Global Information Assurance Certification Paper

Firewalls, Perimeter Protection and VPNs

GCFW Practical Assignment
Version 1.5d
Tim Kidder

Contents

Assignment 1: Definition of a Security Architecture for GIAC Enterprises

Overview

GIAC Enterprises is an Internet based developer, buyer and wholesaler of fortune cookie sayings. After completing a recent merger with another vendor, they anticipate revenues of approximately USD$ 200 million annually. They are operating a cookie saying clearinghouse wherein they perform the following business functions:

1. Develop sayings in house through the R&D unit
2. Purchase sayings from outside suppliers
3. Refine and develop sayings through the use of partners and translators
4. Sell sayings in bulk to customers

It should be noted that this is a Business to Business (B2B) operation. As such there are no e-transactions with the end user or individual consumer (B2C). There is an external web site for the general internet user that gives the company profile and contact information. There is no traffic between this out facing web server and the company databases.

The primary users of the infrastructure will be in the following list:

- External customers buying bulk fortunes
- External suppliers selling bulk fortunes
- External partners providing translation services
- Internal staff developing fortunes
- Internal corporate staff – finance, sales, operations, etc.
- Remote users (branches, subsidiaries, sales, etc.)

Intended Audience

This document is not intended for the complete novice. It assumes some rudimentary knowledge of security goals and the types of tools used to achieve these goals. It should also be noted that this design should not be implemented strictly as is. It is a high level design and specific details concerning implementation should be worked out during a pre-implementation test phase.

Also be sure that any versions of software used are researched and tested before being put into production as new issues or bugs may have been discovered since the initial creation of this design.

Address Space

The ISP will provide public addresses for the border router and the service

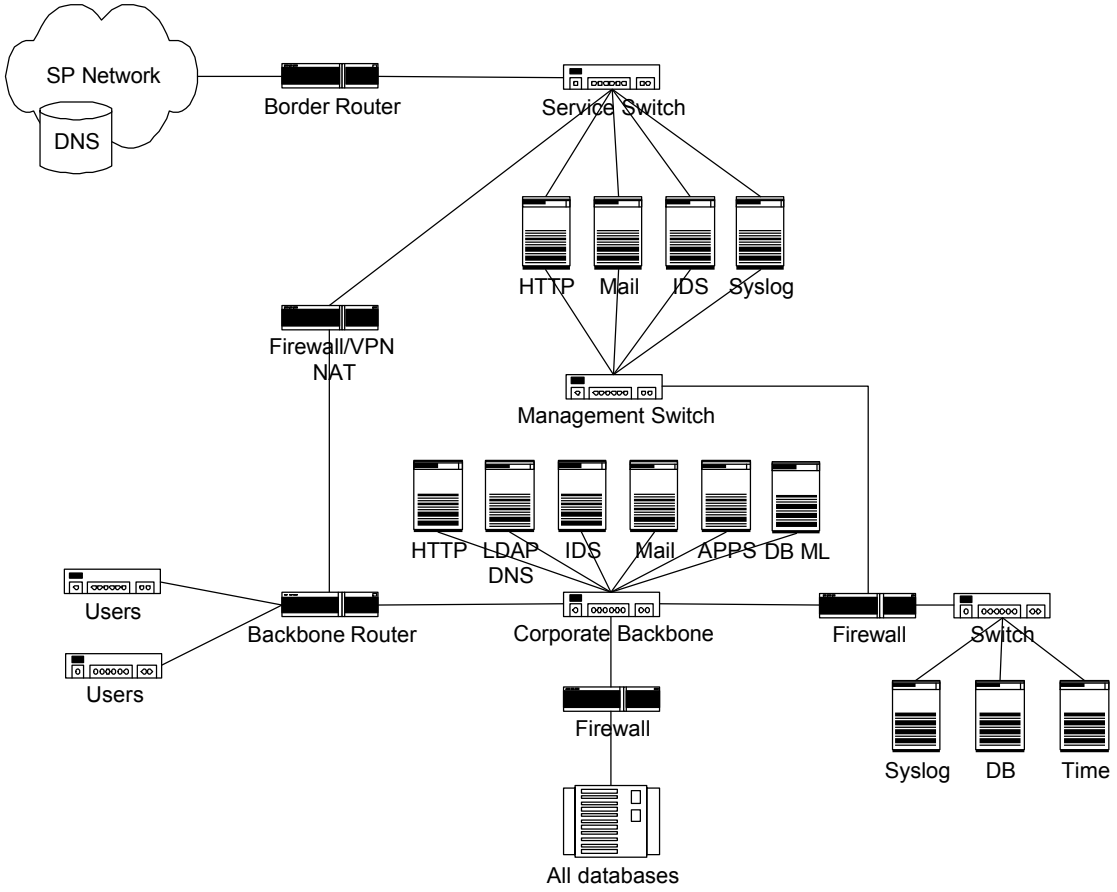
network servers/devices including the Firewall/VPN. The internal network will be numbered as a series of Network 10.x.x.x private subnets:

- 10.10.10.1-254/24—inside access network from Firewall/VPN
- 10.10.20.1-254/24—R&D user segment
- 10.10.30.1-254/24—Corporate user segment
- 10.10.40.1-254/24—Corporate server segment
- 10.10.50.1-254/24—Backend management network
- 10.10.60.1-254/24—Service hosts backend network
- 10.10.100.1-254/24—Database Server Cluster network

The public addresses provided by the ISP (this is in reality a fictitious range for the purpose of this high level design only) will be in the range of 100.100.100.1-254/24. The service network hosts will use addresses in the range of 100.100.100.10/24 to 100.100.100.30/24. The addresses in the range of 100.100.100.50-150/24 will be used as global addresses for the outbound NAT function.

Infrastructure Design

The following diagram describes the overall architecture of the solution.



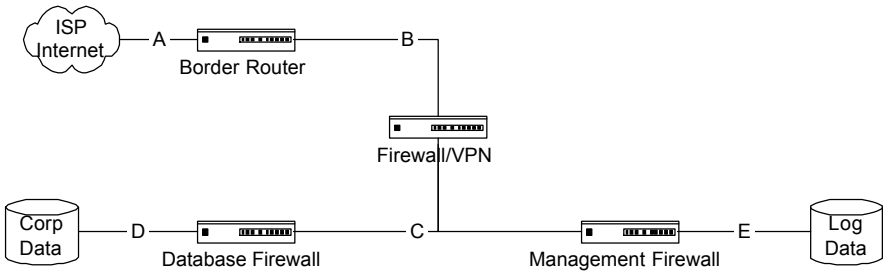
Notes:

1. IDS activity and alerts will be gathered on all segments and coordinated by the management network hosts and DB.
2. Certificate services may be provided by an internal certificate server LDAP or by a third party CA.
3. Internal and external DNS will be entirely separate functions with no Zone transfers or queries from outside. Internal clients will locate external domains via recursion on the internal server or via the proxy function on the PIX.
4. The central database network will consist of a cluster of machines that house all fortune sayings and corporate data. Normal data access will be done through middle ware on the DB ML server. Non-admin workstations will not have direct access to the database server via SSH2.
5. The management DB server will coordinate all alerts, logging and access in order to provide full audit capabilities for every event.

Traffic Profile

The following diagram and associated table illustrate the profile of traffic as is

passes through the GIAC infrastructure.



Segment	Profile
A	Raw Internet Traffic—should be considered hostile
B	Logically clean traffic – no spoofs or non-normal looking traffic Queries to web server SMTP mail traffic to service network mail server VPN inbound traffic
C	Packets with internal addresses only Remote VPNed traffic SMTP from service network mail server Return DNS traffic to DNS Server(queries) Log data
D	Management traffic (SSH2) Middleware server queries Log data
E	Log data only

Border Router

The border router will be a Cisco 3640 with 1x 100mbps fast ethernet interface and 1 high speed serial interface running IOS version 12.1(5)T. The current 256kb circuit will be upgraded to T1. The service provider is supplying necessary public addresses for our exposed (service network) servers as well as DNS services to map them. Standard ACLs will be implemented so that noise and unsophisticated attacks like spoofed addresses can be stopped right here. In effect, this device is preening the inbound traffic to ensure that potentially dangerous packets do not pass this first checkpoint.

Service Switch

The service switch will be a Cisco 2912XL and will handle all inbound/outbound traffic between the border router and the service hosts/GIAC corporate gateway. The service network will be the access segment for all traffic in and out of the GIAC network including all partner/remote VPN encrypted traffic.

Main Firewall/VPN

In order to capitalize on the investment in Cisco products, this device will be a Cisco PIX 525 running software version 6.0. This device has many advantages to bring to this role.

- Handles NAT well with stateful expanded capabilities
- Consolidated VPN access point for remote networks and mobile/remote hosts
- IPSEC with 3DES support
- Supports full session failover with standby (as optional growth path)

Here, all of the port filtering is performed. We will not allow telnet, netbios, r-commands, NFS, X-Windows and small services and the miscellaneous protocols. We will allow VPN connections and internal return traffic through stateful NAT for network 10.10.x on the inside interface for corporate user Internet access.

Backbone Router

This will be a Cisco 3640 running IOS v.12.1(5)T with 4 100mb Ethernet ports. It will perform simple routing on the GIAC 10.x.x.x networks. Filters will drop all traffic between the R&D and corporate users switches to mitigate the risk of internal attacks.

User Switches

These switches will handle user workstation access to the network. They will be Cisco 2948 XLs. Broadcast storm suppression will reduce the risk of these machines from being used in Ddos attacks.

Corporate Backbone Switch

This will be a Cisco 2948XL and will service all of the corporate hosts. It will provide shutdown of any ports that exceed broadcast parameters in order to prevent Ddos attacks wherein a host may be highjacked and used for attacks.

Database Firewall

This will be a Dell PowerEdge 1550 dual 933mhz PIII, 2 GB RAM Bastille hardened Redhat Linux and ipchains. Only SSH (TCP 22) will be allowed in for

direct management of the server and database. Data access externally is provided through the DB Middle Layer server which handles all client access to the databases. This will be configured for access via TCP port 8088 and only from the DB middle layer host.

Management Switch

The management network is housed on a physically separate private network accessed through secondary adapters in the hosts. All routing on these servers will be turned off

This switch will provide connectivity for the back end of the service network. It will be another Cisco 2912XL. This will be a private network 10.10.60.x connected to the internal management firewall.

Management Firewall

This firewall controls access to the company's second most valuable asset – their security logs and associated security management servers. It will be a Dell PowerEdge 1550 dual 933mhz PIII, 2 GB RAM Redhat Linux, ipchains. It will allow no communication between the corporate network and the backend service network. The only traffic allowed through will be the syslog data on UDP 514 and any ports necessary for the IDS host.

Service Network Hosts

HTTP, Mail Relay, IDS, Syslog
These hosts will be Linux boxes hardened with Bastille. Packet filtering will be used on all hosts to block and log access to all ports that are not specifically required by the host's functionality. Each host will have 2 interfaces – one to the service network and one to the backend network. All logging, intrusion detection traffic, etc. will be passed over the management network to the syslog and data mining facilities behind the management firewall. These hosts will not route between the external and management networks.

Corporate Hosts

HTTP, Mail, APPS, IDS, LDAP, DNS, DB ML
These hosts will be Linux boxes hardened with Bastille. Packet filtering will be used to block and log access to all ports not specifically required by the host's function. The DB ML host will act as the primary interface for the corporate and cookie sayings databases and all ordinary non-maintenance functions will be performed through it. All database accesses will be fully logged to the DB server on the management network.

The internal DNS server will map all GIAC devices on the inside network. External hosts will be located by using the DNS proxy capability of the PIX

firewall or through recursion on the internal DNS Server.

IDS functionality is also provided on each segment to track and capture any suspicious activity. The backend management network will handle all alerting and logging.

Database Cluster Hosts

These hosts will house all of the data for GIAC enterprises. Both the cookie sayings database and financials are housed on Oracle 8i servers running Bastille hardened Linux. Packet filtering and logging here will generate appropriate alerts for any non-normal activity or attempted access. All normal traffic will originate from and return to the DB ML server on specific function mapped ports. Maintenance access will be restricted to specific stations that require it (DB admin, etc.) and SSH2- 3DES will be used.

Management Network Hosts

These hosts are the central point for logging all activity through the network. Bastille-Linux boxes will be used to gather all of the logging data and mine it for everything from alerts to correlated data indicating a systematic attack. All database activity will also be logged here. These systems are the central point for providing integrity – ensuring that no unplanned activity is performed and alerting if it does.

Assignment 2: Security Policy for GIAC Enterprises

Policy Abstract

The following represents the high-level security policy items.

- The cookie sayings and corporate databases are the primary company asset and must be protected behind 2 different security solutions.
- System and device logs related to security are the second most valuable company asset in that they represent GIAC's ability to confirm that the security policy is functional and to alert GIAC security staff of any suspicious activity.
- Our business is dependant on the Internet and so we should be good citizens and not allow our infrastructure to be used for any non-legitimate purposes such as attacking other sites.

External access from the Internet is limited to the following:

- DMZ-The average web user (http company site only)
- DMZ-Mail transit traffic (SMTP and POP3 only)
- DMZ-partners & suppliers connecting to the VPN gateway
- Internal return traffic (HTTP, FTP)

Transit traffic across the firewall is limited to:

- Internal users accessing the internet via HTTP and FTP (NAT)
- VPN terminated hosts and remote networks (IPSEC)
- SMTP traffic between the internal and external mail hosts
- DNS queries from the internal DNS service for workstation requests

Internal access is limited to the following:

- Workstation access from the internal network to external web sites (HTTP, FTP) via the NAT firewall
- Workstation access from the user LANs to the corporate server segment

Access to the cookie sayings and corporate financial databases are as follows:

- External partners, remote and mobile users will enter the network through the VPN and submit queries and transactions to the internal databases through the DB Middle Layer box
- Internal R&D and corporate users will access the database through the DB Middle layer
- Direct DBM access is provided through SSH sessions directly to the DB server infrastructure.

Border Router

The primary function of the border router is to filter noise, crafted and illogical

packets from the inbound internet data stream, deny access to unsafe services and to act as a good internet citizen by not allowing any potentially malicious traffic on the outbound data stream. Further, since the design offers only a limited set of services, all traffic which does not conform to expected profiles will be dropped.

Prohibited Traffic

Source	Action	Destination
Any	Anti spoofing	Any
Any	Blocking private addresses	Any
Any	Block ICMP discovery	Any
Any	Block Source Routing	Any
Any	Reject any packets for unsafe services (RPC, NETBIOS, etc)	Any

Allowed Traffic

Source	Profile	Destination
Any	TCP 20-21	HTTP server on service network VPN/NAT Firewall
Any	TCP 25 (SMTP	Mail server on service network
Any	TCP 53 (DNS) UDP53 (DNS)	All servers on service network VPN/NAT Firewall
Any	TCP 80 (HTTP)	HTTP server on service network VPN/NAT Firewall
Any	TCP 443 (SSL)	HTTP server on service network VPN/NAT Firewall
VPN Endpoints	UDP 500 (Cisco-IKE) IP proto 50-51(IPSEC)	VPN/NAT Firewall
Any	TCP > 1023	HTTP server on service network VPN/NAT Firewall

IOS Pseudo configuration:

```
!block private and illogical addresses
access-list 112 deny 10.0.0.0 0.255.255.255
access-list 112 deny 127.0.0.0 0.255.255.255
access-list 112 deny 172.0.0.0 0.255.255.255
access-list 112 deny 192.0.0.0 0.255.255.255
access-list 112 deny 224.0.0.0 31.255.255.255
access-list 112 deny host 0.0.0.0

!allow the IPSEC traffic through
access-list 112 permit ahp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
access-list 112 permit esp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
access-list 112 permit udp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 500

!permit all tcp packets with ACK or RST bits set (return traffic)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.0 established

!permit traffic as profiled
access-list 112 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 20 log
access-list 112 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 21 log
access-list 112 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 25 log
access-list 112 permit udp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 53 log
access-list 112 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 53 log
access-list 112 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 80 log
access-list 112 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 443 log



!reject everything not explicitly accepted above
access-list 112 deny ip any any log
```


Service Switch

This device will provide broadcast flood suppression to inhibit the effects of denial of service attacks.

Main Firewall/VPN

This is the central secure access point for all traffic in and out of the GIAC corporate headquarters facility. All VPNs must implement split horizon, and use both AH and ESP protocols for complete security. 3DES with 168 bit keys must be used for encryption.

Source	Action	Destination
Mobile User	Allow host access via VPN with 3DES encryption and HMAC MD5 authentication	Corporate LAN servers
Remote Office	Allow security gateway access via VPN with 3DES encryption and HMAC MD5 authentication	Corporate LAN servers
Service LAN Mail Server	Allow SMTP	Corporate Mail Server
Internal User	Provide NAT from network 10.x.x.x to outside sources, stateful packet capabilities, HTTP and FTP only	Any Internet service
Any	Deny	any

Sample PIX software version 6.0 pseudo configuration:

```
!Define crypto access lists

access-list 130 permit ip x.x.x.x 0.0.0.255 x.x.x.x 0.0.0.255

!Specify IKE and authentication methods
crypto isakmp policy 1
hash md5
authentication pre-share
lifetime 360

! Define the Pre-Shared Authentication Key of the Peers
crypto isakmp key secret address 201.1.1.1


!Define transform sets for the IPSec encryption, hashing, and other
choices.
crypto ipsec transform-set mydessha esp-des esp-sha-hmac
crypto ipsec transform-set mydesmd5 esp-des esp-md5-hmac


!Define a crypto map, tying peers to SA options and crypto access
lists.
crypto map GIACvpn 10 ipsec-isakmp
set peer x.x.x.x
set transform-set mydesmd5 mydessha
match address 130
```

```
!Apply the crypto map to an interface.
interface ethernet0
crypto map GIACvpn

!define the global pool for NAT
ip nat pool net-100 100.100.100.150 100.100.100.200 prefix-length 28
ip nat inside source list 1 pool net-100
!
interface ethernet 0
 ip address 100.100.100.x 255.255.255.255
 ip nat outside
!
interface ethernet 1
 ip address 10.10.50.1 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.10.50.x 0.0.0.255


!allow traffic between the Service network hosts (for SMTP and POP
mail)
access-list 130 permit tcp any any eq 110
access-list 130 permit tcp any any eq 25
```

Note that this configuration is presented in a Psuedo format to present the steps and options necessary. There are some items that have yet to be determined by the GIAC security committee:

- Will GIAC manage the certificates themselves or is it more feasible to outsource this operation to a CA such as Versign?
- The locations and profiles of all remote users (branch offices, partners, etc)

Once this final information is gathered, the complete configuration can be tested and implemented.

Backbone Router

This router acts as a central junction routing traffic between the access LAN and the internal LANs:

- Routes from the VPN access segment to the corporate services LAN.
- Corporate user segment to the corporate services LAN and access segment
- R&D segment to the corporate services LAN and access segment

User Switches

These will provide broadcast flood suppression to inhibit the effects off denial of service attacks.

Corporate Backbone Switch

This will provide broadcast flood suppression to inhibit the effects off denial of

service attacks.

Database Firewall

The database firewall is designed to protect the company's greatest asset – the fortune sayings database and associated financial and corporate data. Primary access to this database is through the middle layer data server located on the corporate LAN. Secondary access is from the database admin and support workstations on the user switches and is via SSH. The following table defines the traffic flow:

Source	Action	Destination
DB Middle Layer server 10.10.40.20 TCP port 8080	Allow through the db firewall on specific port	DB server cluster 10.10.100.5
Admin Workstations 10.10.50.x	Allow through the firewall using SSH2-3DES	DB Server cluster 10.10.100.5
DB server cluster logs	Allow udp port 514 through firewall	Management network syslog
Any	Deny	any

Management Switch

This will provide broadcast flood suppression to inhibit the effects of denial of service attacks.

Management Firewall

The management firewall is intended to protect the company's second most valuable asset, the log data. All network devices log to the management servers as well as the DB Middle layer which logs all data access.

Source	Action	Destination
Service network servers (incl F/W & VPN) UDP port 514	Allow through the firewall	DB management syslog On 10.10.50.x
Corporate network servers (incl BB router) UDP 514	Allow through the firewall	DB management syslog On 10.10.50.x

Assignment 3: Audit of the GIAC Enterprises Security Architecture

Overview

The only access point to the internal network is the Cisco PIX 525. It sits directly after the border router and so some filtering has already been performed. Rather than accept this and proceed with a false level of comfort, the audit will assume that the service network is just as hostile as the Internet in general. A host will be placed on the service network that will attempt to penetrate the primary firewall using crafted NMAP attacks.

Audit Methodolgy

The following list will present the steps necessary to perform the audit.

1. Obtain full written permission from GIAC C-level management to install a potentially hostile host on the service network and run NMAP scans against the Cisco PIX 525 firewall and internal hosts.
2. Using activity logs from existing systems and documented procedures (backup schedules, maintenance windows, etc) determine the least active time of day/day of week to perform the simulated attack.
3. Obtain further written permission from C-level management to perform the simulated attack at the chosen day and time.
4. Install the Linux host on the service network and give it a public address. Also ensure that TCPdump, HPING and/or NMAP are installed with the libpcap libraries.
5. Run the scans and document the results. Also capture all of the log output on the PIX.
6. Compare the scans and the logs to ensure that all attempted attacks were blocked and logged.
7. Adjust firewall parameters and settings to compensate for found deficiencies.
8. Run scans a second time (again with permission as stated in step3)

Simulated Attack Scan Detail

The following commands will be run to provide the stimulus to prove our firewall rule sets:

HPING 100.100.100.x (where x is the interface of the firewall) –I 50 –S –A
HPING 100.100.100.x (where x is the interface of the firewall) –I 50 -S

These commands will send Syn and SYN/ACK packets to the interface of the

firewall every 50 microseconds.

Results

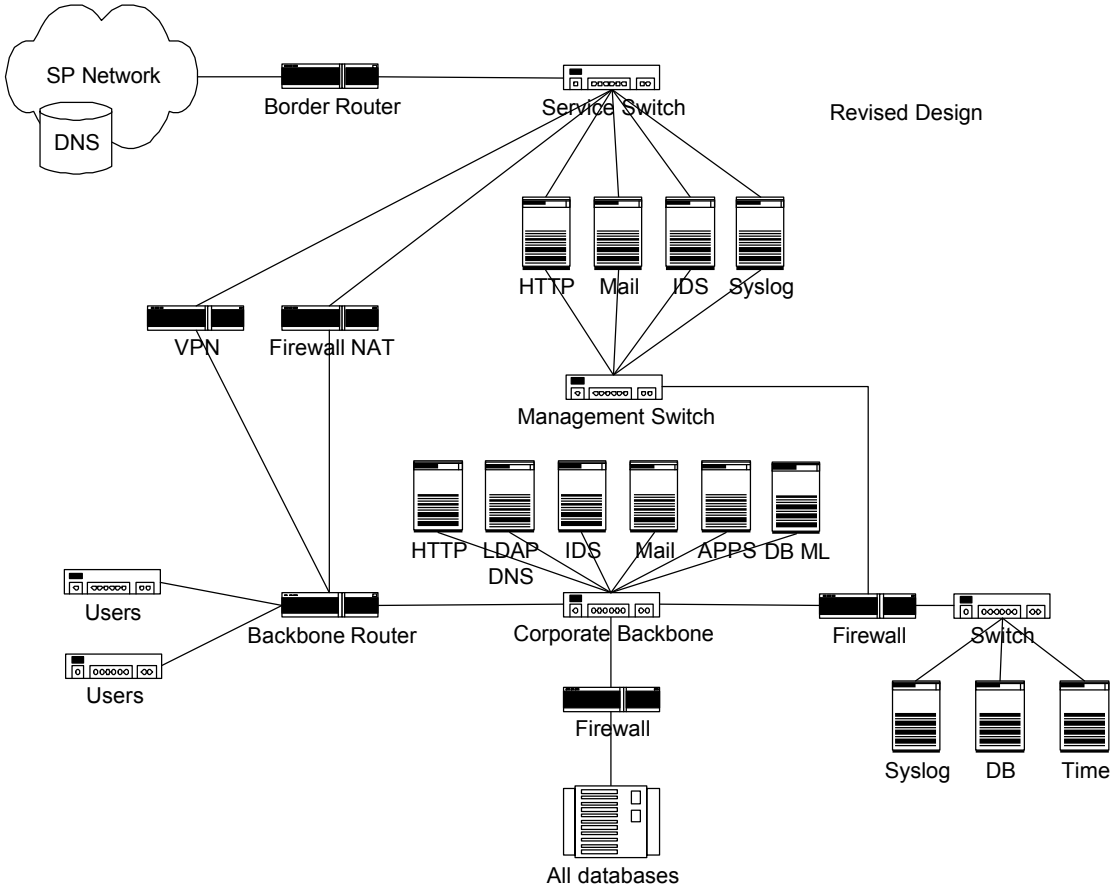
The audit process exposed a very rudimentary problem in the design. There is a single access point to the internal GIAC network, this being the combined Firewall/NAT and VPN box. While the PIX can recover from these floods, there are still issues:

- Network bandwidth is being consumed
- CPU resources are being consumed on the PIX

This could have the effect of resulting in slower access times for legitimate users while this attack is happening.

Solution

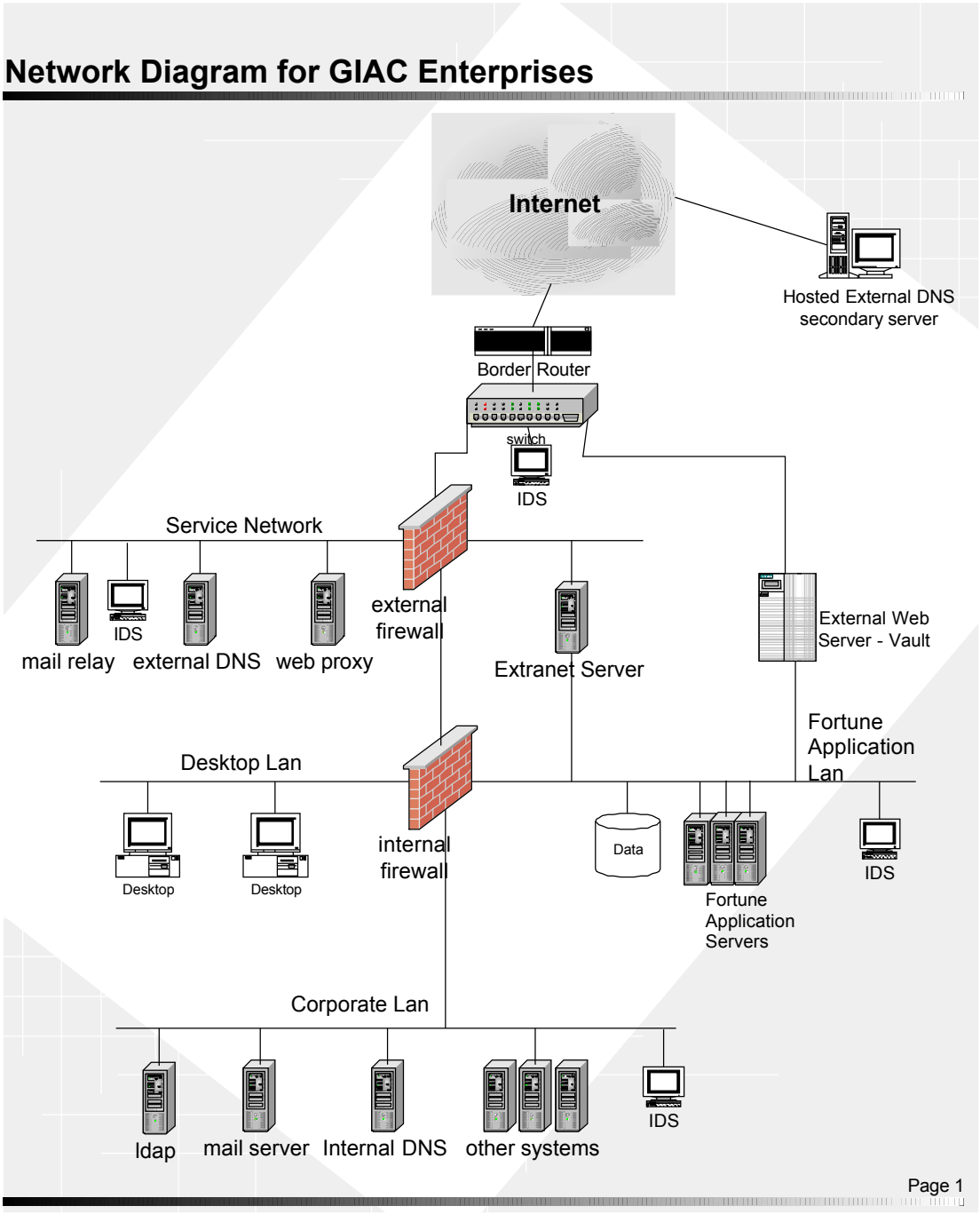
The solution is to separate the VPN and firewall/NAT functionalities across two boxes. This would have the effect of reducing the attack to a single machine without affecting the other. In addition, the border router could be configured with permit statements that deny any traffic other than legitimate packets to each of the boxes (ie, the border router would only allow VPN related traffic to the VPN (IP protocols 50/51 and UDP 500 for Cisco IKE) endpoint device.



Assignment 4: Design Under Fire

Overview

The design that will be attacked in this section is that of Sam Campbell, April 16, 2001. http://www.sans.org/y2k/practical/Sam_Campbell_GCFW.zip



Attack Scenarios

Three attack scenarios will be presented:

Attack on Primary Firewall

The primary firewall is designated in the text as a NT 4.0 sp6a server running the Axent/Symantec Raptor firewall version 6.5. There was a bug reported on

March 24, 2001 concerning this release (http://www.securityfocus.com/bid/2517). Version 6.5 has a software malfunction that allows a user to connect to the firewall interface and then access TCP ports via HTTP. These ports can be in the range of 79-99 and 200-65535 including the port of the admin service (2000). The service, extranet and internal networks are protected by this firewall, many different protocols are passed and there are several servers to attack. It may be possible to compromise one of these servers or the firewall itself.

- The cracker uses reconnaissance to discover the IP address of the firewall
- Crafted packets are sent to this firewall for HTTP proxy to HTTP ports mentioned
- Systems are now being probed and the attacker can start gathering network and host information
- Once more information is gathered, the attacker can target specific systems with specific vulnerabilities for further attack
- If the Raptor admin software is running on TCP port 2000, the attacker may be able to gain access through crafted password cracking and alter the firewall configuration.

The solution as noted in the Security Focus database is to apply the associated patches. Along with that, a test of the firewall for this vulnerability should be executed immediately and any required reconfigurations made. The policy of the firewall and the network configuration may need to be altered if any other vulnerabilities are discovered.

Denial of Service Attack

The border router used in the design screens mostly illogical network addresses along with ICMP and UDP query packets (13, 17). It does allow much traffic through including all TCP traffic and UDP echo requests, redirects, etc. It is therefore possible to flood TCP Syn packets to the external web server vault. The following scenario is possible:
http://www.cert.org/advisories/CA-1996-21.html

hping x.x.x.x –i u50 –p 80

1. Attacker highjacks 50 machines on various cable modem networks.
2. Attacker installs a tool like hping on each of the workstations (via some covert and automatic method like a mail virus).
3. Attacker configures the highjacked machines to send repeated TCP Syn packets to the web server vault. [hping x.x.x.x –i u50 –p80]nmap –xS *address_of_vault*]
4. The web server vault may respond with decreased system response time or worse yet may be able to be taken off line completely.

The solution to the above scenario is to place the web server vault behind one of the firewalls. This would provide the ability to apply a filter and effectively discard these packets long before they reach the interface of the Web Server Vault. Although IDS behind the border router should detect this scan and issue an alert, it would be wiser to further restrict the traffic allowed to hit this server.

Attack on Database Server Located on Fortune LAN

The database server is located on the fortune LAN. To get to that LAN segment, one must traverse 2 firewalls. The fault here is that both firewalls are the same platform and software. Given the exploit mentioned above, it may be possible to circumvent both firewalls by gaining access to an admin port. Both firewalls should be updated with appropriate patches. Better still, the ideal scenario is one where both firewalls are not the same platform. This requires that the hacker have a greater breadth of knowledge and skill and that they are willing to research and use multiple exploits to gain access. The attack would play as follows:

1. Compromise the primary firewall as in the first example exploit.
2. Compromise the secondary firewall as the in the first example exploit.
3. Attack the database server directly through any unsecured ports
4. Perform denial of service, install rootkits, etc.
5. If none of this activity is properly detected, it would be possible for the attacker to build a hole through both firewalls and gain control of the database servers.

The recommended course of action would be to use another firewall product. If the internal firewall were a Cisco PIX or Linux/Ipchains combo, it is less likely that the hacker would be able to continue through the secondary firewall without more research or a time delay wherein he could be detected.

Generally speaking, the more steps that are required to compromise a network or system, the greater the chances that the attacker will not complete them all and penetrate your defences.

References

Well known port numbers
http://www.iana.org/assignments/port-numbers

Cisco 3600 Series
http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm

Cisco 29xx Series
http://www.cisco.com/warp/public/cc/pd/si/casi/ca2900xl/prodlit/2924_ds.htm

Cisco PIX 525
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix2_ds.htm

Configuring the Cisco PIX Firewall
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/config.htm#27785

Configuring the PIX firewall for IPSEC
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/ipsec.htm

Configuring IKE for Cisco PIX
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/ipsec.htm#14944

Bastille Home Page
http://www.bastille-linux.org/

Cert FAQ—Denial of service attacks
http://www.cert.org/tech_tips/denial_of_service.html

TheoryGroup—Rootkits
http://www.theorygroup.com/Theory/rootkits.html

Hping Home Page
http://www.kyuzz.org/antirez/software.html

NMAP Home Page
http://www.insecure.org/nmap/

CiscoWorld, Welcher, Peter,
http://www.ciscoworldmagazine.com/monthly/2001/03/welcher_ipsec2.shtml?printme