ip audit internet_lan in
no ip mroute-cache
no fair-queue
no cdp enable
!
interface Serial0/1
description PRIMARY Connection to Internet
having only one interface up at a time enables cef to function correctly
backup delay 0 100
backup interface Serial0/0
ip address 150.1.1.1 255.255.255.252
access-list from the outside network going to the inside
ip access-group public_to_private in
anti-spoofing check, if reverse path isn't feasible then packet is dropped
ip verify unicast reverse-path
stop the router from being used to influence traffic paths
no ip redirects
don't send out ICMP unreachable
no ip unreachable
enable CBAC on this interface to check matched protocols and addresses
ip inspect allow in
enable IDS on the interface
ip audit internet_lan in
no ip mroute-cache
no ip proxy-arp

```

no fair-queue

disable CDP from functioning and sending out information about this device

no cdp enable

!

stop inadvertent routing to superclass

no ip classless

Primary route to Internet (because of the lower metric ie 10)

ip route 0.0.0.0 0.0.0.0 150.1.1.2 10

Backup route to Internet (because of the higher metric ie 15)

ip route 0.0.0.0 0.0.0.0 160.1.1.2 15

!

route the full IP class of RFC1918 and GIAC addresses to null 0

this prevents “route leakage” and is a backup in case the no ip classless is removed

ip route 10.0.0.0 255.0.0.0 Null0

ip route 172.16.0.0 255.224.0.0 Null0

ip route 192.168.0.0 255.255.0.0 Null0

ip route 167.216.133.0 255.255.255.0 Null0

!

only route known addresses into the inside network

ip route 167.216.133.3 255.255.255.255 172.16.254.125 (DNS)

ip route 167.216.133.4 255.255.255.255 172.16.254.125 (SMTP)

ip route 167.216.133.5 255.255.255.255 172.16.254.125 (HTTP)

ip route 167.216.133.8 255.255.255.255 172.16.254.125 (FTP)

ip route 167.216.133.254 255.255.255.255 172.16.254.125 (IPSEC)

!

route for syslog servers

ip route 172.16.254.2 255.255.255.255 172.16.254.125

ip route 172.16.254.132 255.255.255.255 172.16.254.125

!

!

disable unneeded services

no ip http server

!

ACL for incoming traffic from inside to the Internet, permit in what you want to be inspected

ip access-list extended private_to_public

allow IPSEC out to the Partner1, duplicate entries required for each partner, customer or supplier

CBAC does not recognise IPSEC so it must explicitly be permitted

allow ISAKMP first because it is the first process of the key exchange to set up an IPSEC tunnel

permit udp host 167.216.133.254 host 100.1.1.254 eq isakmp

if you are fastidious about speed ESP takes a little more time than AH because of payload encryption

permit esp host 167.216.133.254 host 100.1.1.254

permit ahp host 167.216.133.254 host 100.1.1.254

!

ACL order should be https, http, DNS, FTP, SMTP and lastly BGP based on required response times.

Only allow http & https from web server out and all internal users will have this web server address as there source IP address

permit tcp host 167.216.133.5 gt 1023 any eq 443

permit tcp host 167.216.133.5 gt 1023 any eq www

!

Only allow DNS requests from the DNS servers

permit udp host 167.216.133.3 any eq domain

!

Ftp and smtp only from their respective bastion hosts

All internal users will use these boxes as their source IP address

```
permit tcp host 167.216.133.8 gt 1023 any eq ftp
```

```
permit tcp host 167.216.133.4 gt 1023 any eq smtp
```

!

Add an explicit deny any statement and log it as we want to see any unauthorised outgoing attempts

```
deny ip any any log
```

!

ACL for incoming traffic from the Internet to the Inside

*****When using CBAC, permit in what you want to be inspected******

This makes is easy to follow our Security Policy of explicitly permitting only recognised traffic and denying everything else.

!

```
ip access-list extended public_to_private
```

Allow IPSEC out to the Partner1, duplicate entries required for each partner, customer or supplier

CBAC does not recognise IPSEC so it must explicitly be permitted

Allow ISAKMP first because it is the first process of the key exchange to set up an IPSEC tunnel

```
permit udp host 100.1.1.254 host 167.216.133.254 eq isakmp
```

If you are fastidious about speed ESP takes a little more time than AH

```
permit esp host 100.1.1.254 host 167.216.133.254
```

```
permit ahp host 100.1.1.254 host 167.216.133.254
```

!

ACL order should be https, http, DNS, FTP, SMTP and lastly BGP based on required response times

Allow Internet hosts to connect to out web servers (http & https)

Https should be first as it is more requires more processing

I did not specify source ports any gt 1023 because CBAC creates individual dynamic entries.

```
permit tcp any host 167.216.133.5 eq 443
```

```
permit tcp any host 167.216.133.5 eq www
```

```
permit udp any host 167.216.133.3 eq domain
```

```
permit tcp any host 167.216.133.8 eq ftp
```

```
permit tcp any host 167.216.133.4 eq smtp
```

!

Allow BGP outgoing updates to occur

```
permit tcp host 150.1.1.2 gt 1023 host 150.1.1.1 eq bgp
```

!

Explicit deny but this time we won't log as the log entries would be too big

```
deny ip any any
```

!

ACL for to deny access into auxiliary port

```
access-list 2 deny any
```

!

This ACL used to define what traffic the IOS IDS will audit

Currently this is all traffic but I used an ACL instead of using a default command line so this can be modified as needed.

```
access-list 99 permit any
```

!

Stop BGP routing table from entering the router as our current infrastructure doesn't require it.

I would also ask our ISPs to stop BGP as we would be charged for traffic leaving their network.

Also this creates a backup scenario if either the ISP or GIAC misconfigures its router.

```
access-list 121 deny tcp any any eq bgp
```

```
access-list 121 permit ip any any
```

!
Stop cdp from advertising router information
no cdp run
!
Route map entry to deny BGP into our network
route-map no_bgp_in deny 10
match ip address 121
!
Customary legal stuff as recommended by AUSCERT
Now we can prosecute and sue people if people think it is OK to hack our site because they think we are a faceless corporate entity.
!
banner motd ^C

Warning: It Is A Criminal offence To:

- i. Obtain access to this network without authority
(Peneltay 2 years imprisonment)
- ii. Damage, delete, alter or insert data on this network without authority
(Penalty 10 years imprisonment)

^C

!

line con 0

timeout of 5 minutes to stop unattended login sessions

exec-timeout 5 0

customary password that is easily cracked if view and copied

password 7 045802150C2E

don't allow any out going communications that originate from the console port

transport output none

!

line aux 0

deny all incoming traffic

access-class 2 in

don't allow any out going communications that originate from the auxiliary port

transport output none

We will have multiple lines of defence to attempted access to the router

line vty 0 4

deny all incoming traffic

access-class 2 in

make the timeout 1 second for another layer of defence

exec-timeout 0 1

no login

don't allow any out going communications that originate from the vty ports

even if we disallow all incoming traffic, add another layer of defence to slow invaders

transport input none

transport output none

!

Allow only secure ntp communication with our Time Server

ntp authentication-key <removed> md5 <removed> 7

ntp authenticate

ntp trusted-key <removed>

ntp clock-period 17180129

ntp server 172.16.254.164 key <removed> prefer

ntp server 172.16.254.164 key <removed>

!
To guarantee CPU time for processes.
scheduler allocate 30000 2000
end

When the CBAC session initiates a correct and valid entry is created in its state table for the connection and dynamic entries are created at the top of the current access lists.

giacnet01#show ip inspect sessions details
Established Sessions

An site is accessing the GIAC Web Server

Session 80DC2398 (147.132.22.87:3976)=>(167.216.133.5:80) http SIS_OPEN
Created 00:00:20, Last heard 00:00:19

A new line is created at the top of the the private_to_public ACL

Bytes sent (initiator:responder) [872:240] acl created 1
Inbound access-list private_to_public applied to interface Ethernet0/0

A new session ID is created each time a different IP Address/Port PAIR initiated ie note the different source ports of 3973 and 3976

Session 80DA1B98 (147.132.22.87:3973)=>(167.216.133.5:80) http SIS_OPEN
Created 00:00:21, Last heard 00:00:19
Bytes sent (initiator:responder) [776:3040] acl created 1
Inbound access-list private_to_public applied to interface Ethernet0/0

The next entry shows the reverse of the above entries. An internal host, in this case I used the External Web Server, is accessing a web page on the Internet. There is no correlation between this entry and the two above. I only used the the same IP addresses for convinience.

Session 80CF06F8 (167.216.133.5:1692)=>(147.132.22.87:80) http SIS_OPEN
Created 00:00:02, Last heard 00:00:02
Bytes sent (initiator:responder) [394:120] acl created 1

The dynamic entries created are now at the beginning of the public_to_private ACL.

Inbound access-list public_to_private applied to interface Serial0/0

Remember that the reason these dynamic ACLs are created is that in this situation, CBAC inspects traffic coming into both interfaces.

I suggest that if you intend to use CBAC read the web pages at:
<http://www.cisco.com/warp/public/707/index.shtml#IOS> (8/7/01)

VPN Router(s)

I have included in this configuration the option of using certificates in case the number of Partners, Suppliers and Customers grew too large to manage with encrypted-nonces. In my tests I didn't use certificates because I was only using a small subset of actual corporate bodies. Split horizon is on by default.

!
stop information being gained from the router
no ip finger

!
encrypt visible passwords on the router with the Vigenere cipher. NB this cipher is easily broken.

This is mainly so people looking over your shoulder don't see the password when you display configs

service password-encryption

!
hostname giacvpn01

!
log to router buffer at debugging (maximum) level. I have seen that Cisco recommends higher memory usage for debugging but this is not necessary in this case because we are logging events to a syslog server. This entry is usually only for interactive debugs as the log can be filled very quickly.

logging buffered 8192 debugging

!
use the inside interface as the source of logging to the syslog servers.
logging source-interface Ethernet0/1

!
the two log servers addresses that will receive all logging information

logging 172.16.254.2

logging 172.16.254.132

!
Highest debugging level is set initially

logging trap debugging

!
hashed MD5 secret password of the router

enable secret 5 <removed>

!
add a timezone to make the logs easier to read and match against other hardware

clock timezone AEST 10

ip subnet-zero

!
Stop IP packets that carry a source route option.

Without this option the sender of an IP datagram can control the route that the datagram will take. Reply packet can also be influenced with source route

no ip source-route

!
cef is enabled so the router can check the source address of packets against the interface they entered. This only works for symmetric routing so meshed networks should not have this command

ip cef

!

We are not using domain names so we disable it. Also if you misspell a command, the router searches for a matching address and this gets annoying. This can be disabled even though CA configuration is put on the router using domain-names and ip hosts.

```
no ip domain-lookup
```

```
!
```

disable services that are not used

```
no ip bootp server
```

```
!
```

the certificate server needs a domain name and address to resolve to

```
ip host host.ca.com.au 150.150.150.254
```

```
!
```

CA requires domain names to be configured

```
ip domain-name giac.com.au
```

```
!
```

Enable the Cisco IOS IDS to log

```
ip audit notify log
```

```
!
```

set spamming threshold for email

```
ip audit smtp spam 100
```

```
!
```

what to do when attack signature is detected and the detect [information signatures](#) from access-list 99 and send an alarm to the syslog server

```
ip audit name vpn_lan info list 99 action alarm
```

```
!
```

will detect [attack signatures](#) from access-list 99 and then send alarm to syslog server, drop the packet and reset TCP connection

```
ip audit name vpn_lan attack list 99 action alarm drop reset
```

```
!
```

create the certificates, where to find them, what port to use and what service/protocol is supported (http)

```
crypto ca identity ca.com.au
```

```
enrollment url http://host.ca.com.au:80
```

```
!
```

We won't be using revocation lists at this stage so we can still accept certificates.

```
crl optional
```

```
crypto ca certificate chain ca.com.au
```

```
certificate ca 01
```

```
<removed>
```

```
quit
```

```
certificate 06
```

```
<removed>
```

```
quit
```

```
!
```

create a list of policies that are acceptable to both GIAC and the associated entity

I have only created on policy here using the highest security available for this router.

Additional entries will be needed for all the other partners, suppliers and customers.

A note about policies. Cisco has intentionally created a default policy that is activated when any policy is created. This policy will be matched last but unfortunately the default policy has the lowest security possible so if no match is found, then the default will be used.

```
crypto isakmp policy 15
```

```
encr 3des
```

```
authentication rsa-encr
```

group 2

!

Encrypted traffic will use criteria that both parties have agreed to.

The choices are dependant on what each entity considers secure and processor speeds at both ends.

In this design, only FTP traffic is to be encrypted with IPSEC. I would use tunnel mode as the overhead is not much more than transport mode. Also, tunnel mode would offer scalability to use private addressing between corporate entities if required. The reasons I would use ESP is to encrypt the data payload and to hide private addressing that is routed via the Internet. In this type of scenario, a tunnel would be created and the original IP Header would be encapsulated within ESP. A new IP Header containing a valid public address is used to route over the Internet. This way only the tunnel end points are know and not the actual source/destination. AH is used to authenticate the IP Header of the packet, provide integrity and non-repudiation (asymmetric keys only). I would use AH if requested and non-repudiation is required.

Both ESP and AH can be used together and frequently are because of the high processing speeds that are available today.

Various transform sets are shown below to illustrate the different combinations.

Split-Horizon is on and not an issue because I am not implementing the VPN on a router stick model.

```
crypto ipsec transform-set partner1 esp-3des esp-sha-hmac ah-sha-hmac
```

```
crypto ipsec transform-set customer1 ah-sha-hmac esp-3des
```

```
crypto ipsec transform-set supplier1 esp-des esp-sha-hmac
```

!

I have included a dynamic map option to allow VPN customers the option of creating an IPSEC tunnel

```
crypto dynamic-map customer1 10
```

```
set transform-set customer1
```

!

A public address is needed to route via the Internet. As stated, only the tunnel end points are known and the source & destination addresses of the actual data traffic are hidden.

```
crypto key pubkey-chain rsa
```

```
addressed-key 100.1.1.254 (Partner1)
```

```
address 100.1.1.254
```

```
key-string
```

```
<removed>
```

```
quit
```

!

Use the loopback as a tunnel end point. This allows multiple connections to the same interface and only one public address is used. The current architecture allows the VPN to have private addresses on the interface and no NATing needs to be used, which would complicate the network.

```
crypto map internet_secure local-address Loopback0
```

!

Check the dynamic map entry first as this would be more prone to error due to the nature of Windows

As stated in Fortune Cookie Access – Customers will have the option of a VPN client infrastructure.

```
crypto map internet_secure 5 ipsec-isakmp dynamic customer1
```

!

Create a map entry for each corporate entity

I did not use Certificates in the scenario but if the number of entities that required IPSEC grew over 10 then I would switch to CAs

```
crypto map internet_secure 10 ipsec-isakmp
```

```
set peer 100.1.1.254           public visible address of Partner1
set transform-set partner1
match address 110              define what traffic you wish to encrypt
!
```

The dynamic customer will also not use CAs at this time (we are using encrypted-nonces)

```
crypto map customer1 5 ipsec-isakmp dynamic customer1
!
```

The Internet visible address that all IPSEC clients will use as the tunnel end point

```
interface Loopback0
ip address 167.216.133.254 255.255.255.255
!
```

```
interface Ethernet0/0
description Connection to Internet Router giacint01
ip address 172.16.254.125 255.255.255.224
```

Even though this router is between the PIX and the Internet router that uses CBAC, we still want to secure it to provide another level of defence, hence the ACL in from the Internal network.

```
ip access-group to_inside in
stop the router from being used to influence traffic paths
no ip redirects
```

don't send out ICMP unreachable

```
no ip unreachable
```

Enable IOS IDS on this router

```
ip audit vpn_lan in
```

Cisco TAC recommends disabling route caching when using IPSEC.

```
no ip route-cache
no ip mroute-cache
no ip proxy-arp
```

Don't send out information about the router.

```
no cdp enable
```

Use this interface as the physical tunnel endpoint

```
crypto map internet_secure
```

```
!
interface Ethernet0/1
description Connection to PIX giacpax03
ip address 172.16.254.94 255.255.255.224
```

Defence in depth ACL to stop the Internet router from receiving anything it shouldn't

```
ip access-group to_outside in
```

We also want to audit with the IOS IDS any abnormal activity on the inside interface

```
ip audit vpn_lan in
```

We will use the same configs for both interfaces (inside and outside) as this creates a more streamlined and manageable router.

```
no ip redirects
no ip route-cache
no ip mroute-cache
no ip proxy-arp
no cdp enable
```

```
!
stop routing to superclass if destination address does not fall into more specific route.
no ip classless
!
```

default route out to Internet router

```
ip route 0.0.0.0 0.0.0.0 172.16.254.126
```

!
route the full IP class of RFC1918 and GIAC address to null 0
this prevents “route leakage” and is a backup in case the no ip classless is removed

```
ip route 10.0.0.0 255.0.0.0 Null0
ip route 192.168.0.0 255.255.0.0 Null0
ip route 172.16.0.0 255.255.224.0 Null0
ip route 167.216.133.0 255.255.255.0 Null0
```

!
Only explicit routes are permitted to the inside network for bastion hosts

```
ip route 167.216.133.3 255.255.255.255 172.16.254.93
ip route 167.216.133.4 255.255.255.255 172.16.254.93
ip route 167.216.133.5 255.255.255.255 172.16.254.93
ip route 167.216.133.8 255.255.255.255 172.16.254.93
```

!
Allow access to syslog servers

```
ip route 172.16.254.2 255.255.255.255 172.16.254.93
ip route 172.16.254.132 255.255.255.255 172.16.254.93
```

!
On the LAN between the Internet router and the VPN router we will have some devices that will need access.

External Admin Console

```
ip route 172.16.254.7 255.255.255.255 172.16.254.93
```

!
ACE/Server for TACACS+ and RADIUS

```
ip route 192.168.254.9 255.255.255.255 172.16.254.93
```

!
Internal Time Server

```
ip route 172.16.254.164 255.255.255.255 172.16.254.93
```

!
Disable unneeded services

```
no ip http server
```

!
Stop unauthorised access to the inside network from the Internet LAN that is between this router and the Internet router.

```
ip access-list extended to_inside
```

!
allow syslog to our two log servers

```
permit udp 172.16.254.96 0.0.0.31 host 172.16.254.2 eq syslog
permit udp 172.16.254.96 0.0.0.31 host 172.16.254.132 eq syslog
```

!
Time updates to occur to and from the outside LAN

```
permit udp 172.16.254.96 0.0.0.31 eq 123 host 172.16.254.164 eq 123
permit udp host 172.16.254.164 eq 123 172.16.254.96 0.0.0.31 eq 123
```

!
Allow non-Cisco devices on the outside LAN to talk to our External Admin Console via SSH

```
permit tcp 172.16.254.96 0.0.0.31 host 172.16.254.7 eq 22
```

!
IPSEC traffic is permitted only from recognised sources, again ISAKMP should be first as key negotiation comes first.

```
permit udp host 100.1.1.254 host 167.216.133.254 eq isakmp
permit esp host 100.1.1.254 host 167.216.133.254
permit ahp host 100.1.1.254 host 167.216.133.254
```

!

HTTP & HTTPS is restricted to explicit IP addresses and port, both to and from the GIAC network.

This web traffic is real time so it should be first with https before http because of the encryption

```
permit tcp any host 167.216.133.5 eq 443
permit tcp host 167.216.133.5 any eq 443
permit tcp any host 167.216.133.5 eq www
permit tcp host 167.216.133.5 any eq www
!
```

I have restricted DNS, both in and out, to port 53; I will use Bind v9.1.2, split DNS and no zone transfers

```
permit udp any host 167.216.133.3 eq 53
permit udp host 167.216.133.3 any eq 53
!
```

FTP only to a dedicated bastion host (with port restrictions)

```
permit tcp any host 167.216.133.8 eq ftp
permit tcp host 167.216.133.8 any eq ftp
!
```

SMTP only to a dedicated bastion host (with port restrictions)

```
permit tcp any host 167.216.133.4 eq smtp
permit tcp host 167.216.133.4 any eq smtp
!
```

Explicitly deny all other access and log any events. This is an important log to view as it shows what non-authorised activity is occurring within our network.

```
deny ip any any log
!
```

Stop unauthorised access leaving our network to the Internet

```
ip access-list extended to_outside
!
```

Time updates to occur to and from the outside LAN

```
permit udp 172.16.254.96 0.0.0.31 eq 123 host 172.16.254.164 eq 123
permit udp host 172.16.254.164 eq 123 172.16.254.96 0.0.0.31 eq 123
!
```

HTTP & HTTPS is restricted to explicit IP addresses and port, both to and from the GIAC network.

This web traffic is real time so it should be first with https before http because of the encryption

```
permit tcp any host 167.216.133.5 eq 443
permit tcp host 167.216.133.5 any eq 443
permit tcp any host 167.216.133.5 eq www
permit tcp host 167.216.133.5 any eq www
!
```

I have restricted DNS, both in and out, to UDP port 53 as I will use split DNS and no zone transfers

```
permit udp any host 167.216.133.3 eq 53
permit udp host 167.216.133.3 any eq 53
!
```

FTP only to a dedicated bastion host (with port restrictions)

```
permit tcp any host 167.216.133.8 eq ftp
permit tcp host 167.216.133.8 any eq ftp
!
```

SMTP only to a dedicated bastion host (with port restrictions)

```
permit tcp any host 167.216.133.4 eq smtp
permit tcp host 167.216.133.4 any eq smtp
!
```

Explicitly deny all other access and log any events. This is an important log to view as it shows what non-authorised activity is occurring within our network.

```
deny ip any any log
```

!

ACL for to deny access into auxiliary port

```
access-list 2 deny any
```

!

ACL used to define what traffic the IOS IDS will audit.

Currently this is all traffic but I used an ACL so this can be modified as needed.

```
access-list 99 permit any
```

!

I have found this a useful ACL to be placed on interfaces when trouble-shooting problems.

It will permit all traffic and display the IP addresses and associated port numbers. This is because of the gt 0 parameter. I have also included ICMP as a separate entry to help distinguish between IP and ICMP entries.

```
access-list 100 permit tcp any gt 0 any gt 0 log-input
```

```
access-list 100 permit udp any gt 0 any gt 0 log-input
```

```
access-list 100 permit icmp any any log-input
```

```
access-list 100 permit ip any any log-input
```

!

ACL defining what will be traffic will be encrypted between GIAC and other parties.

At the moment I have only encrypted FTP and router tunnel end points. This list can be expanded for the matching corporate entity (Partner1 at the moment)

```
access-list 110 permit ip host 167.216.133.254 host 100.1.1.254
```

```
access-list 110 permit ip host 167.216.133.8 host 100.1.1.8
```

!

Don't broadcast router info

```
no cdp run
```

!

Customary legal stuff as recommended by AUSCERT

!

```
banner motd ^C
```

Warning: It Is A Criminal offence To:

i. Obtain access to this network without authority

(Peneltay 2 years imprisonment)

ii. Damage, delete, alter or insert data on this network without authority

(Penalty 10 years imprisonment)

```
^C
```

!

```
line con 0
```

Timeout of 5 minutes to stop unattended login sessions

```
exec-timeout 5 0
```

Customary password that is easily cracked if view and copied

```
password 7 045802150C2E
```

Don't allow any out going communications that originate from the console port

```
transport output none
```

!

```
line aux 0
```

Deny all incoming traffic

```
access-class 2 in
```

Don't allow any out going communications that originate from the auxiliary port

transport output none

line vty 0 4

Deny all incoming traffic

access-class 2 in

Make the timeout 1 second for another layer of defence

exec-timeout 0 1

no login

Don't allow any out going communications that originate from the vty ports, even if we disallow all incoming traffic, add another layer of defence to slow invaders

transport input none

transport output none

!

Allow only secure ntp communication with our Time Server

ntp authentication-key <removed> md5 <removed> 7

ntp authenticate

ntp trusted-key <removed>

ntp clock-period 17180129

ntp server 172.16.254.164 key <removed> prefer

ntp server 172.16.254.164 key <removed>

!

To guarantee CPU time for processes.

scheduler allocate 30000 2000

end

© SANS Institute 2000 - 2005, Author retains full rights.

PIX(es)

This architecture will use five of the six interfaces:

The Outside interface will be connected out to the Internet via the VPN switch then Internet routers

```
nameif ethernet0 outside security0
```

The Inside interface will be our External Management LAN. This LAN will be allowed to access all devices on the external perimeter. Logically it will be a simpler configuration if this is classed as “Inside” because of the relationship between this LAN and all the others.

```
nameif ethernet1 inside security100
```

The Internal interface will be the link from the perimeter network to the other LANs. This is where we will host our internal servers, links to other secure networks and internal staff networks. The Internal network is the second most secure.

```
nameif ethernet2 internal security60
```

The DMZ interface houses our Internet visible bastion hosts: Web, FTP, SMTP and External DNS

```
nameif ethernet3 DMZ security40
```

The Common interface is used by all other networks for shared services such as time servers and Web filtering. The Common network will be accessed by all other LANS and it does not contain sensitive information so this LAN is rated the second least secure on the PIX.

```
nameif ethernet4 common security20
```

Test network

```
nameif ethernet5 test security1
```

!

Secure local access to the PIX

```
enable password 2KFQnbNIdI.2KYOU encrypted
```

```
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
hostname giacpix01
```

!

The protocols that we will be scrutinising at application level

```
fixup protocol ftp 21
```

```
fixup protocol http 80
```

```
fixup protocol h323 1720
```

```
fixup protocol rsh 514
```

```
fixup protocol smtp 25
```

```
fixup protocol sqlnet 1521
```

```
fixup protocol sip 5060
```

```
fixup protocol skinny 2000
```

```
names
```

!

Only allow explicit bastion hosts out from the DMZ. Web Traffic, DNS, FTP and SMTP in that order because of the response times needed.

The fixup protocols will handle http, smtp and ftp

```
access-list dmz_in permit tcp host 172.16.254.35 gt 1023 any eq 443
```

```
access-list dmz_in permit tcp host 172.16.254.35 gt 1023 any eq www
```

```
access-list dmz_in permit udp host 172.16.254.33 any eq domain
```

```
access-list dmz_in permit tcp host 172.16.254.38 gt 1023 any eq ftp
```

```
access-list dmz_in permit tcp host 172.16.254.34 gt 1023 any eq smtp
```

```
access-list dmz_in permit tcp 172.16.254.32 gt 1023 host 172.16.254.140 eq 443
```

I will only let one box on the DMZ get NTP traffic and the rest of the bastion hosts can time sync of this local box. This stops larger holes than is necessary and reduces traffic on the PIX

access-list dmz_in permit udp host 172.16.254.36 eq ntp host 172.16.254.164 eq ntp
access-list dmz_in permit udp host 172.16.254.164 eq ntp host 172.16.254.36 eq ntp

External Admin Console access to all bastion hosts via SSH

access-list dmz_in permit tcp 172.16.254.0 255.255.255.0 eq 22 host 172.16.254.7 gt 1023

Allow bastion hosts access to syslog servers

access-list dmz_in permit udp 172.16.254.32 255.255.255.224 host 172.16.254.2 eq syslog
access-list dmz_in permit udp 172.16.254.32 255.255.255.224 host 172.16.254.132 eq syslog
!

Allow remote management to/from the External Admin Console to Internal Admin Console. This is a time saver so you don't have jump from box to box when administering/debugging multiple hosts.

access-list internal_in permit tcp host 172.16.254.137 gt 1023 host 172.16.254.7 eq 22

Permit the Internal Servers access to the External DMZ servers

access-list internal_in permit tcp host 172.16.254.135 host 172.16.254.35 eq 443
access-list internal_in permit tcp host 172.16.254.140 host 172.16.254.35 eq 443
access-list internal_in permit tcp host 172.16.254.135 host 172.16.254.35 eq www
access-list internal_in permit udp host 172.16.254.133 host 172.16.254.33 eq domain
access-list internal_in permit tcp host 172.16.254.138 host 172.16.254.38 eq ftp
access-list internal_in permit tcp host 172.16.254.134 host 172.16.254.34 eq smtp

Allow TACACS+ to the perimeter network

access-list internal_in permit tcp host 192.168.254.9 172.16.254.0 255.255.255.0 eq tacacs

Allow time sync with the a single device on the Internal LAN. This single device will then provide time to the local LAN

access-list internal_in permit udp host 172.16.254.164 eq ntp host 172.16.254.136 eq ntp
access-list internal_in permit udp host 172.16.254.136 eq ntp host 172.16.254.164 eq ntp

Syslog to other log server on External Management LAN for backup and redundancy

access-list internal_in permit udp 172.16.254.128 255.255.255.224 host 172.16.254.2 eq syslog

Explicit deny statement

access-list internal_in deny ip any any
!

Allow SSH to bastion hosts on perimeter network

access-list inside_in permit tcp host 172.16.254.7 gt 1023 172.16.254.0 255.255.255.0 eq 22

Syslog to other log server on Internal Server LAN for backup and redundancy

access-list inside_in permit udp 172.16.254.0 255.255.255.224 host 172.16.254.132 eq syslog

Explicit deny statement

access-list inside_in deny ip any any
!

Allow access into the perimeter network from the Internet (usual order of https, http, dns, ftp, and smtp)

access-list outside_in permit tcp any gt 1023 host 167.216.133.5 eq 443
access-list outside_in permit tcp any gt 1023 host 167.216.133.5 eq www
access-list outside_in permit udp any host 167.216.133.3 eq domain
access-list outside_in permit tcp any gt 1023 host 167.216.133.8 eq ftp
access-list outside_in permit tcp any gt 1023 host 167.216.133.4 eq smtp

TACACS+ access for hosts (if required) from the two outside perimeter LANs

access-list outside_in permit tcp 172.16.254.96 255.255.255.224 gt 1023 host 192.168.254.9 eq tacacs
access-list outside_in permit tcp 172.16.254.64 255.255.255.224 gt 1023 host 192.168.254.9 eq tacacs

SSH from the External Admin Console from the two outside perimeter LANs

access-list outside_in permit tcp 172.16.254.96 255.255.255.224 eq 22 host 172.16.254.7 gt 1023
access-list outside_in permit tcp 172.16.254.64 255.255.255.224 eq 22 host 172.16.254.7 gt 1023

Allow time sync with the a device on the Outside LANs. This single device will then provide time to the local LAN and reduce traffic on the PIX.

access-list outside_in permit udp host 172.16.254.164 eq ntp host 172.16.254.92 eq ntp

```
access-list outside_in permit udp host 172.16.254.92 eq ntp host 172.16.254.164 eq ntp
access-list outside_in permit udp host 172.16.254.164 eq ntp host 172.16.254.124 eq ntp
access-list outside_in permit udp host 172.16.254.124 eq ntp host 172.16.254.164 eq ntp
```

Allow hosts access to syslog servers

```
access-list outside_in permit udp 172.16.254.96 255.255.255.224 gt 1023 host 172.16.254.2 eq syslog
access-list outside_in permit udp 172.16.254.96 255.255.255.224 gt 1023 host 172.16.254.132 eq syslog
access-list outside_in permit udp 172.16.254.64 255.255.255.224 gt 1023 host 172.16.254.2 eq syslog
access-list outside_in permit udp 172.16.254.64 255.255.255.224 gt 1023 host 172.16.254.132 eq syslog
```

Explicit deny statement

```
access-list outside_in deny ip any any
!
```

Allow WEBSense server to interact with External Web Server

```
access-list common_in permit tcp host 172.16.254.162 host 172.16.254.35
```

TACACS+ access for bastion hosts on Common LAN

```
access-list common_in permit tcp host 192.168.254.9 gt 1023 172.16.254.160 255.255.255.224 eq tacacs
```

Allow SSH to bastion hosts on Common network

```
access-list common_in permit tcp 172.16.254.160 255.255.255.224 eq 22 host 172.16.254.7 gt 1023
```

Allow time syncing with the all devices on the other LANs

```
access-list common_in permit tcp host 172.16.254.164 eq 123 172.16.254.0 255.255.255.0 eq ntp
access-list common_in permit tcp 172.16.254.0 255.255.255.0 eq ntp host 172.16.254.164 eq ntp
```

Allow hosts access to syslog servers

```
access-list common_in permit udp 172.16.254.160 255.255.255.224 host 172.16.254.2 eq syslog
access-list common_in permit udp 172.16.254.160 255.255.255.224 host 172.16.254.132 eq syslog
```

Explicit deny statement

```
access-list common_in deny ip any any
!
```

This is used for debugging connections. Overwrite the interface with this ACL. You can then proceed to debug the PIX interface and determine if the previous ACL was responsible for the problem.

```
access-list 100 permit tcp any gt 0 any gt 0
access-list 100 permit udp any gt 0 any gt 0
access-list 100 permit icmp any any
access-list 100 permit ip any any
!
```

```
pager lines 48
```

```
!
```

Turn logging on, add time stamping to the entries and set at highest level (debug) for all events.

```
logging on
logging timestamp
logging buffered debugging
logging trap debugging
logging history debugging
```

Ensure that the syslog server has been setup to receive these logs at facility 7

```
logging facility 7
```

Syslog servers

```
logging host inside 172.16.254.2
logging host internal 172.16.254.132
```

```
!
```

Bring up the interfaces that are needed and shut down unused ones

```
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
```

```
interface ethernet3 auto
interface ethernet4 auto
interface ethernet5 auto shutdown
```

!

Assume the usual MTU size. This may need to be changed for VoIP but we'll leave it for now

```
mtu outside 1500
mtu inside 1500
mtu internal 1500
mtu DMZ 1500
mtu common 1500
mtu test 1500
```

!

Assign IP addresses to each of the used interfaces. We will assign an address to the unused test interface to prevent it from having a local address of 127.0.0.1 This address is sometimes forgotten when implementing ACL and this entry will help prevent an inadvertent breach. (ie layers of defence)

```
ip address outside 172.16.254.93 255.255.255.224
ip address inside 172.16.254.30 255.255.255.224
ip address internal 172.16.254.158 255.255.255.224
ip address DMZ 172.16.254.62 255.255.255.224
ip address common 172.16.254.190 255.255.255.224
ip address test 172.16.254.254 255.255.255.255
```

!

Enable auditing to the syslog servers

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

!

At this time I won't implement failover but in a real world scenario I would have some sort of redundancy in place.

```
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address internal 0.0.0.0
failover ip address DMZ 0.0.0.0
failover ip address common 0.0.0.0
failover ip address test 0.0.0.0
pdm history enable
```

!

Change the arp timeout from the default of 4 hours to 10 minutes to force the PIX to perform MAC resolution more often. If the PIX experiences performance degradation, increase arp timeout.

```
arp timeout 600
```

!

Allow the Internet to see our viewable bastion hosts after the address has been NATed from our private range. The order here is not that important but to keep in line with the rest of our design we will use the format of Web, DNS, FTP then SMTP.

```
static (dmz,outside) 167.216.133.5 172.16.254.35 netmask 255.255.255.255 0 0
static (dmz,outside) 167.216.133.3 172.16.254.33 netmask 255.255.255.255 0 0
static (dmz,outside) 167.216.133.8 172.16.254.38 netmask 255.255.255.255 0 0
static (dmz,outside) 167.216.133.4 172.16.254.34 netmask 255.255.255.255 0 0
```

We don't wish to NAT any of our private range within our network.

```
static (inside,dmz) 172.16.254.0 172.16.254.0 netmask 255.255.255.224 0 0
static (inside,internal) 172.16.254.0 172.16.254.0 netmask 255.255.255.224 0 0
static (inside,common) 172.16.254.0 172.16.254.0 netmask 255.255.255.224 0 0
static (internal,dmz) 172.16.254.128 172.16.254.128 netmask 255.255.255.224 0 0
static (internal,common) 172.16.254.128 172.16.254.128 netmask 255.255.255.224 0 0
static (dmz,common) 172.16.254.32 172.16.254.32 netmask 255.255.255.224 0 0
```

We need to allow some access from devices that are on the outside PIX interface but within our provate address range. Literally, this creates a translation from 172.16.254.x to 172.16.254.x
Sylsog server access

```
static (internal,outside) 172.16.254.132 172.16.254.132 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.254.2 172.16.254.2 netmask 255.255.255.255 0 0
```

External Admin Console from some devices.

```
static (inside,outside) 172.16.254.7 172.16.254.7 netmask 255.255.255.255 0 0
```

ACE/Server for TACACS+ and RADIUS

```
static (inside,internal) 192.168.254.9 192.168.254.9 netmask 255.255.255.255 0 0
static (inside,outside) 192.168.254.9 192.168.254.9 netmask 255.255.255.255 0 0
```

!

Apply the ACLs to the interfaces to allow access. This will always be coming into the interface.
Without these entries you will not be able to go from higher to lower security levels

```
access-group outside_in in interface outside
access-group inside_in in interface inside
access-group internal_in in interface internal
access-group dmz_in in interface dmz
access-group common_in in interface common
```

Allow ICMP through the PIX for all private perimeter addresses

I don't feel that this is a large security hole because of the other defence layers supplied by the VPN and Internet routers.

```
conduit permit icmp 172.16.254.0 255.255.255.0 any
```

!

Route default traffic to the Internet via the VPN router

```
route outside 0.0.0.0 0.0.0.0 172.16.254.94 1
```

Route the Internal addresses to the GIAC Internal Router

```
route internal 10.128.128.0 255.255.255.0 172.16.254.156 1
```

Route to the Internal Checkpoint Firewall for Protected and Secure traffic.

```
route internal 192.168.254.0 255.255.255.0 172.16.254.157 1
route internal 172.16.252.0 255.255.255.192 172.16.254.157 1
```

!

I will leave the default values for the fixup protocols, NAT translation timeouts and session timeouts as they are. This will only need adjusting when problems arise or policy changes

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
```

I have not chosen to use TACACS+ or RADIUS on any Cisco product at this time because all access will be a console connection. The Terminal Server that used for the console connection will have TACACS+ configured on it and will only be accessible from the External Admin Console.

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
```

!

I will use a WEBSense filter for any http traffic

```
url-server (common) host 172.16.254.162 timeout 5 protocol TCP version 1
```

Block out java and ActiveX from any visible web traffic

```
filter activex 443 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

```
filter java 443 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

!

I will not use SNMP as I have found it to be too unsecure in just about any form. SNMP and security do not mix very well! Scripts are a better option at this stage.

no snmp-server location

no snmp-server contact

snmp-server community @\$eCReT1-4-u

no snmp-server enable traps

floodguard enable

no sysopt route dn timer

!

Minimise chance of telnet into the PIX by using a very small timeout

telnet timeout 1

As stated I would prefer console access to the PIX but I have configured SSH as a standby.

If you are sufficiently paranoid, you can set up an alert/page/email to be generated when someone attempts a connection to the PIX from anything other than the console.

ssh 172.16.254.7 255.255.255.255 inside

ssh timeout 5

terminal width 132

© SANS Institute 2000 - 2005, Author retains all rights.

Assignment 3 - Audit Your Security Architecture (25 Points)

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), analyse the perimeter defence 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.

Pre-Assessment

I will follow the assignment 3 guidelines above for this audit and use the suggested approach in describing the audit.

1. Obtain a written (signed) audit document from all relevant parties and ensure that the signing officers have the required authority to implement any action that is in the audit.
2. When creating an audit document ask yourself:
 - Who – Identify every person who will be involved in the audit (you may wish group people into categories)
 - What – What tasks (exactly) will auditors be doing (contingency plans should be included in this category)
 - When – At what time and date will all events take place and how long will they last
 - Why – This is the business case that originally requested the audit.
3. A risk analysis should be completed for each physical device and each product/service that is used on that device. An audit of all direct and non-direct connections from a common point is a good idea as it will:
 - create a map of what equipment you have
 - what this equipment is used for
 - how individual equipment fits together (network diagram)
4. Validate that the Security Manual is followed in relation to quality procedures such as:
 - Network and host monitoring for abnormal activity
 - Firewall, syslog and IDS log analysis
 - Secure storage of audit trail, backup logs and other relevant data
 - Recovery procedures in place and followed
 - Incident handling procedures in place and followed
 - Forensic analysis of security incidents
 - Vulnerability assessment of all listed physical and service components
 - Periodic review network architecture assessment and design

Plan the Assessment

Technical Approach

Idea of the penetration test will be to simulate generic hacking attempts from different sources to differing target using varying methods; then create a plan to plug any unknown holes that are found in breach of the implemented security policy. Known security holes that are part of current normal business practice should be noted and given to relevant management staff to review.

A risk analysis of your network alleviates the problem of defining how intensive your penetration tests should be for each device/service. A device/service may have a high risk of attack but might not be considered an important business function or the business might view loss/downtime as not critical, so would therefore receive a low rating risk rating. Some businesses might rate an email server as one such example.

Schedule and Risks

The level of testing and what you wish to test will depend on what you are trying to accomplish. Denial of Service attack test will not go down well during peak processing times so you may wish to try these test at offpeak times. DoS attacks serve a purpose of seeing how equipment/services handle high loads and what failover/redundancies are in place. Example, if the ftp server fails at 80% processing, then you should throttle back to that server when 75% thresholds are reached. It's a good idea to benchmark all of your equipment so you get an understanding of network limits.

During business times I would recommend passive scanning, only after these passive scans have been tested during non-peak times. It is not a wonderful experience telling management and clients that your passive scans "should not have" crashed the equipment but they did anyway. Contingency plans are important here as you want to show management that you have done all you can to create a stable environment but some risks must be accepted if scans are taking place during peak times. I would recommend scanning during peak times because some holes are opened up during backups and file downloads that are not evident at off peak times.

The important points to remember are that you want to test as much as possible during off peak times and have contingency plans that management are aware of and have a signed agreement. This would also constitute making relevant network administrators aware of what you are doing. This will allow them to plan their work around the tests and will not make you liable for clashes in critical work. Also these network administrators would then be able to be on standby for "unexpected" events that seem to pop up now and again at the most inopportune times. (such as when everybody is at lunch and the whole system has gone down because of your penetration tests and you are fielding calls from 10 different departments and having people standing over your shoulder asking you every 2 minutes how long to bring the system back)

You should also be aware of possible intrusions that can be carried on the back of on your own intrusion tests. Although the risks are small that this is occurring during such a short window of opportunity, it should be looked for as the logging information might be overlooked. For this reason a planned and structured approach for each individual device. Having a dedicated resource (1 person) to monitor the logs and the target host is a good idea.

I will assume that the people hired to perform the audit (me) is a trusted but would advise GIAC to have security and background checks done if they have not already done so. It is really good business practice to check business partners out before you enter into any deals with them.

Costs and Effort Level

The majority of tests will be at off peak times. This also includes trial-tests that must be done at off-peak hours before business time testing can occur. Relevant network administrators should be oncall or onsite during critical tests in case of network failure. These factors will drive the costs of the exercise up significantly.

I will not include the standby staff in the calculation, as this will depend on variable factors.

Audit

1 business day for setup and network familiarisation, 1 day off peak time and 1 day at business times.

1 person (A) fulltime to initiate and monitor penetration tests

1 person (B) fulltime to monitor targets and send logs to person (C)

1 person (C) fulltime to validate logs against policy

1 person (D) fulltime to coordinate and liase with non audit staff and plan the test and document as results come in.

Report

1 person to do the report over 1 business day (the majority of this work has been done during the testing)

If we work an 8 hour day then time factor would be:

Business day rate = \$150AUS/hour

Off Peak rate = 2 x business day

Audit will be

1 person = 1 business day + [off peak = (2 x business days)] + 1 business day

= 4 business days

4 business days = 32 business hours

therefore 4 staff = 128 business hours

Report will be

1 person = 1 business day

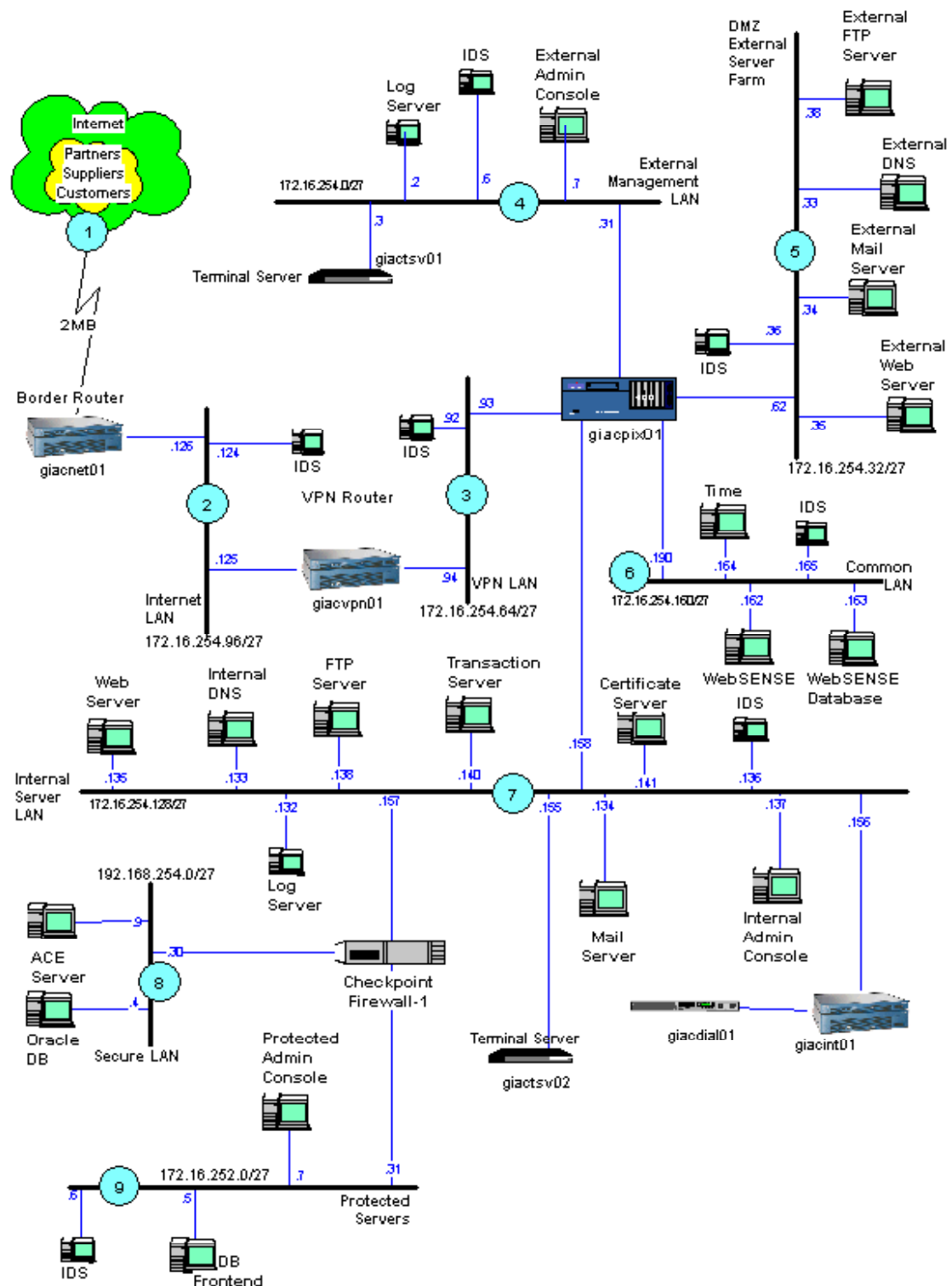
= 8 hours

Total = hours @ 150/hour

= \$20400AUS

All costs will include required equipment and software to do audit.

AUDIT - GIAC Enterprises



Audit Implementation

Reference to Audit Diagram

From the Audit Diagram, the light blue circle with a number in it will represent the source of scans. Any type of port scanning tool can be used (eg <http://www.insecure.org/nmap/> is a popular choice) Audit Points in the diagram determine the source of the scans.

Due to the volume of scans required and resources that I have available (including time) I have not performed and documented all the necessary scanning. I will state the theory and processes required to perform the implementation of the audit, then add some salient scan data with comments.

A local scan on each of the relevant networks is done to determine active and responsive hosts. Scan all possible address on the GIAC network from the Internet. It would be a good idea to scan from each of the Partner, Supplier and Customer networks. This would not be possible in most instances so a dummy network outside the Internet should be created to imitate the different corporate entities.

The following addresses should be scanned from all Audit Points. Scanning also includes pinging and tracerouting to determine what data can be extrapolated from the network.

167.216.133.0/24	Registered GIACAddress
172.16.254.0/24	Address used on Perimeter network
172.16.252.0/24	Address used on Protected network
192.168.254.0/24	Address used on Secure network
10.128.128.0/24	Address used on GIAC Staff Internal network
150.1.1.0/30	Address used on WAN link to ISP for BGP

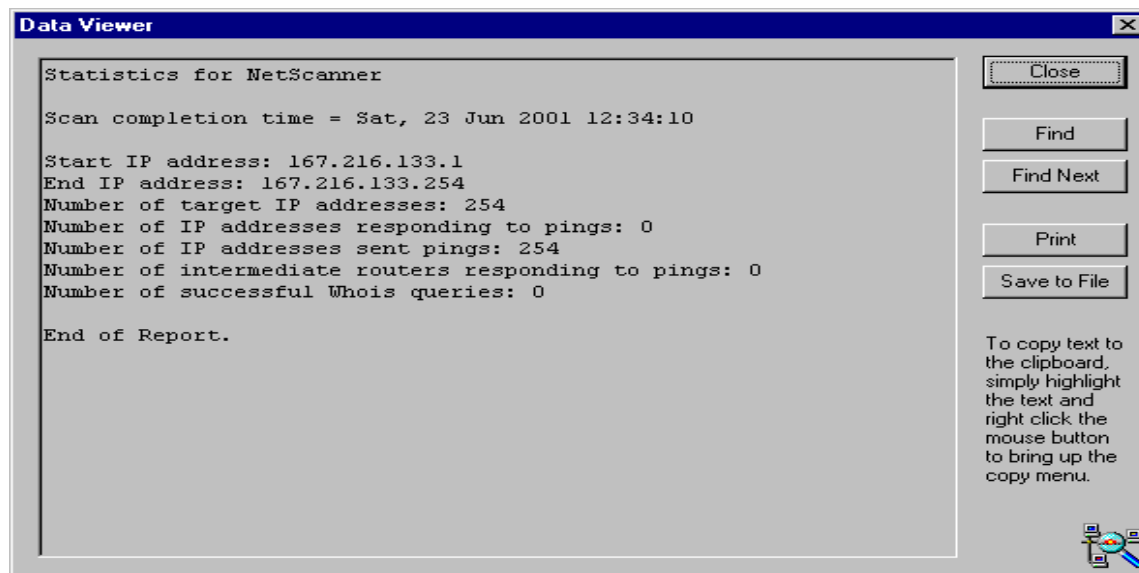
When scanning the above addresses use as the source address:

- real (non-spoofed) address
- spoofed address 167.216.213.x (both valid and non valid address)
- RFC1918 address
- Loopback address
- Tunnel end points at partner, customer and supplier sites

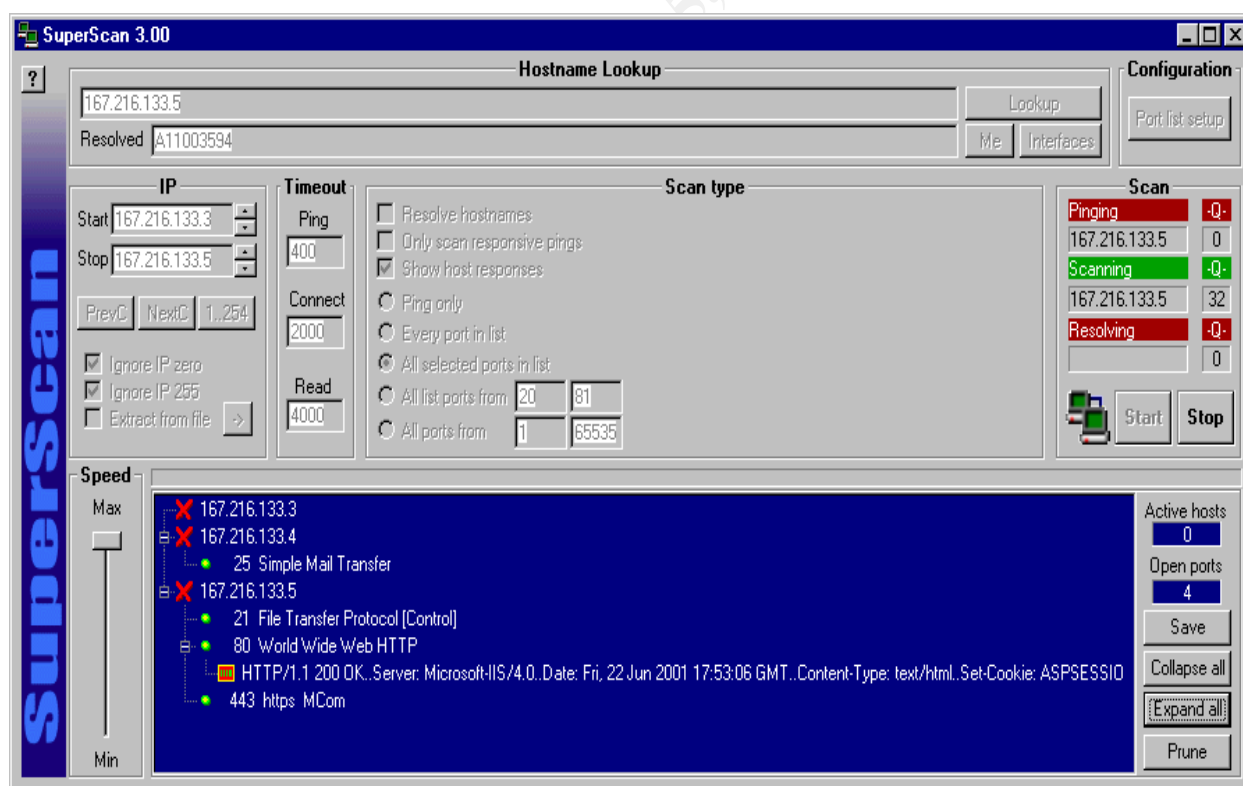
Audit 1 (Internet)

I have not allowed pings into the network so this type of scan won't display much.

More intelligent attacks will be required to enter the network. This will narrow the subset of hackers who will be able to gain access to the next stage



To continue with testing, I will assume that some valid addresses have been found on the DMZ.



Because I was running multiple services on the one box, the ftp port in this case is not on the 167.216.133.8 address but instead I made some modifications and ran ftp on the Web Server. As stated previously, in the real world model I will run a separate FTP Server.

Assuming required ports from the bastion hosts on the DMZ are open are:

167.216.133.5 (HTTPS & HTTP)

167.216.133.3 (DNS)

167.216.133.4 (SMTP)

167.216.133.8 (FTP)

We will scan each of the valid public addresses to determine what ports are open

Audit Point 1 Web Server 167.216.133.5

Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -F -P0 -vv -o nmap5a.txt 167.216.133.5

Interesting ports on a11003594 (167.216.133.5):

(The 1068 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
------	-------	---------------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

Nmap run completed at Wed Jul 11 22:07:00 2001 -- 1 IP address (1 host up) scanned in 638 seconds

Audit Point 1 DNS 167.216.133.3

Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sU -P0 -vv -o nmap3a.txt 167.216.133.3

Interesting ports on e0-0-4-black-hi.digisile.net (167.216.133.3):

(The 982 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

53/udp	open	domain
--------	------	--------

Nmap run completed at Wed Jul 11 23:00:24 2001 -- 1 IP address (1 host up) scanned in 1188 seconds

Audit Point 1 Mail Server 167.216.133.4

Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -F -P0 -vv -o nmap4.txt 167.216.133.4

Interesting ports on (167.216.133.4):

(The 1069 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
------	-------	---------------

25/tcp	open	smtp
--------	------	------

Nmap run completed at Wed Jul 11 23:16:46 2001 -- 1 IP address (1 host up) scanned in 747 seconds

Audit Point 1 FTP Server 167.216.133.8

Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -F -P0 -vv -o nmap8a.txt 167.216.133.8

Interesting ports on (167.216.133.8):

(The 1068 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
------	-------	---------------

21/tcp	open	ftp
--------	------	-----

Nmap run completed at Wed Jul 11 22:41:07 2001 -- 1 IP address (1 host up) scanned in 728 seconds

Audit Point 1 UDP scan of the Web server to show that no UDP services are running as should be the case.

D:\Security\nmapNT>nmapnt -vv -n -sU -F -P0 -o nmap87a.out 167.216.133.5

Initiating FIN,NULL, UDP, or Xmas stealth scan against (167.216.133.5)

The UDP or stealth FIN=NULL/XMAS scan took 1202 seconds to scan 983 ports.

(no udp responses received -- assuming all ports filtered)

All 983 scanned ports on (167.216.133.5) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1202 seconds

Audit Point 1 From the Internet, scan the GIAC side of the ISP WAN connection.

Interesting ports on (150.1.1.1):

(The 1069 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
------	-------	---------------

179/tcp	open	ftp
---------	------	-----

Nmap run completed at Wed Jul 11 08:20:06 2001 -- 1 IP address (1 host up) scanned in 1514 seconds

Audit 2 (Internet LAN)

This is the type of scan that should be done during business hours when active sessions are open. If session timeout values are small and off peak scanning is performed, then this is the result you would get. During business hours, ports will open up to allow differing kinds of traffic out and back in again. This is why scanning MUST be done in a controlled and scheduled manner in conjunction with monitoring and having the current rule sets present.

Audit Point 2 to the Internet Router(s) internal interface.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -F -P0 -vv -o nmap124.out 172.16.254.126
All 1062 scanned ports on (172.16.254.126) are: filtered
# Nmap run completed at Wed Jul 11 10:17:42 2001 -- 1 IP address (1 host up) scanned in 1328 seconds
```

Audit Point 2 to the DMZ

I used a spoofed real Internet address to gain access to the Web server from Audit Point 2. This worked because the VPN Router(s) do not use CBAC and will allow valid addresses to the DMZ.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap124d.out -D147.132.22.87 -p80
167.216.133.5
Interesting ports on (167.216.133.5):
Port      State      Service (RPC)
80/tcp    filtered   http
```

```
# Nmap run completed at Wed Jul 11 18:02:50 2001 -- 1 IP address (1 host up) scanned in 36 seconds
```

Audit Point 2 Same again for ftp into the DMZ from a valid address.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap124e.out -D147.132.22.87 -p21
167.216.133.8
Interesting ports on (167.216.133.8):
Port      State      Service (RPC)
21/tcp    filtered   ftp
```

```
# Nmap run completed at Wed Jul 11 18:05:14 2001 -- 1 IP address (1 host up) scanned in 36 seconds
```

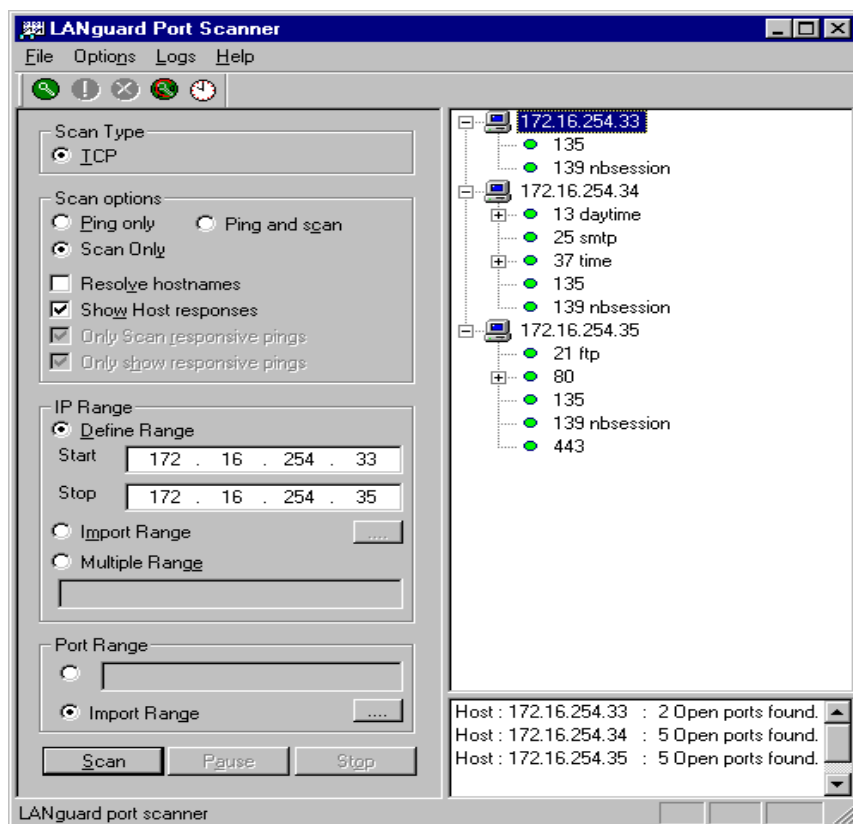
Audit 3 (VPN LAN)

Audit Point 3 The same results occur to the DMZ from this LAN so I will omit them and only add the entry for a scan towards the Internet.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -F -P0 -vv -o nmap92.out 172.16.254.94
All 1062 scanned ports on (172.16.254.94) are: filtered
# Nmap run completed at Wed Jul 11 10:29:13 2001 -- 1 IP address (1 host up) scanned in 1435 seconds
```

Audit 4 (External Management LAN)

A quick scan of the DMZ LAN shows that more than the required ports are open. I did this to verify that my scanning did not get past the PIX and detect these open ports on the box.



Test the log server to make sure it can only receive syslog messages and that it can communicate with other non-syslog hosts.

Audit Point 4 From the log server on the External Management LAN scan the private address of the Web Server.

The PIX does not allow access to the DMZ for this host.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -F -vv -o nmap2.out 172.16.254.35
All 1062 scanned ports on (172.16.254.35) are: filtered
# Nmap run completed at Wed Jul 11 09:17:16 2001 -- 1 IP address (1 host up) scanned in 20 seconds
```

Audit Point 4 From the log server on the External Management LAN scan the inside address of the VPN Router(s).

The PIX filters the scan.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -F -vv -o nmap2a.out 172.16.254.94
All 1062 scanned ports on (172.16.254.94) are: filtered
# Nmap run completed at Wed Jul 11 09:23:49 2001 -- 1 IP address (1 host up) scanned in 20 seconds
```

Audit Point 4 Currently we don't want the routers to accept SSH from any source including the External Admin Console. This is because we will prefer to use a Terminal Server to access the console port of the routers and other Cisco equipment.

Audit Point 4 VPN Router(s)

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -F -P0 -vv -o nmap7a.txt 172.16.254.94
All 1070 scanned ports on (172.16.254.94) are: filtered
# Nmap run completed at Wed Jul 11 15:38:04 2001 -- 1 IP address (1 host up) scanned in 1328 seconds
```

Audit Point 4 Internet Router(s)

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -o nmap7b.txt 172.16.254.126
All 1531 scanned ports on (172.16.254.126) are: filtered
# Nmap run completed at Wed Jul 11 15:45:58 2001 -- 1 IP address (1 host up) scanned in 1682 seconds
```

Audit Point 4 The External Admin Console should be allowed to access the Web Server and other non-Cisco bastion hosts on DMZ

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -vv -F -P0 -o nmap7d.txt 172.16.254.35
Interesting ports on (172.16.254.35):
(The 1069 ports scanned but not shown below are in state: filtered)
Port      State      Service (RPC)
22/tcp    filtered   ssh

# Nmap run completed at Wed Jul 11 15:43:39 2001 -- 1 IP address (1 host up) scanned in 26 seconds
```

Audit Point 4 The External Admin Console should not be able to reach devices on the Internal Server LAN as the hosts on this LAN should only be able to access via the Internal Admin Console.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -o nmap7c.txt 172.16.254.135
All 1531 scanned ports on (172.16.254.135) are: filtered
# Nmap run completed at Wed Jul 11 16:18:26 2001 -- 1 IP address (1 host up) scanned in 21 seconds
```

Audit Point 4 We cannot reach the public address of the Web server from the External Admin Console.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -vv -F -P0 -o nmap7f.txt 167.216.133.5
All 1070 scanned ports on a11003594 (167.216.133.5) are: filtered
# Nmap run completed at Wed Jul 11 16:12:10 2001 -- 1 IP address (1 host up) scanned in 1308 seconds
```

Audit 5 (DMZ LAN)

We will attempt to scan out to the Internet and VPN routers to see what is open from the DMZ Web server

Audit Point 5 We can see currently only web traffic is allowed through the routers because the Web server on the DMZ has a page open on an external web site

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -F -vv -o nmap35.out 172.16.254.94,126
All 1062 scanned ports on (172.16.254.94) are: closed
Interesting ports on (172.16.254.126):
(The 1060 ports scanned but not shown below are in state: closed)
Port      State      Service (RPC)
80/tcp    filtered   http
443/tcp    filtered   https

# Nmap run completed at Wed Jul 11 09:41:59 2001 -- 2 IP addresses (2 hosts up) scanned in 49 seconds
```

Audit Point 5 When the Web traffic stops and the connection is aged out the router show that all ports are now filtered.

This is another reason to have audits during business hours

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -F -vv -o nmap35a.out 172.16.254.94,126
All 1062 scanned ports on (172.16.254.94) are: filtered
All 1062 scanned ports on (172.16.254.126) are: filtered
# Nmap run completed at Wed Jul 11 10:38:37 2001 -- 2 IP addresses (2 hosts up) scanned in 2656 seconds
```

Audit Point 5 The DMZ Web server can communicate to the Internal Transaction Server only on set ports. As explained earlier, this is the central point for requesting/sending fortune cookies via SSL

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -F -o nmap35b.txt 172.16.254.135
Interesting ports on (172.16.254.140):
(The 1061 ports scanned but not shown below are in state: closed)
Port      State      Service (RPC)
443/tcp    filtered   https

# Nmap run completed at Wed Jul 11 16:24:47 2001 -- 1 IP address (1 host up) scanned in 546 seconds
```

Audit 6 (Common LAN)

**I did not run any scans from this network due time and equipment restrictions.
The process of what to scan is explained at the beginning of the Audit section**

Audit 7 (Internal LAN)

Audit Point 7 Check to make sure that the log servers are not able to send any traffic to other non syslog servers

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -F -o nmap132.out 176.16.254.2
All 1062 scanned ports on (176.16.254.2) are: filtered
# Nmap run completed at Wed Jul 11 13:53:21 2001 -- 1 IP address (1 host up) scanned in 1328 seconds
```

Audit Point 7 The Internal DNS should be allowed to forward to the External DNS if it can't resolve locally.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sU -P0 -vv -n -o nmap133c.out -p53 172.16.254.33
Interesting ports on (172.16.254.33):
Port      State      Service
53/udp    open       domain
```

```
# Nmap run completed at Wed Jul 11 21:06:46 2001 -- 1 IP address (1 host up) scanned in 12 seconds
```

Audit Point 7 Allow the Internal Mail server to direct mail to the External Mail server.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap134a.out -p25 172.16.254.34
Interesting ports on (172.16.254.34):
Port      State      Service (RPC)
25/tcp    filtered   smtp
```

```
# Nmap run completed at Wed Jul 11 20:03:01 2001 -- 1 IP address (1 host up) scanned in 36 seconds
```

Audit Point 7 The Internal Mail server can see the real address of the External Mail Server. This may be a cause for concern and should be investigated!!!

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap134c.out -p25 167.216.133.4
Interesting ports on (167.216.133.4):
Port      State      Service (RPC)
25/tcp    filtered   smtp
```

```
# Nmap run completed at Wed Jul 11 20:12:10 2001 -- 1 IP address (1 host up) scanned in 36 seconds
```

Audit Point 7 The Internal Web Server can direct traffic to the External Web server via SSL

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap135a.out -p443 172.16.254.35
Interesting ports on (172.16.254.35):
Port      State      Service (RPC)
443/tcp    filtered   https
```

```
# Nmap run completed at Wed Jul 11 20:06:03 2001 -- 1 IP address (1 host up) scanned in 36 seconds
```

Audit Point 7 The Internal Web Server can direct traffic to the External Web server via HTTP

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap135b.out -p80 172.16.254.35
Interesting ports on (172.16.254.35):
Port      State      Service (RPC)
80/tcp    filtered   http
```

```
# Nmap run completed at Wed Jul 11 20:06:48 2001 -- 1 IP address (1 host up) scanned in 36 seconds
```

Audit Point 7 The Internal Web Server can direct traffic to the External Web server via HTTP and SSL. This address is the real address of the External web server and also may be a cause for concern and should be investigated!!!

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -sR -P0 -vv -n -o nmap135c.out -p80,443 167.216.133.5
```


Interesting ports on (167.216.133.5):

Port	State	Service (RPC)
------	-------	---------------

80/tcp	filtered	http
--------	----------	------

443/tcp	filtered	https
---------	----------	-------

Nmap run completed at Wed Jul 11 20:10:26 2001 -- 1 IP address (1 host up) scanned in 36 seconds

Audit 8 & 9

**I will consider this the Internal network and will therefore not include scanning at this stage.
The process of what to scan for is explained at the beginning of the Audit section.**

© SANS Institute 2000 - 2005, Author retains full rights.

Scan Results

Lets assume that ALL the scanning is complete and the data transformed into useful information.
Within the GIAC network, this is an example of what should be allowed access

SOURCE LAN	TARGET LAN	
Ext Mgmt LAN	Target Address	
Source Address	DMZ LAN	Target Port
172.16.254.7	172.16.254.35	TCP 22
External Admin Console	172.16.254.33	TCP 22
	172.16.254.34	TCP 22
	172.16.254.38	TCP 22
	Internal LAN	Target Port
	172.16.254.132	UDP 514
	Common LAN	Target Port
	172.16.254.164	TCP 22
	172.16.254.162	TCP 22
	172.16.254.163	TCP 22
	172.16.254.165	TCP 22
	VPN LAN	Target Port
	172.16.254.92	TCP 22
	Internet LAN	Target Port
	172.16.254.124	TCP 22
	External LAN	Target Port
	172.16.254.3	TCP 22
	172.16.254.6	TCP 22
	172.16.254.2	UDP 514
	Secure LAN	Target Port
	192.168.254.9	TCP 49
172.16.254.2	Internal LAN	Target Port
Log Server	172.16.254.132	UDP 514
	Secure LAN	Target Port
	192.168.254.9	TCP 49
Common LAN	DMZ LAN	Target Port
172.16.254.164	172.16.254.36	UDP 123
Time Server	Internal LAN	Target Port
	172.16.254.136	UDP 123
	Common LAN	Target Port
	172.16.254.165	UDP 123
	VPN LAN	Target Port
	172.16.254.92	UDP 123
	Internet LAN	Target Port
	172.16.254.124	UDP 123
	External LAN	Target Port
	172.16.254.6	UDP 123
	Secure LAN	Target Port
	192.168.254.9	TCP 49
Internal LAN	DMZ LAN	Target Port
172.16.254.138	172.16.254.38	TCP 21
Internal FTP Server	Internal LAN	Target Port
	172.16.254.132	UDP 514
	External LAN	Target Port
	172.16.254.2	UDP 514
	Secure LAN	Target Port
	192.168.254.9	TCP 49
172.16.254.133	DMZ LAN	Target Port
Internal DNS Server	172.16.254.33	UDP 53
	Internal LAN	Target Port
	172.16.254.132	UDP 514

	External LAN	Target Port
	172.16.254.2	UDP 514
	Secure LAN	Target Port
	192.168.254.9	TCP 49
172.16.254.135	DMZ LAN	Target Port
Internal Web Server	172.16.254.35	TCP 80 / 443
	Internal LAN	Target Port
	172.16.254.132	UDP 514
	External LAN	Target Port
	172.16.254.2	UDP 514
	Secure LAN	Target Port
	192.168.254.9	TCP 49
172.16.254.134	DMZ LAN	Target Port
Internal Mail Server	172.16.254.34	TCP 25
	Internal LAN	Target Port
	172.16.254.132	UDP 514
	External LAN	Target Port
	172.16.254.2	UDP 514
	Secure LAN	Target Port
	192.168.254.9	TCP 49
172.16.254.140	External LAN	Target Port
Transaction Server	172.16.254.2	UDP 514
	Internal LAN	Target Port
	172.16.254.132	UDP 514
	172.16.254.135	TCP 22
	172.16.254.138	TCP 22
	Secure LAN	Target Port
	192.168.254.9	TCP 49
172.16.254.137	Internal LAN	Target Port
Internal Admin Console	172.16.254.132	TCP 22
	172.16.254.133	TCP 22
	172.16.254.134	TCP 22
	172.16.254.135	TCP 22
	172.16.254.136	TCP 22
	172.16.254.138	TCP 22
	172.16.254.140	TCP 22
	172.16.254.141	TCP 22
	Secure LAN	Target Port
	192.168.254.9	TCP 49

We have a picture of what IP address and corresponding ports that can access from all the different areas of the network. Check this table is correct and matches the security policy. I will need to check the source and destination of each type of connection to ensure that the scan is correct. Eg from the External Management Console I would have to SSH to every host in the list. The same goes for the syslog server. I need to verify that logging entries are getting to the syslog server from each of the hosts in the table.

Validation of Security Policy

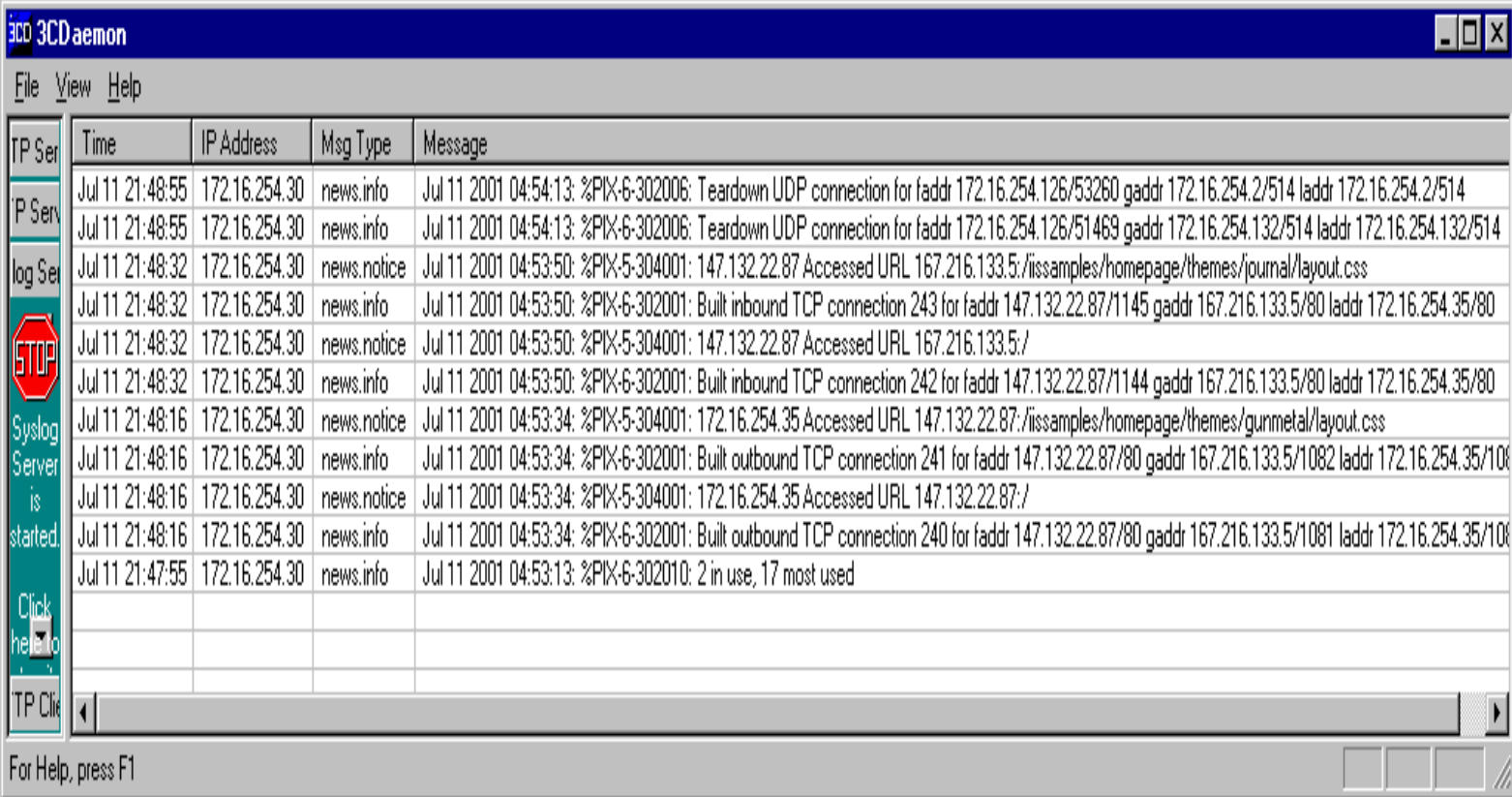
If we set up the syslog server for the Internet Router(s), VPN Router(s) and the PIX(es), we can see what these devices are doing with traffic that is attempting entry into the network.

See diagrams below for syslog information

The [Top Ten Vulnerabilities](#) (23/07/01) provides an excellent checklist so I highly recommend using it.

© SANS Institute 2000 - 2005, Author retains full rights.

In this diagram the PIX is creating a connection to the External Web server from an Internet resident device that is accessing pages. The top two entries identify the Internet router sending syslog information to the two syslog servers and once the data is sent the circuits are deleted. This is the timeout value for UDP being enforced.



Time	IP Address	Msg Type	Message
Jul 11 21:48:55	172.16.254.30	news.info	Jul 11 2001 04:54:13: %PIX-6-302006: Teardown UDP connection for faddr 172.16.254.126/53260 gaddr 172.16.254.2/514 laddr 172.16.254.2/514
Jul 11 21:48:55	172.16.254.30	news.info	Jul 11 2001 04:54:13: %PIX-6-302006: Teardown UDP connection for faddr 172.16.254.126/51469 gaddr 172.16.254.132/514 laddr 172.16.254.132/514
Jul 11 21:48:32	172.16.254.30	news.notice	Jul 11 2001 04:53:50: %PIX-5-304001: 147.132.22.87 Accessed URL 167.216.133.5:/issamples/homepage/themes/journal/layout.css
Jul 11 21:48:32	172.16.254.30	news.info	Jul 11 2001 04:53:50: %PIX-6-302001: Built inbound TCP connection 243 for faddr 147.132.22.87/1145 gaddr 167.216.133.5/80 laddr 172.16.254.35/80
Jul 11 21:48:32	172.16.254.30	news.notice	Jul 11 2001 04:53:50: %PIX-5-304001: 147.132.22.87 Accessed URL 167.216.133.5/
Jul 11 21:48:32	172.16.254.30	news.info	Jul 11 2001 04:53:50: %PIX-6-302001: Built inbound TCP connection 242 for faddr 147.132.22.87/1144 gaddr 167.216.133.5/80 laddr 172.16.254.35/80
Jul 11 21:48:16	172.16.254.30	news.notice	Jul 11 2001 04:53:34: %PIX-5-304001: 172.16.254.35 Accessed URL 147.132.22.87:/issamples/homepage/themes/gunmetal/layout.css
Jul 11 21:48:16	172.16.254.30	news.info	Jul 11 2001 04:53:34: %PIX-6-302001: Built outbound TCP connection 241 for faddr 147.132.22.87/80 gaddr 167.216.133.5/1082 laddr 172.16.254.35/1082
Jul 11 21:48:16	172.16.254.30	news.notice	Jul 11 2001 04:53:34: %PIX-5-304001: 172.16.254.35 Accessed URL 147.132.22.87:/
Jul 11 21:48:16	172.16.254.30	news.info	Jul 11 2001 04:53:34: %PIX-6-302001: Built outbound TCP connection 240 for faddr 147.132.22.87/80 gaddr 167.216.133.5/1081 laddr 172.16.254.35/1081
Jul 11 21:47:55	172.16.254.30	news.info	Jul 11 2001 04:53:13: %PIX-6-302010: 2 in use, 17 most used

In this diagram below we see log messages from the Internet and VPN routers.

Time 09:43:07: Source: VPN Router: Log Message: This group of entries is denying web access to the External Web server from any of our RFC1918 source addresses

Time 09:23:31: Source: Internet Router: Log Message: An audit trail is generated for valid Web connections

Time 08:59:10: Source: Internet Router: Log Message: This group of entries shows Internet router has detected some FIN and SYN scans from the Internet

Time 07:16:55: Source: Internet Router: Log Message: Last two entries show the Cisco IOS IDS denying an Info Signature (2004) Echo Request

TP Ser	Time	IP Address	Msg Type	Message
IP Ser	Jul 11 09:52:48	172.16.254.94	local7.no...	46: *Mar 1 12:41:47 AEST: %SYS-5-CONFIG_I: Configured from console by console
log Se	Jul 11 09:52:31	172.16.254.126	local7.no...	46: *Mar 1 12:42:17.313 AEST: %SYS-5-CONFIG_I: Configured from console by console
	Jul 11 09:51:57	172.16.254.126	local7.no...	45: *Mar 1 12:41:43.001 AEST: %SYS-5-CONFIG_I: Configured from console by console
	Jul 11 09:51:43	172.16.254.94	local7.info	45: *Mar 1 12:40:42 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied icmp 172.16.254.126 -> 172.16.254.125 (3/13), 1 packet
	Jul 11 09:51:43	172.16.254.126	local7.info	44: *Mar 1 12:41:28.637 AEST: %SEC-6-IPACCESSLOGDP: list private_to_public denied icmp 172.16.254.125 -> 172.16.254.126 (8/0), 1 packet
	Jul 11 09:51:42	172.16.254.94	local7.w...	44: *Mar 1 12:40:42 AEST: %IDS-4-ICMP_UNREACH_SIG: 2001:ICMP Host Unreachable - from 172.16.254.126 to 172.16.254.125
	Jul 11 09:51:42	172.16.254.126	local7.w...	43: *Mar 1 12:41:28.633 AEST: %IDS-4-ICMP_ECHO_SIG: Sig:2004:ICMP Echo Request - from 172.16.254.125 to 172.16.254.126
	Jul 11 09:48:50	172.16.254.94	local7.no...	43: *Mar 1 12:37:49 AEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
	Jul 11 09:46:53	172.16.254.94	local7.no...	42: *Mar 1 12:35:52 AEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
	Jul 11 09:43:07	172.16.254.94	local7.info	41: *Mar 1 12:32:06 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(11001) -> 167.216.133.5(80), 3 packets
	Jul 11 09:42:07	172.16.254.94	local7.info	40: *Mar 1 12:31:06 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(11000) -> 167.216.133.5(80), 3 packets
	Jul 11 09:40:55	172.16.254.94	local7.info	39: *Mar 1 12:29:54 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(80) -> 167.216.133.5(41068), 1 packet
	Jul 11 09:40:53	172.16.254.94	local7.info	38: *Mar 1 12:29:52 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(80) -> 167.216.133.5(41066), 1 packet
	Jul 11 09:40:52	172.16.254.94	local7.info	37: *Mar 1 12:29:51 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(80) -> 167.216.133.5(41065), 1 packet
	Jul 11 09:40:50	172.16.254.94	local7.info	36: *Mar 1 12:29:50 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(80) -> 167.216.133.5(41064), 1 packet
	Jul 11 09:40:50	172.16.254.94	local7.info	35: *Mar 1 12:29:49 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(443) -> 167.216.133.5(41065), 1 packet
	Jul 11 09:40:48	172.16.254.94	local7.info	34: *Mar 1 12:29:47 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(443) -> 167.216.133.5(41063), 1 packet
	Jul 11 09:37:30	172.16.254.94	local7.info	33: *Mar 1 12:26:29 AEST: %SEC-6-IPACCESSLOGDP: list to_inside denied tcp 172.16.254.126(11001) -> 167.216.133.5(80), 1 packet
	Jul 11 09:37:27	172.16.254.94	local7.no...	32: *Mar 1 12:26:25 AEST: %SYS-5-CONFIG_I: Configured from console by console
	Jul 11 09:36:32	172.16.254.126	local7.no...	40: *Mar 1 12:26:17.656 AEST: %SYS-5-CONFIG_I: Configured from console by console
	Jul 11 09:36:13	172.16.254.126	local7.no...	39: *Mar 1 12:25:58.713 AEST: %SYS-5-CONFIG_I: Configured from console by console
	Jul 11 09:23:31	172.16.254.126	local7.info	38: *Mar 1 12:13:16.483 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (167.216.133.5:1120) sent 791 bytes -- responder (147.132.22.87:80)
	Jul 11 09:23:31	172.16.254.126	local7.info	37: *Mar 1 12:13:16.483 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (167.216.133.5:1119) sent 613 bytes -- responder (147.132.22.87:80)
	Jul 11 09:23:27	172.16.254.126	local7.info	36: *Mar 1 12:13:12.950 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (147.132.22.87:3014) sent 1851 bytes -- responder (167.216.133.5:80)
	Jul 11 08:59:10	172.16.254.126	local7.w...	35: *Mar 1 11:48:55.464 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 172.16.254.125
	Jul 11 08:58:39	172.16.254.126	local7.w...	34: *Mar 1 11:48:25.419 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 172.16.254.125
	Jul 11 08:58:07	172.16.254.126	local7.w...	33: *Mar 1 11:47:53.343 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 172.16.254.125
	Jul 11 08:57:37	172.16.254.126	local7.w...	32: *Mar 1 11:47:23.305 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 172.16.254.125
	Jul 11 08:57:05	172.16.254.126	local7.w...	31: *Mar 1 11:46:51.241 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 172.16.254.125
	Jul 11 08:56:35	172.16.254.126	local7.w...	30: *Mar 1 11:46:21.220 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 172.16.254.125
	Jul 11 08:51:23	172.16.254.126	local7.w...	29: *Mar 1 11:41:08.487 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 167.216.133.5
	Jul 11 08:51:23	172.16.254.126	local7.w...	28: *Mar 1 11:41:08.483 AEST: %IDS-4-TCP_SYN_FIN_SIG: Sig:3041:TCP - SYN and FIN bits set - from 147.132.22.87 to 167.216.133.5
	Jul 11 08:51:23	172.16.254.126	local7.w...	27: *Mar 1 11:41:08.483 AEST: %IDS-4-TCP_NO_FLAGS_SIG: Sig:3040:TCP - No bits set in flags - from 147.132.22.87 to 167.216.133.5
	Jul 11 08:15:17	172.16.254.126	local7.w...	26: *Mar 1 11:05:03.306 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 150.1.1.1
	Jul 11 08:14:47	172.16.254.126	local7.w...	25: *Mar 1 11:04:33.268 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 150.1.1.1
	Jul 11 08:14:15	172.16.254.126	local7.w...	24: *Mar 1 11:04:01.204 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 150.1.1.1
	Jul 11 08:13:45	172.16.254.126	local7.w...	23: *Mar 1 11:03:31.167 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 150.1.1.1
	Jul 11 08:13:13	172.16.254.126	local7.w...	22: *Mar 1 11:02:59.094 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 150.1.1.1
	Jul 11 08:12:43	172.16.254.126	local7.w...	21: *Mar 1 11:02:29.053 AEST: %IDS-4-TCP_FIN_ONLY_SIG: Sig:3042:TCP - FIN bit with no ACK bit in flags - from 147.132.22.87 to 150.1.1.1
	Jul 11 07:25:29	172.16.254.126	local7.info	20: *Mar 1 10:15:14.831 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (147.132.22.87:2982) sent 399 bytes -- responder (167.216.133.5:80)
	Jul 11 07:25:29	172.16.254.126	local7.info	19: *Mar 1 10:15:14.831 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (147.132.22.87:2983) sent 405 bytes -- responder (167.216.133.5:80)
	Jul 11 07:25:16	172.16.254.126	local7.info	18: *Mar 1 10:15:01.709 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (167.216.133.5:1113) sent 771 bytes -- responder (147.132.22.87:80)
	Jul 11 07:25:16	172.16.254.126	local7.info	17: *Mar 1 10:15:01.705 AEST: %FW-6-SESS_AUDIT_TRAIL: http session initiator (167.216.133.5:1112) sent 633 bytes -- responder (147.132.22.87:80)
	Jul 11 07:17:17	172.16.254.126	local7.info	16: *Mar 1 10:07:02.307 AEST: %SEC-6-IPACCESSLOGDP: list private_to_public denied udp 172.16.254.125(68) -> 255.255.255.255(67), 3 packets
	Jul 11 07:16:55	172.16.254.126	local7.w...	15: *Mar 1 10:06:40.323 AEST: %IDS-4-ICMP_ECHO_SIG: Sig:2004:ICMP Echo Request - from 147.132.22.87 to 167.216.133.5
	Jul 11 07:16:19	172.16.254.126	local7.w...	14: *Mar 1 10:06:04.577 AEST: %IDS-4-ICMP_ECHO_SIG: Sig:2004:ICMP Echo Request - from 147.132.22.87 to 167.216.133.5

In this diagram below we see a log messages from the VPN router that is denying a scan of our Internal syslog server.
The syslog server should only be accepting SSH from 172.16.254.7 and UDP514 for 172.16.254.0

Time	IP Address	Msg Type	Message
Jul 11 14:26:18	172.16.254.94	local7.info	354: *Mar 1 17:15:17 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(191), 1 packet
Jul 11 14:26:12	172.16.254.94	local7.info	353: *Mar 1 17:15:11 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(1521), 1 packet
Jul 11 14:26:06	172.16.254.94	local7.info	352: *Mar 1 17:15:05 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(110), 1 packet
Jul 11 14:26:00	172.16.254.94	local7.info	351: *Mar 1 17:14:59 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(218), 1 packet
Jul 11 14:25:54	172.16.254.94	local7.info	350: *Mar 1 17:14:53 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(281), 1 packet
Jul 11 14:25:48	172.16.254.94	local7.info	349: *Mar 1 17:14:47 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(610), 1 packet
Jul 11 14:25:42	172.16.254.94	local7.info	348: *Mar 1 17:14:41 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(1), 1 packet
Jul 11 14:25:36	172.16.254.94	local7.info	347: *Mar 1 17:14:35 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(505), 1 packet
Jul 11 14:25:30	172.16.254.94	local7.info	346: *Mar 1 17:14:29 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(1367), 1 packet
Jul 11 14:25:24	172.16.254.94	local7.info	345: *Mar 1 17:14:23 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(564), 1 packet
Jul 11 14:25:18	172.16.254.94	local7.info	344: *Mar 1 17:14:17 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(462), 1 packet
Jul 11 14:25:12	172.16.254.94	local7.info	343: *Mar 1 17:14:11 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(6666), 1 packet
Jul 11 14:25:06	172.16.254.94	local7.info	342: *Mar 1 17:14:05 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(65), 1 packet
Jul 11 14:25:00	172.16.254.94	local7.info	341: *Mar 1 17:13:59 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(7010), 1 packet
Jul 11 14:24:54	172.16.254.94	local7.info	340: *Mar 1 17:13:53 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(418), 1 packet
Jul 11 14:24:48	172.16.254.94	local7.info	339: *Mar 1 17:13:47 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(317), 1 packet
Jul 11 14:24:42	172.16.254.94	local7.info	338: *Mar 1 17:13:41 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(178), 1 packet
Jul 11 14:24:36	172.16.254.94	local7.info	337: *Mar 1 17:13:35 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(200), 1 packet
Jul 11 14:24:30	172.16.254.94	local7.info	336: *Mar 1 17:13:29 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(417), 1 packet
Jul 11 14:24:24	172.16.254.94	local7.info	335: *Mar 1 17:13:23 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(356), 1 packet
Jul 11 14:24:18	172.16.254.94	local7.info	334: *Mar 1 17:13:17 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(425), 1 packet
Jul 11 14:24:12	172.16.254.94	local7.info	333: *Mar 1 17:13:11 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(5631), 1 packet
Jul 11 14:24:06	172.16.254.94	local7.info	332: *Mar 1 17:13:05 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(5302), 1 packet
Jul 11 14:24:00	172.16.254.94	local7.info	331: *Mar 1 17:12:59 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(5302), 1 packet
Jul 11 14:23:54	172.16.254.94	local7.info	330: *Mar 1 17:12:53 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(7201), 1 packet
Jul 11 14:23:48	172.16.254.94	local7.info	329: *Mar 1 17:12:47 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(7201), 1 packet
Jul 11 14:23:42	172.16.254.94	local7.info	328: *Mar 1 17:12:41 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(42000) -> 172.16.254.132(189), 1 packet
Jul 11 14:23:36	172.16.254.94	local7.info	327: *Mar 1 17:12:35 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(189), 1 packet
Jul 11 14:23:30	172.16.254.94	local7.info	326: *Mar 1 17:12:29 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(189), 1 packet
Jul 11 14:23:24	172.16.254.94	local7.info	325: *Mar 1 17:12:23 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(42000) -> 172.16.254.132(783), 1 packet
Jul 11 14:23:18	172.16.254.94	local7.info	324: *Mar 1 17:12:17 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(783), 1 packet
Jul 11 14:23:12	172.16.254.94	local7.info	323: *Mar 1 17:12:11 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(783), 1 packet
Jul 11 14:23:06	172.16.254.94	local7.info	322: *Mar 1 17:12:05 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(42000) -> 172.16.254.132(1353), 1 packet
Jul 11 14:23:00	172.16.254.94	local7.info	321: *Mar 1 17:11:59 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(1353), 1 packet
Jul 11 14:22:54	172.16.254.94	local7.info	320: *Mar 1 17:11:53 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(1353), 1 packet
Jul 11 14:22:48	172.16.254.94	local7.info	319: *Mar 1 17:11:47 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(42000) -> 172.16.254.132(771), 1 packet
Jul 11 14:22:42	172.16.254.94	local7.info	318: *Mar 1 17:11:41 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(771), 1 packet
Jul 11 14:22:36	172.16.254.94	local7.info	317: *Mar 1 17:11:35 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(771), 1 packet
Jul 11 14:22:30	172.16.254.94	local7.info	316: *Mar 1 17:11:29 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(42000) -> 172.16.254.132(477), 1 packet
Jul 11 14:22:24	172.16.254.94	local7.info	315: *Mar 1 17:11:23 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(477), 1 packet
Jul 11 14:22:18	172.16.254.94	local7.info	314: *Mar 1 17:11:17 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(477), 1 packet
Jul 11 14:22:12	172.16.254.94	local7.info	313: *Mar 1 17:11:11 AEST: %SEC-6IPACCESSLOGDP: list to inside denied icmp 172.16.254.124 -> 167.216.133.5 (8/0), 3 packets
Jul 11 14:22:12	172.16.254.94	local7.info	312: *Mar 1 17:11:11 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(42000) -> 172.16.254.132(210), 1 packet
Jul 11 14:22:06	172.16.254.94	local7.info	311: *Mar 1 17:11:05 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41999) -> 172.16.254.132(210), 1 packet
Jul 11 14:22:00	172.16.254.94	local7.info	310: *Mar 1 17:11:00 AEST: %SEC-6IPACCESSLOGP: list to inside denied tcp 172.16.254.124(41998) -> 172.16.254.132(210), 1 packet
Jul 11 14:22:00	172.16.254.94	local7.info	309: *Mar 1 17:11:00 AEST: %SEC-6IPACCESSLOGDP: list to inside denied icmp 172.16.254.124 -> 167.216.133.5 (8/0), 1 packet

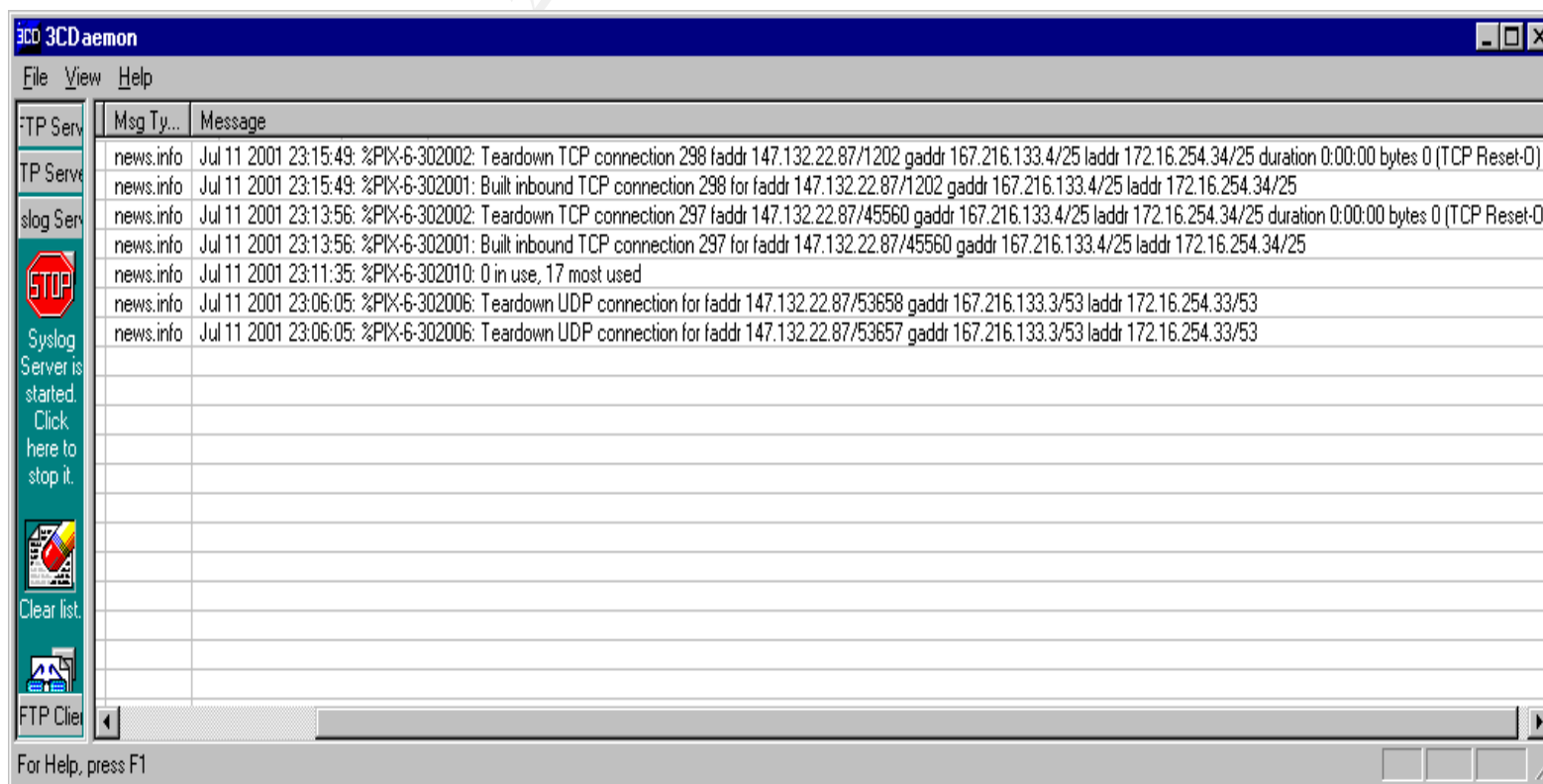
The PIX is creating a valid connection to our SMTP Server from a valid Internet address.

What is of note here is that we can see the times are very close so I would assume that this is some type of scan (note the TCP Reset-0 at EOL).

The next check that should be done after seeing this log is to verify the logs of the Email server and ensure that it has not been tampered with

We can see the same situation for access to our DNS server on the last two lines.

As previously stated, this type of situation highlights the need for a dedicated resource to monitor logs during the scanning process. This person would need to be vigilant to these situations and would need to cross reference logging information to ensure that the full audit trail of scans is implemented.



In this diagram below we see log messages from the PIX.

Time 20:10:29: Source: PIX: Log Message: This group of entries shows valid SSL connections between the Internal and External Web Servers

Time 20:08:59: Source: PIX: Log Message: This group of entries shows valid HTTP connections between the Internal and External Web Servers

Time 20:05:50: Source: PIX: Log Message: This last two entries show DNS transactions occurring between Internal and External DNS Servers.

© SANS Institute 2000 - 2005, Author retains full rights.

3CDaemon

File View Help

Time	IP Address	Msg Type	Message
Jul 11 20:10:29	172.16.254.30	news.info	Jul 11 2001 03:11:08: %PIX-6-302001: Built outbound TCP connection 195 for faddr 172.16.254.35/443 gaddr 172.16.254.135/62021 laddr 172.16.254.135/62021
Jul 11 20:10:23	172.16.254.30	news.info	Jul 11 2001 03:11:02: %PIX-6-302001: Built outbound TCP connection 194 for faddr 172.16.254.35/443 gaddr 172.16.254.135/62020 laddr 172.16.254.135/62020
Jul 11 20:10:17	172.16.254.30	news.info	Jul 11 2001 03:10:56: %PIX-6-302001: Built outbound TCP connection 193 for faddr 172.16.254.35/443 gaddr 172.16.254.135/62019 laddr 172.16.254.135/62019
Jul 11 20:10:11	172.16.254.30	news.info	Jul 11 2001 03:10:50: %PIX-6-302001: Built outbound TCP connection 192 for faddr 172.16.254.35/443 gaddr 172.16.254.135/62018 laddr 172.16.254.135/62018
Jul 11 20:10:06	172.16.254.30	news.info	Jul 11 2001 03:10:45: %PIX-6-302001: Built outbound TCP connection 191 for faddr 172.16.254.35/443 gaddr 172.16.254.135/62017 laddr 172.16.254.135/62017
Jul 11 20:09:48	172.16.254.30	news.info	Jul 11 2001 03:10:27: %PIX-6-302002: Teardown TCP connection 184 faddr 172.16.254.34/25 gaddr 172.16.254.134/38884 laddr 172.16.254.134/38884 duration 0:0
Jul 11 20:09:48	172.16.254.30	news.info	Jul 11 2001 03:10:27: %PIX-6-302002: Teardown TCP connection 183 faddr 172.16.254.34/25 gaddr 172.16.254.134/38883 laddr 172.16.254.134/38883 duration 0:0
Jul 11 20:09:48	172.16.254.30	news.info	Jul 11 2001 03:10:27: %PIX-6-302002: Teardown TCP connection 182 faddr 172.16.254.34/25 gaddr 172.16.254.134/38882 laddr 172.16.254.134/38882 duration 0:0
Jul 11 20:09:18	172.16.254.30	news.info	Jul 11 2001 03:09:57: %PIX-6-302002: Teardown TCP connection 181 faddr 172.16.254.34/25 gaddr 172.16.254.134/38881 laddr 172.16.254.134/38881 duration 0:0
Jul 11 20:09:18	172.16.254.30	news.info	Jul 11 2001 03:09:57: %PIX-6-302002: Teardown TCP connection 180 faddr 172.16.254.34/25 gaddr 172.16.254.134/38880 laddr 172.16.254.134/38880 duration 0:0
Jul 11 20:09:18	172.16.254.30	news.info	Jul 11 2001 03:09:57: %PIX-6-302002: Teardown TCP connection 179 faddr 172.16.254.34/25 gaddr 172.16.254.134/38879 laddr 172.16.254.134/38879 duration 0:0
Jul 11 20:08:59	172.16.254.30	news.info	Jul 11 2001 03:09:38: %PIX-6-302001: Built outbound TCP connection 190 for faddr 172.16.254.35/80 gaddr 172.16.254.135/35414 laddr 172.16.254.135/35414
Jul 11 20:08:53	172.16.254.30	news.info	Jul 11 2001 03:09:32: %PIX-6-302001: Built outbound TCP connection 189 for faddr 172.16.254.35/80 gaddr 172.16.254.135/35413 laddr 172.16.254.135/35413
Jul 11 20:08:47	172.16.254.30	news.info	Jul 11 2001 03:09:26: %PIX-6-302001: Built outbound TCP connection 188 for faddr 172.16.254.35/80 gaddr 172.16.254.135/35412 laddr 172.16.254.135/35412
Jul 11 20:08:41	172.16.254.30	news.info	Jul 11 2001 03:09:20: %PIX-6-302001: Built outbound TCP connection 187 for faddr 172.16.254.35/80 gaddr 172.16.254.135/35411 laddr 172.16.254.135/35411
Jul 11 20:08:35	172.16.254.30	news.info	Jul 11 2001 03:09:14: %PIX-6-302001: Built outbound TCP connection 186 for faddr 172.16.254.35/80 gaddr 172.16.254.135/35410 laddr 172.16.254.135/35410
Jul 11 20:08:30	172.16.254.30	news.info	Jul 11 2001 03:09:09: %PIX-6-302001: Built outbound TCP connection 185 for faddr 172.16.254.35/80 gaddr 172.16.254.135/35409 laddr 172.16.254.135/35409
Jul 11 20:08:18	172.16.254.30	news.info	Jul 11 2001 03:08:57: %PIX-6-302006: Teardown UDP connection for faddr 172.16.254.33/31748 gaddr 172.16.254.133/40560 laddr 172.16.254.133/40560
Jul 11 20:07:48	172.16.254.30	news.info	Jul 11 2001 03:08:27: %PIX-6-302006: Teardown UDP connection for faddr 172.16.254.33/8959 gaddr 172.16.254.133/40559 laddr 172.16.254.133/40559
Jul 11 20:07:33	172.16.254.30	news.info	Jul 11 2001 03:08:12: %PIX-6-302001: Built outbound TCP connection 184 for faddr 172.16.254.34/25 gaddr 172.16.254.134/38884 laddr 172.16.254.134/38884
Jul 11 20:07:27	172.16.254.30	news.info	Jul 11 2001 03:08:06: %PIX-6-302001: Built outbound TCP connection 183 for faddr 172.16.254.34/25 gaddr 172.16.254.134/38883 laddr 172.16.254.134/38883
Jul 11 20:07:21	172.16.254.30	news.info	Jul 11 2001 03:08:00: %PIX-6-302001: Built outbound TCP connection 182 for faddr 172.16.254.34/25 gaddr 172.16.254.134/38882 laddr 172.16.254.134/38882
Jul 11 20:07:15	172.16.254.30	news.info	Jul 11 2001 03:07:54: %PIX-6-302001: Built outbound TCP connection 181 for faddr 172.16.254.34/25 gaddr 172.16.254.134/38881 laddr 172.16.254.134/38881
Jul 11 20:07:09	172.16.254.30	news.info	Jul 11 2001 03:07:48: %PIX-6-302001: Built outbound TCP connection 180 for faddr 172.16.254.34/25 gaddr 172.16.254.134/38880 laddr 172.16.254.134/38880
Jul 11 20:07:04	172.16.254.30	news.info	Jul 11 2001 03:07:43: %PIX-6-302001: Built outbound TCP connection 179 for faddr 172.16.254.34/25 gaddr 172.16.254.134/38879 laddr 172.16.254.134/38879
Jul 11 20:06:14	172.16.254.30	news.warn	Jul 11 2001 03:06:53: %PIX-4-106023: Deny tcp src internal:172.16.254.133/39052 dst dmz:172.16.254.34/25 by access-group "internal_in"
Jul 11 20:05:50	172.16.254.30	news.info	Jul 11 2001 03:06:29: %PIX-6-302005: Built UDP connection for faddr 172.16.254.33/31748 gaddr 172.16.254.133/40560 laddr 172.16.254.133/40560
Jul 11 20:05:45	172.16.254.30	news.info	Jul 11 2001 03:06:24: %PIX-6-302005: Built UDP connection for faddr 172.16.254.33/8959 gaddr 172.16.254.133/40559 laddr 172.16.254.133/40559

TFFTP Client

For Help, press F1

NUM

VPN Validation

To verify that the VPN tunnel is setup and working, a tunnel is created between GIAC Enterprises and an entity called Partner1.

I have included the whole debug so it may be used to check against an incorrect tunnel creation attempt.

Note that my comments are in bold

Clear any existing connections between the two sites

```
giacvpn01#cle cr is
giacvpn01#cle cr sa
```

Set debugging to capture information

```
giacvpn01#deb cr is
Crypto ISAKMP debugging is on
giacvpn01#deb cr ip
Crypto IPSEC debugging is on
giacvpn01#deb cr ke
Crypto Key Exchange debugging is on
giacvpn01#deb cr en
Crypto Engine debugging is on
giacvpn01#deb cr se
Crypto Session Management debugging is on
```

To bring up a VPN tunnel, we will initiate a ping from the VPN Router. The ping must be sourced at the loopback interface because the ACL for the VPN tunnel have been configured using loopbacks

```
giacvpn01#ping
Protocol [ip]:
Target IP address: 100.1.1.254 (Partner1)
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: loopback 0 (VPN Router)
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 100.1.1.254, timeout is 2 seconds:
```

Here we see that the security association request for the ISAKMP Protocol between the two sites.

```
*Mar 1 10:11:09: IPSEC(sa_request): ,
(key eng. msg.) src= 167.216.133.254, dest= 100.1.1.254,
src_proxy= 167.216.133.254/255.255.255.255/0/0 (type=1),
dest_proxy= 100.1.1.254/255.255.255.255/0/0 (type=1),
```

We are using ESP protocol in tunnel mode in this example

```
protocol= ESP, transform= esp-3des esp-sha-hmac ,
```

The lifetimes is set at 1 hour or 4.6MB of data

```
lifedur= 3600s and 4608000kb,
```

The SPI (security parameter index) together with the source and destination address uniquely identify the security association

```
spi= 0xF6F0A3B(258935355), conn_id= 0, keysize= 0, flags= 0x4004
*Mar 1 10:11:09: ISAKMP: received ke message (1/1)
*Mar 1 10:11:09: ISAKMP: local port 500, remote port 500
*Mar 1 10:11:09: CRYPTO: Allocated conn_id 1 slot 0, swidb 0x0,
*Mar 1 10:11:09: ISAKMP (0:1): beginning Main Mode exchange
*Mar 1 10:11:09: ISAKMP (1): sending packet to 100.1.1.254 (I) MM_NO_STATE
*Mar 1 10:11:09: ISAKMP (1): received packet from 100.1.1.254 (I) MM_NO_STATE
```

*Mar 1 10:11:09: ISAKMP (0:1): processing SA payload. message ID = 0

The list of policies is searched from lowest to highest until a match is found and then whatever is configured in the policy is used to match against the other sites policy list, if a match occurs we begin the key exchange

*Mar 1 10:11:09: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 15 policy

*Mar 1 10:11:09: ISAKMP: encryption 3DES-CBC

*Mar 1 10:11:09: ISAKMP: hash SHA

*Mar 1 10:11:09: ISAKMP: default group 2

*Mar 1 10:11:09: ISAKMP: auth RSA encr

With the above policy we have found a match. The next section is the crypto engine encrypting the data payload

*Mar 1 10:11:09: ISAKMP (0:1): atts are acceptable. Next payload is 0

*Mar 1 10:11:09: CryptoEngine0: generate alg parameter

*Mar 1 10:11:09: CRYPTO_ENGINE: Dh phase 1 status: 0

*Mar 1 10:11:09: CRYPTO_ENGINE: Dh phase 1 status: 0

*Mar 1 10:11:09: CRYPTO: DH gen phase 1 status for conn_id 1 slot 0:OK

We are using encrypted nonces and not Certificates.

*Mar 1 10:11:09: ISAKMP (0:1): Unable to get router cert or routerdoes not have a cert: needed to find DN!

*Mar 1 10:11:09: ISAKMP (0:1): SA is doing RSA encryption authentication

*Mar 1 10:11:09: ISAKMP (1): SA is doing RSA encryption authentication using id type ID_IPV4_ADDR

*Mar 1 10:11:09: ISAKMP (1): ID payload

next-payload : 10

type : 1

protocol : 17 (UDP)

port : 500 (ISAKMP port number)

length : 8

*Mar 1 10:11:09: Crypto engine 0: RSA encrypt with public key

*Mar 1 10:11:09: CryptoEngine0: CRYPTO_RSA_PUB_ENCRYPT

*Mar 1 10:11:09: CRYPTO: RSA public encrypt finished with status=OK

*Mar 1 10:11:09: ISAKMP (1): length after encryption 64

*Mar 1 10:11:09: ISAKMP (1): Total payload length: 68

*Mar 1 10:11:09: Crypto engine 0: RSA encrypt with public key

*Mar 1 10:11:09: CryptoEngine0: CRYPTO_RSA_PUB_ENCRYPT

*Mar 1 10:11:09: CRYPTO: RSA public encrypt finished with status=OK

*Mar 1 10:11:09: ISAKMP (1): sending packet to 100.1.1.254 (I) MM_SA_SETUP

*Mar 1 10:11:10: ISAKMP (1): received packet from 100.1.1.254 (I) MM_SA_SETUP

*Mar 1 10:11:10: ISAKMP (0:1): processing KE payload. message ID = 0

*Mar 1 10:11:10: CryptoEngine0: generate alg parameter

*Mar 1 10:11:10: CRYPTO: DH gen phase 2 status for conn_id 1 slot 0:OK

*Mar 1 10:11:10: ISAKMP (0:1): processing ID payload. message ID = 0

*Mar 1 10:11:10: Crypto engine 0: RSA decrypt with private key

*Mar 1 10:11:10: CryptoEngine0: CRYPTO_RSA_PRIV_DECRYPT

*Mar 1 10:11:10: CRYPTO_ENGINE: key process suspended and continued

*Mar 1 10:11:11: CRYPTO: RSA private decrypt finished with status=OK

*Mar 1 10:11:11: ISAKMP (0:1): processing NONCE payload. message ID = 0

*Mar 1 10:11:11: Crypto engine 0: RSA decrypt with private key

*Mar 1 10:11:11: CryptoEngine0: CRYPTO_RSA_PRIV_DECRYPT

*Mar 1 10:11:11: CRYPTO_ENGINE: key process suspended and continued

*Mar 1 10:11:11: CRYPTO: RSA private decrypt finished with status=OK

Our ping succeeded after encryption and initial routing resolution.

*Mar .!!!

Success rate is 60 percent (3/5), round-trip min/avg/max = 12/12/12 ms

giacvpn01# 1 10:11:11: CryptoEngine0: create ISAKMP SKEYID for conn id 1

ISAKMP creates temporary sessions to for IPSEC

*Mar 1 10:11:11: ISAKMP (0:1): SKEYID state generated

*Mar 1 10:11:11: ISAKMP (0:1): processing vendor id payload

*Mar 1 10:11:11: ISAKMP (0:1): speaking to another IOS box!

*Mar 1 10:11:11: CryptoEngine0: generate hmac context for conn id 1

*Mar 1 10:11:11: ISAKMP (1): sending packet to 100.1.1.254 (I) MM_KEY_EXCH

*Mar 1 10:11:11: ISAKMP (1): received packet from 100.1.1.254 (I) MM_KEY_EXCH

*Mar 1 10:11:11: ISAKMP (0:1): processing HASH payload. message ID = 0
 *Mar 1 10:11:11: CryptoEngine0: generate hmac context for conn id 1
 *Mar 1 10:11:11: ISAKMP (0:1): SA has been authenticated with 100.1.1.254
 *Mar 1 10:11:11: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -954693944
 *Mar 1 10:11:11: CryptoEngine0: generate hmac context for conn id 1
 *Mar 1 10:11:11: ISAKMP (1): sending packet to 100.1.1.254 (I) QM_IDLE
 *Mar 1 10:11:11: CryptoEngine0: clear dh number for conn id 1
 *Mar 1 10:11:11: CRYPTO: Crypto Engine clear dh conn_id 1 slot 0: OK
 *Mar 1 10:11:11: ISAKMP (1): received packet from 100.1.1.254 (I) QM_IDLE
 *Mar 1 10:11:11: CryptoEngine0: generate hmac context for conn id 1
 *Mar 1 10:11:11: ISAKMP (0:1): processing SA payload. message ID = -954693944
 *Mar 1 10:11:11: ISAKMP (0:1): Checking IPsec proposal 1
 *Mar 1 10:11:11: ISAKMP: transform 1, ESP_3DES
 *Mar 1 10:11:11: ISAKMP: attributes in transform:
 *Mar 1 10:11:11: ISAKMP: encaps is 1
 *Mar 1 10:11:11: ISAKMP: SA life type in seconds
 *Mar 1 10:11:11: ISAKMP: SA life duration (basic) of 3600
 *Mar 1 10:11:11: ISAKMP: SA life type in kilobytes
 *Mar 1 10:11:11: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
 *Mar 1 10:11:11: ISAKMP: authenticator is HMAC-SHA
 *Mar 1 10:11:11: validate proposal 0
 *Mar 1 10:11:11: ISAKMP (0:1): atts are acceptable.
 *Mar 1 10:11:11: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) dest= 100.1.1.254, src= 167.216.133.254,
 dest_proxy= 100.1.1.254/255.255.255.255/0/0 (type=1),
 src_proxy= 167.216.133.254/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
 *Mar 1 10:11:11: validate proposal request 0
 *Mar 1 10:11:11: ISAKMP (0:1): processing NONCE payload. message ID = -954693944
 *Mar 1 10:11:11: ISAKMP (0:1): processing ID payload. message ID = -954693944
 *Mar 1 10:11:11: ISAKMP (0:1): processing ID payload. message ID = -954693944
 *Mar 1 10:11:11: CryptoEngine0: generate hmac context for conn id 1
 *Mar 1 10:11:11: ipsec allocate flow 0
 *Mar 1 10:11:11: ipsec allocate flow 0
 *Mar 1 10:11:11: CRYPTO: Allocated conn_id 2000 slot 0, swidb 0x817A0030,
 *Mar 1 10:11:11: CRYPTO: Allocated conn_id 2001 slot 0, swidb 0x817A0030,
 *Mar 1 10:11:11: ISAKMP (0:1): Creating IPsec SAs
 *Mar 1 10:11:11: inbound SA from 100.1.1.254 to 167.216.133.254 (proxy 100.1.1.254 to
 167.216.133.254)
 *Mar 1 10:11:11: has spi 258935355 and conn_id 2000 and flags 4
 *Mar 1 10:11:11: lifetime of 3600 seconds
 *Mar 1 10:11:11: lifetime of 4608000 kilobytes
 *Mar 1 10:11:11: outbound SA from 167.216.133.254 to 100.1.1.254 (proxy 167.216.133.254 to
 100.1.1.254)
 *Mar 1 10:11:11: has spi 57285841 and conn_id 2001 and flags 4
 *Mar 1 10:11:11: lifetime of 3600 seconds
 *Mar 1 10:11:11: lifetime of 4608000 kilobytes
 *Mar 1 10:11:11: ISAKMP (1): sending packet to 100.1.1.254 (I) QM_IDLE
 *Mar 1 10:11:11: ISAKMP (0:1): deleting node -954693944 error FALSE reason ""
 *Mar 1 10:11:11: IPSEC(key_engine): got a queue event...
 *Mar 1 10:11:11: IPSEC(initialize_sas): ,
 (key eng. msg.) dest= 167.216.133.254, src= 100.1.1.254,
 dest_proxy= 167.216.133.254/255.255.255.255/0/0 (type=1),
 src_proxy= 100.1.1.254/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac ,
 lifedur= 3600s and 4608000kb,
 spi= 0xF6F0A3B(258935355), conn_id= 2000, keysize= 0, flags= 0x4
 *Mar 1 10:11:11: IPSEC(initialize_sas): ,
 (key eng. msg.) src= 167.216.133.254, dest= 100.1.1.254,
 src_proxy= 167.216.133.254/255.255.255.255/0/0 (type=1),

```

dest_proxy= 100.1.1.254/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x36A1CD1(57285841), conn_id= 2001, keysize= 0, flags= 0x4
*Mar 1 10:11:11: IPSEC(create_sa): sa created,
(sa) sa_dest= 167.216.133.254, sa_prot= 50,
sa_spi= 0xF6F0A3B(258935355),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
*Mar 1 10:11:11: IPSEC(create_sa): sa created,
(sa) sa_dest= 100.1.1.254, sa_prot= 50,
sa_spi= 0x36A1CD1(57285841),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001

```

To verify that the ISAKMP exchange is created between the two sites the router configs should have the following output.

The security association is setup and waiting in QM_IDLE mode with the source and destination of the tunnel endpoints NOT the source/destination of the communicating hosts.

```

giacvpn01#show crypto isakmp sa
*Mar 1 10:12:01: ISAKMP (0:1): purging node -954693944
  dst      src      state      conn-id  slot
100.1.1.254 167.216.133.254 QM_IDLE      1      0

```

To verify that the IPSEC tunnel is created between the two sites.

Note that IPSEC shown here is the actual tunnel and not the association that is needed to exchange session keys (that is shown above with ISAKMP)

```
giacvpn01# show crypto ipsec sa
```

```
interface: Ethernet0/0
```

```
  Crypto map tag: internet_secure, local addr. 167.216.133.254
```

Source and destination of the actual sending and receiving hosts.

In this situation, this happens to be the same as the tunnel end points but you will find that this is usually the list of allowed addresses in the IPSEC ACLs)

```

local ident (addr/mask/prot/port): (167.216.133.254/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (100.1.1.254/255.255.255.255/0/0)
current_peer: 100.1.1.254
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

```

```

local crypto endpt.: 167.216.133.254, remote crypto endpt.: 100.1.1.254
path mtu 1500, media mtu 1500
current outbound spi: 36A1CD1

```

```

inbound esp sas:
spi: 0xF6F0A3B(258935355)
  transform: esp-3des esp-sha-hmac ,
  in use settings = {Tunnel, } (this is in configured in tunnel mode)
  slot: 0, conn id: 2000, flow_id: 1, crypto map: internet_secure

```

Check the lifetime of the association, I have left it at 1 hour but as GIAC is using IPSEC for FTPing Fortune Cookies and as the download time will most likely not go over 10 minutes this value should be changed to about 30 minutes. Off course if GIAC is sending huge files down 56K lines then this time should be increased.

```

sa timing: remaining key lifetime (k/sec): (4607998/3526)
IV size: 8 bytes

```

replay detection support: Y

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

spi: 0x36A1CD1(57285841)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: internet_secure
sa timing: remaining key lifetime (k/sec): (4607998/3517)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcsp sas:

local ident (addr/mask/prot/port): (167.216.133.4/255.255.255.255/6/0)
remote ident (addr/mask/prot/port): (147.132.22.87/255.255.255.255/6/0)
current_peer: 100.1.1.254
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 167.216.133.254, remote crypto endpt.: 100.1.1.254
path mtu 1500, media mtu 1500
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

outbound ah sas:

outbound pcsp sas:

local ident (addr/mask/prot/port): (167.216.133.5/255.255.255.255/6/0)
remote ident (addr/mask/prot/port): (147.132.22.87/255.255.255.255/6/0)
current_peer: 100.1.1.254
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 167.216.133.254, remote crypto endpt.: 100.1.1.254
path mtu 1500, media mtu 1500
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

giacvpn01#

© SANS Institute 2000 - 2005, Author retains full rights.

**This is the reciprocal site (Partner1) that is accepting IPSEC from our GIAC VPN router.
I have added it for reference material only and will not be documenting these configs.
They are much the same as the above VPN router because they are both Cisco routers**

```
Partner1#cle cr sa
Partner1#deb cr is
Crypto ISAKMP debugging is on
Partner1#deb cr ip
Crypto IPSEC debugging is on
Partner1#deb cr ke
Crypto Key Exchange debugging is on
Partner1#deb cr en
Crypto Engine debugging is on
Partner1#deb cr se
Crypto Session Management debugging is on
Partner1#
*Jun 24 16:43:11: ISAKMP (0): received packet from 167.216.133.254 (N) NEW SA
*Jun 24 16:43:11: ISAKMP: local port 500, remote port 500
*Jun 24 16:43:11: CRYPTO: Allocated conn_id 1 slot 0, swidb 0x0,
*Jun 24 16:43:11: ISAKMP (0:1): processing SA payload. message ID = 0
*Jun 24 16:43:11: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 15 policy
*Jun 24 16:43:11: ISAKMP:      encryption 3DES-CBC
*Jun 24 16:43:11: ISAKMP:      hash SHA
*Jun 24 16:43:11: ISAKMP:      default group 2
*Jun 24 16:43:11: ISAKMP:      auth RSA encr
*Jun 24 16:43:11: ISAKMP (0:1): atts are acceptable. Next payload is 0
*Jun 24 16:43:11: CryptoEngine0: generate alg parameter
*Jun 24 16:43:11: CRYPTO_ENGINE: Dh phase 1 status: 0
*Jun 24 16:43:11: CRYPTO_ENGINE: Dh phase 1 status: 0
*Jun 24 16:43:11: CRYPTO: DH gen phase 1 status for conn_id 1 slot 0:OK
*Jun 24 16:43:11: ISAKMP (0:1): Unable to get router cert or router does not have a cert: needed to find DN!
*Jun 24 16:43:11: ISAKMP (0:1): SA is doing RSA encryption authentication
*Jun 24 16:43:11: ISAKMP (1): SA is doing RSA encryption authentication using id type ID_IPV4_ADDR
*Jun 24 16:43:11: ISAKMP (1): sending packet to 167.216.133.254 (R) MM_SA_SETUP
*Jun 24 16:43:11: ISAKMP (1): received packet from 167.216.133.254 (R) MM_SA_SETUP
*Jun 24 16:43:11: ISAKMP (0:1): processing KE payload. message ID = 0
*Jun 24 16:43:11: CryptoEngine0: generate alg parameter
*Jun 24 16:43:12: CRYPTO: DH gen phase 2 status for conn_id 1 slot 0:OK
*Jun 24 16:43:12: ISAKMP (0:1): processing ID payload. message ID = 0
*Jun 24 16:43:12: Crypto engine 0: RSA decrypt with private key
*Jun 24 16:43:12: CryptoEngine0: CRYPTO_RSA_PRIV_DECRYPT
*Jun 24 16:43:12: CRYPTO: RSA private decrypt finished with status=OK
*Jun 24 16:43:12: ISAKMP (0:1): processing NONCE payload. message ID = 0
*Jun 24 16:43:12: Crypto engine 0: RSA decrypt with private key
*Jun 24 16:43:12: CryptoEngine0: CRYPTO_RSA_PRIV_DECRYPT
*Jun 24 16:43:12: CRYPTO: RSA private decrypt finished with status=OK
*Jun 24 16:43:12: CryptoEngine0: create ISAKMP SKEYID for conn id 1
*Jun 24 16:43:12: ISAKMP (0:1): SKEYID state generated
*Jun 24 16:43:12: ISAKMP (0:1): processing vendor id payload
*Jun 24 16:43:12: ISAKMP (0:1): speaking to another IOS box!
*Jun 24 16:43:12: ISAKMP (1): ID payload
    next-payload : 10
    type          : 1
    protocol       : 17
    port           : 500
    length         : 8
*Jun 24 16:43:12: Crypto engine 0: RSA encrypt with public key
*Jun 24 16:43:12: CryptoEngine0: CRYPTO_RSA_PUB_ENCRYPT
*Jun 24 16:43:12: CRYPTO: RSA public encrypt finished with status=OK
*Jun 24 16:43:12: ISAKMP (1): length after encryption 64
*Jun 24 16:43:12: ISAKMP (1): Total payload length: 68
```

*Jun 24 16:43:12: Crypto engine 0: RSA encrypt with public key
 *Jun 24 16:43:12: CryptoEngine0: CRYPTO_RSA_PUB_ENCRYPT
 *Jun 24 16:43:12: CRYPTO: RSA public encrypt finished with status=OK
 *Jun 24 16:43:12: ISAKMP (1): sending packet to 167.216.133.254 (R) MM_KEY_EXCH
 *Jun 24 16:43:13: ISAKMP (1): received packet from 167.216.133.254 (R) MM_KEY_EXCH
 *Jun 24 16:43:13: ISAKMP (0:1): processing HASH payload. message ID = 0
 *Jun 24 16:43:13: CryptoEngine0: generate hmac context for conn id 1
 *Jun 24 16:43:13: ISAKMP (0:1): SA has been authenticated with 167.216.133.254
 *Jun 24 16:43:13: CryptoEngine0: generate hmac context for conn id 1
 *Jun 24 16:43:13: CryptoEngine0: clear dh number for conn id 1
 *Jun 24 16:43:13: CRYPTO: Crypto Engine clear dh conn_id 1 slot 0: OK
 *Jun 24 16:43:13: ISAKMP (1): sending packet to 167.216.133.254 (R) QM_IDLE
 *Jun 24 16:43:13: ISAKMP (1): received packet from 167.216.133.254 (R) QM_IDLE
 *Jun 24 16:43:13: CryptoEngine0: generate hmac context for conn id 1
 *Jun 24 16:43:13: ISAKMP (0:1): processing SA payload. message ID = -954693944
 *Jun 24 16:43:13: ISAKMP (0:1): Checking IPsec proposal 1
 *Jun 24 16:43:13: ISAKMP: transform 1, ESP_3DES
 *Jun 24 16:43:13: ISAKMP: attributes in transform:
 *Jun 24 16:43:13: ISAKMP: encaps is 1
 *Jun 24 16:43:13: ISAKMP: SA life type in seconds
 *Jun 24 16:43:13: ISAKMP: SA life duration (basic) of 3600
 *Jun 24 16:43:13: ISAKMP: SA life type in kilobytes
 *Jun 24 16:43:13: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
 *Jun 24 16:43:13: ISAKMP: authenticator is HMAC-SHA
 *Jun 24 16:43:13: validate proposal 0
 *Jun 24 16:43:13: ISAKMP (0:1): atts are acceptable.
 *Jun 24 16:43:13: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) dest= 100.1.1.254, src= 167.216.133.254,
 dest_proxy= 100.1.1.254/255.255.255.255/0/0 (type=1),
 src_proxy= 167.216.133.254/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
 *Jun 24 16:43:13: validate proposal request 0
 *Jun 24 16:43:13: ISAKMP (0:1): processing NONCE payload. message ID = -954693944
 *Jun 24 16:43:13: ISAKMP (0:1): processing ID payload. message ID = -954693944
 *Jun 24 16:43:13: ISAKMP (1): ID_IPV4_ADDR src 167.216.133.254 prot 0 port 0
 *Jun 24 16:43:13: ISAKMP (0:1): processing ID payload. message ID = -954693944
 *Jun 24 16:43:13: ISAKMP (1): ID_IPV4_ADDR dst 100.1.1.254 prot 0 port 0
 *Jun 24 16:43:13: ISAKMP (0:1): asking for 1 spis from ipsec
 *Jun 24 16:43:13: IPSEC(key_engine): got a queue event...
 *Jun 24 16:43:13: IPSEC(spi_response): getting spi 57285841 for SA
 from 167.216.133.254 to 100.1.1.254 for prot 3
 *Jun 24 16:43:13: ISAKMP: received ke message (2/1)
 *Jun 24 16:43:13: CryptoEngine0: generate hmac context for conn id 1
 *Jun 24 16:43:13: ISAKMP (1): sending packet to 167.216.133.254 (R) QM_IDLE
 *Jun 24 16:43:13: ISAKMP (1): received packet from 167.216.133.254 (R) QM_IDLE
 *Jun 24 16:43:13: CryptoEngine0: generate hmac context for conn id 1
 *Jun 24 16:43:13: ipsec allocate flow 0
 *Jun 24 16:43:13: ipsec allocate flow 0
 *Jun 24 16:43:13: CRYPTO: Allocated conn_id 2000 slot 0, swidb 0x61272B24,
 *Jun 24 16:43:13: CRYPTO: Allocated conn_id 2001 slot 0, swidb 0x61272B24,
 *Jun 24 16:43:13: ISAKMP (0:1): Creating IPsec SAs
 *Jun 24 16:43:13: inbound SA from 167.216.133.254 to 100.1.1.254 (proxy 167.216.133.254 to
 100.1.1.254)
 *Jun 24 16:43:13: has spi 57285841 and conn_id 2000 and flags 4
 *Jun 24 16:43:13: lifetime of 3600 seconds
 *Jun 24 16:43:13: lifetime of 4608000 kilobytes
 *Jun 24 16:43:13: outbound SA from 100.1.1.254 to 167.216.133.254 (proxy 100.1.1.254 to
 167.216.133.254)
 *Jun 24 16:43:13: has spi 258935355 and conn_id 2001 and flags 4
 *Jun 24 16:43:13: lifetime of 3600 seconds

*Jun 24 16:43:13: lifetime of 4608000 kilobytes
 *Jun 24 16:43:13: ISAKMP (0:1): deleting node -954693944 error FALSE reason "quick mode done (await())"
 *Jun 24 16:43:13: IPSEC(key_engine): got a queue event...
 *Jun 24 16:43:13: IPSEC(initialize_sas): ,
 (key eng. msg.) dest= 100.1.1.254, src= 167.216.133.254,
 dest_proxy= 100.1.1.254/0.0.0.0/0/0 (type=1),
 src_proxy= 167.216.133.254/0.0.0.0/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac ,
 lifedur= 3600s and 4608000kb,
 spi= 0x36A1CD1(57285841), conn_id= 2000, keysize= 0, flags= 0x4
 *Jun 24 16:43:13: IPSEC(initialize_sas): ,
 (key eng. msg.) src= 100.1.1.254, dest= 167.216.133.254,
 src_proxy= 100.1.1.254/0.0.0.0/0/0 (type=1),
 dest_proxy= 167.216.133.254/0.0.0.0/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac ,
 lifedur= 3600s and 4608000kb,
 spi= 0xF6F0A3B(258935355), conn_id= 2001, keysize= 0, flags= 0x4
 *Jun 24 16:43:13: IPSEC(create_sa): sa created,
 (sa) sa_dest= 100.1.1.254, sa_prot= 50,
 sa_spi= 0x36A1CD1(57285841),
 sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
 *Jun 24 16:43:13: IPSEC(create_sa): sa created,
 (sa) sa_dest= 167.216.133.254, sa_prot= 50,
 sa_spi= 0xF6F0A3B(258935355),
 sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001

Partner1#

Partner1#

*Jun 24 16:44:03: ISAKMP (0:1): purging node -954693944

Partner1#sh cr is sa

dst	src	state	conn-id	slot
100.1.1.254	167.216.133.254	QM_IDLE	1	0

Partner1#sh cr ip sa

interface: Serial0

Crypto map tag: giac, local addr. 100.1.1.254

local ident (addr/mask/prot/port): (100.1.1.254/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port): (167.216.133.254/255.255.255.255/0/0)
 current_peer: 167.216.133.254
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
 #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

local crypto endpt.: 100.1.1.254, remote crypto endpt.: 167.216.133.254
 path mtu 1500, media mtu 1500
 current outbound spi: F6F0A3B

inbound esp sas:

spi: 0x36A1CD1(57285841)
 transform: esp-3des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 2000, flow_id: 1, crypto map: giac
 sa timing: remaining key lifetime (k/sec): (4607999/3478)
 IV size: 8 bytes
 replay detection support: Y

inbound ah sas:

inbound pcg sas:

outbound esp sas:

spi: 0xF6F0A3B(258935355)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: giac
sa timing: remaining key lifetime (k/sec): (4607998/3478)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcg sas:

local ident (addr/mask/prot/port): (147.132.22.87/255.255.255.255/6/0)
remote ident (addr/mask/prot/port): (167.216.133.4/255.255.255.255/6/0)
current_peer: 167.216.133.254
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 100.1.1.254, remote crypto endpt.: 167.216.133.254
path mtu 1500, media mtu 1500
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

Partner1#

Alternate Architectures

This will depend on the business case of how much money GIAC wishes to spend to secure their information. Simpler and cheaper solutions exist with the cost of less security. The idea is to maximise the security with what you have rather than spending dollars on firewalls that have security holes (for business reasons) and out of date patches.

What was discovered in the above design during the scanning phase of the audit, was that Audit Point 7 had 2 noticeable anomalies. The Internal Mail and DNS servers could communicate to the public Internet addresses of their External counterparts. The ACLs of the PIX Internal interface do not explicitly permit this so I am suspicious of why this occurred and would investigate further. This is not a major cause for concern as the PIX is stopping other outgoing connections to foreign addresses from the Internal Servers but I would still like to know why this occurred.

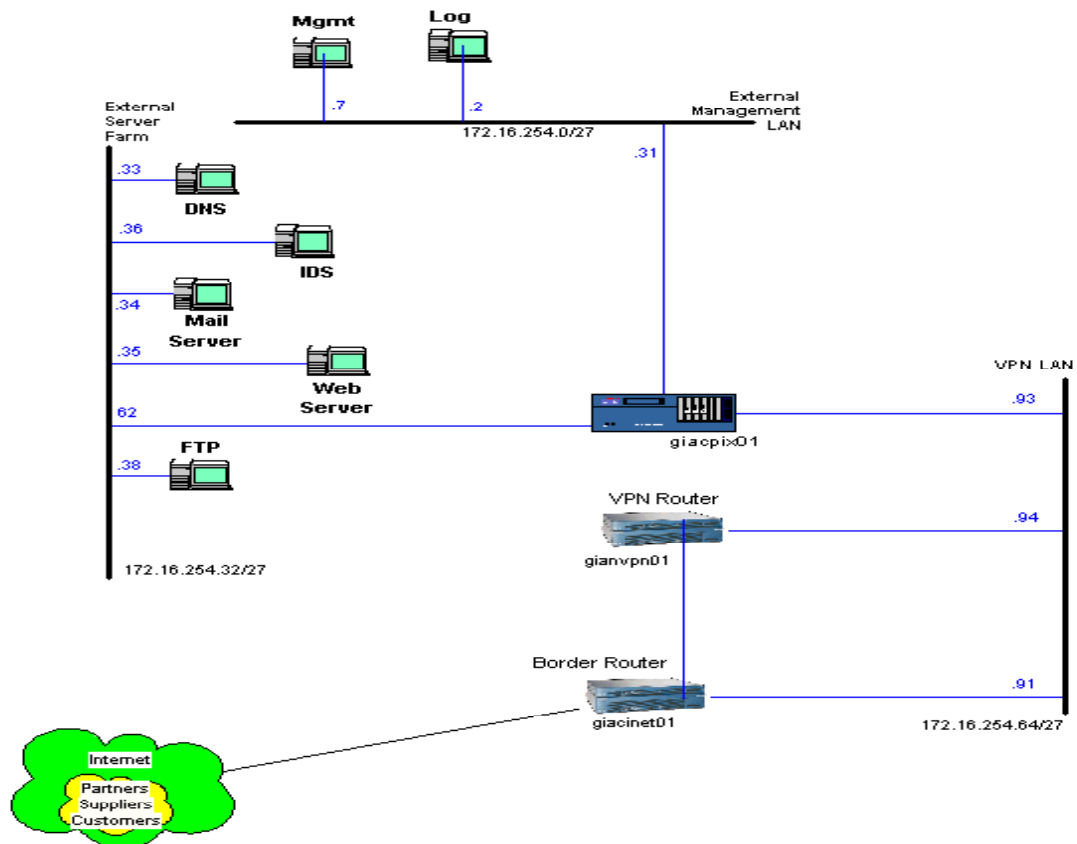
I would also recommend that a mail sweeper be placed in front of the Internal Mail server to protect against viruses and provide another layer of defence where the PIX and routers cannot.

If the number of Partners, Suppliers and Customers became too large, I would look at using a Certificate Authority instead of encrypted nonces.

Internet traffic passing through both the VPN and Internet routers may theoretically provide a greater risk of failure but this is a trade between layered defence and uptime. I believe that the addition of failover routers adequately covers this problem

© SANS Institute 2000 - 2005, Author retains full rights.

Alternate Architecture 2

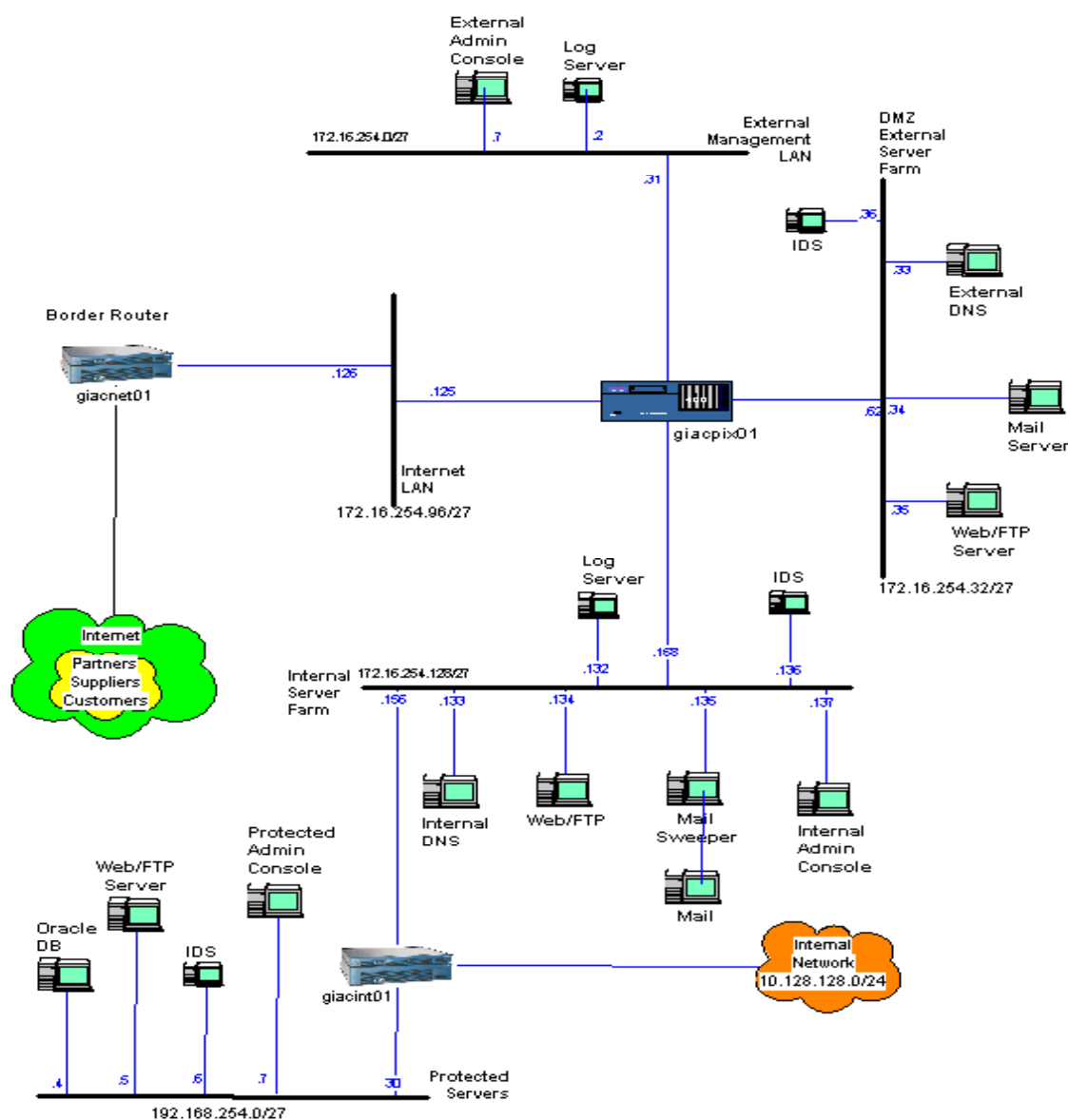


I have slightly altered the design to provide a more secure environment for the VPNs. Instead of all Internet traffic passing through the VPN router, only VPN traffic will be directed to this router. All other Internet traffic will go straight to the PIX. This design provides more security to the VPNs at the expense of removing a layer of defence to the PIX. A smaller router than a 3640 can be used here because the amount of traffic through the VPN router would be significantly less. A 2611, 2621 or 2651 can be used as these routers also have the capability to use the VPN encryption card if required.

Alternate 3

This design is much cheaper than the original because the CheckPoint Firewall has been replaced from the interior of the network with a Cisco 3640 router and the VPN router has been removed completely. All VPN tunnels will be terminated on the PIX and the Internal router will use CBAC to provide protection to the Oracle database. The Interior router will act as the Internal firewall with the Outside connection going to the PIX, the DMZ going to the Internal network and the Inside network will be where secure data will be kept. I have also added a Mail sweeper for content filtering to limit the amount of viruses into the network

Alternate Architecture 3



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.
4. **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.

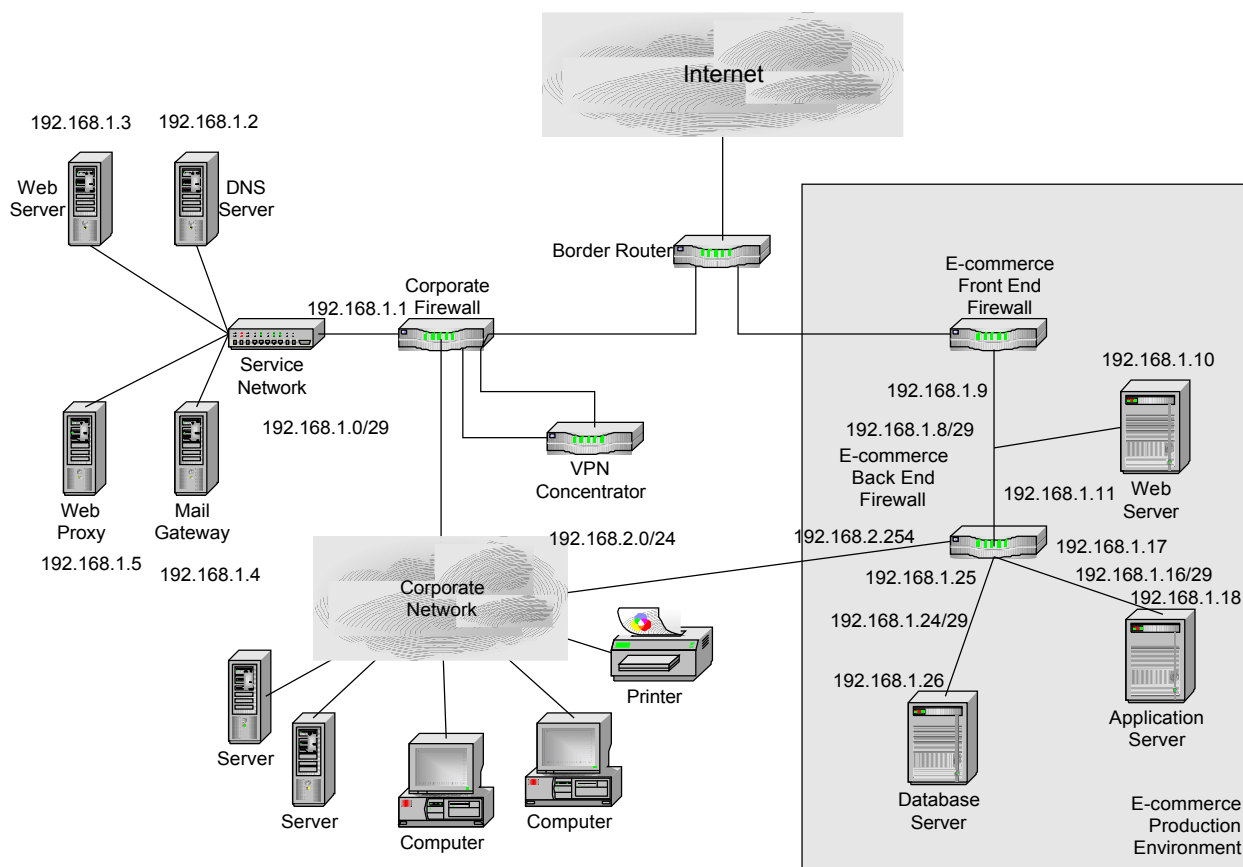
I will use Michael Warner's practical for this section.

http://www.sans.org/y2k/practical/Michael_Warner_GCFW.doc (25/07/01)

For the purposes of Assignment 4, I will cut & paste relevant elements from Michael Warner's document and then examine elements from his practical that I consider worthy of mention with regards to security incursions.

When required I will place extracts of Mr Warner's practical in italics and indent it.

Network Architecture.



Security Architecture

The use of PIX 515 5.1(3) for every firewall device is a point worth mentioning. This provides an easier to manage environment at the cost of having the same vulnerability on all firewalls. If multiple firewalls are to be used then at least should be from a different vendor. The first point of entry after the border router will be two of same firewall platforms. This would slow an attack down if the hacker had to break two different types of firewall devices.

As Cisco seems to be the vendor of choice, I believe that the security officers have more knowledge about this product and the E-Commerce Front End Firewall looks to have the simpler configuration to maintain so I think that this firewall should be the different vendor

I don't agree with the choice of a VPN Concentrator in this design as it is looping traffic through the Corporate Firewall and using up an additional PIX interface. I would recommend connecting the outside interface of the Concentrator to a new switch between the Corporate Firewall and the Border Router. This would stop the loop and still allow the firewall to examine unencrypted traffic. Minor route changes on the PIX and Border router would easily accommodate this design.

Security Policy

Border Router

This router has not been secured sufficiently. ACL's denying RFC1918 addresses, spoofing, NetBIOS, NetBUS and Back Orifice are the only addresses and ports blocked. There is an explicit permit any any statement that will allow any type of scans through to map the network.

The suggested list of ports and addresses that should not be allowed from the site below has not been implemented fully.

How To Eliminate The Ten Most Critical

Internet Security Threats

The Experts' Consensus

Version 1.33 June 25, 2001

Copyright 2000 - 2001, The SANS Institute

<http://www.sans.org/top10.htm> (25/07/01)

This design is relying on the too heavily on the firewall to block these scans mentioned in the URL above. (they should never have been allowed into the network). There is now a good opportunity to sufficiently map the interior network and create a "hook" for attackers to try to have some fun. Once someone has gained partial access to your network they are encouraged to spend more time analysing your network and trying and get further inside.

Firewalls

Here, the firewalls of choice are PIX 515 version 5.3(1)

I have found these vulnerabilities at <http://www.securityfocus.com> (25/07/01)

These bugs have probably been fixed in 5.3(1) but I would give them a try just in case.

bugtraq id 1698 : Failure to Handle Exceptional Conditions:

Like other firewalls, the Cisco PIX Firewall implements technology that reads the contents of packets passing through it for application-level filtering. In the case of SMTP, it can be configured so only certain smtp commands can be allowed through (for example, dropping extra functionality, such as HELP or commands that could be a security concern, like EXPN or VRFY). When receiving messages, it allows all text through between "data" and "<CR><LF><CR><LF>.<CR><LF>", as this is where the body of the message would normally go and there could be words in it that are smtp commands which shouldn't be filtered. Due to the nature of SMTP and flaws in exceptional condition handling of PIX, it is reportedly possible to evade the smtp command restrictions by tricking the firewall into thinking the body of the message is being sent when it isn't.

During communication with an smtp server, if the "data" command is sent before the more important information is sent, such as "rcpt to", the smtp server will return error 503, saying that rcpt was required. The firewall, however, thinks everything is alright and will let everything through until receiving "<CR><LF><CR><LF>.<CR><LF>". It is then possible for the attacker to do whatever he wishes on the email server.

This would allow an attack from the SMTP server as the PIX would allow the contents through without checking.

The next bug is more of interest because of the ability to run scans directly to the PIX without much filtering at the Border router.

bugtraq id 1454 class Access Validation Error

A connection through a Cisco Secure PIX Firewall can be reset by a third party if the source and destination IP addresses and ports of the connection can be determined or inferred. This can be accomplished by sending a forged TCP Reset (RST) packet to the firewall, containing the same source and destination addresses and ports (in the TCP packet header) as the connection to be disrupted. The attacker would have to possess detailed knowledge of the connection table in the firewall (which is used to track outgoing connections and disallow any connections from the external network that were not initiated by an internal machine) or be able to otherwise determine the required IP address and port information to exploit this.

/data/vulnerabilities/exploits/pix_reset_state.c

As stated above “the attacker would have to possess detailed knowledge of the connection table in the firewall”, we should be able to get this information as ICMP is allowed through the network.

I have not found any active bugs in this version so I would attempt a DoS or a DDoS against the PIX because of the comments about heavy traffic loads on the PIX 515 found at:

<http://www.shmoo.com/mail/firewalls/apr00/msg00030.shtml> (25/07/01)

Excerpt “The PIX 515 is definitely not meant for sites with heavy traffic, if you have more than 2-3Mbs sustained the 515 won't cut it”

Denial of Service

As the Border router is fairly open to most traffic it should be no problem in overloading these PIXes. I will assume that I have run a ping scan on the Internet and came up with a few addresses in the 99.99.99.0 range. A more detailed port scan would find the open ports that Mr Warner has listed:

Interesting ports on (99.99.99.3):

(The 65533 ports scanned but not shown below are in state: filtered)

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

Interesting ports on (99.99.99.4):

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
25/tcp	open	smtp

Interesting ports on (99.99.99.10):

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
443/tcp	open	https

Steve Gibson has a very good article about DDoS at <http://grc.com/dos/intro.htm> (25/07/01)

In this article he explains how a DDoS was used to bring down his two T1 trunks. The same principles of using remote control IRC Zombie/Bots from compromised hosts can be used here.

The design uses a 7200 for the Border router and there is no mention of using TCP Intercept on the router to prevent SYN floods. When comparing the 7200 border router and the pix515, I say that this is an unbalanced

network with regards to throughput. Two 515s do not match the speed of the 7200 and the 515 have more work to do than the 7200. When attempting a SYN flood, the Border router will happily pass the traffic through without much trouble and it is up to the PIXes to monitor the threshold levels. This will also apply to any type of UDP attack. The Border router should use CBAC to control UDP timeouts and also protect the Internal networks from SYN floods.

Quality of Service features can be enabled on the Border router to help alleviate the some flood attacks. With the current router policy of open ICMP, I would use Weighted Fair Queueing because it is more effective against ping floods than SYN floods because the ping flood appears as a single traffic flow. SYN packets appear as separate flows.

The corporate firewall is allowing out ICMP any any echo so I would be curious to see how many large pings from multiple sources it could handle from valid Internet addresses. A SMURF attack would gain further strength because the Border Router has no configuration for prevention of directed-broadcasts. This only increases the amplification of attacks on the Internal networks.

Source routing and ICMP redirects have not been addressed at the Border Router so I can control where my intrusive packets would be going. This would help me direct attacks at specific targets once the interior network has been mapped through the use of the allowed ICMP packets.

Attempted Compromise

Mr Warner has not stated what type of platform of OS he is using for his DNS server so it will be difficult to demonstrate how to compromise this host. I attempt to use generic terms that may be applied to most platforms.

The target chosen for attack would be the DNS service because of the allowed zone transfers from the ISP address 88.88.88.88

Mr Warner has stated

The external DNS server provides resolution of external DNS names for the internal DNS server, as well as the authoritative source for GIAC public addresses. A secondary DNS server is provided by the ISP. Access to the DNS server is allowed from both the Internet and the internal DNS server on the corporate network to resolve DNS queries (UDP port 53). In addition the secondary external DNS server (hosted by the ISP) is allowed access to perform zone transfers (TCP port 53). To allow external name resolution, the DNS server must also be allowed to initiate outbound queries (UDP port 53).

Mr Warner has indicated that he will be allowing zone transfers from the ISP to the Internal DNS server. If I can manage to spoof the ISP address of 88.88.88.88 I may be able to place false entries in the DNS.

```
access-list acl_outside permit tcp host isp_dns host pub_dns_server eq 53
```

As this is a DNS a good place to start is the one suggested at <http://www.sans.org/topten.htm> (25/07/01). The first entry is DNS BIND exploits.

According to the following web site all BIND versions “except 4.9.8, 8.2.3, and 9.*” are vulnerable to an Iquery that will crash the box.
<http://maclux-rz.uibk.ac.at/~maillists/vuln-dev/msg00113.shtml> (4/7/01)

To get some usefull information from the name servers have a look at

<http://securityportal.com/cover/coverstory20001113.html> (4/7/01)

This site uses nslookup and dig to get information about the name servers. The information that was found here (such as the OS) can then be used to further look up exploits and glean information about the network. A root shell might be gained if the BIND version is 8.2 – 8.2.2

See <http://www.enteract.com/~lspitz/NXT-Howto.txt> (4/7/01) how to do this.

If root access is established, I would modify a few DNS entries to allow my addresses access to further internal servers in an attempt to get information about these boxes and then trying to exploit platform and OS vulnerabilities.

© SANS Institute 2000 - 2005, Author retains full rights.

Bibliography

Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, Building Internet Firewalls, O'Reilly & Associates, Inc. 2000

Bradley Dunsmore, Joli Annette Ballew, Jeffery W. Brown, Michale Cross, Jason Harper, Stace Cunningham, Mission Critical Internet SecuritySyngress Publishing , Inc. 2001

Managing Cisco Networks, Michael Winstrom, Cisco Press, 2001

In addition to the below sites it seemed like the Entire Internet was surfed in research.

Cisco

[Cisco 3600 4-slot Modular Router-AC](#)

[IP/FW/IDS](#)

[information signatures](#)

[attack signatures](#)

[PIX 525UR Bundle \(Chassis, unrestricted SW, 2 FE ports\)](#)

[WS-C2924-XL-EN 24-port 10/100 Switch \(Enterprise Edition\)](#)

CBAC

<http://www.cisco.com/warp/public/707/index.shtml#IOS>

Miscellaneous

[SonicWALL PRO-VX](#)

[Zeus Load Balancer](#)

[SysMaster](#)

[Tripwire](#)

SANS

How To Eliminate The Ten Most Critical Internet Security Threats

The Experts' Consensus

Version 1.33 June 25, 2001

Copyright 2000 - 2001, The SANS Institute

<http://www.sans.org/topten.htm> (21/07/2001)

Distributed Denial of Service attack

<http://grc.com/dos/intro.htm> (25/07/01)

DDoS against PIX

<http://www.shmoo.com/mail/firewalls/apr00/msg00030.shtml> (25/07/01)

PIX 515 version 5.31 vulnerabilities

<http://www.securityfocus.com> (25/07/01)

BIND Exploits

<http://maclux-rz.uibk.ac.at/~maillists/vuln-dev/msg00113.shtml> (4/7/01)

<http://securityportal.com/cover/coverstory20001113.html> (4/7/01)

<http://www.enteract.com/~lspitz/NXT-Howto.txt>