Global Information Assurance Certification Paper

SANS GIAC Level 2
GCFW - Firewalls, Perimeter Protection, and VPNs
Practical Assignment

Baltimore SANS 2001

Ping Luo

July 31, 2001

Assignment 1 -- Security Architecture

Define security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- *Customers (the companies that purchase bulk online fortunes);*
- *Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);*
- *Partners (the international partners that translate and resell fortunes).*

Goal of Design

The goal of the proposed design is to build a layered GIAC secure Internet infrastructure with redundancy that provides high availability for customers, suppliers, partners and employees.

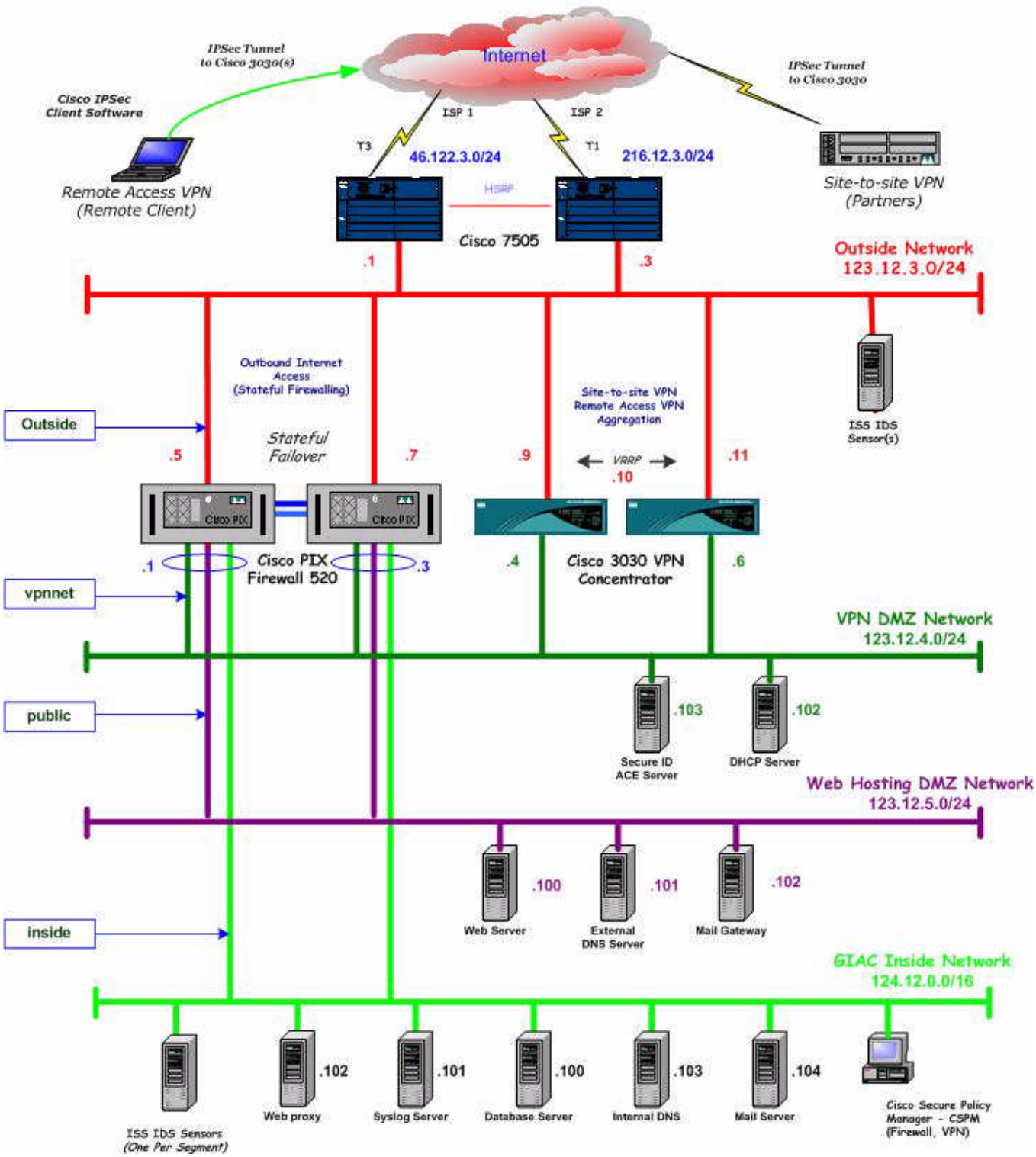
Identify the Business Requirements

1. Customers access GIAC Enterprises via Internet by HTTP and HTTPS to buy fortune cookies online.
2. Suppliers access GIAC Enterprises via Internet by HTTPS to supply fortune cookies sayings.
3. Partners access GIAC Enterprises to use shared software programs etc. through dedicated IPSEC VPN tunnels.
4. Employee remote access to GIAC Enterprises by dialing to local ISP, establishing IPSEC VPN connection with GIAC and using SecureID token authentication.

Identify the Security Requirements

1. Maximize security against various attacks from Internet to ensure the high availability of the e-commerce infrastructure.
2. Provide secure access for customers, suppliers, partners and employees to the confidentiality and integrity of the business information.
3. Maximize security against sabotage from disgruntled employees.

GIAC Security Architecture and VPN



Identify the Architecture Components

Border Routers

As we indicate at security requirements, availability is one of the most important requests for GIAC e-commerce. High bandwidth, redundant Internet access and fast routing equipments are needed to against various possible DDOS attacks thus ensure GIAC 24x7 Internet existence. We select a pair of Cisco 7505 running IOS 12.1 software as border routers; primary router connects to ISP through HSSI interface via a T3 link, secondary router connects to backup ISP via a T1 link. HSRP is configured to eliminate possible single point of failure[1].

External and Internal Firewalls

One pairs of Cisco PIX 520 firewalls running version 5.3 software serve as External and internal firewall. PIX 520 firewall has a throughput of 370 Mbps with the ability to handle as many as 250,000 simultaneous sessions. Stateful Failover option is being configured and connection states are automatically relayed between two units when fail over occurs, it takes 15 to 45 seconds to cause a switchover[2].

VPN Concentrators[3]

This is a pair of Cisco 3030 VPN Concentrators; The 3030 is designed for medium to large sized organizations with bandwidth requirements from full T1/E1 through fractional T3 (50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration.

Servers

GIAC has standardized SUN E250 with Solaris 8 operating system as following servers: DNS servers, Syslog Server, SMTP mail gateway, IDS and FTP server. OS lock down has been done according to the current best practice; Security package Autosecure (SeOS) from Computer Associates has been deployed on the above system as well as web servers and database servers.

DMZ

GIAC has two DMZs, one DMZ is for partner VPN access and the other DMZ is for web hosting. Partners access GIAC's VPN DMZ by establishing IPSEC tunnels from its VPN device to GIAC PIX firewall. Web servers, external DNS servers and SMTP gateways are located on web hosting DMZ.

Secure Remote Access

Remote users run Cisco VPN 3000 Client software on their PCs, GIAC has standardized to use IBM T21 Thinkpad laptop with windows NT4 workstation for remote users. NT4 has been locked down and customized properly according to the best practices. User authenticates by SecureID token.

[1] http://www.cisco.com/warp/public/cc/pd/rt/7500/
[2] http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/
[3] http://www.cisco.com/warp/public/cc/pd/hb/vp3000/

Assignment 2 -- Security Policy

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

- *Border Router*
- *Primary Firewall*
- *VPN*

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

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

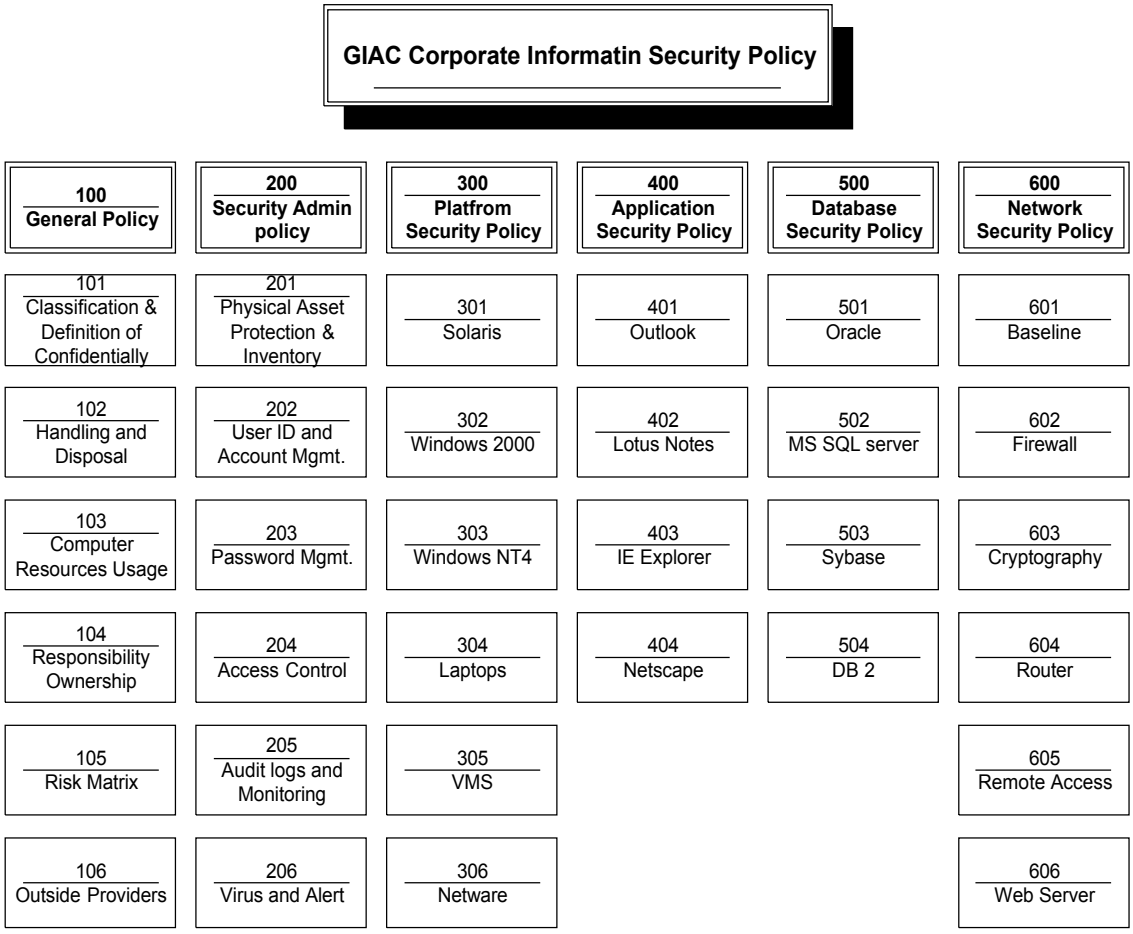
For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. *The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.*
2. *Any relevant information about the behavior of the service or protocol on the network.*
3. *The syntax of the ACL, filter, rule, etc.*
4. *A description of each of the parts of the filter.*
5. *An explanation of how to apply the filter.*
6. *If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)*
7. *Explain how to test the ACL/filter/rule.*

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

Corporate Security Policy

GIAC has a set of comprehensive written security policies. These policies include security administrations, platform security, application security, database security and network security, labeled from 100 to 600. Router, firewall, VPN and remote access are under chapter of Network Security Policy. Below, only Network Security policy and Firewall Policy are listed[4].



[4] Below policies are cited from my corporate policies

NETWORK SECURITY POLICY (Policy Number 600)[5]

Policy Statement	The integrity, confidentiality, and availability of all network resources will be protected and secured according to the criticality and potential impact of loss.
Security Requirements	**1. Identification and Authentication** 1.1 Utilize identification and authentication methods, in accordance with existing standards, to establish and verify the identity of each request for connection (i.e., person, process or job function) to a network device. 1.2 Uniquely and positively identify the user or entity requesting the connection.
	2. Authorization/Access Control 2.1 Grant authorization based on the identity and authentication credentials of the user or entity and provide only access privileges required to perform job functions. 2.2 Utilize access control methods to provide access to specified information resources for authenticated users or entities. 2.3 Control access to network resources and assignment of access privileges based on job function and separation of duties.
	3. Configuration Implement configuration parameters on all network devices to protect the information (data) and programs, and to prevent, detect and/or correct violations.
	4. Auditing 4.1 Utilize secure auditing facilities, where feasible and appropriate, to capture and provide sufficient evidence of the actions performed by users or entities to support monitoring of activity in order to enforce compliance of policies, directives and standards.
	5. Physical Security
	6. Change Management
	7. Backup and Recovery

[5] Cited from my corporate policies

Firewall Security Directive (policy number 602)[6]

	1. Firewall Architecture A firewall is a dedicated host or network appliance that restricts access between two or more networks. The firewall is configured with a policy that allows, disallows, encrypts and/or performs network address translation for all traffic destined through the firewall. The firewall itself must be resistant to penetration and must not be vulnerable to probing or scanning tools that may be used in attempts to gain access to corporate information resources. Implement a firewall solution to: ♦ Control access between internal networks and external networks (perimeter firewalls), ♦ Control access between publicly accessible servers and publicly inaccessible servers (DMZ firewalls), ♦ Control access between internal networks of differing security and access requirements, ♦ Control access through modem pools and private dial networks, ♦ Control access to and from vendor managed hosts and networks, ♦ Encrypt sensitive data traversing internal and external networks, and ♦ Hide internal network addresses from external networks (NAT).
	2. Internet Connectivity Obtain CISG (or designee) approval prior to establishing connectivity from the corporate network to the Internet. CISG, or their designated representatives, must be involved in the design, deployment and implementation of all Internet connectivity projects/activities. Internet connectivity solutions that do not meet CISG's security, management and monitoring requirements are prohibited.
	3. Identification and Access Control All access to internal information resources traversing a firewall must be identified by one or more of the following methods: ♦ Username and password, possibly augmented through a token based solution such as SecureID, and ♦ Through encrypted and secured application services running within a DMZ. In addition, the following two methods must be used to further restrict access: ♦ Match a specified static IP address or IP subnet, and ♦ Conform to specified protocol and content restrictions.

[6] Cited from my corporate policies

	4. General Firewall and Network Configuration 4.1 Install firewall software on dedicated hosts or network appliances. These firewalls will be used for access control and filtering, encryption, and network address translation only. DNS services, mail services, server load balancing, are not appropriate functions for firewalls to perform. 4.2 Delete or disable all non-firewall related software and services (e.g., compilers, editors, communications software, etc.). 4.3 Configure the firewall system to prohibit restricted internal DNS information from becoming available via the Internet. 4.4 Configure the firewall to "fail closed". If necessary, work with the firewall vendor to ensure this functionality is implemented. 4.5 Configure firewalls to conceal corporate network information from external sources. 4.6 Use a firewall that supports a "deny all services except those explicitly permitted" security paradigm. 4.7 Select a firewall system that is flexible enough to effectively and efficiently implement GIAC's security policy. 4.8 Implement firewalls that support proxy servers and / or "stateful inspection," rather than simple packet filtering solutions. 4.9 Ensure that no inside addresses designated as non-routable are passed to the outside by the firewall. For hosts with internal non-routable IP addresses that are allowed to communicate with the internet, network address translation must be utilzed to translate those address to either GIAC owned routable addresses or IP addresses assigned by the ISP
	5. Auditing, Monitoring and Alert Management 5.1 Real-time firewall alerts will be monitored 24x7 and appropriate review and escalation procedures utilized. 5.2 Firewalls will log all activity to a firewall console, management station or permanent log. 5.3 Sensitive connections secured by firewalls must also be augmented by network based intrusion detection and host based intrusion detection where appropriate.
	6. Physical Security Proper physical controls over the firewall system components minimize the risk that an unauthorized user may gain access to the firewall by exploiting weaknesses in physical security. Locate firewall components in secure areas, limiting physical access to authorized technical and administrative personnel through the use of user authentication, badges, special keys, or other appropriate security devices.
	7. Change Management
	8. Management Station(s) Backup and Recovery Proper backup and contingency planning of a firewall system is essential in preventing the disruption of Internet connectivity if the primary firewall or link fails. Without adequate backup and recovery procedures, there is a risk the firewall may not be recovered in an acceptable amount of time should a disruption occur.

	9. Firewall Backup and Recovery

Border Router

Cisco border router setup for basic screening and sanity checking, ingress and egress rule sets are being set to prevent invalid traffic entering or exiting our network. The security policy includes:

1. **Router access control**
   - Separation of duty - assign different privileges to different user; network administrator could able to change router configuration, but operators could only perform certain function.

```
username admin privilege 15 password 7 05030M12549400AA1710422
username operator privilege 2 password 7 01234B1D491123
privilege interface level 2 shutdown
privilege interface level 2 no shutdown
privilege interface level 2 no
privilege configure level 2 interface
privilege configure level 2 logging
privilege exec level 2 write terminal
privilege exec level 2 write network
privilege exec level 2 write
privilege exec level 15 enable
privilege exec level 2 configure terminal
privilege exec level 2 configure
privilege exec level 2 undebug
privilege exec level 2 terminal monitor
privilege exec level 2 terminal
privilege exec level 2 no debug
privilege exec level 2 no
privilege exec level 2 debug
privilege exec level 2 clear line
privilege exec level 2 clear counters
privilege exec level 2 clear
```

   - Turn off all unnecessary services – pad service, source route service, finger service, domain lookup, don't respond to bootp/DHCP requests, http server and turn off Cisco Discovery Protocol.

```
no service pad
no ip source-route
no ip finger
no ip domain-lookup
!
no ip bootp server
no ip http server
no cdp run
```

   - Banner

```
banner login ^C


      +---------------------------------------------+
      |                                             |
      |    ********** W A R N I N G **********      |
      |                                             |
      |  This system is private and is RESTRICTED   |
      |  to authorized users only.                  |
      |  If you are not authorized, DISCONNECT NOW! |
      |                                             |
      +---------------------------------------------+


^C
```

- Restricted login from local consol only - telnet transport disabled

```
line con 0
 exec-timeout 15 0
 password 7 1542220A06ABCD252637
 login local
 transport input none
line aux 0
 exec-timeout 15 0
 password 7 23361B0DABCD262A2SSS
 login local
line vty 0 4
 no exec
 exec-timeout 15 0
 no login
 transport input none
```

- Access list defined legal and illegal networks and hosts that allowed coming in or going out of border router. Access lists on the router should only require changes to reflect structural changes in the GIAC network it is fairly generic. Non-routable, spoofed and smurfed packets coming in from Internet are not allowed.

```
access-list 20 permit 123.12.26.12
access-list 101 permit ip 123.12.0.0 0.0.255.255 any
access-list 102 permit ip host 123.12.3.21 any
access-list 102 permit ip host 123.12.3.73 any
access-list 102 permit ip host 123.12.3.72 any
access-list 102 deny   ip 123.12.0.0 0.0.255.255 any
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any
access-list 102 deny   ip 172.0.0.0 0.31.255.255 any
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any
access-list 102 deny   ip 224.0.0.0 31.255.255.255 any
access-list 102 permit ip any any
```

2. Ingress and Egress Filters and border router interfaces

- Ingress filter applied on the interface connected to primary ISP, blocks non-routable, spoofed and smurfed packets coming in from Internet.

```
interface Hssi0/0/0
 description Connected to ISP 1 router.
 ip address 46.122.3.226 255.255.255.252
 ip access-group 102 in
 ip access-group 101 out
 no ip redirects
 no ip proxy-arp
 encapsulation frame-relay IETF
 no ip route-cache distributed
 frame-relay map ip 46.122.3.225 500 IETF
 frame-relay lmi-type ansi
```

- Egress packet filtering is being applied at firewall interface rather than at the border router.

```
interface FastEthernet0/1/0
 description Connected to external switch (fa0/1).
 ip address 123.12.3.2 255.255.255.0
 no ip redirects
 no ip proxy-arp
 no ip route-cache distributed
 full-duplex
 no cdp enable
!
interface FastEthernet1/1/0
 description Reserved for Inter-Router Link (x-Over) to GIAC-border-b(faa/1/0).
 ip address 123.12.3.4 255.255.255.0
 no ip redirects
 no ip proxy-arp
 no ip route-cache distributed
 full-duplex
 no cdp enable
```

3. Routing

- Only static route defined.

```
ip classless
ip route 0.0.0.0 0.0.0.0 Hssi0/0/0
ip route 123.12.0.0 255.255.0.0 Null0
ip route 123.12.3.0 255.255.255.0 Null0
```

4. Management

- Only allow read from management station.

```
snmp-server engineID local 00009086F9U
snmp-server community GIAC-MGT RO 20
snmp-server trap-source Loopback0
snmp-server packetsize 2048
snmp-server enable traps snmp
snmp-server host 123.12.26.12 GIAC-MGT
```

5. Global Internet access redundancy

- BGP peering with primary ISP.

```
router bgp 13463
 no synchronization
 network 123.12.0.0
 network 123.12.26.0 mask 255.255.255.0
 neighbor internal peer-group
 neighbor internal remote-as 13463
 neighbor internal update-source Loopback0
 neighbor internal version 4
 neighbor internal next-hop-self
 neighbor 46.122.3.225 remote-as 701
 neighbor 46.122.3.225 version 4
 neighbor 46.122.3.225 prefix-list GIAC_NETWORKS out
 neighbor 123.12.3.3 peer-group internal
 neighbor 123.12.26.6 peer-group internal
 neighbor 123.12.26.2 peer-group internal
 no auto-summary
```

Core Firewall

The firewall is a pair of Cisco PIX 520s running 5.3.1 software with Stateful failover implemented. Two units connect to each other by two cables, a failover serial cable and a crossover cable. When a failover occurs, each unit changes state. The newly active unit assumes the IP and MAC addresses of the previously active unit and begins accepting traffic, and the new standby unit assumes the failover IP and MAC address of the previous active unit. It takes about 15 to 45 seconds to cause a switchover[7].

The PIX has 5 interfaces configured as follows

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 public security20
nameif ethernet3 vpnnet security80
nameif ethernet4 failover security15
```

Here, ethernet0 is the outside network, ethernet1 is GIAC corporate LAN, ethernet2 is the web hosting DMZ, ethernet3 is the VPN DMZ network, ethernet4 is for failover.

```
ip address outside 123.12.3.5  255.255.255.0
ip address inside 124.12.0.1 255.255.0.0
ip address public 123.12.5.1 255.255.0.0
ip address vpnnet 123.12.4.1 255.255.0.0
ip address failover 192.168.0.1 255.255.0.0
```

Failover configure as follow.

```
failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 123.12.3.7
failover ip address inside 124.12.0.3
failover ip address public 123.12.5.3
failover ip address vpnnet 123.12.4.3
failover ip address failover 192.168.0.3
failover link fail
arp timeout 14400
```

Inbound connections from outside are enabled via static NAT translation slots as follows. Where 123.12.3.100 is the virtual web server, 123.12.3.101 is the virtual external dns server, and 123.12.3.102 is the virtual smtp gateway. Database server (IP 124.12.0.100) located at the inside network maps to VPN DMZ network as 123.12.4.100, it allows site-to-site VPN partners access. Syslog server (IP 124.12.0.101) located at the inside network maps to VPN DMZ network as 123.12.4.101 allow VPN concentrator to write logs.

[7] http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

```
static (public,outside) 123.12.3.100 123.12.5.100 netmask 255.255.255.255 0 0
static (public,outside) 123.12.3.101 123.12.5.101 netmask 255.255.255.255 0 0
static (public,outside) 123.12.3.102 123.12.5.102 netmask 255.255.255.255 0 0
static (inside,vpnnet) 123.12.4.100 124.12.0.100 netmask 255.255.255.255 0 0
static (inside,vpnnet) 123.12.4.101 124.12.0.101 netmask 255.255.255.255 0 0
```

Outbound connections are enabled via nat and global statements. Our policy only allow GIAC user located on inside network access outside network and Internet

```
nat (inside) 1 124.12.0.0 255.255.0.0 0 0
global (outside) 1 123.12.3.110 netmask 255.255.255.0
global (outside) 1 123.12.3.111-123.12.3.151 netmask 255.255.255.0
```

In addition to the access list, we implement the protocol-specific filters and fix-ups, so that the activeX and java applets will be blocked.

```
fixup protocol smtp 25
fixup protocol http 80
fixup protocol sqlnet 1521

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

SNMP is disabled as following

```
no snmp-server location
no snmp-server contact
snmp-server community getabettername
no snmp-server enable traps
```

Logging is enabled to the inside Syslog server.

```
logging on
logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered debugging
logging trap debugging
logging history warnings
logging facility 20
logging queue 512
logging host inside 124.12.0.101
```

IP Routing is simple here since all network are direct connected.

```
route outside 0.0.0.0 0.0.0.0 123.12.3.1 1
route inside 124.12.0.0 255.255.0.0 123.12.0.1 1
route vpnnet 123.12.4.0 255.255.255.0 123.12.4.1 1
```

Access Control

Since sanity check for inbound traffic has been done at the border router, the major concern here is what do we allow for inbound and outbound. Base on GIAC corporate security policy, we implement following policies for the core firewall.

- Permit inbound http and https access from outside network to web servers located at web hosting DMZ network through PIX's Ethernet 0 interface.
- Permit inbound dns and smtp access from outside network to dns server and smtp gateway located at web hosting DMZ network through PIX's Ethernet 0 interface.
- For remote access VPN, Permit inbound access from VPN DMZ network to web hosting DMZ network and GIAC inside network through PIX's Ethernet 3 interface.
- For site-to-site VPN, Permit inbound access from VPN DMZ network to web hosting DMZ network through PIX's Ethernet 3 interface.
- Permit outbound dns and smtp access from dns server and smtp gateway located at web hosting DMZ network through PIX's Ethernet 2 interface.
- Permit outbound http and https access from inside network to outside network through PIX's Ethernet 1 interface.

```
access-group outside_in in interface outside
access-group inside_in in interface inside
access-group public_in in interface public
access-group vpnnet_in in interface vpnnet
```

For outside interface, we allow incoming http, https, smtp, icmp and dns.

```
access-list outside_in permit udp any host 123.12.3.101 eq domain
access-list outside_in permit tcp any host 123.12.3.102 eq smtp
access-list outside_in permit tcp any host 123.12.3.100 eq www
access-list outside_in permit tcp any host 123.12.3.100 eq 443
access-list outside_in permit icmp any any
access-list outside_in deny ip any any
```

For public interface, we allow smtp and dns outbound connections only .

```
access-list public_in permit udp host 123.12.5.101 any eq domain
access-list public_in permit tcp host 123.12.5.102 any eq smtp
access-list public_in deny ip any any
```

For VPN network interface we permit site-to-site VPN access to database server, and everything for remote-access VPN.

```
access-list vpnnet_in permit tcp 10.10.10.0 255.255.255.0 123.12.4.100 eq sqlnet
access-list vpnnet_in permit udp 10.10.10.0 255.255.255.0 123.12.4.101 eq syslog access-
list vpnnet_in permit ip 123.12.4.0 255.255.255.0
access-list vpnnet_in deny ip any any
```

For inside interface, we allow outbound dns from internal DNS server, outbound http and https from web proxy, and outbound smtp from internal mail server to external mail gateway.

```
access-list inside_in permit udp host 124.12.0.103 any eq domain
access-list inside_in permit udp host 124.12.0.102 any eq www
access-list inside_in permit udp host 124.12.0.102 any eq 443
access-list inside_in permit udp host 124.12.0.104 123.12.5.102 eq smtp
access-list inside_in deny ip any any
```

Remote access VPN and site-to-site VPN

Cisco VPN concentrator 3030 provide VPN connection to partner network and serves as access point for mobile users. Remote users get their IP information including IP address, mask, dns server IP, and default gateway address from DHCP server 123.12.4.102. User authentication is done through external Secure ID ACE server 123.12.4.103. Static route is configured to enable partner network access the VPN DMZ network only. Only one partner is connected to GIAC at this point, it may grow in the future. To avoid potential routing problem, no default route for the concentrator itself is configured; Syslog server is configured to NAT to 123.12.4.101 to facilitate the logging requirement.

```
This table shows current IP addresses.
Interface IP Address/Subnet Mask MAC Address
----------------------------------------------------------------
Ethernet 1 - Private | 123.12.4.4/255.255.255.0 | 00.10.5A.1F.4F.0A
Ethernet 2 – Public  | 123.12.3.9/255.255.255.0 | 00.10.4F.99.7E.A2
Ethernet 3 - External | 0.0.0.0/0.0.0.0 |
----------------------------------------------------------------
```

VRRP Redundancy:
Enable VRRP
Group ID = 1
Group Password =
Role = Master
Advertisement Interval = 1
Group Shared Addresses
1(Private) = 123.12.4.5
2(Public) = 123.12.3.10

IPSec remote-access VPN Connection:
IPSec SA = ESP-3DES-MD5
Tunnel Type = Remote Access
Authentication = SDI

Remote Access User authentication:
Server Type = SDI
Authentication Server = 123.12.4.103
Server Port = 5500
Time out = 4
Retries = 2

DHCP Server:
DHCP Server = 123.12.4.102
Server Port = 67

IKE Proposal:
Proposal name = IKE-3DES-MD5
Authentication Mode = Preshared Keys
Authentication Algorithm = MD5/HMAC-128
Encryption Algorithm = 3DES-168
Diffie-Hellman Group = Group2(1024-bit)
Lifetime Measurement
Data Lifetime = 10000
Time Lifetime = 86400

IPSec site-to-site Partner VPN connection 1:
Name = partner_a
Interface = Ethernet 2 (Public) (123.12.3.9)
Peer = 10.10.10.1
Preshared Key = secret
Authentication = ESP/MD5/HMAC-128
Encryption = 3DES-168
IKE Proposal = IKE-3DES-MD5
Local Network
IP Address = 123.12.4.0
Wildcard Mask = 0.0.0.255
Remote Network
IP Address = 10.10.10.0
Wildcard Mask = 0.0.0.255

IP Routing:
Static Routes = 10.10.10.0/255.255.255.0 -> 123.12.3.9

Syslog:
Syslog Server = 123.12.4.101
Port = 514
Facility = Local7

Filter rules are based on only allow ICMP and sqlnet access to database:

```
IPSec-ESP: allow inbound, protocol ESP, source  0, destination 0, log to Syslog
SQLNET: allow inbound, protocol TCP, source  10.10.10.0/0.0.0.255, destination
123.12.4.101/0.0.0.0, log to Syslog
SQLNET: allow outbound, protocol TCP, source  123.12.4.101/0.0.0.0, destination
10.10.10.0/0.0.0.255, log to Syslog
ICMP: allow inbound, protocol ICMP, source  10.10.10.0/0.0.0.255, destination
123.12.4.101/0.0.0.0
```

Assignment 3 -- Audit Your Security Architecture

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

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

2. *Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.*

3. *Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.*

Auditing Proposal

Two proposals have been submitted to GIAC senior management team, one from independent security consulting firm, one from the security engineer who implemented the DMZ infrastructure.
Management team has made a decision to pursue the internal auditing first, the hire consulting firm base on the result if needed. I list two proposals here, because normally, it is unusual for the same group of person to audit an architecture they designed and built. Nevertheless, the internal engineer will follow the consulting firm's methodology to audit GIAC's DMZ network in a shrink-wrapper fashion. Since all needed disclosure requirement is handy, the required auditing work for internal engineers to do is to scan each network components, we will only show the internal scanning result here.

Proposal #1

GIAC outsource its security assessment to a security-consulting firm called eSecurity. This firm has developed a unique, multi-disciplined methodology to address the most significant sources of security risk. This proposal covers the risk reduction methodology, scope of the auditing, program deliverables, project timeline, and cost.

TIMELINE:

One month, from 12/15/2001 to 1/15/2002.

COST:

Base cost:	$79,000
One week on site:	$2,995/person x 5
Total:	$93,975

Scope and Objectives:
The objective is to work with GIAC in implementing a sound security infrastructure within its internal and external networks. The scope is based on an analysis of GIAC's internal and external network presence at its location and the application of the eSecurity methodology at that site.

General GIAC Responsibilities:

- Review the forms and the information requested in the SecureGuide
- Thoroughly complete all forms and return to designated eSecurity security analyst
- Determine the appropriate person with GIAC to complete the requested information

PLAN[8]:

I. Introductory Conference Call

Once project starts, eSecurity will conduct a formal conference call on the eSecurity program, looking for establishing following goal.

1. Provide an overview of how the process works
2. Set expectations of information, documentation, and personnel that needed to gather and interact with throughout the process
3. Overview remote scanning methodology
4. Schedule a date for the initial on-site to conduct a review of the SecureGuide and gather docs and data for the process

II. Initial Remote Discovery Scan

This procedure attempts to identify what hosts are active and visible from GIAC's Internet points of presence. The electronic sweep attempts to open connections to ports corresponding to know services on all hosts that comprise GIAC's Internet perimeter.

III. Remote Vulnerability Assessments

Once GIAC and eSecurity have completed the remote discovery scan, eSecurity's security analyst will perform a remote vulnerability assessment, know as Perimeter Check. This Check uses the information derived from the output of the Discovery Scan, it conducted with a combination of commercial and/or proprietary tools. The output provides eSecurity's analyst with the information necessary to spot possible weakness in the GIAC's network perimeter, e.g. outdated version of software, improperly or insecurely configured software, unnecessary or undocumented services, and improperly or dangerously configured hosts.

IV. Discovery and Disclosure Onsite

1. Essential Practices Overview

   Five areas will be considered: environment, connectivity, platform, services, and human factor.
2. Disclosure – Data Collection

   GIAC will be required to supply following materials:
   a. Internal and external topology diagrams and network maps
   b. IP addresses and descriptions of the associate hosts
   c. Services running on the hosts
   d. DNS and registrations info
   e. Firewall configuration and rule base
   f. VPN configuration and rule base
   g. IDS configuration and rule base
3. Discovery – DMZ Review

   ESecurity will review the documentation provided from GIAC through following process:
   a. Disclose how GIAC's DMZ functions and what the requirements are
   b. Disclose what hosts and services reside with DMZ: how they are administered, maintained and secured
   c. Disclose connectivity characteristics of DMZ: Links to Internet/intranet/partners, map of DMZ and description of information flow, controls applied
   d. Audit/monitoring characteristics of DMZ: what is monitored, how often, by whom, with what, process of handling exceptions/issues
4. Discovery – Physical Security and Environmental Review

V. Follow-up Vulnerability Testing

VI. Internal Assessment Onsite

Esecurity will conduct network scanning on each GIAC DMZ and internal network segments, and will perform network statistical sampling on GIAC internal network within 4 hour time period on a single day; data will be analyzed at a later time and be used to provide general architectural recommendations.

VII. Report and Presentation

[8] Partially from my corporate auditing plan

Proposal #2

TIMELINE:

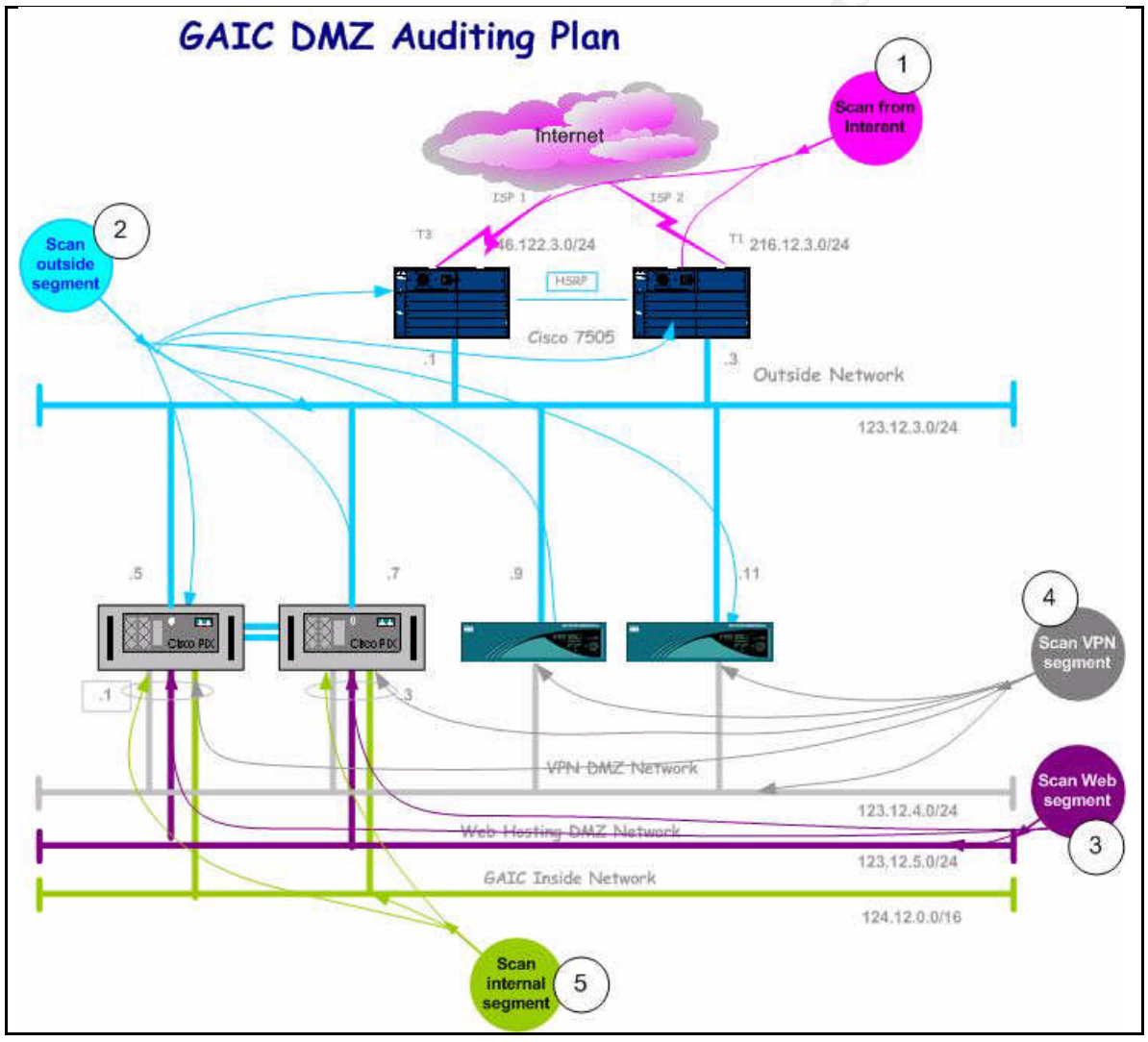
One week, from 12/15/2001 to 12/22/2001.

COST:

Equipment cost:	$0 x 3 Laptops
Labor cost:	$salary of 3 engineers
Software cost:	$0 – all free tools
Total cost:	$salary of 3 engineers

PLAN:

Scan DMZ from each access points/network segments, see the diagram below.



IMPLEMENTATION:

From audit point 1:

1. Scan hosts and services.

We use nmap to scan the Internet exposed IP addresses, to identify what hosts are active and visible from GIAC's Internet points of presence and the running services on each hosts. After scan the Class C network segment 123.12.3.0/24, we found following address are alive:

123.12.3.1, 123.12.3.3, 123.12.3.9, 123.12.3.11, 123.12.3.100, 123.12.3.101, 123.12.3.102, 123.12.3.104

The running services for each host are:

123.12.3.1:	none
123.12.3.3:	none
123.12.3.9,	none
123.12.3.11,	none
123.12.3.100,	tcp/80, tcp/443
123.12.3.101,	none
123.12.3.102,	tcp/25
123.12.3.104	none

2. Test router ingress filters.
   With the assistants from our ISP, we use packet craft tool to generate and fire packets with following source addresses to test the border routers' ingress filter rules.

   123.12.3.11,
   123.12.3.71,
   10.10.10.1,
   192.168.0.1,
   127.1.1.1,
   224.0.0.1

   From sniffer located at outside segment, we don't see any packets from the source above.

From audit point 2 (outside network segment):

1. Use nmap again to scan the active hosts and ports for following hosts:
   123.12.3.1, 123.12.3.3, 123.12.3.9, 123.12.3.11, 123.12.3.100, 123.12.3.101, 123.12.3.102, 123.12.3.104

2. Test firewall rules sets
   Again, we use packet craft tool to generate faked packets and fire them to the firewall, from firewall logs we saw them get dropped. From the sniffer running at inside network, VPN DMZ network, and public DMZ network, we don't find any faked packets.

3. Scan firewall open ports
   We use Firewalk(http://packetstorm.security.com/UNIX/audit/firewalk) to send packets through our firewall to determine which ports are open through it, we find out that our firewall open tcp/80, tcp/443, tcp/53, and tcp/25.

From audit point 3 (public/Web network segment):

1. Use nmap again to scan the active hosts and ports for following IP address,
   123.12.5.100, 123.12.5.101, 123.12.5.102, 123.12.5.1, 123.12.5.3
   The running services for each host are:

123.12.5.100,	tcp/80, tcp/443
123.12.5.101,	none
123.12.5.102,	tcp/25
123.12.5.1,	none
123.12.5.3,	none

2. Test firewall egress filter
   a. We spoofed our laptop IP address to 10.10.10.1, tried to connect to outside segment, VPN segment, and internal segment, all failed.
   b. We use a real IP address on the public network try to connect to Internet, VPN segment,

and internal segment, failed.

From audit point 4 (on VPN DMZ network segment):

1. Use nmap again to scan the active hosts and ports for following IP address, 123.12.4.100, 123.12.4.101, 123.12.4.102, 123.12.4.103, 123.12.4.1, 123.12.4.3 123.12.4.4, 123.12.4.6
   The running services for each host are:

123.12.4.100,	udp/514
123.12.4.101,	tcp/1251
123.12.4.102,	tcp/5500
123.12.4.102,	none
123.12.4.1,	none
123.12.4.3,	none
123.12.4.4,	none
123.12.4.6	none

2. Test firewall egress filter
   a. We spoofed our laptop IP address to 10.10.10.1, tried to connect to outside segment, public segment, and internal segment, all failed.
   b. We use a real IP address on the VPN DMZ network try to connect to Internet, failed.

3. Test VPN
   We scanned our partner's peer network but we could not find anything since they have firewall rules to drop connection from GIAC site. We also performed scanning from our partner's site, as expected, we find only host alived is 123.12.4.101

From audit point 5 (internal network segment):

1. Use nmap again to scan the active hosts and ports for following IP address, 124.12.0.100, 124.12.0.101, 124.12.0.102, 124.12.0.103, 124.12.0.104
   The running services are:

124.12.0.100,	tcp/1251
124.12.0.101,	udp/514
124.12.0.102,	tcp/80, tcp/443
124.12.0.103,	none
124.12.0.104,	tcp/25

2. Test firewall egress filter
   a. We spoofed our laptop IP address to 10.10.10.1, tried to connect to outside segment, public segment, and VPN segment, all failed.
   b. We use a real IP address on the internal network try to connect to VPN network, failed.

ANALYSIS:

The security architecture assessment was successful and did not contain any known security flaws or issues. The router and firewall rules were validated for proper functioning. However, some key points that GIAC Enterprises may want to consider.

1. Consider to use dedicated VPN segment for connectivity with partners
2. Consider implementing another pair of internal firewalls to offload the external firewall.
3. Consider tightening the ICMP protocol to disallow ICMP TTL Exceeded messages from leaving GIAC's public network.
4. Consider using digital certificates for partner VPN connection.
5. Consider to implement content filtering to block Java and activeX at Web Proxy level rather than PIX

firewall

6. Create a disaster recovery plan.
7. Consider implementing a business plan to do vulnerability assessment in a regular bases.

Assignment 4 - Design Under Fire

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

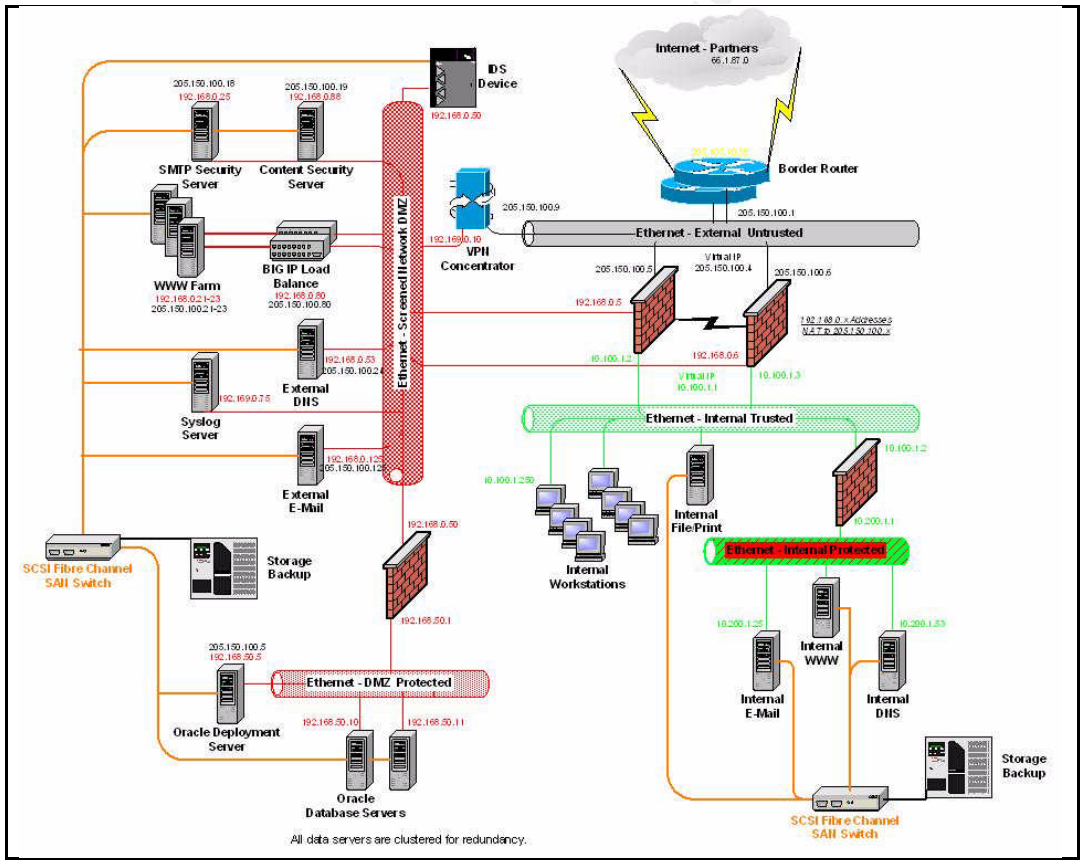
Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. *An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.*

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

3. *An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.*

http://www.sans.org/y2k/practical/Daniel_Martin_GCFW.doc



Attack Firewall

" GIAC Enterprise firewalls are comprised of Sun hardware and software incorporating CheckPoint Firewall-1 version 4.1 with service pack 3."

There are several vulnerabilities have been found for Checkpoint FW-1 with service pack 3:

1. RDP Communication Vulnerability: http://www.checkpoint.com/techsupport/alerts/rdp.html
2. Denial of Service Vulnerability: www.securityfocus.com [Bugtraq ID 2238].
3. Management Station Format String Vulnerability : www.securityfocus.com [Bugtraq ID 3021]
4. Firewall-1 SecureRemote Network Information Leak Vulnerability: www.securityfocus.com [Bugtraq ID 2238].

The simplest attack to this firewall is to take advantage of its Reliable Data Protocol to poke holes on firewall. Another attack is to utilize the Denial of Services vulnerability, since this vulnerability only applied to inside network adapter, we need to take over some internal hosts before we could attack firewall.

The result of RDP communication attack will allow us to gain access to internal hosts, which lead us to compromise the firewall eventually.

Here is the detail information of the 4 vulnerabilities above:

RDP Communication Vulnerability

Check Point uses a proprietary protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/FireWall-1 allows RDP packets to traverse firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/FireWall-1 gateway without being explicitly allowed by the rule base. In the 4.1 SP4 hotfix and all future service packs and releases, this default behavior is changed and RDP communication is blocked unless a specific access rule is written.

Denial of Service Vulnerability:

A problem with the license manager used with the Firewall-1 package could allow a Denial of Service. The problem manifests itself when the internal interface receives a large number of packets that are source routed and containing ficticious (or even valid) addresses. In a system containing a license with a limited number of protected IP addresses, the license manager calculates the address space protected by counting the number of addresses crossing the internal interface. When the large number of packets cross the internal interface, each IP address is added to the number calculated under license coverage. When the number of covered IP addresses is exceeded, an error message is generated on the console for each IP address outside of the covered range. With each error message generated, the load on the Firewall system CPU raises. This makes it possible for a user with malicious motives to make a firewall system inaccessible from the console by sending a large number of IP addresses to the internal interface.

Check Point Software has acknowledged this vulnerability and a workaround is available. For the workaround, see the solution section of this vulnerability database entry. This issue will be resolved in the next service pack.

Management Station Format String Vulnerability

Firewall-1/VPN-1 management station contains a format string vulnerability.
The vulnerability is the result of passing client-supplied data to a printf* function as the format string argument.

This vulnerability can only be exploited by a client that is authenticated as an administrator and connected from an authorized IP address.

Administrators with limited privileges (such as read-only) may be able to exploit this vulnerability to gain control over the management station.

Firewall-1 SecureRemote Network Information Leak Vulnerability

SecureRemote is the proprietary VPN infrastructure designed by Check Point Software, and included with some versions of Firewall-1.

A problem with the package allows remote users to gain information about internal networks. Older versions of the package send network topology information to SecureRemote connections prior to authentication, allowing an information gathering attack.

Denial of service attack

Because the "primary Internet connection is supplied by a lightning fast T3", and we have only 50 compromised hosts, it is difficult to lunch Dos attack from Internet that could either saturate the bandwidth or flood the Checkpoint firewall with SYNDefender properly configured. But Dos attacks to external DNS and web server are feasible.

Several Dos attack could be use are: Jolt2, Smurf, SYNFlood, Targa, TFN2K, and Trin00.

1. Jolt2 could be used to send a stream of fragmented packets to Windows systems. Its defense could be found from www.mcrosoft.com/technet/security/bulletin/
2. Smurf could be used to direct broadcast attacks to the victims. Its defenses could be filtering the ICMP at the router or firewall level.
3. SYNFlood could be used to open a large number of half-open TCP/IP connection. Its defenses has been implement in most firewall and router, nevertheless, it is still useful to attack a host.
4. Targa is a package that combines several attacking tools together, it could be used to lunch attacks like bonk, jolt, land, nestea, syndrop, teardrop, and winnuke etc.
5. TFN2K stands for Tribe Flood Network 2000, it could be used for ddos attack, similarly, Trin00 has the same functionalities.

Internal Host Attack

ATTACK PLAN[9]:

Step 1: establish a foothold on one internal host.

1. Social Engineering
2. Spam Email
3. War Dial
4. Steal salesperson's laptop
5. Hacking remote user's home PC

Step 2: Scan the Intranet.

1. Use nessus to map the internal network.
2. Use nmap/netcat to scan individual hosts, find out the running services.

Step 3: Get user ID and password.

1. Use sniffer to gather Unix user ID and password if possible.
3. Install Back Orifice to gain NT user ID and passwords.
4. Get /etc/password from Unix hosts, crack it on outside network.

[9] Methodology cited from Sans Institute, Track 4 – LevelTwo Advanced Incident Handle And Hacker Exploits

Step 4: Keep multiple backdoors for access

1. Install rootkit (both kernel level and application level)in unix system
2. Install netcat, tini in NT and Unix
3. Install Ddos tools: TFN2K and Trin00 on every compromised system
4. Install Loki, Https reverse proxy, covert_TCP programs.

Step 5: Cover the tracks on the network

1. Edit Unix log files and accounting entries.
2. Corrupt NT event log.

Step 6: Gain firewall access.

1. Poison internal DNS server or poison DNS cache, so that firewall management station will try to connect to the compromised hosts for authentication, then we can sniff out the admin password.

References:

1. http://www.cisco.com/warp/public/cc/pd/hb/vp3000/
2. http://www.cisco.com/warp/public/cc/pd/rt/7500/
3. http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/
4. http://www.checkpoint.com/techsupport/alerts/rdp.html
5. www.mcrosoft.com/technet/security/bulletin/
6. www.securityfocus.com
7. http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm.
8. http://www.cisco.com/warp/customer/707/advisory.html.
9. http://www.cisco.com/warp/customer/707/21.html.
10. http://www.inside-security.de/advisories/fw1_rdp.html
11. http://www.cert.org/advisories/CA-2001-17.html
12. Sans Institute, Track 4 – LevelTwo Advanced Incident Handle And Hacker Exploits
13. My corporate security policies