Global Information Assurance Certification Paper

GIAC Enterprises
Security Requirements

Table of Contents

GIAC ENTERPRISES REQUIREMENTS 3

TASKS 3
Security architecture 3
Security Policy 4
Audit your Security Architecture 4
Design Under Fire 5

ASSUMPTIONS 5

SECURITY ARCHITECTURE 6

DESCRIPTION OF GIAC ENTERPRISES NETWORK ARCHITECTURE 6

SECURITY POLICY 7

INITIAL OPERATIONAL PROCEDURES 7

GIAC ENTERPRISES HOST INVENTORY 7

EXTERNAL NETWORK 7
INTERNAL NETWORK 7
NETWORK MANAGEMENT NETWORK 8
SERVICES 8
BANNERS AND MESSAGE OF THE DAY (MOTD) 8
EXTERNAL PASSWORDS 8
NETWORK ACCESS 8
Database 8
Network Management 8
Internal Network 8
GIAC Enterprises Access 8
EXTERNAL SERVER AUDITING 9
BATCH PROCESSING 9
BORDER AND CORE ROUTER BASE SECURITY CONFIGURATION 9
FIREWALLS 10
INTRUSION DETECTION SYSTEMS (IDS) 10

DEVICE SPECIFIC CONFIGURATIONS 10

BORDER ROUTER CONFIGURATION 10
Physical Access 10
Border Router & Stateful Inspection 10
CBAC and IPSec Compatibility 11
Outbound Access Lists 11
Inbound Access Lists 11
Note: IPSec protocols and key exchange protocols 12
IPSEC CONFIGURATION 13
GIAC Border Router IPSec configuration 13
Partner Router IPSec configuration 13
Supplier IPSec Configuration 14
IPSec Implementation Warning: 15
CORE ROUTER CONFIGURATION 15
Outbound Access Lists 15
Inbound Access Lists 16
FIREWALL, FW-A1 16
FIREWALL, FW-C1 17
INTRUSION DETECTION SYSTEMS (IDS) POLICY 18

AUDIT THE DESIGN 18

STEP 1- INFORMATION GATHERING; PUBLIC NETWORK 18
STEP 2- INFORMATION GATHERING; INTERNAL NETWORK (THROUGH FIREWALL) 18
STEP 3- BEGIN PORT SCANNING 19
NMAP USAGE 19
STEP 4- CONCURRENT SYSLOG AND IDS LOGGING 21
STEP 5- WAR DIALING 22
ROUTER TESTING AND DIAGNOSTICS 22
FOR FIREWALL TROUBLESHOOTING AND TESTING 23
DESIGN UNDER FIRE 23
STEP 1- INFORMATION GATHERING 24
SAMPLE OUTPUT for DNS zone transfer 24
STEP 2- PORT SCAN FOR VULNERABLE SERVICES 25
STEP 3- QUICK SNMP SCAN 25
STEP 4- REVIEW AND PLAN THE INTRUSION/ATTACK 26
REFERENCES 26

Table of Tables

TABLE 1: EXTERNAL HOST INVENTORY 7
TABLE 2: INTERNAL HOST INVENTORY 7
TABLE 3: MANAGEMENT NETWORK HOST INVENTORY 8

Table of Figures

FIGURE 1: ILLUSTRATES THE RECOMMENDED SECURITY ARCHITECTURE FOR GIAC ENTERPRISES. 6
FIGURE 2 24

GIAC Enterprises Requirements

Tasks

Security architecture

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense 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).

Security Policy

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

- Border Router
- Primary Firewall
- VPN

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

By 'security policy' we mean the specific ACLs, firewall 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 behavior of the service or protocol on the network.
3. The syntax of the ACL, filters, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

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

Audit your Security Architecture

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

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

2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

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

Design Under Fire

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

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

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

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

Assumptions

The focus of this document will be on network infrastructure and access methods. All servers will be updated to the most current revision and security patch level. Users will be trained on GIAC Enterprise internal security policies. While data exists on the external servers, before batch process backup occurs, it will be encrypted. UID will remain the same across all systems to ensure user identity throughout the network by logging systems.

Security Architecture

The following diagram is our proposed security architecture designed to meet the needs outlined in the GIAC Enterprises requirement section.

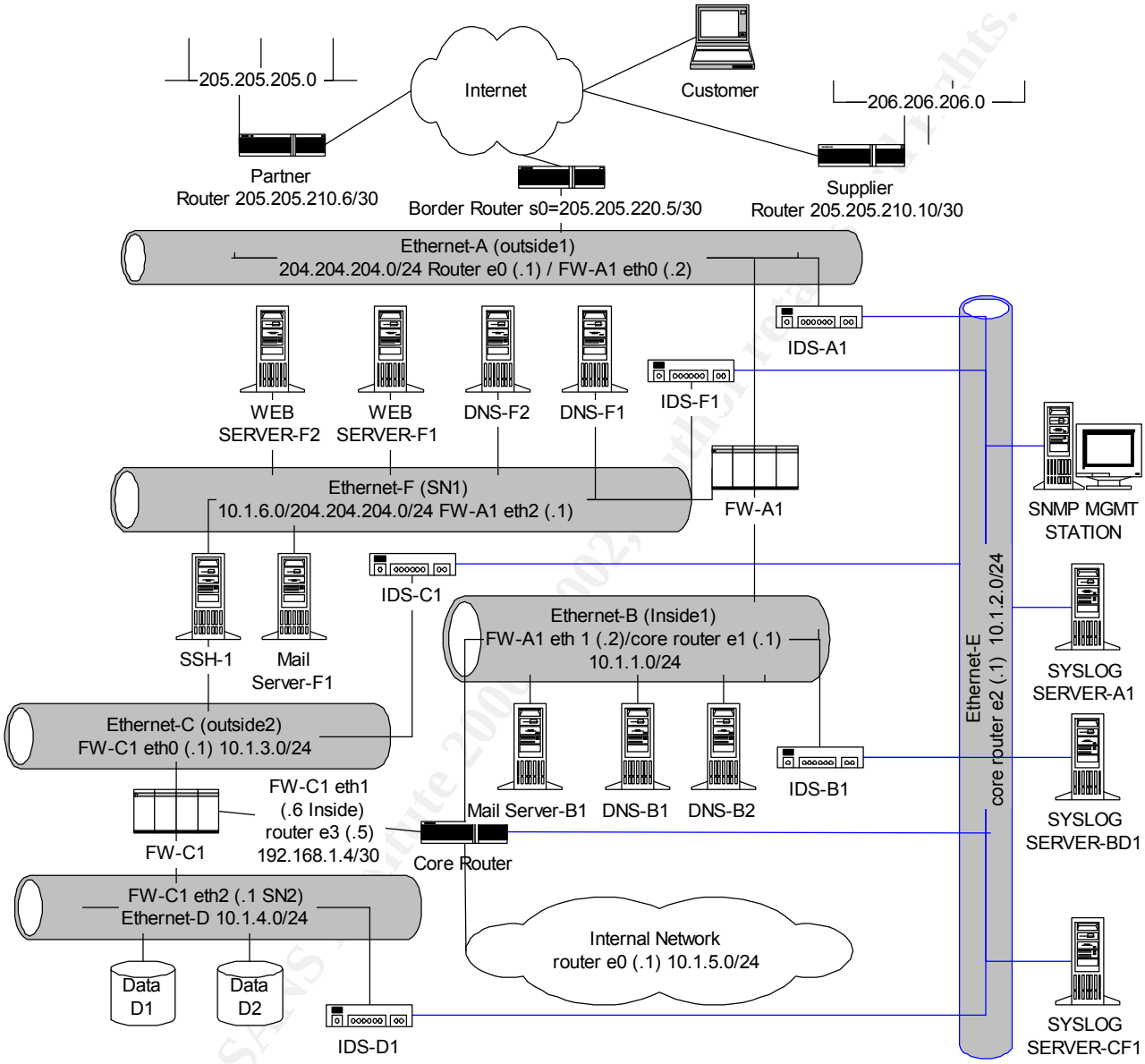

Figure 1: Illustrates the recommended security architecture for GIAC Enterprises.

Description of GIAC Enterprises Network Architecture

The border router is a Cisco 3640, running on an IP Firewall Plus IPSec 56 IOS, with one serial and two Fast Ethernet interfaces. The core router is a Cisco router with a current image providing Fast Ethernet connectivity to the internal networks. The cloud representing the internal network comprises the initial network that was setup to aid in the administrative tasks of startup operations for GIAC Enterprises and has less than 100 employees connected to it. The computing environment is comprised of both Microsoft systems for the user environment and several Linux and Solaris UNIX machines that were used for the development of the database systems that would be needed to support the companies current business

plans. User authentication is done utilizing NT primary and backup domain controllers. All internal network access is based on strong user/password authentication. Current remote access has been performed via dial-in access, in the past, to modems connected to user workstations and servers, with simple user/password authentication.

Security Policy

Initial Operational Procedures

The method of remote access via modem will be discontinued immediately. Security auditing using war-dialer software to find any remaining violations of this policy will be performed bi-monthly. IPSec [5] and SSH version2 [3] will be implemented in combination as a VPN architecture for supplier and partner access.

GIAC Enterprises Host Inventory

Before developing the diagram of the new architecture, an inventory of current and future hosts has been performed. The result of the inventory is listed below in Tables 1 through three.

External Network

Hostname	Inside Address	Outside Address
Border Router Egress (e0)	204.204.204.1	
Border Router Ingress (s0)	67.67.67.5	
FW-A1 e0	204.204.204.2	outside1
FW-A1 e1	10.1.1.2	inside1
FW-A1 e2	10.1.6.1	sn1
Mail Server-F1	10.1.6.104	204.204.204.104
Web Server-F1	10.1.6.100	204.204.204.100
Web Server-F2	10.1.6.101	204.204.204.101
DNS Server-F1	10.1.6.103	204.204.204.103
DNS Server-F2	10.1.6.102	204.204.204.102
SSH-F1 e0	10.1.6.200	204.204.204.200
VPN-AC	10.1.3.15	204.204.204.15
SSH-F1 e1	10.1.3.200	

Table 1: External Host Inventory

Internal Network

Hostname	Inside Address	Outside Address
Core Router e0	10.1.5.1	
Core Router e1	10.1.1.1	
Core Router e2	101.2.1	
Core Router e3	192.168.1.5	
VPN-AE	10.1.2.16	204.204.204.16
Users/internal servers	10.1.5.20-254	
FW-C1 e0	10.1.3.1	outside2
FW-C1 e1	192.168.1.6	inside2
FW-C1 e2	10.1.4.1	sn2
Mail Server-B1	10.1.6.104	204.204.204.104
DNS Server-B1	10.1.6.103	204.204.204.103
DNS Server-B2	10.1.6.102	204.204.204.102

Table 2: Internal Host Inventory

Network Management Network

Hostname	Inside Address	Outside Address
SNMP-E1	10.1.2.50	
SYSLOG-A1	10.1.2.100	
SYSLOG-BD1	10.1.2.101	
SYSLOG-CF1	10.1.2.102	
IDS-A1	10.1.2.200	unnumbered
IDS-B1	10.1.2.201	unnumbered
IDS-C1	10.1.2.202	unnumbered
IDS-D1	10.1.2.203	unnumbered
IDS-F1	10.1.2.204	unnumbered

Table 3: Management Network Host Inventory

Services

The base configuration for all routers onsite will be to disable all unnecessary services that can be used to gather information from the routers, both internally and externally.

Banners and message of the day (MOTD)

All application specific banners will be modified to conceal the identity of the application type and version, replacing them with legal notices. Also all MOTD will state the legal implications to misuse of the system and state the fact that violations will be prosecuted. Violations will consist of intrusion, exceeding authority within any of the systems and services, etc.

External passwords

Administrative passwords on the border router and External servers, located on Ethernet F, will be different from internal network device passwords. Key network management personnel will change passwords every thirty days.

Network Access

Database

No direct access will be given to the database network. Internet sales functions (Customer credit card information storage and trending) and database administration will be performed on Ethernet D.

Network Management

No direct access, by users, will be allowed to the management network, Ethernet E. All traffic to and from Ethernet E will be required to conform to this security policy.

Internal Network

Users will have access to the user network and to Ethernet B and the internal network, where domain servers reside. Internet access will also be allowed for http and email access. No other protocols will be allowed to traverse the core router from the internal network to the Internet.

GIAC Enterprises Access

GIAC Enterprises customer access

Customer access will be provided via Linux based web servers, Web Server-F1 and Web Server-F2, running HTTP and HTTPS. Each Linux server has been updated with the latest security patches. Orders will be placed on these servers and batch processes will collect the data on an hourly basis, removing all customer information each hour.

Internal administrative access

Remote administration will be performed via SSH2 access [3].

Supplier/Partner Access

Partner- provides fortune cookie translation services to GIAC Enterprises. Each partner will have a secured folder on the web server. The partners cannot access any other locations on the web server. Bulk fortune cookie sayings are placed in the appropriate folders by batch database processes on a nightly basis, as defined by the database administrator, for partners to download for translation.

Supplier- provides the raw fortune cookie sayings to GIAC Enterprises. SSH-F1 will be setup with folders for each supplier in the same manner that partner access is implemented.

Access Method- A decision was made to utilize Secure Shell (SSH) version 2 for both partner and suppliers access, instead of VPN gateway technologies. 3DES encryption with 1024-bit length will be implemented. All file transfers will be with secure copy (scp), the file transfer utility included with SSH. In addition, to SSH access to the folders each partner and supplier must setup IPSec authentication using pre-shared keys. The routers will maintain security associations for partners and suppliers, which is where the IPSec will be implemented. The combination of SSH encryption and IPSec authentication is believed to be adequate for this business operation. This will also serve to eliminate telnet access to the web servers. Access could also have been provided by SSL transport but the IPSec/SSH was chosen instead due to the bulk nature of task to be performed by both suppliers and partners.

Physical Access

All communications and server equipment will be located in one room that implements access card readers. The network management network, Ethernet E, as well as personnel are also housed in this area of the facility.

External Server Auditing

All servers on Ethernet F1 will have tripwire [1] running on them for nightly auditing of changes to sensitive files and folders, as well as host sentry [2] to detect any intrusions at the host level. Batch processes will copy logs to secure location on management network, Ethernet E. This level of auditing is in addition to the IDS listening on the LAN. A non-networked management machine will gather console port logging information for the border router via the serial port.

Batch Processing

All mention of batch processes refers to data collection that is performed by internal network management devices that initiate the collection process. This is to allow collection without opening pinholes toward the internal network.

Border and Core Router base security configuration

Basic measures are to be taken to prevent known vulnerabilities inherent to networks in general and specifically to known router weaknesses. In global configuration mode we will disable small services, finger, pad, ip directed broadcast, ip proxy arp, ip source route, cdp, and bootp.

```
********** Begin base **********************
! prevents exploits against chargen, echo, discard, and daytime services using both udp and tcp
no service tcp-small-servers
no service udp-small-servers
! prevents information gathering of user activity
no service finger
no service pad
! prevents routing tables, configurations, adjacent neighbors from being given
no cdp run
! prevents users from manipulating the path of their routes through the network
no ip source-route
```

```
! prevents forwarding of directed broadcast that could be used as a denial of service attack
no ip directed-broadcast
! prevents the router from providing MAC addresses of its networks to other hosts.
no ip proxy arp
! prevents devices from gathering configuration files, also prevents devices from providing bogus
! false configuration information
no ip bootp server
********** End base **********
```

Firewalls

The two firewalls will be used as choke points to the database and internal networks. Both firewalls will enable logging capabilities. Firewall syslog messages will be destined for the management network, via the inside interfaces, from each firewall.

Intrusion Detection Systems (IDS)

The IDS devices will be made up of Linux machines running Snort. The interface touching the networks being monitored will be unnumbered. All IDS collection interfaces will be connected directly to the management LAN, Ethernet E.

Device Specific Configurations

Border Router Configuration

The border router provides Internet connectivity. The border router has the IP Firewall Plus IPSec 56 IOS image loaded on it. This IOS also includes a feature known as CBAC Content Based Access Control. CBAC will allow a form of stateful inspection.

Physical Access

Auxiliary port

The auxiliary port will also be disabled on the border router, in the configuration using the following commands:

```
line aux 0
no exec
transport input none
```

Console Port

The console port will be directly connected to a dedicated non-network machine that will maintain logging information of console error messages.

Logging and Timestamps

Logging timestamps need an accurate detailed output, which will be synchronized via NTP.

```
! maintain uniform timestamps
service timestamps log date time local time show time zone
```

System logging will be made to the console port.

```
logging on
logging console information
```

Border Router & Stateful Inspection

According to Cisco literature "CBAC—Provides secure, per-application access control for all IP

traffic across perimeters (for example, between private enterprise networks and the Internet)"
The following rules have been defined:
int s0
ip inspect inbound in
ip inspect name inbound http timeout 3600
ip inspect name inbound smtp timeout 3600
ip inspect name inbound tcp timeout 3600
ip inspect name inbound udp timeout 15

Note: We have also set a timeout on each of these to illustrate that this is definable.

CBAC and IPSec Compatibility

Due to the fact that we will utilize CBAC and IPSec on the same router, the following consideration has been noted. When CBAC and IPSec are enabled on the same router, and the target router is an endpoint for IPSec for the particular flow, then IPSec is compatible with CBAC (that is, CBAC can do its normal inspection processing on the flow). If the router is not an IPSec endpoint, but the packet is an IPSec packet, then CBAC will not inspect the packets because the protocol number in the IP header of the IPSec packet is not TCP or UDP. CBAC only inspects UDP and TCP packets. [5]

Outbound Access Lists

The following protocols will be denied for all outbound traffic to prevent information gathering or leakage of information from internal devices, either by accident or on purpose.

Throughout this document, since we implement total Cisco solutions, access lists follow this convention:

access-list <list name or number> permit|deny <protocol> <source IP> <source mask> <source port> <destination IP> <destination mask> <destination port>

Access lists operate top down, meaning that the topmost list entry is read first then the next and then the next. List order matters. One entry if improperly worded can allow traffic, intended to be blocked, to pass through.

Serial 0
! log attempted snmp traffic
access-list 102 deny udp any any eq 161 log
access-list 102 deny udp any any eq 162 log
! log attempted syslog traffic
access-list 102 deny udp any any eq 514 log
! Permit any traffic not specified above to leave the network.
access-list 102 permit ip any any

Inbound Access Lists

Next anti-spoofing rules will be placed in the router starting with the private network address space. The private 10-network address space resides on the internal network but should not be seen as source addresses entering the network from the outside. In addition, the protocols listed below will not be allowed to enter the network for the same reasons as listed above. These will be applied to serial 0.

Serial 0

```
! we will not apply and established rule use to the fact that we implement CBAC.
! Deny private net spoofing
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 171.16.0 0.240.255.255 any
access-list 101 deny ip 192.168.0 0.0.255.255 any
! the following also denies spoofing of our internal 10 network addresses as a source.
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
! deny multicast traffic
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
! Just for the sake curiosity, we will log our public network if it is seen spoofed inbound.
access-list 101 deny ip 204.204.204.0 0.255.255.255 any log
! denied services
!log attempted snmp traffic
access-list 101 deny udp any any eq 161 log
access-list 101 deny udp any any eq 162 log
! log attempted zone transfers
access-list 101 deny tcp any any eq 53 log
! log attempted syslog traffic
access-list 101 deny udp any any eq 514 log
! Allowed services
! mail, http, https, dns and ssh are allowed in
access-list 101 permit tcp any host 204.204.204.104 eq 25
access-list 101 permit tcp any host 204.204.204.100 eq 80
access-list 101 permit tcp any host 204.204.204.101 eq 80
access-list 101 permit tcp any host 204.204.204.100 eq 443
access-list 101 permit tcp any host 204.204.204.101 eq 443
access-list 101 permit udp any host 204.204.204.102 eq 53
access-list 101 permit udp any host 204.204.204.103 eq 53
access-list 101 permit udp any any eq 500
access-list 101 permit ip any any eq 51
access-list 101 permit ip any any eq 50
! Partner and supplier access method
access-list 101 permit tcp partner_network host 204.204.204.200 eq 22
access-list 101 permit tcp supplier_network host 204.204.204.200 eq 22
! Deny all other traffic
access-list 101 deny ip any any
```

Note: IPSec protocols and key exchange protocols

IPSec uses IP protocols 50 and 51, and IKE traffic passes on protocol 17, port 500 (UDP 500). We must ensure that these are permitted appropriately for to allow only those networks that we wish to allow access to our network using IPSec, as listed above. [5]

Enable Access Lists

```
! Note that the following interface configuration applies access list 102 to
! inbound traffic at the external serial interface. (Inbound traffic is
! entering the network.) When CBAC inspection occurs on traffic exiting the
! network, temporary openings will be added to access list 101 to allow returning
! traffic that is part of existing sessions.
!
int s0
access-group 101 out
```

access-group 102 in

IPSec Configuration

The following configuration commands set up the IPSec configuration that we will use for partners and suppliers. In combination with IPSec, for authentication, and SSH2, for encryption, we will effectively have a reasonably fast VPN solution with the limited resources on hand.

GIAC Border Router IPSec configuration

This access list if used to create the IPSec security associations used by the IPSec configuration between partner and supplier networks. In our case, everything between these networks is authenticated, encryption is provided by SSH version 2.

```
access-list 110 permit ip 205.205.205.0 0.255.255.255 204.204.204.0 0.255.255.255
access-list 110 permit ip 206.206.206.0 0.255.255.255 204.204.204.0 0.255.255.255

The following commands setup IPSec for this router.
! setup IPSec
crypto isakmp policy 1

! Setup pre authentication policy, pre-share in this case
authentication pre-share

! set the transform set, which states the type of encryption to use for pre-share keys
crypto ipsec transform-set fortunecookies ah-sha-hmac

! setup the shared keys. This must be the same for each peer routers defined.
crypto isakmp key partner_key address 205.205.210.6
crypto isakmp key supplier_key address 205.205.210.10

! Setup the crypto map for the partner router
crypto map giac 1 ipsec-isakmp
set peer 205.205.210.6
set transform-set fortunecookies
match address 110

! setup crypto map for the supplier router
crypto map giac 2 ipsec-isakmp
set peer 205.205.210.10
set transform-set fortunecookies
match address 110

! apply these crypto maps to the ingress of the border router

int s0
  crypto map giac
```

Partner Router IPSec configuration

The partner router is also a Cisco 3640 router implementing a current IPSec IOS. This access list if used to create the IPSec security associations used by the IPSec configuration between partner and supplier networks. In our case, everything between these networks is authenticated,

encryption is provided by SSH version 2.

access-list 110 permit ip 204.204.204.0 0.255.255.255 205.205.205.0 0.255.255.255

The following commands setup IPSec for this router.

```
! setup IPSec
crypto isakmp policy 1

! Setup pre authentication policy, pre-share in this case
authentication pre-share

! set the transform set, which states the type of encryption to use for pre-share keys
crypto ipsec transform-set fortunecookies ah-sha-hmac

! setup the shared keys. This must be the same for each peer routers defined.
crypto isakmp key partner_key address 205.205.220.5

! Setup the crypto map for the giac router
crypto map giac 1 ipsec-isakmp
set peer 205.205.220.5
set transform-set fortunecookies
match address 110

! apply these crypto maps to the ingress of the border router

int s0
  crypto map giac
```

Supplier IPSec Configuration

The supplier router is also Cisco 3640 router implementing a current IPSec IOS. This access list if used to create the IPSec security associations used by the IPSec configuration between partner and supplier networks. In our case, everything between these networks is authenticated, encryption is provided by SSH version 2.

access-list 110 permit ip 204.204.204.0 0.255.255.255 206.206.206.0 0.255.255.255

The following commands setup IPSec for this router.

```
! setup IPSec
crypto isakmp policy 1

! Setup pre authentication policy, pre-share in this case
authentication pre-share

! set the transform set, which states the type of encryption to use for pre-share keys
crypto ipsec transform-set fortunecookies ah-sha-hmac

! setup the shared keys. This must be the same for each peer routers defined.
crypto isakmp key supplier_key address 205.205.220.5

! setup crypto map for the giac router
crypto map giac 2 ipsec-isakmp
set peer 205.205.220.5
```

```
set transform-set fortunecookies
match address 110

! apply these crypto maps to the ingress of the border router

int s0
  crypto map giac
```

IPSec Implementation Warning:

One note when applying IPSec on a Cisco router is to ensure that each location has someone performing the configuration on the console port, either via modem or physically at the location. Trying to perform the access-list entry or the crypto commands remotely can lead to connectivity issues. This needs to be performed at the same time as well to limit the amount of downtime at the level being protected.

Core Router Configuration

The core router provides access for internal network routing. It also provides connectivity for network management, database, and Internet edge networks.

Cisco routers utilize packet-filtering techniques known as access lists. The syntacx of an access list is:

Outbound Access Lists

Access list will allow only management traffic to and from Ethernet E.
Internet connectivity will not be allowed to Ethernet E.

Ethernet 0

```
! e0 outbound access list;  To internal
no rules needed
```

Ethernet 1

```
! e1 outbound access list;  To FW-A1
no rules needed, they will be implemented o the firewall.
```

Ethernet 2

```
! e2 outbound access-list ; To management
! need to restrict network traffic going in and out of management LAN
access-list 100 permit tcp any any eq 22
access-list 100 permit udp any any eq 162
access-list 100 permit udp any any eq 514
access-list 100 permit icmp 10.1.2.0 0.0.0.255 any
! Deny all other traffic
access-list 100 deny ip any any
```

Ethernet 3

```
! e3 to outbound access list; To FW-C1
! allow anything between management network and database network
access-list 102 permit ip 10.1.2.0 0.0.0.255 10.1.4.0 0.0.0.255
```

```
access-list 102 permit icmp 10.1.2.0 0.0.0.255 10.1.4.0 0.0.0.255
! deny all other traffic through this interface
access-list 102 deny ip any any
```

Inbound Access Lists

Ethernet 0

```
! e0 inbound access-list;From Internal
no rules needed
```

Ethernet 1

```
! e1 inbound access-list; From FW-A1
no rules needed
```

Ethernet 2

```
! e2 inbound access-list; From management
access-list 101 permit tcp any any eq 22
access-list 101 permit tcp 10.1.2.0 0.0.0.255 any eq 23
access-list 101 permit udp any any eq 161
! allow web management of internal switches and servers
access-list 101 permit tcp 10.1.2.0 0.0.0.255 10.1.0.0 0.0.255.255 eq 80
! Deny all other traffic
access-list 101 deny ip any any
```

Ethernet 3

```
! e3 inbound access-list; from FW-C1
access-list 103 permit ip 10.1.4.0 0.0.0.255  10.1.2.0 0.0.0.255
access-list 103 permit icmp 10.1.4.0 0.0.0.255  10.1.2.0 0.0.0.255
access-list 103 deny ip any any
```

Apply Access Lists

```
Int e2
Ip access-group 100 out
Ip access-group 101 in
Int e0
Ip access-group 102 out
Ip access-group 103 in
```

Firewall, FW-A1

Firewall FW-A1 is a Cisco PIX 525 used to access the Internet and service network, the latter has sole access to the database network for queries and updates.

```
! define interfaces
nameif ethernet0 outside1 security0
nameif ethernet1 inside1 security100
nameif ethernet2 sn1 security50

! define global address for nat
global (outside1) 1 204.204.204.10

! define nat for service network and internal network
```

```
nat (sn1) 1 10.1.6.0 255.255.255.0 0 0
nat (inside1) 1 10.0.0.0 255.0.0.0

! define static translations for SSH, web, mail, and dns servers
! together with conduit commands allows Internet access to the publicly offered services
Static (sn1, outside1) 204.204.204.100 10.1.6.100 netmask 255.255.255.255 0 0
Static (sn1, outside1) 204.204.204.100 10.1.6.101 netmask 255.255.255.255 0 0
Static (sn1, outside1) 204.204.204.100 10.1.6.102 netmask 255.255.255.255 0 0
Static (sn1, outside1) 204.204.204.100 10.1.6.103 netmask 255.255.255.255 0 0
Static (sn1, outside1) 204.204.204.100 10.1.6.104 netmask 255.255.255.255 0 0
Static (sn1, outside1) 204.204.204.100 10.1.6.200 netmask 255.255.255.255 0 0
Static (inside,sn1) 204.204.204.104 10.1.6.104 netmask 255.255.255.255 0 0
Static (inside,sn1) 204.204.204.104 10.1.6.102 netmask 255.255.255.255 0 0
Static (inside,sn1) 204.204.204.104 10.1.6.103 netmask 255.255.255.255 0 0

Conduit permit tcp host 204.204.204.100 eq 80 any
Conduit permit tcp host 204.204.204.101 eq 80 any
Conduit permit tcp host 204.204.204.100 eq 443 any
Conduit permit tcp host 204.204.204.101 eq 443 any
Conduit permit udp host 204.204.204.102 eq 53 any
Conduit permit udp host 204.204.204.103 eq 53 any
Conduit permit tcp host 204.204.204.104 eq 25 any
Conduit permit tcp host 204.204.204.200 eq 22 any

Conduit permit tcp host 204.204.204.104 eq 25 10.1.1.104
Conduit permit tcp host 204.204.204.103 eq 53 10.1.1.102
Conduit permit tcp host 204.204.204.103 eq 53 10.1.1.103

Access-list 190 permit tcp 10.0.0.0 255.0.0.0 any eq 80
Access-list 190 permit tcp 10.0.0.0 255.0.0.0 any eq 443
Access-list 190 deny ip 10.0.0.0 255.0.0.0 any


Access-group 190 in interface inside1
```

Service network will only allow Internet based communications to the SSL server; on port 80 and 443, nothing can establish connectivity to the Internet from the service network.

Firewall, FW-C1

Firewall FW-C1 is a Cisco PIX 525 and offers protection for the database network from any attacks that might make it through the border router and FW-A1. It also provides a single point of access for Ethernet C and Ethernet D management traffic.

```
! define interfaces
nameif ethernet0 outside2 security0
nameif ethernet1 inside2 security100
nameif ethernet2 sn2 security50

! disable nat for service network and internal network
nat (sn2) 0
nat (inside2) 0
```

```
access-list 1 permit ip 10.1.4.0 255.255.255.0 10.1.3.2 255.255.255.0
access-group 1 in interface sn2

access-list 2 permit ip 10.1.2.0 255.255.255.0 10.1.3.0 255.255.255.0
access-list 2 permit ip 10.1.2.0 255.255.255.0 10.1.4.0 255.255.255.0
access-group 2 in interface inside2
```

Intrusion Detection Systems (IDS) Policy

The intrusion detection of choice is snort, which is a packet sniffer that can determine whether an intrusion or attack is occurring based on signatures that are configurable. Snort will be implemented on Linux machines, as stated earlier.

The Linux machines will have two NICs, one of which is unnumbered and the other that is addressed and connected to Ethernet E, the management network. The unnumbered interface connects to the target network to detect anomalies. The IDS only function is that of detection.

All of the rules listed on the snort web site, except for those with high false alarms or in beta state are applied on each IDS. snortsnarf is used to manage the snort systems as well as snortnet to manage the many IDS implemented onsite. [4]

Audit the Design

The following steps have been defined to evaluate the strength of security implemented on the network. The audit will occur during normal business hours to mingle scanning traffic with normal traffic to test the IDS systems, as well as the administrators' ability to recognize such anomalies. The level of effort for this audit is actually quite low since the majority of it will be scripted ahead of time. The actual audit may take no more than 3 hours to perform given the size of the network. Since this audit will occur during normal business hours, a team consisting of one person from each department will be gathered as a quick response team in the event that services become disrupted.

Step 1- Information Gathering; Public Network

UDP and TCP port Scanning will be performed against all public address space on the perimeter of the network. The tool of choice will be nmap performed on a Linux laptop. Full logging of the scan will be performed and a report will be generated indicating any ports other than the ones allowed through the firewall.

Step 2- Information Gathering; Internal Network (Through Firewall)

UDP and TCP port Scanning will be performed against all private network address space used internally, spoofing private addresses as the source IP of the scan, on the perimeter of the network to see if any get through the firewall. The router should prevent all of these packets from passing through. The tool of choice will be nmap [4] performed on a Linux laptop.

Some of the features that I will use to determine the security of the network are listed as follows on the nmap website:

" Specifically, nmap supports:
Vanilla TCP connect () scanning,
TCP SYN (half open) scanning,
TCP FIN, Xmas, or NULL (stealth) scanning,
TCP ftp proxy (bounce attack) scanning
SYN/FIN scanning using IP fragments (bypasses some packet filters),

TCP ACK and Window scanning,
UDP raw ICMP port unreachable scanning,
ICMP scanning (ping-sweep)
TCP Ping scanning
Direct (non portmapper) RPC scanning
Remote OS Identification by TCP/IP Fingerprinting, and
Reverse-ident scanning.

Nmap also supports a number of performance and reliability features such as dynamic delay time calculations, packet timeout and retransmission, parallel port scanning, detection of down hosts via parallel pings.

Nmap also offers flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, and output to machine parseable or human readable log files. " [4]

Full logging of the scan will be performed by the IDS systems installed at each level of the network and reports will be generated indicating any ports that responded other than the ones allowed through the firewall, as defined in the security policy.

Step 3- Begin Port Scanning

UDP and TCP port Scanning will be performed against all private address space used internally. The tool of choice will be nmap performed on a Linux laptop. Full logging of the scan will be performed and a report will be generated indicating any ports other than the ones allowed through the firewall.

NMAP USAGE

Public Network Assessment

Fist lets define the flags used by nmap before we discuss the details of our assessment. The following flags, -v = verbose mode, -sS = TCP SYN scan, -sF= TCP FIN scan, -sN=TCP NULL Scan, -sX= TCP XMAS tree Scan (more on this later), -sP= Ping scan (this is actually performed with the other modes to scan only live targets but I will include it here as a full example), -sU= UDP port scanning (good way to find those backdoor and SUN RPC vulnerabilities, among other things), -sT= TCP port Scan, -O = OS detection, -oN <filename> logs everything to the file named.

To assess the public network on Ethernet F the following commands are issued:

```
nmap -sS -O -v -oN public.log 204.204.204.0/24
nmap -sF -O -v -oN public.log 204.204.204.0/24
nmap -sN -O -v -oN public.log 204.204.204.0/24
nmap -sX -O -v -oN public.log 204.204.204.0/24
nmap -sP -O -v -oN public.log 204.204.204.0/24
nmap -sU -O -v -oN public.log 204.204.204.0/24
nmap -sT -O -v -oN public.log 204.204.204.0/24
```

See the internal scans to view a description of scans above.

Launches a stealth SYN scan against each machine that is up out of the entire class C network. It also tries to determine what operating system is running on each host that is up and running. This requires root privileges because of the SYN scan and the OS detection.

Internal Network Assessment

Determine that the firewall does not allow SYN packets, which sends a SYN packet and waits for a response (RST means not listening, SYN ACK means listening), through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sS -O -v -oN internal.log 10.1.1.0/24
nmap -sS -O -v -oN internal.log 10.1.2.0/24
nmap -sS -O -v -oN internal.log 10.1.3.0/24
nmap -sS -O -v -oN internal.log 10.1.4.0/24
nmap -sS -O -v -oN internal.log 10.1.5.0/24
nmap -sS -O -v -oN internal.log 10.1.6.0/24
```

Determine that the firewall does not allow FIN scans; a bare FIN is sent as a probe, through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sF -O -v -oN internal.log 10.1.1.0/24
nmap -sF -O -v -oN internal.log 10.1.2.0/24
nmap -sF -O -v -oN internal.log 10.1.3.0/24
nmap -sF -O -v -oN internal.log 10.1.4.0/24
nmap -sF -O -v -oN internal.log 10.1.5.0/24
nmap -sF -O -v -oN internal.log 10.1.6.0/24
```

Determine that the firewall does not allow NULL scans, which turns off all TCP flags, through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sN -O -v -oN internal.log 10.1.1.0/24
nmap -sN -O -v -oN internal.log 10.1.2.0/24
nmap -sN -O -v -oN internal.log 10.1.3.0/24
nmap -sN -O -v -oN internal.log 10.1.4.0/24
nmap -sN -O -v -oN internal.log 10.1.5.0/24
nmap -sN -O -v -oN internal.log 10.1.6.0/24
```

Determine that the firewall does not allow XMAS tree scans (which turns on the FIN, URG, and PUSH flags), through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sX -O -v -oN internal.log 10.1.1.0/24
nmap -sX -O -v -oN internal.log 10.1.2.0/24
nmap -sX -O -v -oN internal.log 10.1.3.0/24
nmap -sX -O -v -oN internal.log 10.1.4.0/24
nmap -sX -O -v -oN internal.log 10.1.5.0/24
nmap -sX -O -v -oN internal.log 10.1.6.0/24
```

Determine that the firewall does not allow UDP connections through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sU -O -v -oN internal.log 10.1.1.0/24
nmap -sU -O -v -oN internal.log 10.1.2.0/24
```

```
nmap -sU -O -v -oN internal.log 10.1.3.0/24
nmap -sU -O -v -oN internal.log 10.1.4.0/24
nmap -sU -O -v -oN internal.log 10.1.5.0/24
nmap -sU -v -oN internal.log -O 10.1.6.0/24
```

Determine that the firewall does not allow TCP connections through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sT -O -v -oN internal.log 10.1.1.0/24
nmap -sT -O -v -oN internal.log 10.1.2.0/24
nmap -sT -O -v -oN internal.log 10.1.3.0/24
nmap -sT -O -v -oN internal.log 10.1.4.0/24
nmap -sT -O -v -oN internal.log 10.1.5.0/24
nmap -sT -O -v -oN internal.log 10.1.6.0/24
```

Determine that the firewall does not allow pinging through to the internal networks. This should not be possible due to the fact that the networks are behind an implementation of NAT.

```
nmap -sP -O -v -oN internal.log 10.1.1.0/24
nmap -sP -O -v -oN internal.log 10.1.2.0/24
nmap -sP -O -v -oN internal.log 10.1.3.0/24
nmap -sP -O -v -oN internal.log 10.1.4.0/24
nmap -sP -O -v -oN internal.log 10.1.5.0/24
nmap -sP -O -v -oN internal.log 10.1.6.0/24
```

These scans also include the -O flag. This instructs nmap to try to determine the OS of the target machines.

Results of Port Scans

Logging results should yield information such as web server F1 and Web server F2 having port 80 and port 443 open, Mail Server F1 listening on port 25, etc. Any ports other than these such as some of the default services sometimes seen running on Sun and Linux machines such as finger, portmapper etc, that were not intended to be functional would require attention. The recommended action would be to disable those services. In our case, only those services specifically intended for public use were enabled all other services found in inetd and in the startup scripts (typically found under /etc/rc.d/init.d, have beed disabled). In addition, ip forwarding and routed have been disabled on all public servers (and on all internal servers for that matter. The only devices allowed to route on this network are the core router. None of the devices are running routing protocols, as static routing has been implemented network wide.

Step 4- Concurrent Syslog and IDS Logging

In addition to Step 1, 2, and 3 logging performed by nmap during the scan, and by the router and firewall, the internal intrusion detection systems will also be logging all activity as it would in real time to verify the results of the port scanning. Careful attention will be paid to each level of the network using snort logs gleaned form the IDS' throughout the network.

Step 5- Login Password Guessing

Brute force password guessing will be conducted using Expect scripts [9] and dictionaries, against the routers, and any devices running rlogin, ftp, telnet, ssh/scp (if it is determined that

the device is ssh version 1 compatible, which doesn't disable x-number of failed logins). Expect is a script language that provides interaction with devices that require human interaction. A script can be setup to receive a response from a device and enter a response as if someone were typing it in at a console. Utilizing a list of common usernames and passwords is a simple undertaking when using Expect. This a short simple attempt to determine the complexity of password choices used for administration, as well as to determine if there are mechanisms to disable bad logins after x-number of failed logins. If any of these services can be compromised then the site can be deemed vulnerable.

Step 6- War Dialing

Combined with regular war dialing, to determine if there are any modems on the analog phone lines, it is believed that this security architecture and the included policy will protect the database and day-to-day business operations as the network evolves. Each quarter the design will be re-evaluated to determine current needs as the fortune cookie offerings and e-commerce mechanisms begin to evolve. These needs will determine the next step. The design was performed on a need toady basis so further security developments will be ongoing.

Router Testing and Diagnostics

The following is a list router diagnostics and statistics commands that are helpful in testing and troubleshooting.

For access mechanisms:

```
! Use without list number to show all access lists defined.
show ip access-list <access-list number>
! Use without an access group number to show all access groups defined.
show access-group <access-group number>
```

Logging activity or statistics:

The following command will indicate logging levels, logging hosts that are defined, number of messages logged by type, etc.

```
show logging
```

Output from the router might look something like this:

```
Jun 6 20:01:55: %FW-6SESS_AUDITTRAIL:tcp session initiator (204.204.204.10:65032) sent
1112 bytes -- responder ( 199.200.12.1:443) sent 1419 bytes
Jun 6 20:02:35: %FW-6SESS_AUDITTRAIL:tcp session initiator (10.1.5.12:65032) sent 512 bytes
-- responder ( 199.200.12.1:443) sent 1419 bytes
Jun 6 20:02:40: %FW-6SESS_AUDITTRAIL:tcp session initiator (10.1.5.12:65032) sent 1012
bytes -- responder ( 199.200.12.1:443) sent 1419 bytes
Jun 6 20:04:35: %FW-4-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator
(192.168.12.3:52419)
```

For stateful mechanisms:

These commands will indicate active connections, the state of all active sessions, source IP address, source port, destination IP address, and destination port to name a few.

```
show ip inspect session all
show ip inspect session detail
```

Output from the router may look like the following:
Session 61EBF312 (204.204.204.10:32180)=>(199.200.192.12:443)tcp SIS_OPEN
Session 61E2F3BA (204.204.204.10:32090)=>(199.200.192.12:443)tcp SIS_CLOSING
Session 61ABF3E2 (204.204.204.10:32600)=>(199.200.192.12:25)smtp SIS_OPEN
Session 65EBFE1A (204.204.204.10:31180)=>(199.200.192.12:80)http SIS_OPEN

For IPSec testing and diagnostics:
The following command will show statistics about all active security associations, number of encapsulated and decapsulated packets, level of protection offered by IPSec, etc.

show crypto ipsec sa

For examples of output messages, visit Cisco and search on troubleshooting IPSec, Log, inspect, etc. [5]

For firewall Troubleshooting and Testing

For access mechanisms:
! Use without list number to show all access lists defined.
show ip access-list <access-list number>
! Use without an access group number to show all access groups defined.
show access-group <access-group number>

Logging activity or statistics:
The following command will indicate logging levels, logging hosts that are defined, number of messages logged by type, etc.

show logging

Troubleshooting and log output is very similar between the PIX and the local routers.
For other troubleshooting and diagnostic information, visit Cisco and perform a search on troubleshooting and PIX. [5]

Design under Fire

The steps used above to determine open ports will be used against the victim network below, refer to Figure 2. Due to the fact that the public servers are located outside of a firewalls protective umbrella, it may be possible that one or more of the machines can be compromised with little or no detection. Even if a machine cannot be compromised, the fact that it is in front of a firewall makes it more susceptible to a direct DoS attack. It is recommended that the services be placed behind a firewall on a service network that can be accessed by the public. In this manner, the firewall can buffer the possible damage by a DoS attack.

One good point about this design, created by Christopher Suknundun as a practical for a previous GCFW class submission, is that later in the practical he includes intrusion detection systems to detect possible security infractions.

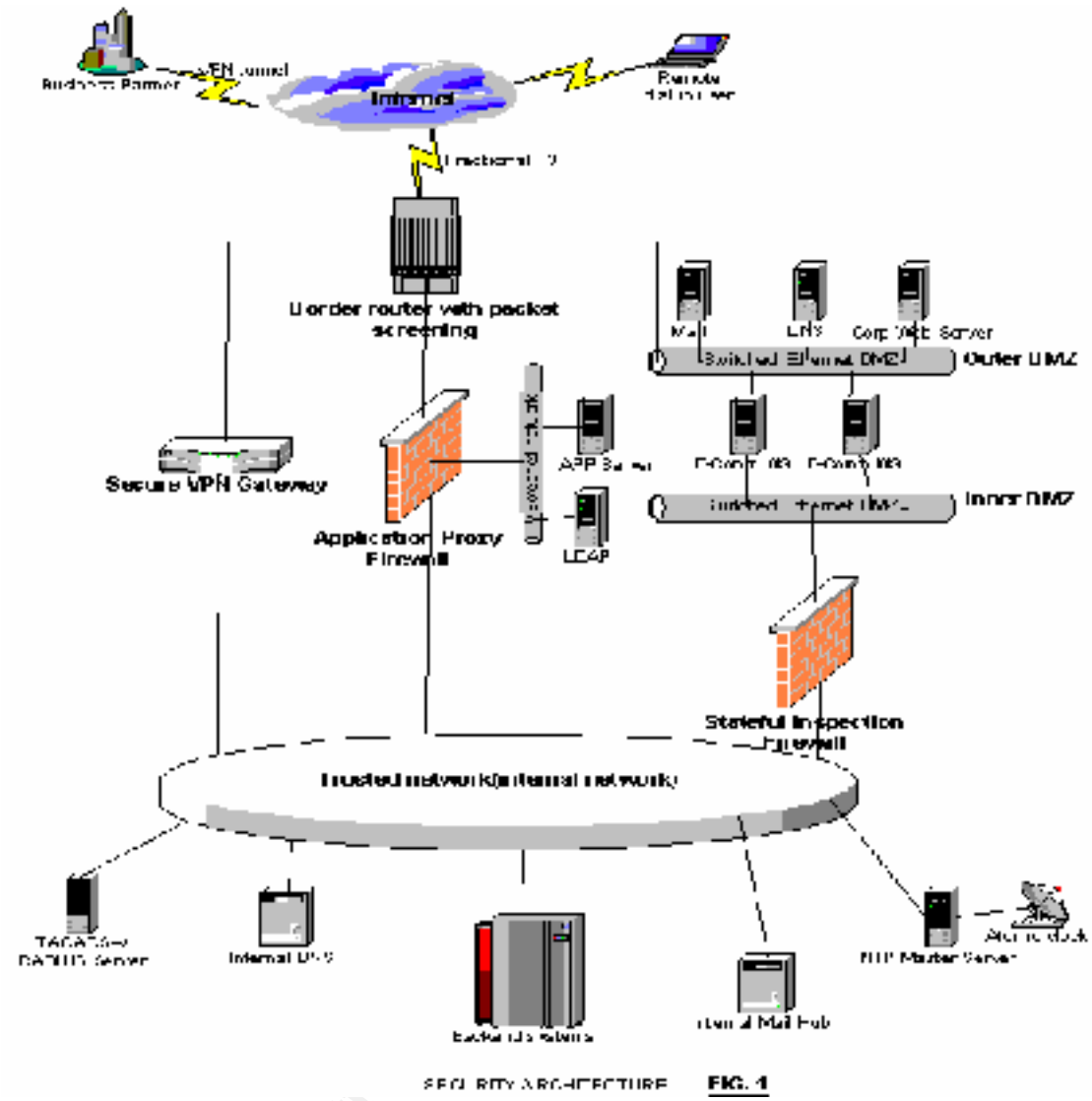

Figure 2: Design Under Fire

Step 1- Information Gathering

The first step to determining the possible weaknesses in this design is to gather information about the public architecture. The key components that I want to gather information about are routers, firewalls, switches, and servers.

For this step, we will first perform an nslookup to try to determine the hosts assigned to the public network.

From my UNIX prompt, I perform a zone transfer, using nslookup, if this hasn't been prevented by the design. We'll call this network, depicted in figure 2, target.com.

SAMPLE OUTPUT for DNS zone transfer

```
UNIX_PROMPT# nslookup
    > ls target.com
```

```
@   4D IN SOA     ns1 root.ns1 (
                  1998090705; serial
                  3H; refresh
                  1H; retry
                  4w2d;expiry
                  1D);minumum

            4D IN NS      ns1
ns1         4D IN A       192.192.192.10
            4D IN MX      10 mail
mail        4D IN MX      192.192.192.12
rtr-1-core  4D IN A       192.192.192.1
cat1-edge   4D IN A       192.192.192.5
www         4D IN A       192.192.192.100
www         4D IN A       192.192.192.101
www         4D IN A       192.192.192.102
www         4D IN A       192.192.192.103
www         4D IN A       192.192.192.104
www         4D IN A       192.192.192.105
pix1        4D IN A       192.192.192.2
nai-1       4D IN A       192.192.192.3
```

More information may have followed but we will show the output to this point to continue the tutorial.

Don't laugh; you would be surprised at the number of networks that don't prevent zone transfers from their DNS servers. Even more laughable is the fact that the naming scheme listed as an example has been seen a lot in this authors experience as well. Based on this information, yielded from nslookup, I may decide to continue gathering information, due to the fact that they allow zone transfers to yield so much information.

Step 2- Port Scan for Vulnerable Services

Now we will move on to nmap, since we were able to gather the IP addresses of existing devices at the target network. Refer to the section on auditing your architecture for the use of nmap, or visit the website. [4] The steps included in the Audit section would be performed in the same manner to determine such items such as is it behind a firewall or in the open.

Step 3- Quick SNMP Scan

Automate a quick SNMP scan of target machines listening on UDP 161/162 and see if they use default community strings. I wont delve too far into this but a quick command line for UNIX will be provided, also you may download a good freeware tool called Getif that does a nice job of gathering snmp information.

The snmpwalk command takes on this format:
Usage: snmpwalk [options...] <hostname> {<community>} [<objectID>]

An example would be: snmplwalk rtr1-core.target.com public

If the community string was valid, i.e., the admin did not change the default community strings of public or private, we can verify in a blink of an eye, whether the machines are in front of or behind the firewall. This can be performed by viewing the addresses MIB,

".iso.org.dod.internet.mgmt.mib-2.at", or, .1.3.6.1.2.1.3, well as several others, which will display until all MIBS are exhausted with the above command.

Step 4- Review and Plan the Intrusion/Attack

Upon reviewing the logs, or should I say scripting a review of the logs for possible anomalies, we compare our findings to current and past Bugtraq [6], SANS [7], or CERT [8] alerts for vulnerabilities that match any of the easy to exploit services.

We can also determine, from the DNS zone transfer, that the firewalls are a Cisco PIX [5] and possibly a Network Associates (denoted by nai) firewall [10]. The first place that I would look for vulnerabilities on these solutions are Bugtraq [6], SANS [7], and CERT [8]. The second place that I would look is on the vendor websites.

If SNMP community strings are default on any of the devices we may have another method of determining the firewall type based on their MAC address, the first half of which will indicate the vendor of the NIC, in some instances this is common on various vendor equipment.

If the router and IDS are setup correctly, DoS attacks may be diverted. If the router is not blocking or buffering for this type of attack it may be possible to render the entire e-commerce infrastructure inoperable, effectively bringing down the network at the router.

References

[1] For more information about tripwire and its operation visit: http://www.tripwire.org

[2] For more information about host sentry visit: http://www.psionic.com

[3] More information about Secure Shell setup and usage can be found at: http://www.freessh.org/open-or-free.html

[4] For more information about nmap visit: http://www.nmap.org

[5] For more information on Cisco implementation of IPSec visit: http://www.cisco.com

[6] For more information on Bugtraq please visit: http://www.securityfocus.com

[7] For more information on SANS alerts please visit: http://www.sans.org

[8] For more information on CERT alerts please visit: http://www.cert.org

[9] For more information on Expect, and TCL/TKWARE visit http://expect.nist.gov.

[10] For more information on Gauntlet Firewalls visit: http://www.nai.com