Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment

Version 1.6

Written By:
Sherman R. Slade

Contents

Assignment 1 – Security Architecture …… 3

Assignment 2 – Security Policy ……. 18

Assignment 3 – Audit Your Security Architecture …… 41

Assignment 4 – Design Under Fire …….. 48

References …….. 51

Assignment 1 – Security Architecture.

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must include the following components:

- filtering routers;
- firewalls;
- VPNs to business partners;
- secure remote access; and
- internal firewalls.

Your architecture must consider access requirements (and restrictions) 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).

Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

Design Philosophy

The basic philosophy behind the network design is to only trust the network administrators and not trust anyone else either from inside or outside the network. This protective design stems from the responsibilities, trusts and expectations given to the network administrators for safe guarding the companies' valuable fortune cookie data assets. Because the administrators' jobs are at stake they will be actively involved with the dissemination of data and verification of its integrity.

Defense in-depth

The defense in-depth design of the network consists of six secure zones. **Figure 1** shows each defined zone and the role that it performs. These zones are established to provide layers of defense against both outside and inside intruders. Each zone is responsible for a customized security function. This delegated approach to the network security design simplifies the rule sets being applied on the firewalls and routers. An overview of the functions each Zone performs follows below.

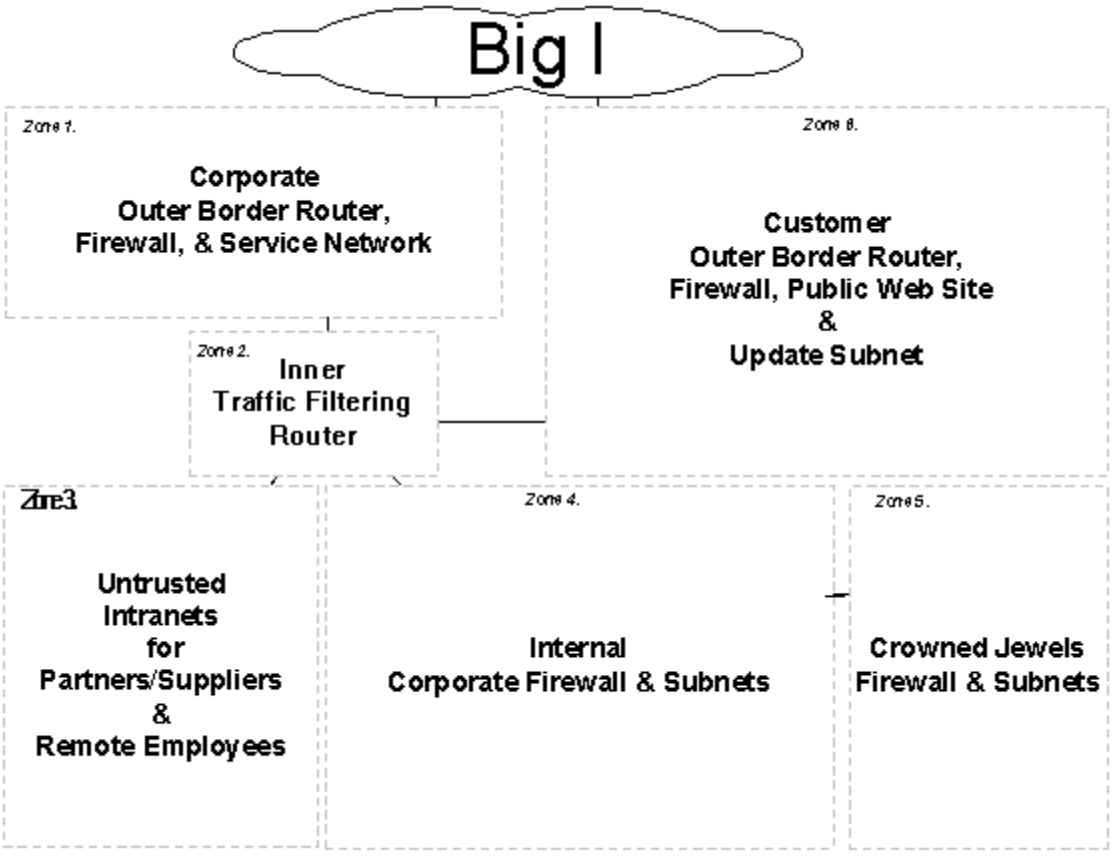


Figure 1. Network block diagram

Security Zones

The Network block diagram reveals the placement of six zones of security for the fortune cookie network. The network is to have two Frac. T1 (512 Kbps) connections to the Internet connected at Zones 1 and 6. One connection is dedicated to corporate traffic while the other is dedicated to the publish web site. A different ISP is used for each connection. All corporate traffic to the Internet will only be directed through the corporate link. Likewise all advertised web services are destined for the customer link. Separating the corporate network from the customer network by using segregated connections also separates the IP identities of the corporation and the web site. This arrangement is meant to keep the corporate network unaffected from any attacks against the web site.

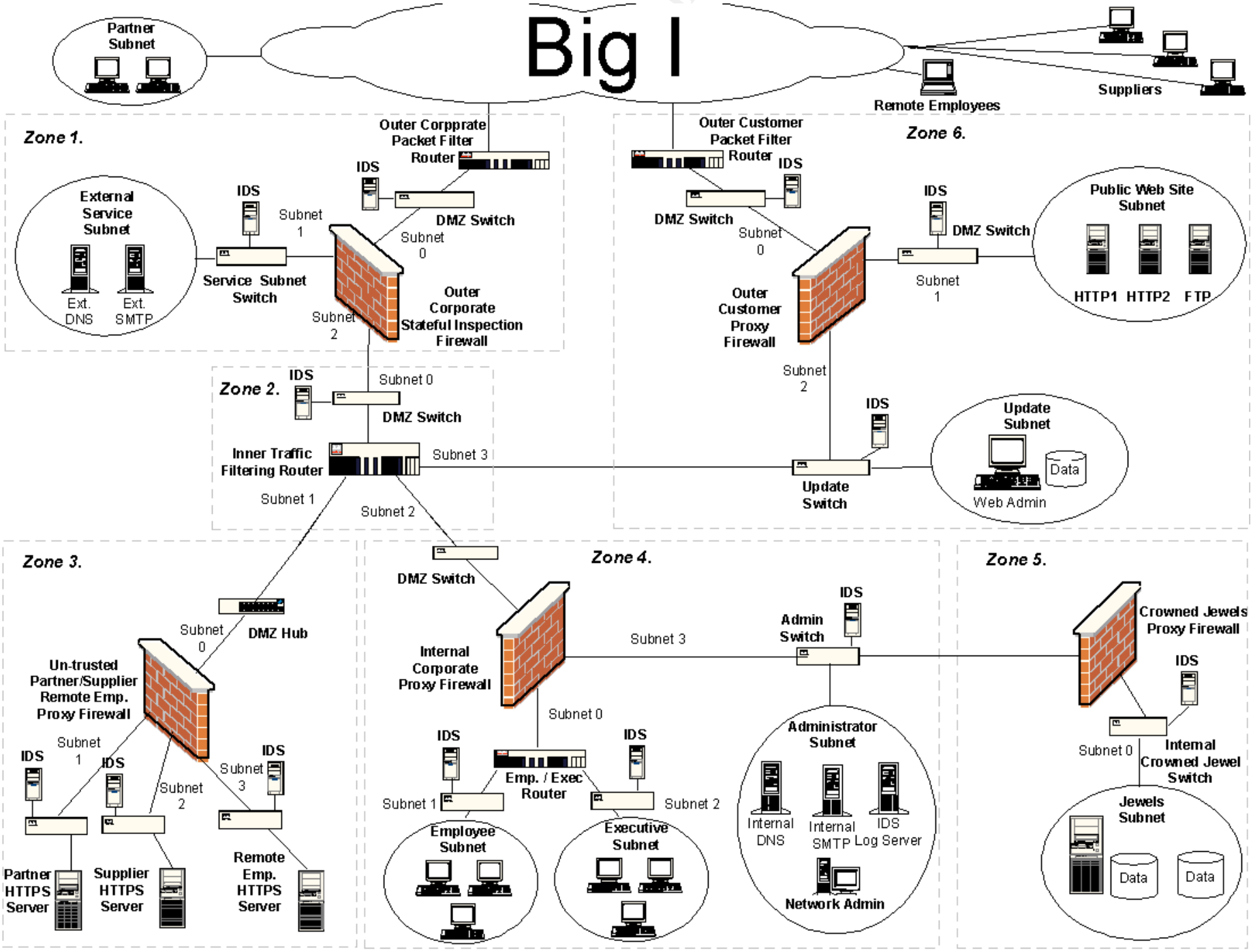
An added benefit of having independent connections to the Internet is that the rule sets on both the border routers and the state full inspection firewalls in these Zones can be more narrowly defined. Reports and analysis from IDS can also be focused to detect abnormal traffic from the outside. The combination of simple rule-sets and focused IDS servers make it easier to adjust ACLs and rules during responses to detected network attacks.

The devices used in this network architecture are shown below:

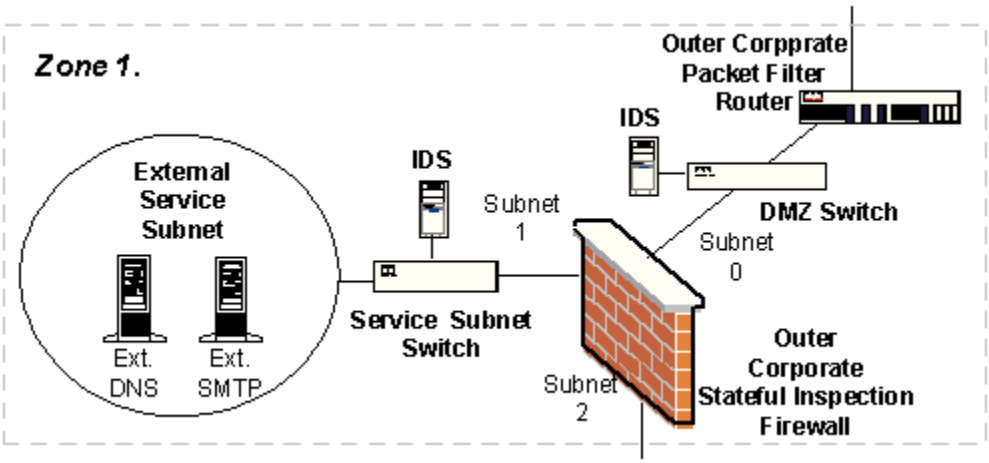
Device Type	QTY	Description	Software Version	OS Platform
Border routers	2	Cisco 2650	IOS v12.2	IOS
Inner routers	2	Cisco 2500	IOS v12.2	IOS
Ext. Corporate Firewall	1	Cisco PIX 520 Stateful Inspection	v5.1	IOS
Ext. Customer Firewall	1	Sidewinder Proxy	V5.1	Solaris
Ext. DNS servers	1	Bind	v8.2.4	OpenBSD 2.9
Ext. SMTP servers	1	sendmail	v8.2.1	OpenBSD 2.9
Ext. HTTP servers	2	Internet Server	v4.2	OpenBSD 2.9
Ext. FTP server	1	Free_BSD	v2.1	OpenBSD 2.9
Int. DNS servers	2	Bind	v8.2.4	OpenBSD 2.9
Int. SMTP servers	2	sendmail	v8.2.1	OpenBSD 2.9
Int. HTTP servers	3	Internet Server	v4.2	OpenBSD 2.9
IDS servers	13	snort	v1.8.1	RedHat Linux 7.1

Detailed Network Diagram

A detailed diagram indicating the type of equipment used within these security Zones is displayed in **Figure 2**. The network diagram reveals the machine connections within each zone and the association between the six security zones. The actual type of equipment to be used within each zone will be detailed below.



Zone 1



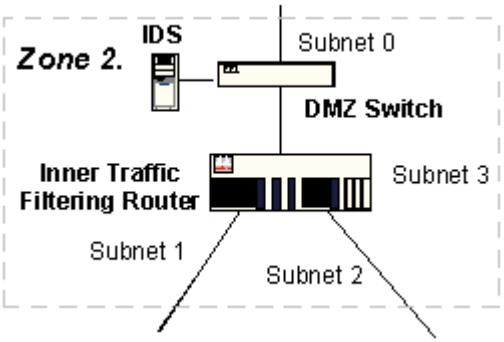
Zone 1 contains the first line of defense. Here reside the external border router, the external corporate a stateful inspection firewall and the service network.
The router chosen for the border router is a Cisco 2650. The router will be configured with ACLs that allow a very sparse set of TCP/IP traffic into and an equally sparse set of traffic out of the corporate network. The advertised services will be configured as a split DNS and a SMTP server. These services will run on separate hardened BSD servers. The DMZ between the border router, the firewall and the service network will be monitored using IDS servers. Undesirable traffic will be detected and logged to a central IDS logging server residing in Zone 4 to notify administrators when abnormal traffic is detected. A Cisco PIX stateful inspection firewall will be used here due to its security features and increased throughput performance over proxy firewalls. The PIX firewall will also be used to establish VPN connections to the outside.

Zone 1 Subnet IP address layout

Description:	Subnet 0	Subnet 1	Subnet 2
IP Address:	200.10.30.0 /29	172.16.150.1/29	192.168.10.0 /29
Subnet Mask:	255.255.255.248	255.255.255.248	255.255.255.248
# of Subnets:	1	1	1
# of IP:	8	8	8
# of Hosts:	6	6	6

Subnet	Network	Min IP	Max IP	Broadcast
0	200.10.30.0	200.10.30.1	200.10.30.6	200.10.30.7
1	172.16.150.0	172.16.150.1	172.16.150.6	172.16.150.7
2	192.168.10.0	192.168.10.1	192.168.10.6	192.168.10.7

Zone 2



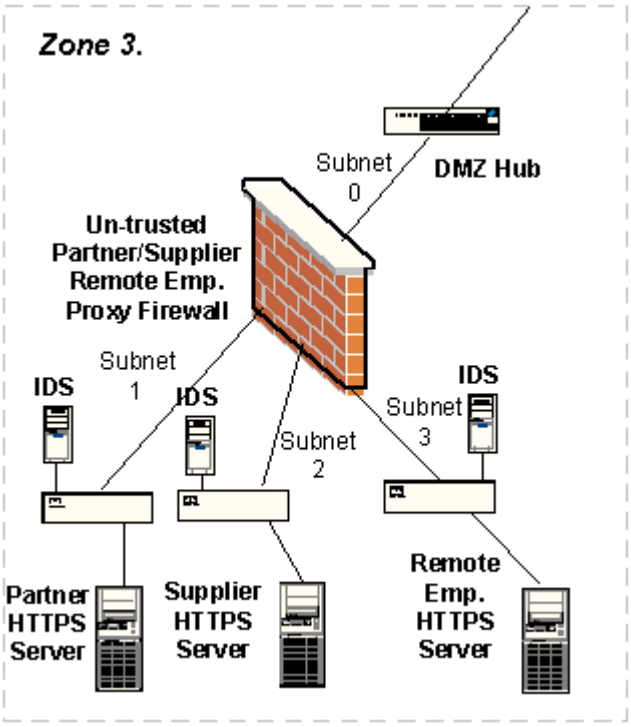
Zone 2 is the key area of the network. Here all corporate traffic will be filtered between the internal corporate subnet, the un-trusted partner/supplier subnets and the update subnet. Internal traffic isolation is important to the overall security and efficiency of the network. Strict static routes and ACLs are applied at this level to enforce the designated flow of traffic and services, which will be allowed between these independent subnets. The router used here is a Cisco 2650.

Zone 2 Subnet IP address layout

Description:	Subnet 0	Subnet 1	Subnet 2	Subnet 3
IP Address:	192.168.10.0 /29	192.168.10.8 /29	192.168.10.16 /29	192.168.10.24 /29
Subnet Mask:	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248
# of Subnets:	1	1	1	1
# of IP:	8	8	8	8
# of Hosts:	6	6	6	6

Subnet	Network	Min IP	Max IP	Broadcast
0	192.168.10.0	192.168.10.1	192.168.10.6	192.168.10.7
1	192.168.10.8	192.168.10.9	192.168.10.14	192.168.10.15
2	192.168.10.16	192.168.10.17	192.168.10.22	192.168.10.23
3	192.168.10.24	192.168.10.25	192.168.10.30	192.168.10.31

Zone 3



Zone 3 is dedicated to providing a secure connection between the corporate assets and those of the partners, suppliers and remote employees. Within this zone only narrowly defined service types will be allowed to the stub networks. Here data to the partners/suppliers/remote employees from the Internet will have been exchanged using VPN equipment located in Zone1. The partners, suppliers and the remote employees will have their own Intranet server operating on its' own stub network segment. Only the partners, suppliers or remote employees and designated personnel within the internal corporate subnet will be allowed to connect to these https servers. These https servers will be the only corporate devices that will be allowed direct inside connections to the corporate network from the outside. Because of this external exposure, these internal stub networks will be placed behind a dedicated SideWinder 5.1 proxy firewall. By isolating this external traffic only to dedicated computers, an added measure of protection is provided for all parties.

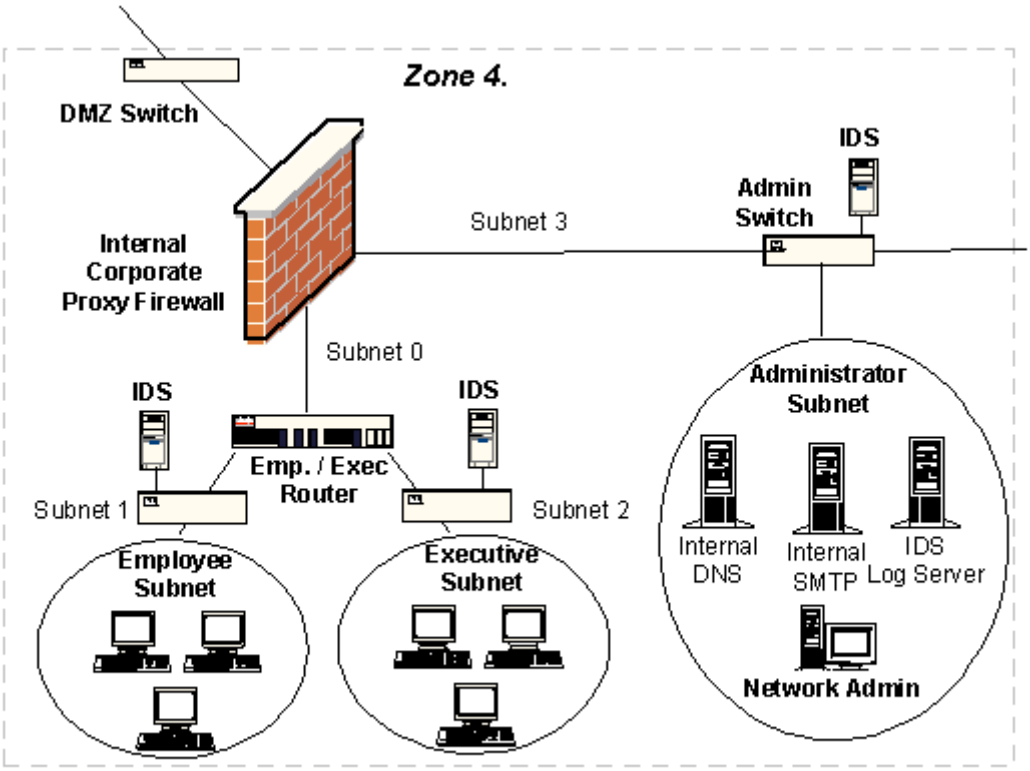
Zone 3 Subnet IP address layout
Number of Subnets: 3
Number of IP: 8
Number of Hosts: 6

Description:	Subnet 0	Subnet 1	Subnet 2	Subnet 3
IP Address:	192.168.10.8 /29	192.168.10.232 /29	192.168.10.240 /29	192.168.10.248 /29
Subnet Mask:	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248
# of Subnets:	1	1	1	1
# of IP:	8	8	8	8

# of Hosts:	6	6	6	6

Subnet	Network	Min IP	Max IP	Broadcast
0	192.168.10.8	192.168.10.9	192.168.10.14	192.168.10.15
1	192.168.10.232	192.168.10.233	192.168.10.238	192.168.10.239
2	192.168.10.240	192.168.10.241	192.168.10.246	192.168.10.247
3	192.168.10.248	192.168.10.249	192.168.10.254	192.168.10.255

Zone 4



Zone 4 comprises the bulk of the Internal corporate LANs. Within Zone 4 the subnets are design along the corporate hierarchal structure. There are three divisions within the subnets; employee, executive, and administrator. Each subnet will be isolated from the other using an internal Sidewinder 5.1 proxy firewall and router. Internal policies for allowed traffic flow between these subnets would be enforced at both the proxy firewall and router.

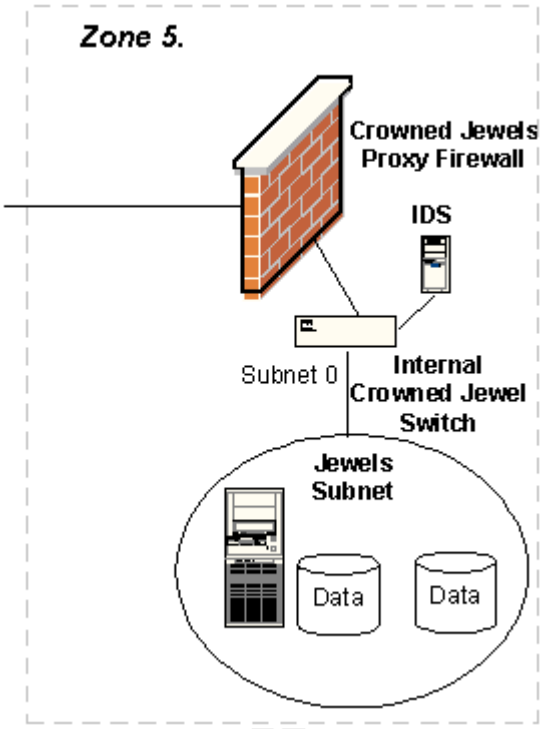
The administrator subnet is used to provide all internal network services to the employee and executive subnets. Within the administrator subnet reside the DNS, SMTP, NTP and logging IDS servers. The DNS and SMTP servers are hardened bastion hosts running BSD/OS. The NTP and logging servers are hardened bastion hosts running on Redhat Linux 7.1. They are consolidated on this subnet so that they can be strictly monitored and protected by the watchful eye of the administrators. A devoted IDS server will monitor traffic on each subnet to warn of any unusual activity originated internally from or going to any of these subnets.

Zone 4 Subnet IP address layout

Description:	Subnet 0	Subnet 1	Subnet 2	Subnet 3
IP Address:	10.150.210.0 /27	10.150.210.32 /27	10.150.210.64 /27	10.150.210.96 /27
Subnet Mask:	255.255.255.224	255.255.255.224	255.255.255.224	255.255.255.224
# of Subnets:	4	4	4	4
# of IP:	32	32	32	32
# of Hosts:	30	30	30	30

Subnet	Network	Min IP	Max IP	Broadcast
0	10.150.210.0	10.150.210.1	10.150.210.30	10.150.210.31
1	10.150.210.32	10.150.210.33	10.150.210.62	10.150.210.63
2	10.150.210.64	10.150.210.65	10.150.210.94	10.150.210.95
3	10.150.210.96	10.150.210.97	10.150.210.126	10.150.210.127

Zone 5



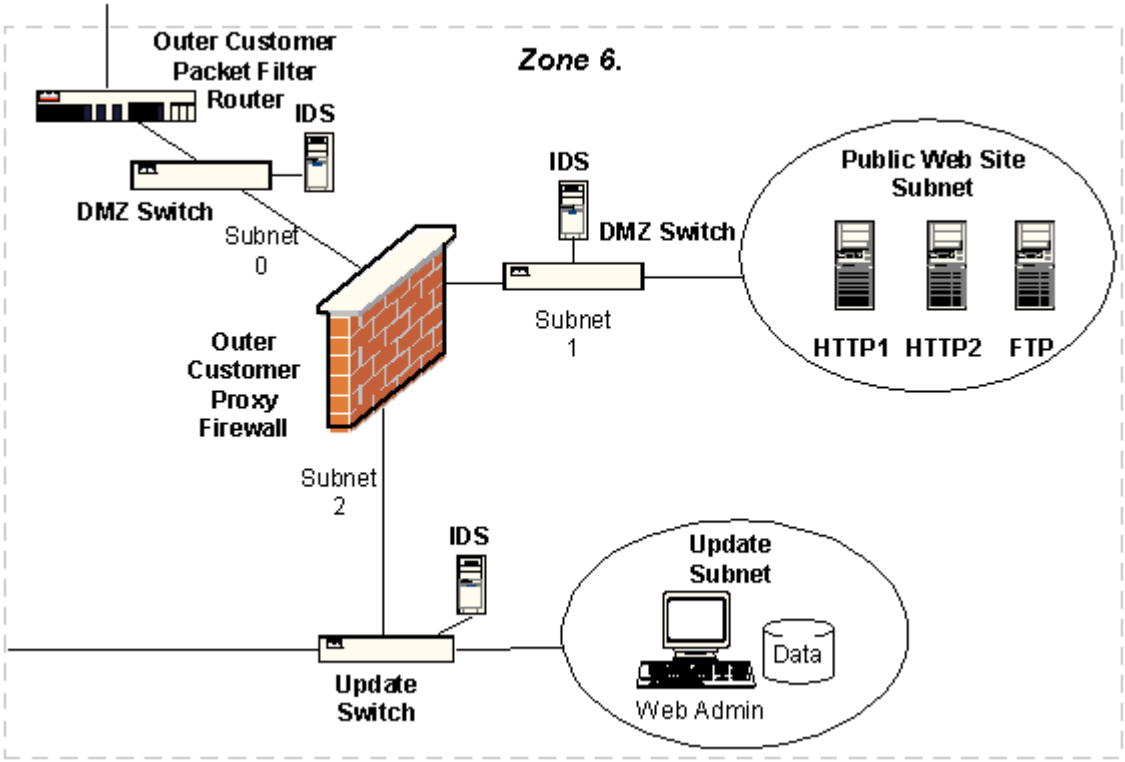
Zone 5 is where the subnet containing the valuable corporate assets reside. These assets include the master copies of the all of the fortunes and the financial records. Due to the importance of the data, it will be protected with a dedicate Nokia appliance firewall. Traffic to this subnet can only originate from the administrative subnet all other sources will be rejected at the firewall. The subnet will have a dedicated IDS server to notify the administrators of any unauthorized traffic patterns or types.

Zone 5 Subnet IP address layout

Description:	Subnet 0
IP Address:	10.200.210.0 /29
Subnet Mask:	255.255.255.248
# of Subnets:	1
# of IP:	8
# of Hosts:	6

Subnet	Network	Min IP	Max IP	Broadcast
0	10.200.210.0	10.200.210.1	10.200.210.6	10.200.210.7

Zone 6



Zone 6 comprises the customer-focused subnet. Here the Web and FTP servers reside. They will be protected using a tightly configured border router, which will only allow four tcp ports in; 80, 443, 20 and 21. All traffic across this subnet will be monitored with an IDS server on the DMZ and one on the same subnet as the web servers. Only traffic coming from the Internet and going to the web servers will allowed through the customer border router.

To maintain the web servers from within the internal network, an internal connection to the customer subnet is established using an isolated update subnet. The update subnet will act as mediator between the Web server data and the corporate assets. All updates to the web servers will be made from within this update subnet, which is devoted to that function.

Any direct internal connection between the external customer subnet and the internal corporate network will be prohibited. All daily customer order data will be sent to data base server residing on the update subnet. Any new html information like the latest fortunes will be sent from the corporate network in Zone 4 to the Web servers via the update subnet. To transfer data between the update and administrator subnets an update the trusted admin staff uses an approved procedure and schedule. This will ensure the integrity of the information. The update subnet will also have an IDS server in place to detect and report any undesired traffic.

Zone 6 Subnet IP address layout

Description:	Subnet 0	Subnet 1	Subnet 2
IP Address:	193.234.10.0 /29	172.16.5.0 /29	192.168.10.10 /29
Subnet Mask:	255.255.255.248	255.255.255.248	255.255.255.248
# of Subnets:	1	1	1

# of IP:	8	8	8
# of Hosts:	6	6	6

Subnet	Network	Min IP	Max IP	Broadcast
0	193.234.10.0	193.234.10.1	193.234.10.6	193.234.10.7
1	172.16.5.0	172.16.5.1	172.16.5.6	172.16.5.7
2	192.168.10.24	192.168.10.25	192.168.10.30	192.168.10.31

Assignment 2 – Security Policy.

Part 1 – Define Your 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.

Part 2 – Security Policy Tutorial (10 points)

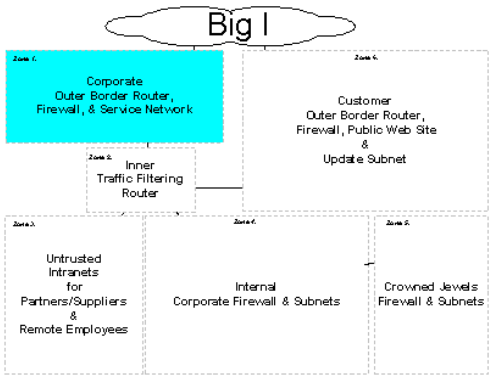
Select **one** of the three security policies defined above and write a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

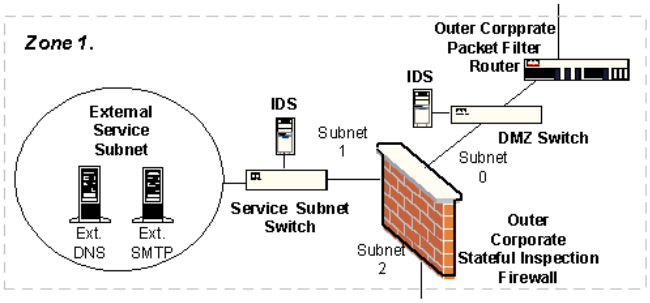
1. A general explanation of the syntax or format of the ACL, filter, or rule for your device.
2. A general description of each of the parts of the ACL, filter, or rule.
3. An general explanation of how to apply a given ACL, filter, or rule.
4. For each ACL, filter, or rule in your security policy, describe:
    - the service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.
    - Any relevant information about the behavior of the service or protocol on the network.
    - If the **order** of the rules is important, include an explanation of why certain rules must come before (or after) other rules.
5. Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

Be certain to point out any tips, tricks, or potential problems ("gotchas").

The security policy for each of the security zones is detailed below.

Zone 1. Corporate Outer Router, Firewall & Service Network





External Border Router

The role of the corporate external border router is to be the first line of defense for the GIAC Fortune Cookie (GFC) corporate network. Due to its exposure to the Internet extra protection features are added to the configuration of the border router to harden it.

Protection configuration

Login encryption will be enabled to prevent the enabled password to be visible. Login to virtual terminals will be narrowed to the Firewall residing on the DMZ. This will require the administrators to first use SSH to connect to the Firewall and from there telnet into the border router. All under the watchful gaze of the IDS server located on the DMZ.

The following internal router services will be disabled on the router so that they cannot be exploited.
These include: snmp, tcp-small services, udp-small services, finger, ntp, bootp, cdp, http.

Safeguarding options such as the following will also be applied to the router.

To protect VTYs exec-timeouts will be used to prevent an idle session from tying up a VTY indefinitely. Also the command: *service tcp-keepalives-in* will be used to guard against both malicious attacks and "orphaned" sessions.

The following commands will be applied to defend against possible smurf attacks.
No ip directed-broadcast
No ip source-route
ip verify unicast rpf.

To prevent the router from using all its processing time responding to interrupts from the network interfaces during fast packet floods the following command will be used:
scheduler interval 500

This command instructs the router to stop handling interrupts and to instead attend to other business at regular intervals.

To drop packets with invalid destination addresses quickly the following command will be used:
.
ip route 0.0.0.0 0.0.0.0 null 0 255

Cisco Express Forwarding (CEF) will be enabled on the border router to allow the use of the following protection features: Unicast RFP and CAR. The following examples are found using the following reference:
Cisco Systems Inc., Improving Security on Cisco Routers
URL: http://www.cisco.com/warp/public/707/21.html

To protect the internal network from IP address source spoofing Unicast reverse-path forwarding (RFP) can be used. With Unicast RFP enabled if the router has not previously established a connection with the source IP using the same interface then the packet is considered invalid and it is dropped

To limit icmp packets Committed Access Rate (CAR) will be enabled on the router. By using CAR, once a predetermined threshold for icmp packets is met on the router then the icmp packets will be discarded.
Example:
access-list 110 deny icmp any any
interface <Internet interface> <interface #>
rate-limit input access-group 110 64000 8000 8000 conform-action transmit exceed-action drop

Here icmp traffic is transmitted if it conforms to the rate policy of 64000 bps, with a normal burst size of 8000 bytes and an excess burst size of 8000 bytes If the ICMP traffic exceeds the rate policy, it is dropped.

A similar application of CAR is designed to reduce attempted port scans by limiting the rate of SYN packets.
Example:
!-- Let established sessions run fine
access-list 110 deny tcp any any established
!—Now rate limit the initial tcp SYN packet, the other packets in the TCP session would have been allowed by
!-- the prior entry in the ACL.
access-list 110 permit tcp any any
interface < Internet interface> <interface #>
rate-limit input access-group 110 64000 8000 8000 conform-action transmit exceed-action drop

Here tcp SYN packets are limited to 64000 bps, with a normal burst size of 8000 bytes and an excess burst size of 8000 bytes. If the SYN traffic exceeds the rate policy, it is dropped.

In addition to enabling CEF, Unicast RFP and CAR on the border router, it will also be configured to use an extended ACL to prevent Anti-Spoofing. The ACL 110 is applied inbound to the interface connected to the Internet.

```
! access-list 110 to protect the external border router.

!block private RFC 1918 addresses.

access-list 110 deny 10.0.0.0 255.255.255.255 log
access-list 110 deny 172.16.0.0 0.15.255.255 log
access-list 110 deny 192.168.0.0 0.0.255.255 log

!block loopback address
access-list 110 deny 127.0.0.0 0.255.255.255 log

!block all zero octets and multi-cast addresses
access-list 110 deny 0.0.0.0 255.255.255.255 log
access-list 110 deny 224.0.0.0 31.255.255.255

!deny any traffic trying to spoof our internal networks
access-list 110 deny 200.10.30.0 0.0.0.255 log

!block all broadcast traffic aimed at 255 subnets
access-list 110 deny ip any 0.0.0.255 255.255.255.0 log
access-list 110 deny ip any 0.0.255.0 255.255.0.255 log
access-list 110 deny ip any 0.0.255.255 255.255.0.0 log

!block icmp traffic to the corporate network excepted to the designated ping and traceroute host.
access-list 110 permit icmp any host 200.10.30.5 unreachable
access-list 110 permit icmp any host 200.10.30.5 time-exceeded
access-list 110 permit icmp any host 200.10.30.5 echo-reply
access-list 110 deny icmp any any redirect
 access-list 110 deny icmp any any

!allow other established internally solicited traffic
access-list 110 permit any any established
```

Inbound traffic configurations

The policy toward inbound Internet traffic is to prevent all traffic that is not essential to the corporation. Therefore unsolicited TCP traffic is restricted to only allow three port types inbound at the border router. The tcp and udp ports allowed inbound are:

NTP = 123 tcp
SMTP = 25 tcp
DNS = 53 tcp
DNS = 53 udp

With this approach the administrator does not have to maintain a growing ACL list trying to block onesy-twosy ports out of all the 65,535 possibilities. This policy will also prevent the corporate network from being port scanned using random ports in an attempt to map the hosts within the corporate network. To enforce this policy the following extended ACL is applied inbound to the border router at the interface connected to the Internet.

```
!permit only essential tcp ports to specific external servers.
access-list 110 permit tcp any 172.16.150.2 255.255.255.248 eq 53
access-list 110 permit tcp any 172.16.150.1 255.255.255.248  eq 25
access-list 110 deny tcp any any
```

To facilitate having VPN connections to the partner and supplier networks and the remote employees connecting to the PIX firewall the border router must pass the necessary IP Security protocols (IPSEC). The IPSec protocols were designed for VPN connections by the Internet Engineering Task Force (IETF) to support the secure exchange of packets at the IP layer.
The IP protocols allowed inbound are:
General Routing Encapsulation = 47
SIPP Encap Security Payload = 50

To enforce this policy this following ACL is applied inbound to the Internet interface.
!permit VPN protocols
access-list 110 permit 47 any 200.10.30.2 255.255.255.248
access-list 110 permit 50 any 200.10.30.2 255.255.255.248

For IPSec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol (ISAKMP), which allows the receiver to obtain a public key and authenticate the sender using digital certificates. Therefore this udp service will be allowed through the border router.
The udp service allowed inbound is isakmp:
isakmp= 500.

To enforce this policy this following ACL is applied inbound to the Internet interface.
!permit only IPSec and NTP udp ports to the PIX firewall and service network..
access-list 110 permit udp any 200.10.30.2 255.255.255.248 eq 500
access-list 110 permit udp any 172.16.150.2 255.255.255.248 eq 123
access-list 110 permit udp any 172.16.150.1 255.255.255.248 eq 123
access-list 110 deny udp any any

Outbound traffic configurations

The policy toward outbound corporate traffic to the Internet is to prevent all traffic that is not essential to the corporation. To enforce this policy an extended ACL is used to limit the available tcp and udp ports outbound. Those port numbers that are allowed will have to be established from within the corporate network in order to pass through the outer border router.
The tcp ports allowed into the router at the internal interface are:

NTP = 123
FTP data = 20
FTP session = 21
SSH = 22
TELNET = 23
TFTP = 69
HTTP = 80
HTTPS = 443
Netshow = 210

To enforce this policy this following ACL is applied outbound to the Internet interface.
!permit only essential tcp ports to Internet servers.
access-list 120 permit tcp any any eq 123 established
access-list 120 permit tcp any any eq 20 established

```
access-list 120 permit tcp any any eq 21 established
access-list 120 permit tcp any any eq 22 established
access-list 120 permit tcp any any eq 23 established
access-list 120 permit tcp any any eq 69 established
access-list 120 permit tcp any any eq 80 established
access-list 120 permit tcp any any eq 443 established
access-list 120 permit tcp any any eq 220 established
access-list 120 deny tcp any any
```

The IPSec protocols must also be allowed outbound to the partner and supplier networks and the remote employees.
The IP protocols allowed outbound are:
General Routing Encapsulation = 47
SIPP Encap Security Payload = 50

To enforce this policy this following ACL is applied outbound to the Internet interface.

```
!permit VPN protocols
access-list 120 permit 47  200.10.30.2 255.255.255.248 any
access-list 120 permit 50  200.10.30.2 255.255.255.248 any
```

The udp service allowed outbound is isakmp to facilitate key exchanges:
IPSEC = 500.

To enforce this policy this following ACL is applied outbound to the Internet interface.

```
!permit only IPSec udp ports out of the router.
access-list 120 permit udp  200.10.30.2 255.255.255.248  any eq 500
```

To enforce the FTP outbound policy the following ACL is applied outbound to the Internet interface.

```
!permit only essential udp ports to Internet hosts.
access-list 120 permit udp any any eq 20 established
access-list 120 deny udp any any
```

The DMZ traffic must be allowed out of the outside interface to allow DNS resolution and mail transfers.
To enforce this policy the following extended ACL is applied outbound to the border router at the interface connected to the Internet.

```
!permit only essential tcp ports to specific external servers.
access-list 110 permit tcp 172.16.150.2 255.255.255.248 any eq 53
access-list 110 permit tcp 172.16.150.1 255.255.255.248 any eq 25
access-list 110 deny tcp any any
```

With these configuration items in place the router will be able to screen much of the unwanted traffic and still provide good performance in handling corporate traffic with the outside world.

The DMZ

Located within the DMZ will be an IDS server to monitor traffic that is allowed in by the border router or out by the firewall. The server will report all alerts to an internal logging server located in Zone 4 on the administrator subnet. The IDS computer will also be used as a platform to conduct network troubleshooting using ping and traceroute to probe external connections with the Internet. To protect the IDS computer from exposure to the Internet a strict ACL will be applied at the outside interface of the border router to prohibit any contact with the server from the Internet. Also to protect the IDS from internal users only workstations residing on the administrator subnet will be allowed to connect to it.

External Corporate Firewall

The external corporate firewall is configured to provide quick throughput while ensuring only established connections are allowed to pass. The rule-sets on the firewall will reinforce the ACLs that exist on the border router. Due to the way that security roles have been distributed throughout the corporate network the rules-set can be narrowed down to a reduced number of required services. Network Address Translation (NAT) will be performed by the firewall to shield the internal addresses of the corporate subnets from the Internet.

The firewall chosen for this role is a Cisco PIX 520. It was selected because it can perform stateful inspection of packet traffic and it supports VPN communication.

The stateful inspection feature of the firewall provides a security advantage over a simple packet filtering firewall and a performance advantage over proxy firewalls. With PIX stateful inspection, packets are checked to determine whether they are part of established connections. In addition, the actual bits within the packet are further analyzed to verify if the tcp service allowed on a port is actually what is expected. This ability goes beyond the traditional role of a packet filter firewall and functions more like a limited proxy firewall. However, unlike a full-blown proxy firewall, which evaluates the entire packet at the application protocol level. The PIX "fixup" option for protocols and services allows the stateful inspection firewall to look for certain, known protocol commands that belong within a chosen tcp service. Once certain commands are validated to be present in the packet it is then allowed through without inspecting the packet further. The result is a higher performance throughput for packet throughput.

The external firewall needs to quickly pass legitimate traffic to both the external service subnet and on through to the rest of the internal corporate subnets. Using the stateful inspection firewalls simplified application level checking reduces the time required identifying legitimate packets. The overall affect is to increase the throughput of the firewall while still providing a higher degree of security over just packet filtering alone. At the external DMZ the volume of traffic allowed in by the border router is at its highest. Increased firewall throughput is just what is needed at this location in the perimeter defense.

A sluggish proxy firewall is more efficient when handling reduced packet amounts. Further within the security perimeter, where traffic volumes are distributed more, is where the full-blown internal proxy firewalls are placed. There proxy firewalls will intercept packets, which might be masquerading as allowed tcp/udp services or have known exploit features that fooled the stateful

inspection router. Waiting to fully validate application layer packets at locations closer to internal subnets having distributed traffic decreases the resulting latency on traffic throughput across the network. The overall affect is improved forwarding performance to all of the subnets. Therefore the Cisco PIX stateful inspection firewall is a good choice to be our external firewall.

VPN capabilities

The use of a Cisco Pix firewall at this location is also advantageous because of its VPN capabilities. VPN connections will be used to communicate with the partners, suppliers and remote employees. Each of these three groups will be configured with their own crypto map entries.

The partners will establish their VPN using a 3000 Concentrator. As a partner the VPN connection is anticipated to be more constant than those form the suppliers and the remote employees. Therefore, the partner network will be given a hardware solution to configure as a VPN peer to connect their network to the PIX firewall.

The connection needs of the suppliers and remote employees are considered to be more intermittent. Therefore they will be configured using VPN client software. Cisco Secure VPN Client v1.1 software running on host computers will be used by both the suppliers and the remote employees.

The Partners VPN type

The setup of the partner VPN will use a predefine IPSec policy to negotiate IPSec connections. The peer connection between the VPN firewall and the partners concentrator will rely on static crypto maps and pre-established manual security associations. Crypto maps are groups of variables detailing required IPSec values that specify information pertaining to VPN peers which is needed to establish communication exchanges. The kind of parameters contained in the crypto map are; the peers IP address, the type of service used in key exchanges, the lifetime value for the encryption key, which access list to use to filter packets and the order of encryption or transform set to be used.

The VPN configuration settings of the Cisco PIX firewall

The following configuration entries will be used at the external firewall.

```
access-list 155 permit ip host <partner addr> host 200.10.30.l      <- Extended ACL used for partners
access-list 155 deny any ip host <partner addr > any                <- Extended ACL used for partners

access-list 166 permit ip 172.16.1.0 0.0.0.255 host 200.10.30.1     <- Extended ACL used for suppliers
access-list 166 deny any ip 172.16.1.0 0.0.0.255 any                <- Extended ACL used for suppliers

access-list 177 permit ip 172.16.1.0 0.0.0.255 host 200.10.30.l     <- Extended ACL  for remote empl.
access-list 177 deny any ip 172.16.1.0 0.0.0.255 any                <- Extended ACL  for remote empl.

nat (inside) 0 access-list 155                                      <- Nat the inner addr of the network
nat (inside) 0 access-list 166                                      <- Nat the inner addr of the network
nat (inside) 0 access-list 177                                      <- Nat the inner addr of the network
sysopt connection permit-ipsec                                      <- enable packets to bypass conduits
```

The Manual Static IPSec configuration for Partners

```
crypto map rmt_emp client configuration address initiate            <- specify map that sets IP to Dyn. clients
crypto map rmt_emp client configuration address respond             <- specify map to respond to IP requests
crypto ipsec transform-set partner_set esp-des esp-sha-hmac         <- the transform set
crypto map partner 5 ipsec-manual dynamic supplier rmt_emp          <- IPSec in manual & dynamic mode
crypto map partner 5 match address 155                              <- specify the access-list to use
crypto map partner 5 set peer <partner address>                     <- specify the peers IP address
crypto map partner 5 set transform-set partner_set                  <- select which transform-set to use
crypto map partner 5 set security-association lifetime seconds 3600 kilobytes
                                                                    ^- specify the lifetime of the sa
crypto map partner interface outside                                <- dynamic map to an interface
```

The Suppliers and Remote Employees VPN type

The suppliers and remote employees will be setup to use Internet Key Exchange (IKE) Configuration Mode to produce dynamic IP address assignments. It allows the PIX VPN firewall to send to a VPN client a temporary IP address for the VPN and other configuration data, during the initial IKE negotiation. This exchange provides the client with an inner IP address from a known address pool that is encapsulated under IPSec. With this IP address the VPN client can be matched against the IPSec policy.

The transfer of IKE information uses the isakmp service running on udp port 500. The VPN clients will be initiating the traffic connections, therefore the firewall will use dynamic crypto maps for them. A dynamic crypto map entry is like a static crypto map entry except that not all of the parameters are configured. It is used as a policy template where the missing parameters are dynamically configured later during IPSec negotiation to match the peer's requirements. These templates enable the PIX firewall to exchange traffic with a remote peer even if the

firewall does not have a crypto map entry specifically configured to meet all the peer's requirements.

The Dynamic IPSec Configuration for Suppliers

```
crypto ipsec transform-set supplier_set esp-sha-hmac esp-3des          <- custom transform set
crypto dynamic-map supplier 30 ipsec-isakmp                            <- IPSec in isakmp dynamic mode
crypto dynamic-map supplier 30 match address 166                       <- specify the access-list to use
crypto dynamic-map supplier 30 set transform-set supplier_set          <- select which transform-set to use
crypto dynamic-map supplier 30 set security-association lifetime seconds 2700 kilobytes
                                                                       ^- specify the lifetime of the sa
crypto dynamic-map supplier interface outside                          <- dynamic-map to an interface
```

The Dynamic IPSec Configuration for Remote Employees

```
crypto ipsec transform-set rmt_emp_set esp-3des esp-sha-hmac           <- custom transform set

crypto dynamic-map rmt_emp 40 ipsec-isakmp                             <- puts IPSec in isakmp dynamic mode
crypto dynamic-map rmt_emp 40 match address 177                        <- specify the access-list to use
crypto dynamic-map rmt_emp 40 set transform-set rmt_emp_set            <- select which transform-set to use
crypto dynamic-map rmt_emp 40 set security-association lifetime seconds 3600 kilobytes
                                                                       ^- specify the lifetime of the sa
crypto dynamic-map rmt_emp interface outside                           <- associate the map to an interface
```

The IKE configuration for Dynamic IP addressing

```
ip local pool rem_emp 172.16.1.1-172.16.1.254                          <- define Ip address pool
isakmp enable outside                                                  <- enable IKE on the interface
isakmp client configuration address-pool local rmt_emp outside         <- reference the IP pool
isakmp policy 10 authentication pre-share                              <- specify key authentication method
isakmp key ******** address 200.10.30.2 255.255.255.248 no-config-mode     <- specify key
isakmp policy 10 encryption des                                        <- specify encryption algorithm
isakmp policy 10 hash sha                                              <- specify hash algorithm
isakmp policy 10 group2                                                <- specify Diffie-Hellman group Id
isakmp policy 10 lifetime 4000                                         <- security association lifetime
```

External Firewall Rule-set
The rules applied on this firewall are listed below.

Traffic origin Relative to Firewall	Traffic Type	From: Source	To: Destination	Proxy Service	Action
External	Dns	Any	Ext. DNS	dns	log
External	smtp	Any	Ext. SMTP	smap	log
External	Any	Any	Internal	-	block

			LANs		
External	GRE	Any	Internal untrusted	-	permit
External	SIPP-ESP	Any	Internal untrusted	-	permit
External	SWIPE	Any	Internal untrusted	-	permit
External	isakmp	Any	Internal untrusted	-	permit
Internal	GRE	Internal untrusted	Any	-	permit
Internal	SIPP-ESP	Internal untrusted	Any	-	permit
Internal	SWIPE	Internal untrusted	Any	-	permit
Internal	isakmp	Internal untrusted	Any	-	permit
Internal	dns	Emp. subnet	Service subnet	dns	
Internal	http	Emp. subnet	Internet	http	
Internal	https	Emp. subnet	Internet	https	
Internal	ftp	Emp. subnet	Internet	ftp	log
Internal	ftp data	Emp. subnet	Internet	ftp data	
Internal	dns	Exec. subnet	Service subnet	dns	
Internal	http	Exec. subnet	Internet	http	
Internal	https	Exec. subnet	Internet	https	
Internal	ftp	Exec. subnet	Internet	ftp	log
Internal	ftp data	Exec. subnet	Internet	ftp data	
Internal	dns	Admin. subnet	Service subnet	dns	
Internal	http	Admin. subnet	Internet	http	
Internal	https	Admin. subnet	Internet	https	
Internal	ftp	Admin. subnet	Internet	ftp	log
Internal	ftp data	Admin. subnet	Internet	ftp data	

External Service Subnet

The external service subnet is a stub subnet connected to the external corporate firewall. The service subnet will house the external DNS and SMTP servers along with an IDS server. The administrator using SSH will maintain them. The servers will run on separate Intel platforms running the BSD/OS hardened and configured with the latest patches. Aside from the main service assigned to it the servers will only be configured to run the syslogd daemon to enable them to send logs to the logging server in Zone 4.

To allow limited port access from this subnet the following extended ACL is applied outbound from the border router at the interface connected to the Ext. Service subnet.

```
!permit only essential tcp ports to specific external servers.
access-list 110 permit tcp 10.150.210.96 255.255.255.224 172.16.150.2 255.255.255.248 eq 22
access-list 110 permit tcp any 172.16.150.2 255.255.255.248 eq 53
access-list 110 permit udp any 172.16.150.2 255.255.255.248 eq 53
access-list 110 permit tcp any 172.16.150.1 255.255.255.248 eq 25
access-list 110 deny udp any any
access-list 110 deny tcp any any
```

To allow connections to the administrator subnet and the Internet the following extended ACL is applied inbound to the border router at the interface connected to the Ext. Service subnet.

```
!permit only essential tcp ports to specific external servers.
access-list 110 permit tcp 172.16.150.2 255.255.255.248 10.150.210.96 255.255.255.224 eq 22 established
access-list 110 permit tcp 172.16.150.2 255.255.255.248 any eq 53
access-list 110 permit udp 172.16.150.2 255.255.255.248 any eq 53
access-list 110 permit tcp 172.16.150.1 255.255.255.248 any eq 25
access-list 110 deny tcp any any
access-list 110 deny udp any any
```

External DNS server

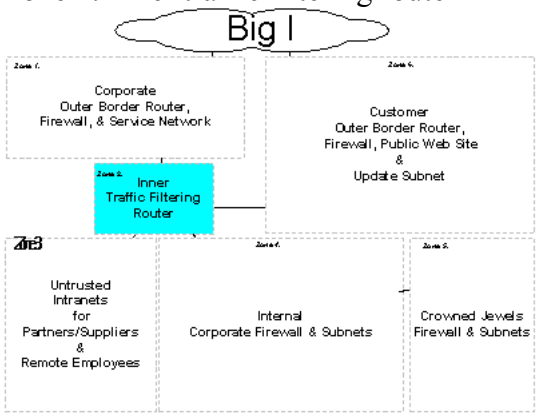
The external DNS server will run the version 8.2.4 of BIND setup in a split DNS configuration. It will contain only information regarding public accessible assets of the GAIC corporation such as the; Ext. SMTP, Ext. HTTP and the Ext. DNS servers. It is configured to ignore external zone transfers and recursive queries. All dynamic updates will be restricted to the identified internal DNS server operating in Zone 4. As far as running BIND as root goes that will not be allowed. Instead chroot will be used to substitute that function to different account. It will handle only internal queries to the Internet.

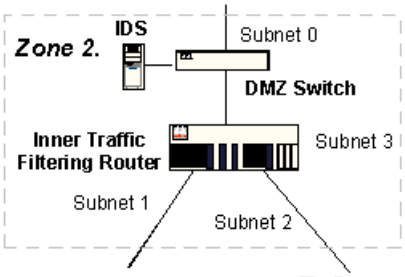
External SMTP Server

The SMTP server will run the latest version of SMTP. The configuration of a the smtp program will be adjusted to accommodate the use of scripts running under cron to analyze the payload of each mail for executables, vbs programs and oversized attachments. These mail types are deemed to inevitably be virus based and will not be allowed.

The sendmail server will be prevented from relaying any mail outside of its domain. In addition such features as vrfy and expn will be disabled. To aid against DDOS attacks the number of child sessions allowed to be spawned will be limited by using the feature: confMAX_DAEMON_CHILDREN.

Zone 2. Inner traffic filtering router





The inner filtering router is the key component within the corporate network. It is used to connect four separate security zones, 1, 3, 4 and 6. The router will segregate the data flow from the Internet the internal subnets as well as between separate internal subnets.

Here the decrypted VPN traffic from the partners/suppliers/remote employees will be directed to the stub subnets contained Zone 3. Traffic destined for the internal corporate subnets will be directed to Zone 4.

Using ACLs the router will also be used to filter traffic flowing out from the corporate network to the Internet. It will additionally provide an internal connection from the administrator subnet of Zone 4 to the update subnet of Zone 6 for maintaining the published web site.

The router will be configured with the same internal configuration protections as is used on the border router.

Interface to Zone 1.

The policy toward inbound traffic from Zone1 will be to restrict the port types allowed in to the same limited set used at the border router. This will reinforce the policy used at the border router by preventing all unsolicited traffic resulting from administrative "accidents" at the border router from getting past the inner router. The router will allow through, established traffic originating from within the inner corporate subnets. The following extended ACL is applied inbound to router at the interface connected to Zone 1.
The tcp and udp ports allowed inbound are:
SMTP = 25 tcp
DNS = 53 tcp
DNS = 53 udp

The following ACL will be used:

```
!permit only essential tcp ports to specific external servers.
access-list 110 permit tcp 172.16.150.1 255.255.255.248  10.150.210.96 255.255.255.224 eq 25
access-list 110 permit tcp 172.16.150.2 255.255.255.248  10.150.210.97 255.255.255.224 eq 53
access-list 110 permit udp 172.16.150.2 255.255.255.248  10.150.210.97 255.255.255.224  eq 53
access-list 110 deny tcp any any
```

!block icmp traffic outbound from the corporate network
access-list 110 deny icmp any any

Interface to Zone 4.

The policy toward outbound corporate traffic to the Internet is to prohibit traffic that is not essential to the corporation. To enforce this policy an extended ACL is used to limit the available tcp and udp ports applied inbound on the Zone 4 interface of the router. Those port numbers that are allowed must be established from within the corporate subnets in order to pass through the inner filtering router.
The tcp ports that are allowed outbound from the corporate network are:

NTP	= 123
FTP data	= 20
FTP session	= 21
SSH	= 22
HTTP	= 80
HTTPS	= 443
Netshow	= 210

The following ACL will be used:

```
!permit only essential tcp ports to Internet servers.
access-list 120 permit tcp any any eq 123 established
access-list 120 permit tcp any any eq 20 established
access-list 120 permit tcp any any eq 21 established
access-list 120 permit tcp any any eq 22 established
access-list 120 permit tcp any any eq 80 established
access-list 120 permit tcp any any eq 443 established
access-list 120 permit tcp any any eq 220 established
access-list 120 deny tcp any any
```

Interface to Zone 3.

The policy toward the partner/supplier/remote employee subnets is to prohibit traffic to the Zone 3 http servers that is not essential to the corporation. The traffic coming the partners/suppliers/remote employees will be allowed through to the Internet. However, the only other traffic that will be allowed into the partner and supplier subnets must originate internally from the administrator, executive and the employee subnets. To implement this policy an ACL will be applied outbound from the router to the Zone 3 interface.
The tcp ports that are allowed outbound from the corporate network through the router are:

FTP data	= 20
FTP session	= 21
SSH	= 22
HTTP	= 80
HTTPS	= 443

The following ACL will be used:

```
!permit only essential tcp ports to Partner https server.
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.232 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.232 255.255.255.248 eq 21 established
```

```
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.232 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.232 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.232 255.255.255.248 eq 443 established
!
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.232 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.232 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.232 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.232 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.232 255.255.255.248 eq 443 established
!
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.232 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.232 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.232 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.232 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.232 255.255.255.248 eq 443 established
!
!permit only essential tcp ports to Supplier https server.
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.240 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.240 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.240 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.240 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.240 255.255.255.248 eq 443 established
!
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.240 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.240 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.240 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.240 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.240 255.255.255.248 eq 443 established
!
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.240 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.240 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.240 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.240 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.240 255.255.255.248 eq 443 established
!
!permit only essential tcp ports to Remote Employee https server.
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.248 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.248 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.248 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.248 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.96 255.255.255.224  192.168.10.248 255.255.255.248 eq 443 established
!
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.248 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.248 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.248 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.248 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.64 255.255.255.224  192.168.10.248 255.255.255.248 eq 443 established
!
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.248 255.255.255.248 eq 20 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.248 255.255.255.248 eq 21 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.248 255.255.255.248 eq 22 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.248 255.255.255.248 eq 80 established
access-list 121 permit tcp 10.150.210.32 255.255.255.224  192.168.10.248 255.255.255.248 eq 443 established
access-list 121 deny tcp any any
```

These ACLs will ensure that only ftp, ssh, http and https traffic will be allowed through to the http servers residing within Zone 3.

Interface to Zone 6.

The policy toward the update subnet is that only ssh traffic originating from the administrative network will be allowed to the update subnet. There is to be no other data going between the internal corporate network and the update subnet. This strict policy will be enforced using a small extended ACL applied outbound to the router on the Zone 6 interface.
The tcp port that is allowed outbound from the router to the update subnet is:
SSH = 22

The following ACL will be used:

```
!permit only SSH connections from the administrator subnet for updates to the Update network.
access-list 122 permit tcp 10.150.210.96 255.255.255.248 192.168.10.24 255.255.255.248 eq 22 established
access-list 122 deny tcp any any
```

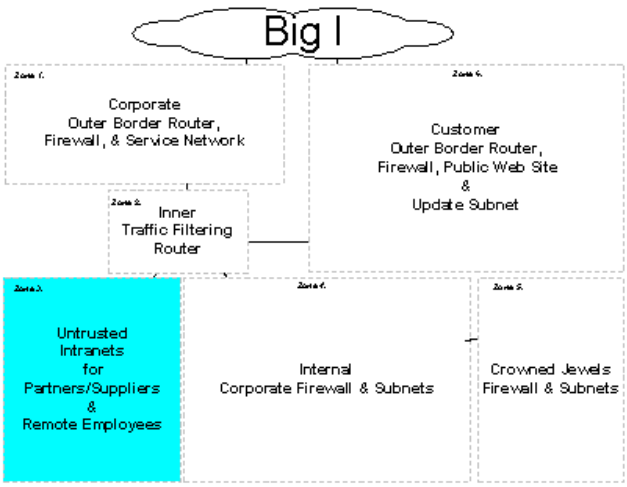
Conversely, only traffic destined to the administrator subnet will be allowed from the update subnet through the router. The security policy will allow ssh file transfer between the web administrator workstation of the update subnet to the trusted administrator subnet to be used to upload the latest released fortunes to the web server. This policy will be enforced using an extended ACL applied inbound to the router on the Zone 6 interface.
The tcp port that is allowed inbound to the router for the administrator subnet is:
SSH = 22

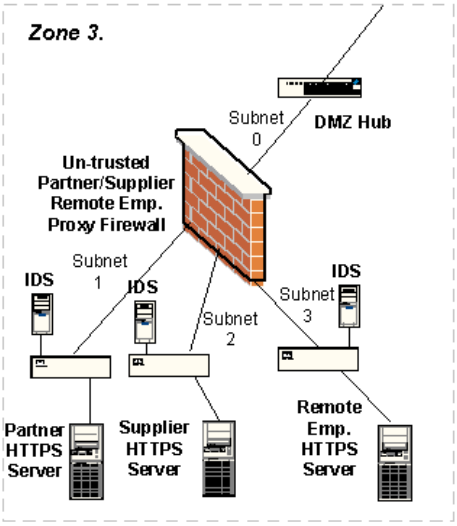
The following ACL will be used:

```
!permit only connections from the update network to the administrator subnet.
access-list 123 permit tcp 192.168.10.24 255.255.255.248 10.150.210.96 255.255.255.248  eq 22 established
access-list 123 deny tcp any any
```

These ACLs will ensure that only ssh, traffic will be allowed through to the update subnet of Zone 6.

Zone 3. Untrusted Intranets for Partners and Suppliers





The policy for zone 3 is to allow decrypted traffic from the partners, suppliers and remote employees to be sent directly to independent subnets. All will be required to authenticate at the HTTPS servers. Only designated employees, executives and administrators will be given access to the HTTPS servers on these subnets to exchange information via the intranet server. However, the partners and suppliers will be prohibited from communicating between each other or directly to the internal corporate subnets.

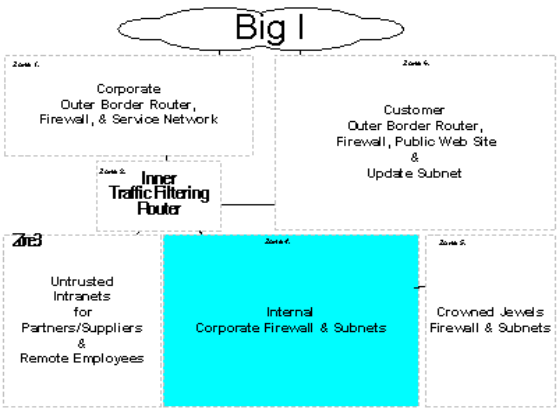
To monitor the type a traffic being transmitted through this security zone, IDS servers will be placed within the DMZ and the subnets of the partners and suppliers. Each of these IDS servers will transmit the log files to a logging server located within the Administrator subnet of Zone 4.

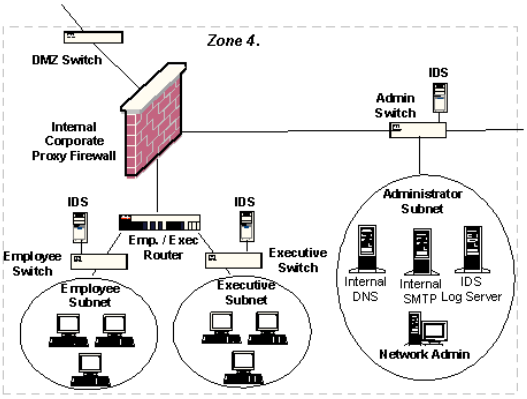
To enforce this policy the proxy firewall is used. Proxy services will provide the necessary application layer protection. It will be configured to prevent any unsolicited traffic originating from a HTTPS server from going out of Zone 3. In this way, in the event that a server becomes compromised the trouble will be isolated to that stub subnet. The IDS servers will report any suspicious attempts originating from the HTTPS servers, which may be used to target the firewall. This policy is designed to safeguard all parties against malicious activities.

Packets arriving from the Internet will come into Zone 3 after being filtered and routed at the inner filter router of Zone 2. Once in Zone 3 the packets will be sent to the proxy firewall. The firewall will then analyze the packets using application level proxies. Because the only packet types allowed through will be 20, 21 and 443 the firewall will be kept up to date with the latest packet signatures used to detect malicious contents for these service types. Once the packets are verified to be valid they are routed to the appropriate destination subnet where the HTTPS servers reside.

The three web servers will be identical to each other. They will be run on hardened BSD/OS on multi-processor Intel platforms. The Web server used will be Internet Server v4.2, which is integrated into the operating system.

Zone 4. Internal Corporate Firewall & Subnets





This policy of this zone is designed to protect the corporation assets from the outside as well as from within. To provide defense in depth protection the internal proxy services of the firewall will provide the necessary application layer protection. The SideWinder 5.1 firewall and router are also configured to isolate the subnets along corporate hierarchical divisions. These divisions are the employee, executive and administrator subnets.

The established policy will be that no direct communication will be allowed between the employee and executive subnets. Only designated users from each subnet will be allowed to exchange information with the partner/supplier HTTPS servers residing in Zone 3.

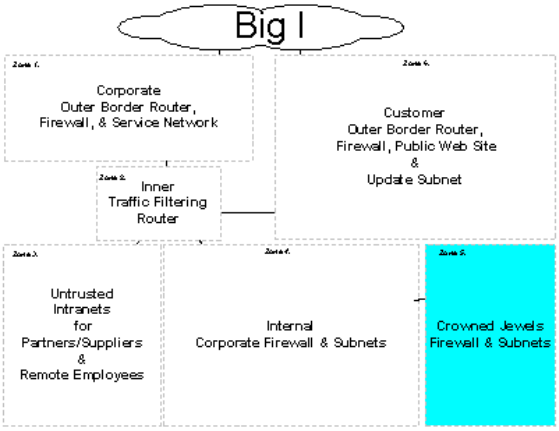
All personnel will be allowed access to the Internet for http, https and ftp services. However, no internal web servers will be allowed. IDS servers will be placed on each subnet to detect abnormal traffic emanating from the within the subnet as well as possibly coming through the firewall. The IDS servers will report any alerts to the logging server residing on the administrator subnet.

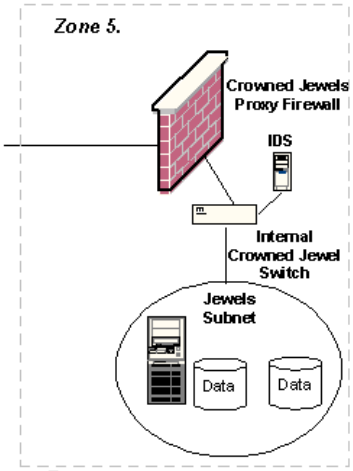
The admin staff workstations on the administrator subnet will be allowed to exchange data directly to the other subnets using PCDUO remote control software and ssh. The employee and executive subnets will only be allowed to connect to the administrator subnet to receive essential internal services such as; DNS, SMTP and NTP exclusively.

Once finished data residing on the employee or executive subnets is ready to be protected, the admin staff will pull the data onto a data server within the administrator subnet. There the integrity of the data will be verified. Once verification is complete the data will be sent on to the Crowned Jewels subnet within Zone 5 for safekeeping.

The router will be hardened in the same manner that was used for the border router.

Zone 5. Crowned Jewels Firewall & Subnet

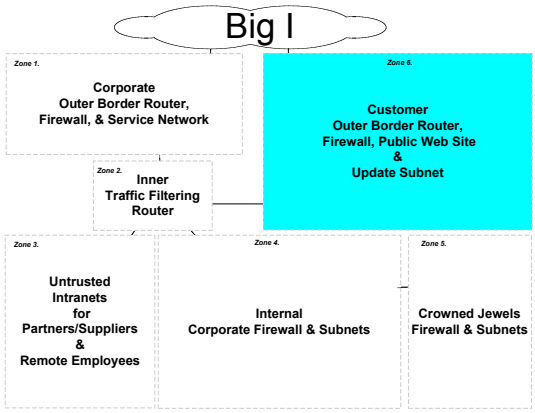


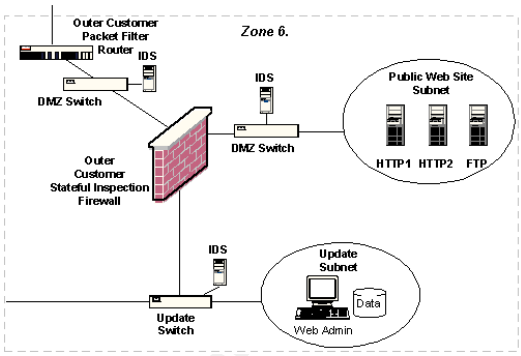


Zone 5 is the stub subnet which houses the data repository for the corporations most trusted assets. The policy for this Zone is that only workstations from the administrator subnet are allowed to connect to the crowned jewels subnet. The data will be pushed from the admin staff to the Jewels database server after it has been verified at the admin data server on the administrator subnet.

When data is needed only the admin staff will be able to pull the information from this stub subnet. This will ensure that only an authorized admin staff member has been involved in transferring the data assets. This procedure will increase the reliability and authenticity of the data assets.

Zone 6. Customer Outer Border Router, Firewall, Public Web Site & Update Subnet





The policy for this zone is to first allow customers to securely get to the web servers and no where else. To accomplish this the zone will have two ingress and egress paths. The customer path will connect the customer web subnet to the Internet through an outer border router and a proxy firewall.

The tcp ports allowed into and out of the customer border router at the Internet interface are:
FTP data = 20
FTP session = 21
HTTP = 80
HTTPS = 443

To enforce this policy this following ACL is applied inbound to the Internet interface.
!permit only essential tcp ports to Internet servers.
access-list 110 permit tcp any any eq 20 established
access-list 110 permit tcp any any eq 21 established
access-list 110 permit tcp any any eq 80 established
access-list 110 permit tcp any any eq 443 established
access-list 110 deny tcp any any

To enforce this policy this following ACL is applied outbound to the Internet interface.
!permit only essential tcp ports to Internet servers.
access-list 120 permit tcp any any eq 20 established
access-list 120 permit tcp any any eq 21 established
access-list 120 permit tcp any any eq 80 established
access-list 120 permit tcp any any eq 443 established
access-list 120 deny tcp any any

A connection will be allowed between the customer subnet and the update subnet, to provide a means for the corporation to receive orders and update the web servers from within the internal subnets securely. The order data will be sent interactively to the database server running on the hardened bastion web administrator workstation located on the update subnet.
The intermediary update subnet will connect the inner administrator subnet of Zone 4. The update subnet connects to the internal administrator via Zone 2. Only authorized admin staff are

allowed to send data to and from the update network. This policy will be enforced by the customer firewall.

Customer Firewall Rule-set

The rules applied on this firewall are listed below.

Traffic origin Relative to Firewall	Traffic Type	From: Source	To: Destination	Proxy Service	Action
External	http	Any	Customer HTTP server	http	permit / log
External	https	Any	Customer HTTPS server	https	permit / log
Internal	http	Customer HTTP server	Any	http	permit / log
Internal	https	Customer HTTPS server	Any	https	permit / log
External	ftp	Any	Customer FTP server	ftp	permit / log
External	ftp data	Any	Customer FTP server	ftp data	permit
Internal	ftp	Customer FTP server	Any	ftp	permit / log
Internal	ftp data	Customer FTP server	Any	ftp data	permit
Internal	ssh	Admin Subnet	Customer HTTP server	ssh	permit / log
Internal	ssh	Admin Subnet	Customer HTTPS server	ssh	permit / log
Internal	ssh	Admin Subnet	Customer FTP server	ssh	permit / log
external	sql	Customer HTTPS server	Update Subnet	sql	permit / log
Internal	sql	Update Subnet	Customer HTTPS server	sql	permit / log

The two web servers will be identical to each other. They will be run on hardened BSD/OS on multi-processor Intel platforms. The Web server used will be Internet Server v4.2, which is integrated into the operating system. It features TCP/IP and rate filtering as well as an FTP proxy.

Critical files will be compared using cron controlled scripts designed to run the diff application against read only compies of the web site html pages. If changes to the html pages are detected an alert is sent to the administrator. Syslog information will be sent to the logging server located in Zone 4.

The web admin workstation is the dedicated computer used to exchange information between the web site and the coporate network. The workstation runs hardened Redhat Linux 7.1

All traffic on each subnet in this zone is monitored by IDS servers that report all detected trouble to the logging server on the administrator subnet in Zone 4.

Assignment 3 – Audit Your Security Architecture.

You have been asked to conduct a technical audit of the **primary firewall** (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

1. Plan the audit. Describe the technical approach you recommend to assess the firewall. 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. Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' 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. Evaluate the audit. 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.

Audit approach

Once all of the equipment has been purchased prior to going "live" by connecting to the Internet management has asked that audit should be conducted. The risks for taking / not taking an audit from managements perspective are pretty cut and dry. The nature of the business is to provide product originality to the customers. To accomplish this any foreknowledge of the products would prevent the company from establishing trademarks of origin for their fortunes. If the original fortunes can be access by competitors then the business compromised and tied up in endless litigations to regain ownership of the information. With this position in mind a reasonable expense allocated now for an audit will be well worth it. The audit is intended to verify that the security architecture of the fortune cookie company is effectively protecting the companies' assets.

The approach taken in performing the audit is to first analyze the daily usage of the network from within. Next target the key components of the network prior to connecting to the Internet. Once assurance is obtained that the network is adequately protected an initial connection to the Internet will be allowed.
This is when we bring on the big guns. A third party consultant will be hired to attempt to penetrate our defenses or disrupt our E-commerce site.
The next stage will be to audit are VPN safeguards towards are partners, suppliers and remote employees.

Time periods for the Audit.

Prior to the network going online the audits will be performed during the normal business hours by the admin staff. The time allocated for the audit is two weeks, one for an internal audit and one for a VPN and third party audit.

The internal audit will be conducted as part of a scheduled production role out. It will be conducted over a one-week period.
The internal audit schedule is shown below:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
testing	testing	analyzing	analyzing	modify	re-testing	analyze/mod.

The VPN audit will be done one the second week during a normal business week.
The VPN audit schedule is shown below:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	testing	analyzing	modify	re-testing	analyze/mod	

The third party testing will be done on the second week. The last two days within that week will permitted for the testing. One weekday and one weekend will be tested.
The third party audit schedule is shown below:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					testing	testing

Money costs

The cost of the audit is justified when compared to the cost of the lost assets if the defenses are compromised. A break down of the anticipated cost is as follows.

Internal audit:
Time 56 Hrs x 2 Admin staff wage $60/hr = $6,720
Software Tools = $ 500
Internal Total = $7,220

Internal audit:
Time 40 Hrs x 2 Admin staff wage $60/hr = $4,800

Third Party:
Time 48 Hrs x 1 Third party wage $70/hr = $3,360

Total Audit Price: = $ 15,380

The Conducted audit

Inside sniffing

The normal working habits of the GIAC personnel will be put to the test. The network will be analyzed for password sniffers by using antisniff. Once is run dsniff will be launched to see what kind of clear passwords are being used throughout the network.

Ext. Border router

The goal of the audit of the border router is to prove that the configured protections for the router are working as designed in the security plan. From the hackers perspective before are router can be compromised it first must be correctly identified. To accomplish this, tools such as; nslookup, traceroute, ncat and nmap are used to determine IP addresses and available ports. Every brand of routers have routers will respond to these tools in an identifiable way. By profiling these responses the hackers will narrow down the router types to a particular manufacturer.

The audit will attempt to compromise the router and identify its limits for handling data attacks. First we connect to the routers destined Internet interface via a 10/100Mbps hup and a couple of laptops running Linux and Windows 2000 and our favorite hacking tools and scripts.

The routers IP address is assumed to known via a normal nslookup. Then we would map the ports using nmap.
Example:

```
hack_station #nmap –p1-25,69,79,80,161,512-514,4001,6001,9001 179.14.2.16
Interesting port on (179.14.2.16)
```

Port	State	Protocol	Service
23	Open	tcp	telnet
69	Open	udp	tftp
79	Open	tcp	finger
80	Open	tcp	http
512	Open	tcp	exec
513	Open	tcp	login
514	Open	tcp	shell
9001	Open	tcp	XRemote Service

From this output we could safely presume that we were dealing with a Cisco router.
Then the obvious attempts would occur like: telnet, finger, tftp and http attacks.
The Xremote Service being left on seems inviting. We can use ncat to look at it.
Example:

```
hack_station #nc –nvv 179.14.2.16 9001
--- Outbound Xremote service ---
Enter X server name or IP address:
```

Yikes. Better take care of that.

Then the routers ability to handle excessive ICMP request via smurf attacks will be put to the test. Again the tools of choice here would be scripts utilizing nmap, TFN, Trino and

stacheldraht. These tools, working in concert together should be able to stress the poor router and provide us with necessary baselines and breakpoints. We will measure the routers performance using CiscoWorks 2000 software.

Then the audit will focus upon the routers abilities for enforcing the ACL restrictions. Attempts will be made to communicate beyond the router into the network. Again the tools of choice here would be the hacker scripts using nmap, TFN, Trino and stacheldraht. We will attempt to spoof internal addresses, broadcast traffic aimed at 255 subnets and send in packets with invalid destination addresses. To try to map the network form the outside we will find out the effect that running Cheops will have from the out side looking in as wee as from the Inside looking out.

While these tools are run at outer interface of the router, we will analyze the traffic that appears on the DMZ using tcpdump and the IDS servers running snort. A revue of the routers logs and the show access-list command will be performed to verify the type and amount of traffic that it is dumped on the outside interface.

Firewall

One goal of the firewall audit will be to determine how well the stateful inspection filters are working. We will determine this by again, running the scripted hacker tools of choice from the outside of the border router and from within the DMZ. Analyzing the resulting syslogs from the Firewalls and the surrounding IDS servers will give us information to compare and contrast.

We will test functionality of the firewalls VPN features. Are they stable? Will they prevent intruder masquerading as suppliers or remote employees? We will accomplish this by setting up the laptops as remote employees. First well get them working with the correct parameters to verify that authentication is being performed. Next we will tweak the parameters and attempt to by-pass the authentication process.

Finally the firewall itself will come under scrutiny. Can it be compromised from the outside or inside? Here again we will use the hacker scripts using nmap, TFN, Trino and stacheldraht to target the PIX Firewall itself. We will determine which ports are open and attempt to overwhelm its stateful inspection features. We will try to gain access using the ssh port. CodeRed variant viruses will be aimed at the Firewall to see the affect it has on the http proxy.

Ext. DNS

The DNS server will be tested to determine if it has really been hardened. This will be done using our hacker scripts from the external service subnet and from the internal subnets. Once the server has been finger printed we will target the OS on which it is launched to determine if we can obtain root access.
The DNS server will be tested for vulnerabilities associated with port 53. Then the Server will be tested whether it allows zone transfers using nslookup.
Example:

```
dserv# nslookup
Default server: dserv.giac.com
Address:  176.16.150.2
```

> ls-d giac.net

Then using nslookup, the server will be tested for recursive queries. We will verify whether or not our ACLs for queries is working.

Ext. SMTP

The SMTP server will be tested for vulnerabilities associated with port 25. Sendmail username mapping exploits will also be attempted. Sendmail DDOS attacks will be run to verify if limiting precautions are effective.

IDS reporting system.

The IDS servers will be subjected to attacks designed to compromising the OS and exploit port 22.

Web server syslogs.

The Web servers will be subjected to attacks designed to compromising the OS.
They will also be subjected to numerous attack scripts used to exploit ports 80, 443, 20 and 21.

Web server diff scripts.

To verify that the reporting of changes to the website are working the scripts will be run while modifications are made to the web site's html structure.

Result analysis and evaluation

The internal audit revealed some unhardened systems at key points in the network. Namely the IDS servers running snort on Linux. To much reliance was given to hardening scripts, which did not disable all that they advertised. In addition some of our employees were sending clear text passwords that were the same as their network passwords via ftp to personal FTP servers that they had loaded onto their desktops. The FTP servers were being used to skirt around the established network share restrictions that were implemented.

The remedy was to return to IDS servers and manual harden the identified services that should not have been running. As for the FTP employees, the remedy for this was to reprimand the employees involved and remove the FTP servers. The employees were then asked them to attend security awareness training during their lunch hour.

The result of our VPN audit showed that the connections to the PIX Firewall were successful to the Partners concentrator. However the VPN software used for the Suppliers and remote employees had a problem. The software would cause their machines to lockup and required rebooting.

The remedy was a patch from Cisco for the client software for Windows 2000.

The results of the third party audit revealed an area of weakness in the GIAC network design. The weakness turned out to be our sendmail server. The third party analyst was able to successfully compromise our server using a pipe exploit using sendmail. Even though we had the most recent patches applied.

As a remedy for this weakness, it was decided that we should use qmail instead of sendmail. Qmail designed in security overcomes many of the limitations of sendmail and free the administrators from constantly applying yet another patch as a band-aid solution after the damage has been done.

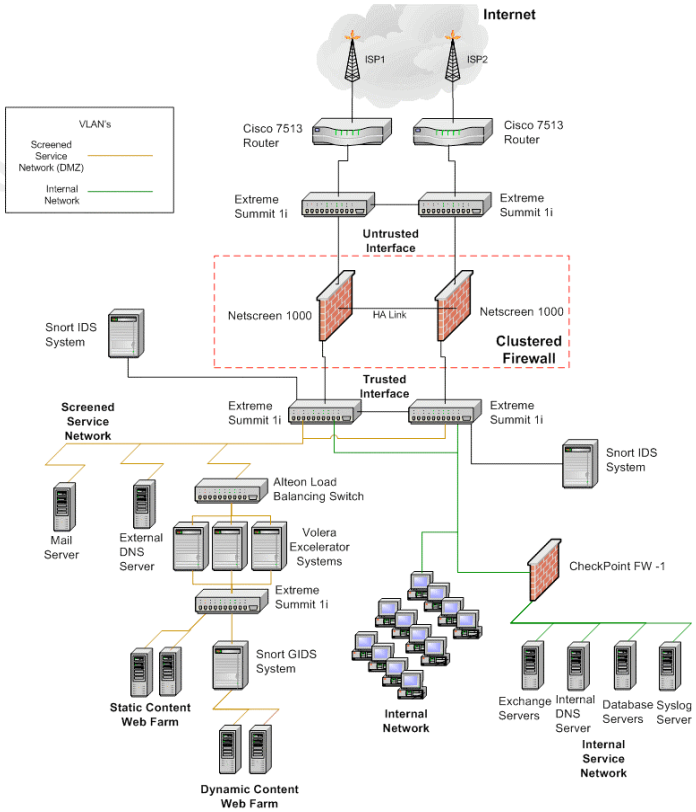
Assignment 4 – Design Under Fire

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 and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design. Choose **one** of the vulnerabilities, design an attack based on the vulnerability, 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.

Chosen Target

The network selected for attack is that of Chris Roberts. His architecture is very balanced and appears to be providing plenty of data throughput for GAIC Enterprises and their customers. The design presents a challenge for the effectiveness of DDOS attacks.



Attacking the Firewall

After reading the corporate monthly newsletter that I found in the lobby of GIAC Enterprises. I read that GIAC had just installed NetScreen-1000 Firewalls for its perimeter defense. This was good news to me because I had just read about three vulnerabilities that NetScreen-1000 Firewalls were susceptible to. I decided to have another look at the articles to give me clues for my attack.

Article 1. SecuriTeam.com ™ (NetScreen Allows Attackers to Send Forbidden Traffic to the DMZ Network) *http://www.securiteam.com/securitynews/5GP0I1F4KY.html* Provided

information concerning a possible kink in NetScreen-1000s defensive armor. It reports that a bug exists for version 2.5 of the ScreenOS for the NetScreen-100 series. The condition allows traffic that should be blocked by the policy configuration, under certain circumstances, to reach the DMZ network. The condition exists in all modes of operation on NetScreen-100 when the DMZ is active for network traffic. The vulnerability manifests itself only after specific traffic patterns have been present for some time. The result is that some packets that are denied by the policy configuration in fact are allowed to pass to the DMZ network. It does not allow all denied packets to pass; only a select few packets may incorrectly be passed. My thinking is that if the smaller product has a weakness then possibly the NetScreen-1000 would too. However, this particular bug did not reliably allow in any significant amounts of packets to reek havoc with so I decided to keep looking.

Article 2. SecuriTeam.com ™ (Hardware Defenses against SYN Flooding) *http://www.securiteam.com/securitynews/5PP0M1F55E.html* This second article gave me more hope for accomplishing my evil designs. The article details a recent benchmarking effort of SYN attacks conducted against a variety of firewalls. The results of the study made me happy. Apparently the NetScreen-100 firewall is not invincible to SYN attacks. Although the test was not conducted against the NetScreen-1000 series I'm inclined to believe that the ScreenOS behalves similarly to smaller series. The result is that the re-try and timeout periods can add up to over three minutes per bogus connection. So even a modest flood of unanswerable SYN packets can overwhelm the server in short order. I propose to use an immodest flood of packets when I attack. I will incorporate this into my attack strategy.

Article 3. SecuriTeam.com ™ (NetScreen Firewall WebUI buffer overflow vulnerability) *http://www.securiteam.com/securitynews/5LP0B1535K.html* This article gave me just the thing I was looking for. The article describes how I can effectively bring the mighty NetScreen-100 firewall crashing to its knees. All it takes is a simple oversized URL request to port 80 which it listens to by default for its Web administration interface. Although this article describes the NetScreen-100 firewall as having this weakness I feel confident that it is worth a try on the larger Firewall series. What do I have to loose the exploit is so small that I'll show it to you here.

The Exploit:
Once the input URL is longer than 1220 bytes. NetScreen firewall will crash:

$ **echo -e "GET /`perl -e 'print "A"x1220'` HTTP/1.0\n\n"|nc netscreen_firewall 80**

Following information will appear on firewall console.
********** EXCEPTION **********

Bus error exception (data reference: load or store)

EPC = 0x8009AA1C, SR = 0x34501007, Cause = 0x0080001C

Firewall halts now.

The Attack
Armed with this new knowledge I plan my attack. First, using my 50 Internet zombie PC's, I will weaken both firewalls be launching SYN attacks against them using nmapnt.
Example: nmap -v -sS -O www.giac.com

The Firewall administrators will be busy trying to defend against my attacks from their Web administration interfaces. Once I have their attention and they are staring at their firewall management GUI, I will send in the deathblow. The oversized URL request is sent to both Firewalls, the exception error appears on their GUI and the administrators look at each other and ask "What did you just do?". Mission accomplished.

Attacking with a DDOS
With all router attacks you initially hit it subtly with all the tools that you've got to determine where the weaknesses are. After conducting my profile scanning I discovered using traceroute that the GIAC web traffic was being sent to two different Internet addresses. I also discovered that there was a configuration whole in the router. It had not been configured to prevent SYN Floods or ICMP attacks directed at it.

With this information I decided to attack the network using the ole smoke screen approach. I would go after the External SMTP server after first conducting a DDOS attack against the border routers. My objective would be to compromise the smtp server using a sendmail pipe attack. My assumption, because it was not clearly specified otherwise, is that with all the new hardware changes to the network the last thing that they would upgrade is the indispensable yet fragile mail system. It is still using sendmail 4.1 under the assumption that if it isn't broken don't fix it. Well I don't want to break it I just want to modify the sendmail configuration so that it will send copies of certain employees' emails to me. I could care less about the fortunes, instead I will use these emails to sell critical information to GIAC's competitors. Whoo! Ha! Ha! Ha!

With fifty cable modem zombies I would go to work. The mission is a simple one, distract the administrators by hitting one router at a time alternately. While doing so I use my pipe bomb smtp message similar to this.
example:
helo
mail from: |
rcpt to: bounce
data
.
mail from:bin

rcpt to: | sed '1,/^$/d" | sh
data
Stuart McClure., Joel Scambray, George Kurtz, Hacking Exposed.
Berkeley: Osborne / McGraw-Hill, 1999.

Of course I didn't have to perform the DDOS attack to compromise the smtp server. But, it is a good distraction. Fifty T1 connected zombies can easily tie up a single T3 long enough to divert attention away from a little pipe attack. If the snort box became to nosy I would also direct a zombied SYN attack against port 53 on the external service network. Let the administrators wade through all of the data false DNS attack data. Once my modification is completed on the sendmail.cf file, I'll just take my time checking my phony hotmail account. Hey look. I've got mail!

Attacking from within

This kind of attack always gets someone hurt. In this case it is going to be that new executive assistant that they just hired on in human relations. I know all about it because I read about her in one of my pirated emails and I've got her email address.

It turns out that she is not to savvy with the whole email policy and that's where I come in. I added her to my list of special emails to capture and I have been doing a little social engineering work on her.

I found out that she loves to movie preview using Media Player and Active X on her Windows 98 box. So I send here a little enticement to come see the latest preview of her favorite actor at a special web site just for her. When she connects to the movie I tag along on the data port sending ActiveX commands to her desktop.

Before you know it I have successfully added a little script of mine to her startup folder. Every time she logins to her computer a little back-door program that executes into memory and sends domain information to another one of my bogus hotmail accounts. Soon I will have a detailed map of most of the internal layout of the network.

With that kind of road map I attempt compromise the Checkpoint FW1 firewall with this slicky-doo exploit that I read about in the referenced article. SecuriTeam.com ™ (FireWall-1 stateful inspection vulnerability allows attacking of internal hosts)
http://www.securiteam.com/exploits/5QP0C0A0KW.html

This exploit can be launched from my newly acquired compromised system from the internal network. The attack is performed by triggering an internal host to generate a TCP packet that, when inspected by the firewall, will change the firewall's internal state and enable an attacker to establish a TCP connection to a filtered port through the firewall. Using this I connect to the MSSQL database server on port 1433 and soon I will be privy to all of the latest snappy fortunes. Which I sell to the competitors for a tidy sum.

References

Printed Material

The SANS Institute., Firewalls, Perimeter Protection, and VPNs Course Reference.
The SANS Institute, 2001.

Stephen Northcutt., Judy Novak, Network Intrusion Detection: An Analyst's Handbook.
Indianapolis: New Riders Publishing, 2000.

Stuart McClure., Joel Scambray, George Kurtz, Hacking Exposed.
Berkeley: Osborne / McGraw-Hill, 1999.

Bob Toxen., Real World Linux Security
New Jersey: Prentice Hall PTR, Prentice-Hall, Inc., 2001

Scott M. Ballew., Managing IP Networks with Cisco Routers.
Sebastopol: O'Reilly and Associates Inc., 1997.

Online Resources

Cisco Systems Inc., An Introduction to IP Security (IPSec) Encryption Configuring IPSec
URL: http://www.cisco.com/warp/public/105/IPSECpart5.html

Cisco Systems Inc., Configuring PIX-to-VPN Client Wild-card, Pre-shared, No Mode-Config
URL: http://www.cisco.com/warp/public/707/29.html

Cisco Systems Inc., Improving Security on Cisco Routers
URL: http://www.cisco.com/warp/public/707/21.html

Cisco Systems Inc., Configuring IPSec
URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/ipsec.htm

Linux Journal Home., Securing Name Servers on UNIX
URL: http://www2.linuxjournal.com/lj-issues/issue68/3691.html

Network Magazine., Special Report: Firewalls For All
URL: http://www.networkmagazine.com/article/NMG20010521S0007

RedHat, Inc., "RedHat Linux 7.1",
URL: http://www.redhat.com/products/software/linux/7-1_standard.html

Marty Roesch., "Snort",
URL: http://www.snort.org

Bastille Linux Project., "Bastille Hardening System",
URL: http://www.bastille-linux.org/

Fyodor., "Nmap",
URL: http://www.insecure.org/nmap/