Susan Caskey
Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5e

Assignment 1 – Security Architecture

1.1 Background

GIAC Enterprises is a successful fortune cookie saying seller that grosses about $200 million in business per year. During the past few months, they have completed a merger with Wang Chung (WC) Inc., a smaller but very creative saying developer. Initially GIAC purchased all fortunes from a variety of suppliers, but with the merger with WC they will be developing some of their fortunes in house. They still maintain relations with a small set of suppliers, two currently, who provide fortunes based on haikus. They also are working with two partners who translate fortunes and resell them abroad.

GIAC developed their network based on Suns running Solaris (mostly 2.7 and 8, but there are a few others around) and designed a network with security as a primary focus. WC works on windows based PC's and Mac's and used NT for all their servers. They did not focus on security but rather on making the system easy to use and as a result had a number of security problems (a likely cause to their assimilation by GIAC). After the merger, GIAC took to the initiative to design a secure network that provided the flexibility the WC employees were used to.

1.1.1 GIAC's Internal Details and requirements

The company is divided between two network segments: the finance group and the design group. The finance group work mostly on PC's and need to be able to email anyone, browse the web, download occasional files and run video conferencing to suppliers and partners. They also have a robust database that houses all the internal financial information and external billing, as well as other company information. This system is open to all on the finance network, but only to a few in the design group.

The design group runs PC's and Mac's on their network and need the ability to email anyone, browse the web, download files, and being the creative type, they love to listen to music while they work. A small number need limited access to the finance database. The design group is also responsible for maintaining the website and uploading new sayings to the sayings database.

The entire staff would like the ability to work from home or on the road. This was one of the benefits WC had that GIAC did not; so, GIAC does not have the dial-in infrastructure in place. In addition, GIAC does a great deal of business internationally and would like to avoid the International Road Warriors dialing back to the United States for Internet access; they have chosen to use International ISPs like CompuServe or iPass and VPN software.

1.1.2 Partner, Supplier, and Customer requirements

There are three external entities that require access to GIAC: the company's customers, suppliers, and partners. The customers need access to the website and email servers, as well as the sayings database in order to download their bulk sayings. The suppliers need to transmit their sayings the sayings database. They also need to send and receive emails. Finally, the partners need to access the sayings database in order to download sayings for translation and of course they need to be able to email. The partners also need occasional resources located on the design network.

1.2 Company Security Plan

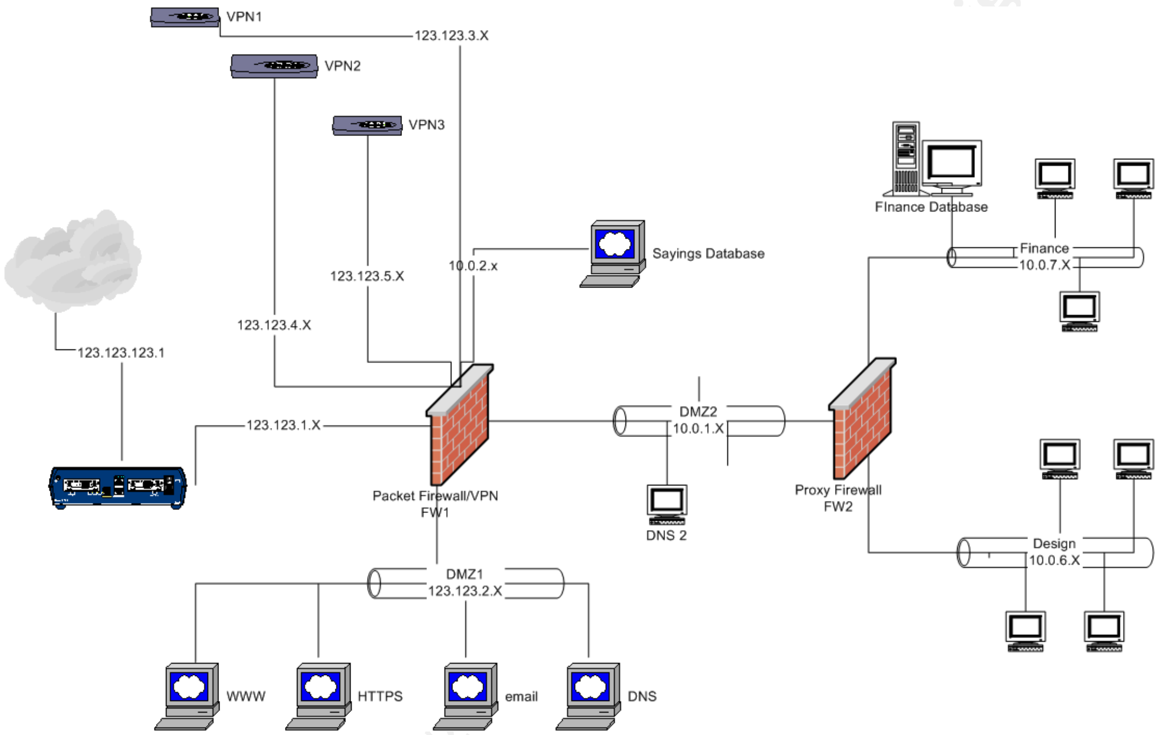
GIAC had previously established five rules of thumb for security and have continued to maintain these rules after the merger:

All connections from the Internet to either internal network or database must be encrypted
All data coming in from the Internet must go through a firewall
No direct dial-up on the internal network (no functional modems)
All downloads must be virus checked
Email clients must not auto-run anything (macro's disabled by default)

GIAC's most valuable asset is the sayings database. Since the sayings database needs to be accessed by customers via the Internet, it requires some form of connection to the Internet. To handle security for this system they only allow SQL requests for download from an https system or from the internal network. All SQL requests for upload can only come via a VPN tunnel or from the internal network.

1.3 Detailed Network Design [Diagram 1.1]

GIAC has two T1s to the Internet that is run through a Cisco router. This router contains a standard good practice list of ACL's but does not do any additional packet fire walling or VPN. The Cisco is connected to a Sun Solaris system running the Checkpoint FW-1 packet filtering firewall with 6 network connections.



[1.1]

This firewall (FW1) uses NAT to limit the number of real IP's needed and to take advantage of the NAT security bonus on some of the network segments.

The first DMZ (DMZ1) contains the web server, email server, external DNS, and secure web server. It also contains a little snort sniffer running on a Linux box.

The third, fourth, and fifth interfaces are connected to the three Network Alchemy (now Nokia) VPN systems. The use of three different VPN systems allows for specific rules for the three different VPN users (suppliers, partners, and road warriors).

The sixth interface connects to the sayings database. This system lives on its own subnet to limit all connections to it and avoid needing any other connections on its subnet.

The seventh, and final, interface connects to the second DMZ (DMZ2).

This network contains the DNS server for the outgoing requests and the second firewall (FW2). FW2 is a BSD system running OpenBSD's ipf with three used network interfaces. This firewall does packet filtering and proxy http, https, and ftp. There is also a little Linux sniffer on DMZ2. The design network is housed off of one of FW2's interfaces and the finance network is off the other.

1.3.1 Data Flow for Customers [Diagram 1.2]

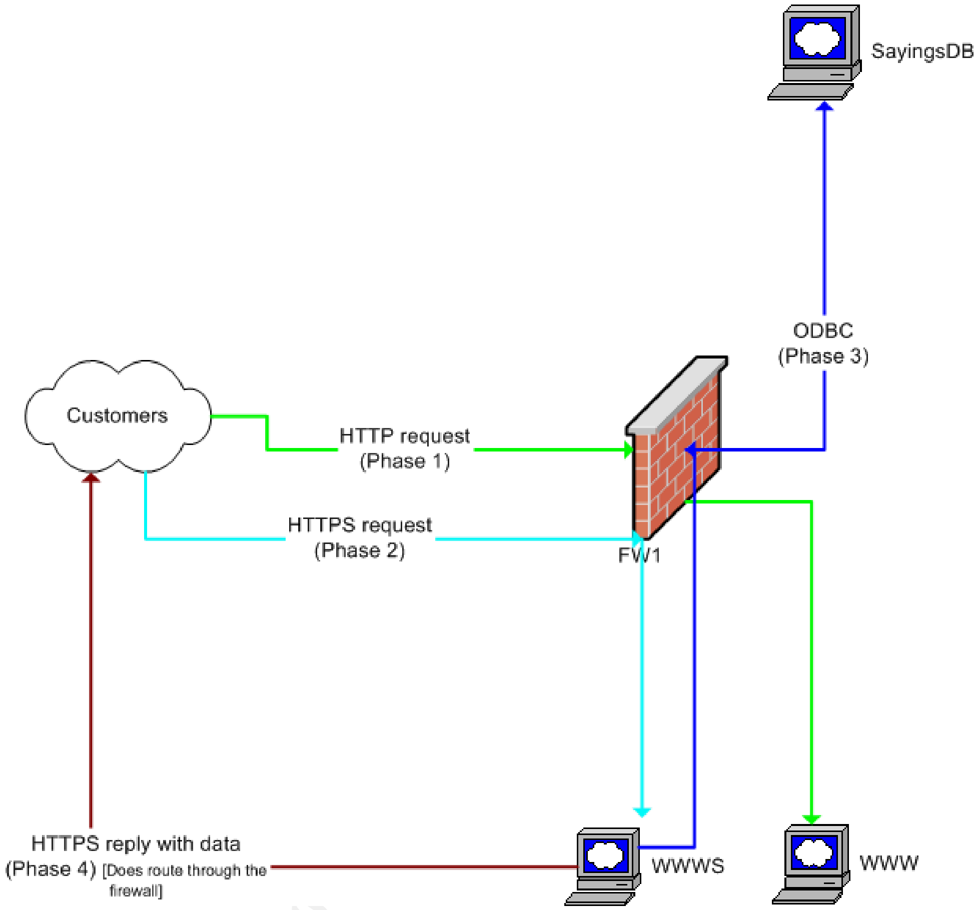
A company that makes fortune cookies needs a supplier for fortunes; they will find GIAC on the Internet via GIAC's external website. If they choose to become a customer of GIAC, which of course they will, they are passed to the secure web server to create a customer account. This account includes all their billing information and other related stuff. Once they have an account, they are provided with the order form. This order form determines what type of fortunes they are looking for and the amount. This information is used to create an SQL query.

The secure web server sends the query through the firewall to the sayings database. The database processes the query and returns the requested fortunes. This file is now located on the secure web server and linked for download by the customer. This file is removed from the secure web server upon a session timeout.

Established customers can connect directly to the secure web server via cookies or username and password. They will then order fortunes in the same manner as new customers.

1.3.2 Data Flow for Suppliers

Suppliers need to access the sayings database for the purpose of adding sayings only. They connect to the network via a VPN tunnel, through the firewall. Once the data has been decrypted, it is passed back through the firewall and sent to the sayings database. The database allows appending of data only from the suppliers. All the suppliers are required to use VPN to transmit the sayings into the database.



[1.2]

1.3.3 Data Flow for Partners

GIAC's partners also use a VPN tunnel to connect to the sayings database to request sayings for translation and resell. They can also use the VPN tunnel to connect to the design network to access a limited set of resources.

1.3.4 Data Flow for Road Warriors and Telecommuters

For GIAC's employees that travel and the employees that telecommute, GIAC has provided them with VPN client software and personal firewalls. They connect to the company's network via the VPN in a client mode. They can filter email and web applications, as well as development systems through the VPN.

Assignment 2 – Security Policy

2.1 Cisco Router

The router is a Cisco 3620 with a dual T1 and Ethernet interface. It is running the Cisco IOS with standard and extended ACL's.

```
Inbound and Outbound:   Access-list 12 deny 10.0.0.0 0.255.255.255
                        Access-list 12 deny 172.16.0.0 0.15.255.255
                        Access-list 12 deny 192.168.0.0 0.0.255.255
                        Access-list 12 deny 127.0.0.0 0.255.255.255

          Inbound:      Access-list 12 deny 123.123.0.0. 0.0.255.255
                        Access-list 152 Allow tcp any any eq http
                        Access-list 152 Allow tcp any any eq https
                        Access-list 152 Allow tcp any any eq dns
                        Access-list 152 Allow udp any any eq dns
                        Access-list 152 Allow tcp any any eq smtp
                        Access-list 152 Allow tcp any any eq ESP
                        Access-list 152 deny any any any
```

2.2 FW1 (Checkpoint FW-1 on Solaris)

FW1 is the heart of this network doing all the routing and security for all the servers, the sayings database as well as the internal users. It does NAT for the sayingsDB network and DMZ2 (the internal users). Routable IP's are used for DMZ1 (the servers' network).

2.2.1 OS Hardening

Checkpoint is running on Sun system with Solaris 7. The operating system is the bare minimum core install and almost all startup scripts have been removed from the /etc/rc directories.

2.2.2 Firewall Config

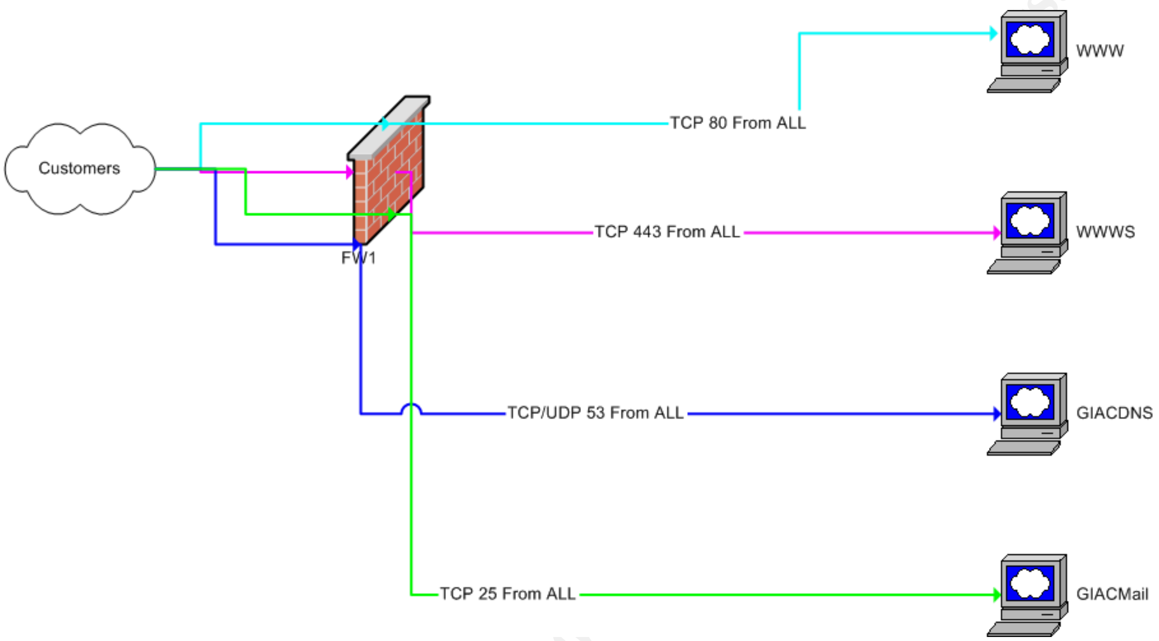
The firewall configuration has been broken down into five areas based on the source and destination of the traffic. These are the external customer's needs, the supplier's needs, the partner's, the road warrior's and the internal system's needs. The networks are defined as External is anything coming from the Internet, DMZ1 is the network with the servers; they are www for the web server, wwws for the secure web server, GIACmail for the mail server and GIACdns for the dns server. DMZ2 is the DMZ that leads to the internal users systems and, finally, SayingsDB is the sayings database system.

2.2.2.1 The Customer [Diagram 2.1]

The customers need access to the servers, but nothing else. This constitutes 4 rules for the database:

Src	Dest	Service	Action	Comment

All	www	http	Accept	TCP 80
All	wwws	https	Accept	TCP 443
All	GIACmail	smtp	Accept	TCP 25
All	GIACdns	dns	Accept	TCP/UDP 53

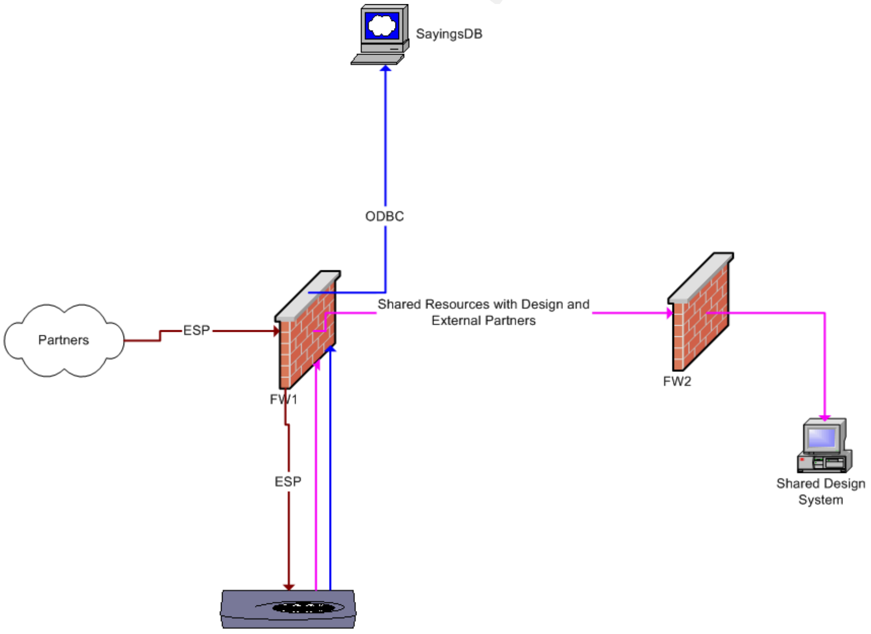


[2.1]

2.2.2.2. The Partner [Diagram 2.2]

The partners require access to the sayings database and to a shared system on the design network. This connection is done via VPN. The VPN tunnel for partners is defined as IPSec using DES3/SHA1 public/private key, with an 8-hour re-key using Diffie-Helman. (Initial keys are snail mailed.) The ESP packets are allowed from the Partner's network and once decrypted, specific rules are used to limit the access within the rest of the network. These rules are:

Src	Dest	Service	Action	Comment
Partners	VPN1	ESP	Accept	
VPN1	SayingDB	ODBC	Accept	TCP 1527[1]
VPN1	DMZ2dgn	SSH	Accept	TCP port 22



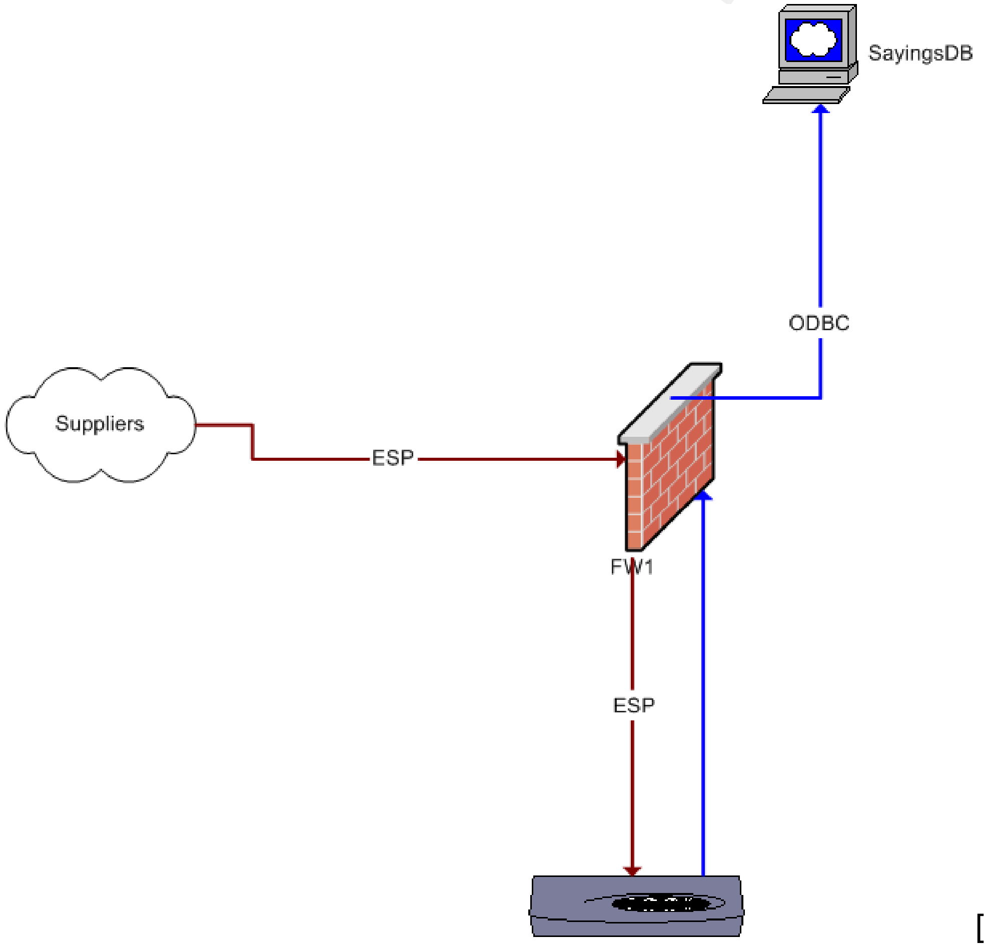
[2.2]

[1] TCP Port 1527 is the port configured to send ODBC requests to the firewall.

2.2.2.3 The Supplier [Diagram 2.3]

The suppliers only require access to the sayings database and this is done via VPN. The VPN tunnel for the suppliers is defined in the same way as for the partners: IPSec using DES3/SHA1 with public/private key, 8-hour re-key using Diffie-Helman. There is a single rule defined each of the supplier's access once the packet has been decrypted, but a separate rule will be used for each unique supplier coming into VPN2:

Src	Dest	Service	Action	Comments
Suppliers	VPN2	ESP	Accept	
VPN2	SayingDB	ODBC	Accept	TCP 1527



[2.3]

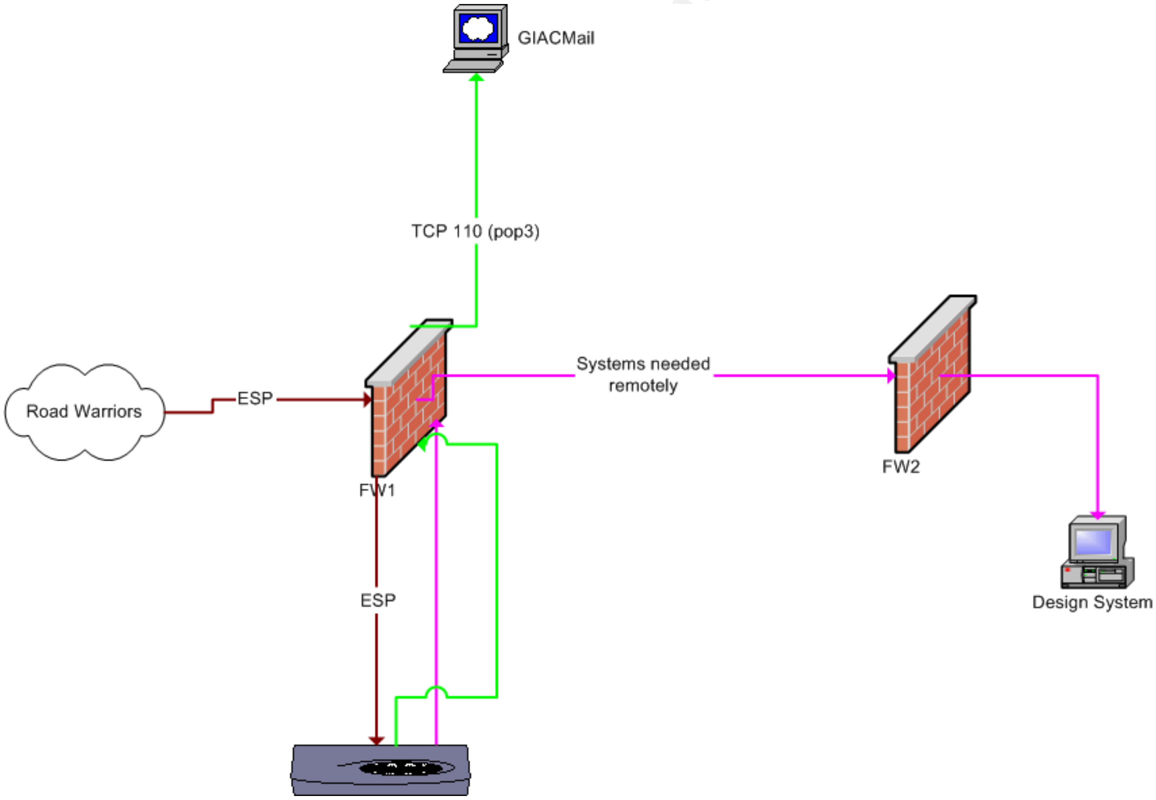
2.2.2.4 The Road warriors [Diagram 2.5]

The road warriors and telecommuters are all able to connect to the internal network using VPN, once connected they have total access to the systems on the internal network.

The VPN system they are required to use is PGP's VPN and personal firewall software. The PGP software has a nice auto discover feature that allows a user to specify the security policy without knowledge of ports and also quickly shows if anything odd is trying to connect from the PC out (a Trojan program or something like Microsoft Office). The road warriors are using certificates to establish the VPN connection.

Once decrypted, the road warriors have total access to the systems within the DMZ2 network. They also have pop3 and smtp access to the mail server on DMZ1.

Src	Dest	Service	Action	Comment
ALL[2]	VPN3	ESP	Accept	
VPN3	DMZ2	ALL	Accept	
VPN3	GIACmail	pop3/SMTP	Accept	



[2.5]

[2] Since most dial-up providers use dynamic ips, you can't limit on the source address. Hopefully the road warrior's personal firewall and the use of certificates will be sufficient.

2.2.2.5 Internal Requirements [Diagram 2.6]

Various systems need to interact with systems on other network segments. These needs define the internal configuration requirements. Starting from DMZ1, the secure web server need to send ODBC messages to the sayings database and receive responses. The users on DMZ 2, specifically the design group (DMZ2dgn), also need to send ODBC messages to the sayings database, plus ssh into the system for system maintenance. These same design users need ssh to maintain the servers on DMZ1.

All the internal users, both design and finance, need to connect to the mail server via pop3 and smtp. The initial design of this network used a proxy email server, but that forced a hole in the firewall allowing an externally accessible server to connect to an internal server. Instead, the mail is served from the external server and users are required to store email on their local system.

The internal dns server, DNS2, needs to request dns information from the main dns server, GIACdns via TCP and UDP 53.

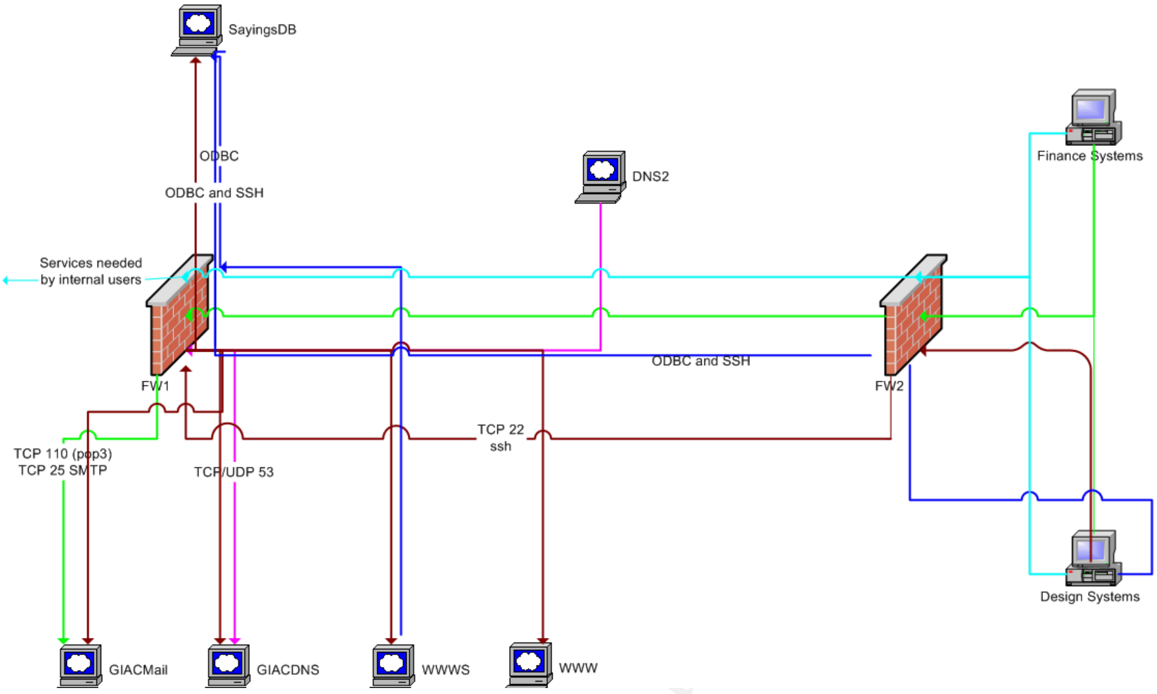
The internal users need a limited set of connections to the outside world. These include ssh, real-audio, Netmeeting, http, https, Cu-SeeMe, and ftp. All other connections to the outside world are dropped. The plan of limiting outbound connections is often debated as it can lead to a feeling of frustration between the IT department and the rest of the users. However, GIAC has good communication[3] between all the departments making this work successfully.

The firewall rules for the internal systems are:

Src	Dest	Service	Action	Comment
WWWS	SayingDB	ODBC	Accept	TCP 1527
DMZ2dgn	SayingDB	ODBC/ssh	Accept	
DMZ2dgn	DMZ1	ssh	Accept	
DMZ2	GIACmail	pop3/smtp	Accept	
DNS2	GIACdns	dns	Accept	TCP/UDP 53
DMZ2	External	ssh/Real-audio Netmeeting/http https/ftp/Cu-Seeme[4]	Accept	

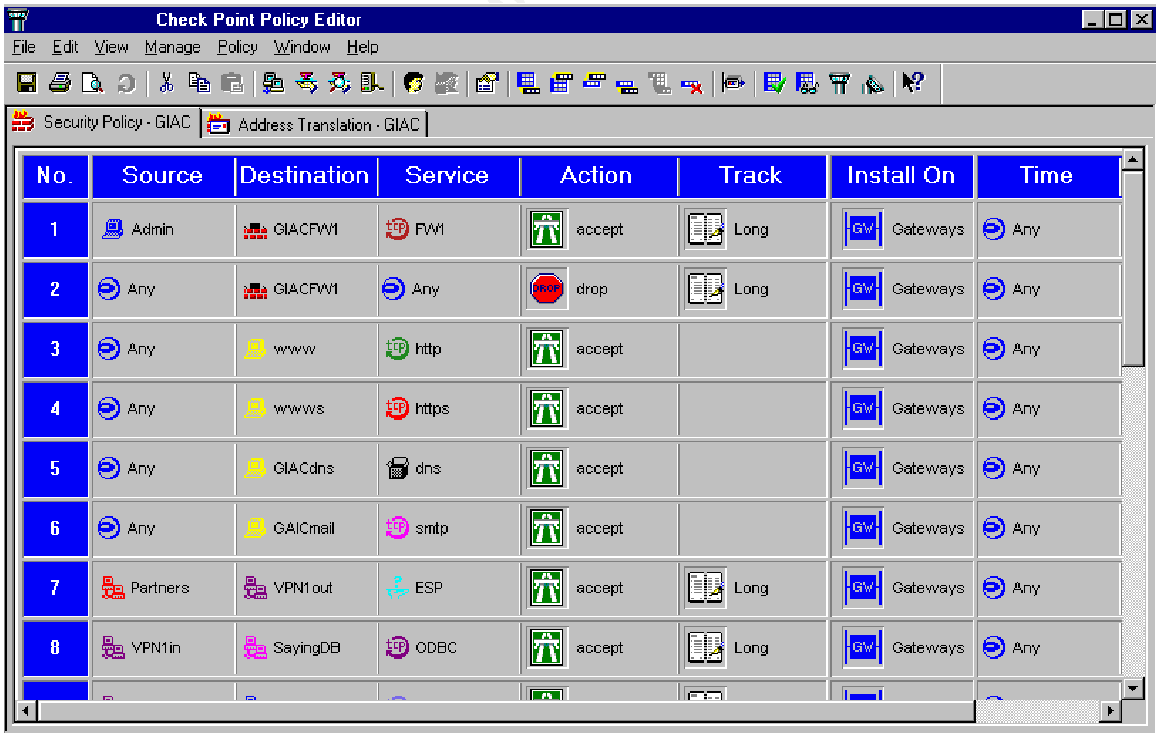
[3] Since GIAC is a fictitious company, it can have good communication between all the departments.

[4] Other services can be added as specific needs come up. These are just the common things needed by the GIAC employees.

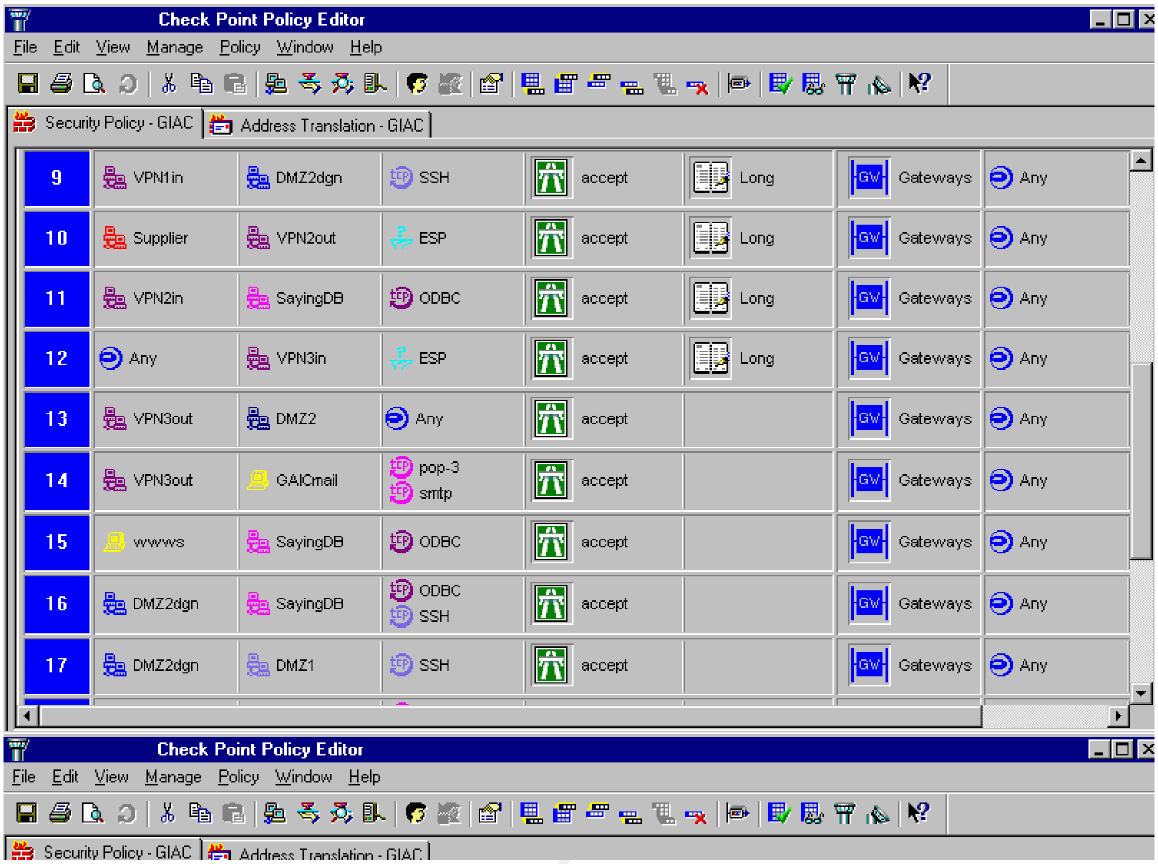


[2.6]

2.2.3 Complete Checkpoint Policies:


Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - GIAC
Address Translation - GIAC

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Admin	GIACFW1	FW1	accept	Long	Gateways	Any
2	Any	GIACFW1	Any	drop	Long	Gateways	Any
3	Any	www	http	accept		Gateways	Any
4	Any	wwws	https	accept		Gateways	Any
5	Any	GIACdns	dns	accept		Gateways	Any
6	Any	GAICmail	smtp	accept		Gateways	Any
7	Partners	VPN1out	ESP	accept	Long	Gateways	Any
8	VPN1in	SayingDB	ODBC	accept	Long	Gateways	Any


Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - GIAC
Address Translation - GIAC
Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - GIAC
Address Translation - GIAC

9	VPN1in	DMZ2dgn	SSH	accept	Long	Gateways	Any
10	Supplier	VPN2out	ESP	accept	Long	Gateways	Any
11	VPN2in	SayingDB	ODBC	accept	Long	Gateways	Any
12	Any	VPN3in	ESP	accept	Long	Gateways	Any
13	VPN3out	DMZ2	Any	accept		Gateways	Any
14	VPN3out	GAICmail	pop-3 smtp	accept		Gateways	Any
15	wwws	SayingDB	ODBC	accept		Gateways	Any
16	DMZ2dgn	SayingDB	ODBC SSH	accept		Gateways	Any
17	DMZ2dgn	DMZ1	SSH	accept		Gateways	Any

2.3 DMZ1

2.3.2 Email Server

The email system, GIACmail, is running on a Solaris 7 system using the free sendmail 9.X. The system has been hardened and is only running essential services. For email virus protection, it is running the MacAfee virus scanner with Amavis. At this time, ssh (sshd) is not running on this system.

An nmap scan shows what is running on this system:

```
(The 3078 ports scanned but not shown below are in state: closed)
Port            State     Service
25/tcp          open      smtp
```

```
110/tcp         open      pop-3
587/tcp         open      submission
6000/tcp        open      X11

TCP Sequence Prediction: Class=random positive increments
                Difficulty=42155 (Worthy challenge)
Remote OS guesses: Solaris 2.6 - 2.7, Solaris 7
```

2.3.3 Web Server

The web server is a Sun system running Solaris 8 and the Apache web server. The web process is running as user and group *web*. The system has been hardened and only essential services are running.

```
(The 3065 ports scanned but not shown below are in state: closed)
Port                    State     Service
22/tcp                  open      ssh
80/tcp                  open      http
514/udp         open      syslog
6000/tcp        open      X11

Remote OS guesses: Solaris 2.6 - 2.7, Solaris 2.6 - 2.7 with tcp_strong_iss=0,
Solaris 2.6 - 2.7 with tcp_strong_iss=2, Solaris 7
```

2.3.4 Secure Web Server

This system is also a Sun running Solaris 7 and Apache's secure web server. This system has also been hardened.

```
(The 3065 ports scanned but not shown below are in state: closed)
Port            State     Service
22/tcp          open      ssh
443/tcp                 open      https
3306/tcp        open      mysql
6000/tcp        open      X11

Remote OS guesses: Solaris 2.6 - 2.7, Solaris 2.6 - 2.7 with tcp_strong_iss=0,
Solaris 2.6 - 2.7 with tcp_strong_iss=2, Solaris 7
```

2.3.5 DNS

This is another Sun running Solaris and BIND.

```
(The 3065 ports scanned but not shown below are in state: closed)
Port            State     Service
22/tcp          open      ssh
53/tcp          open      domain
53/udp          open      domain
6000/tcp        open      X11

Remote OS guesses: Solaris 2.6 - 2.7, Solaris 2.6 - 2.7 with tcp_strong_iss=0,
Solaris 2.6 - 2.7 with tcp_strong_iss=2, Solaris 7
```

2.3.6 Sniffer

The sniffer for DMZ1 is a Linux box running snort. For this network, the snort rules have been modified from those provided by whitehat.org. These are very detailed rules and can often provide too much information, but are an excellent starting point. The modifications made were to reduce alarms from port 80 requests to the web server and 443 to the secure web server. A subset of the rules are as follows[5]:

```
# Change these next lines to match your network!
var INTERNAL 123.123.2.0/24
var EXTERNAL !123.123.2.0/24

preprocessor http_decode: 80 443 8080
preprocessor minfrag: 128
preprocessor portscan: $INTERNAL 3 5 /var/log/snort/portscan

alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS116/SourceRoute-ICMP-lssr"; ipopts:
lsrr ;)
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS117/SourceRoute-ICMP-lssre";
ipopts: lsrre ;)
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS118/Traceroute-ICMP"; ttl: 1; itype:
8;)
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS135/icmp-redirect_host"; itype: 5;
icode: 1;)
[…]
alert TCP $EXTERNAL 80 -> !www.giac.com
alert TCP $EXTERNAL 443 -> !wwws.giac.com
alert UDP $INTERNAL 31337 -> $EXTERNAL any (msg: "IDS189/trojan-active-back-orifice";)
alert UDP $INTERNAL any -> $EXTERNAL 20433 (msg: "IDS256/ddos-shaft-agent-to-handler";
content: "alive";)
alert UDP 255.255.255.255/32 any -> $INTERNAL any (msg: "IDS201/backdoor-Q-udp"; dsize:
>1;)
alert UDP any any -> any 31335 (msg: "IDS187/trin00-daemon-to-master-pong"; content:
"PONG";)
#end arachNIDS export
```

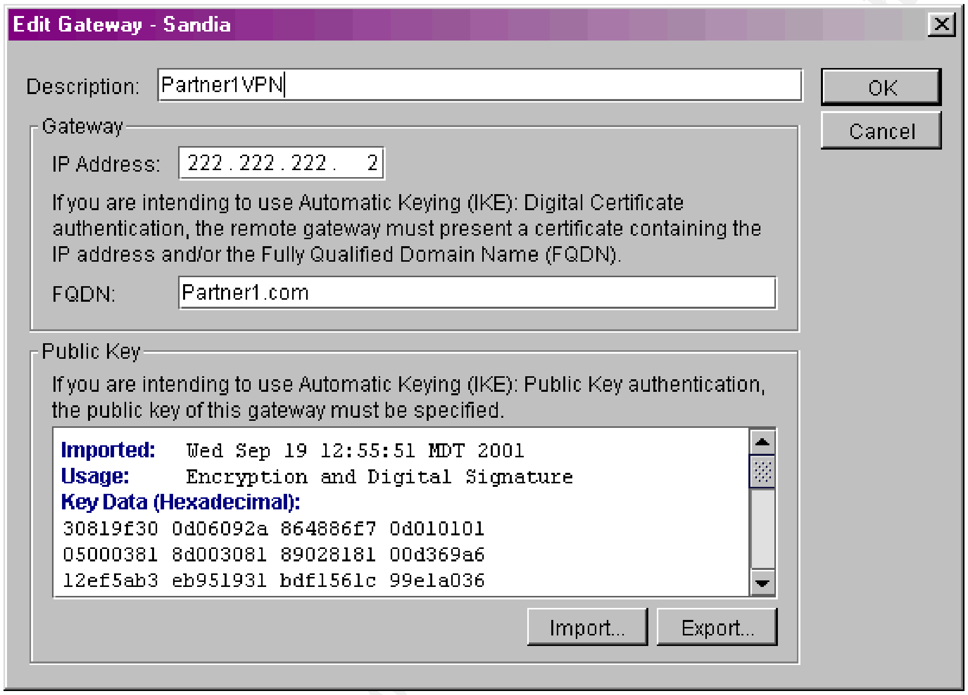
2.4 VPN

The entire VPN system is running on clusters of Network Alchemy cc500 boxes (now Nokia). For each of the three clusters, the IP for the external interface is a routable IP, while the internal interface is using a non-routable IP. The systems provide tunnels to the suppliers and the partners. The supplier's tunnels allow routes to the Sayings DB, but the partners have access to both the Sayings DB and a limited number of systems on the design network (DMZ2dgn).

The firewall has static routes from DMZ2 to the VPNs for tunneling that is initiated within GIAC.

[5] This is just a small portion of the rules since they span 10 pages.

VPN1 and VPN2 are configured for tunneling to the partners and suppliers systems, respectfully. The networks at the partners and suppliers ends have met GIAC's standards for security to limit the worry of VPN session hijacking. These both use public/private key.



Edit Gateway - Sandia

Description: Partner1VPN

Gateway

IP Address: 222 . 222 . 222 . 2

If you are intending to use Automatic Keying (IKE): Digital Certificate authentication, the remote gateway must present a certificate containing the IP address and/or the Fully Qualified Domain Name (FQDN).

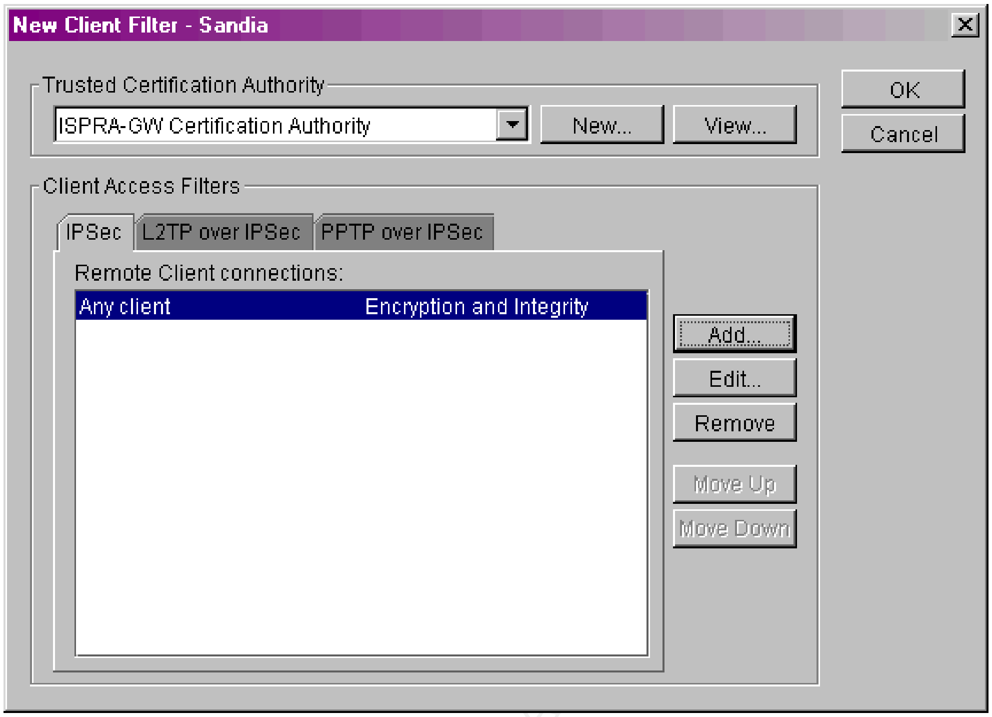
FQDN: Partner1.com

Public Key

If you are intending to use Automatic Keying (IKE): Public Key authentication, the public key of this gateway must be specified.

```
Imported:   Wed Sep 19 12:55:51 MDT 2001
Usage:      Encryption and Digital Signature
Key Data (Hexadecimal):
30819f30 0d06092a 864886f7 0d010101
05000381 8d003081 89028181 00d369a6
12ef5ab3 eb951931 bdf1561c 99e1a036
```

VPN3 uses certificates for the road warriors and telecommuters to the company.



New Client Filter - Sandia

Trusted Certification Authority: ISPRA-GW Certification Authority

Client Access Filters

Remote Client connections:

Any client Encryption and Integrity

2.5 Sayings DB

The sayings database is a SQL database (MySQL) running on a Sun Solaris system. This is another bastion system like the other servers and has a very limited set of open ports:

```
(The 3065 ports scanned but not shown below are in state: closed)
Port          State     Service
22/tcp        open      ssh
1527/tcp      open      odbc
3306/tcp      open      mysql
6000/tcp      open      X11

Remote OS guesses: Solaris 2.6 - 2.7, Solaris 2.6 - 2.7 with tcp_strong_iss=0,
Solaris 2.6 - 2.7 with tcp_strong_iss=2, Solaris 7
```

2.6 DMZ2

2.6.2 Sniffer

Like the sniffer on DMZ1, this is a Linux system running snort with a modified set of rules from whitehat.org.

2.6.3 DNS

The internal DNS server is configured like the external with only the ports necessary for DNS to function open. This is also a Sun Solaris system running OS 7.

```
(The 3065 ports scanned but not shown below are in state: closed)
Port          State     Service
```

```
22/tcp       open    ssh
53/tcp       open    domain
53/udp       open    domain
6000/tcp     open    X11

Remote OS guesses: Solaris 2.6 - 2.7, Solaris 2.6 - 2.7 with tcp_strong_iss=0,
Solaris 2.6 - 2.7 with tcp_strong_iss=2, Solaris 7
```

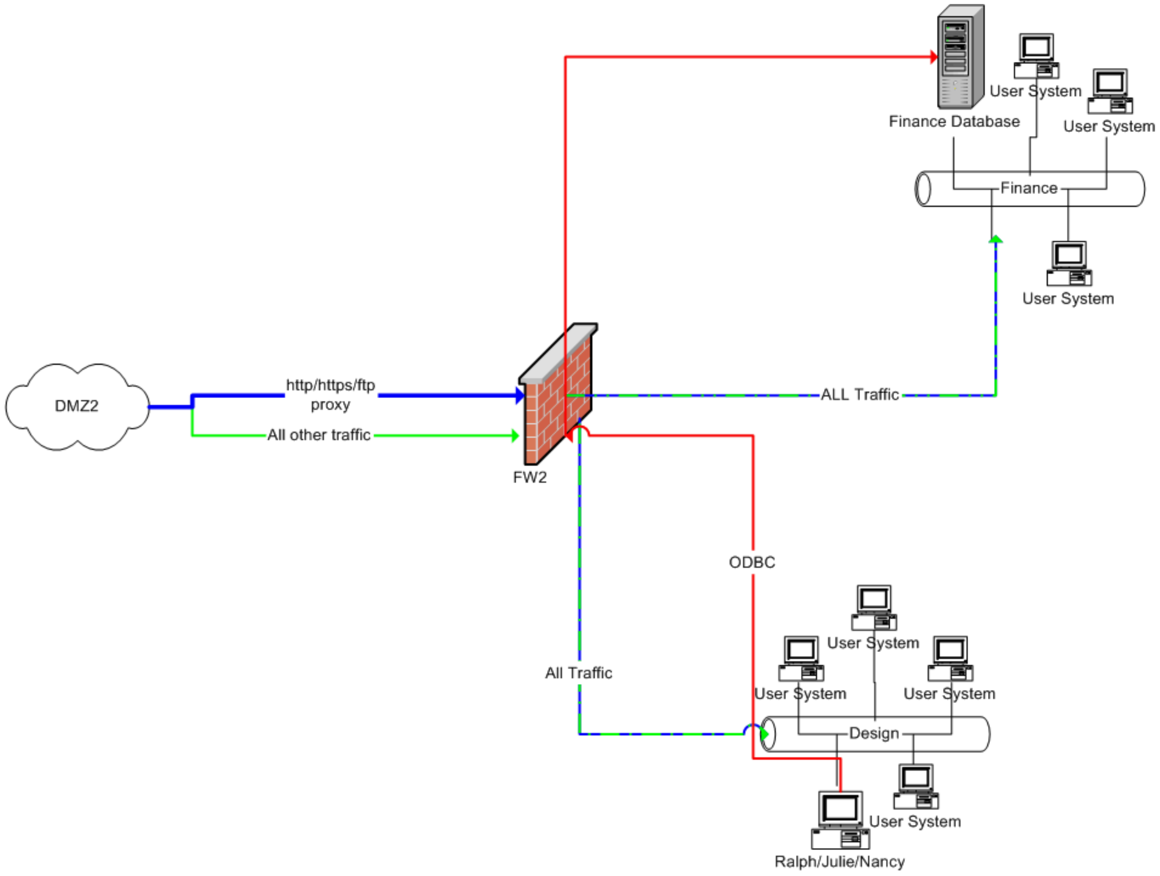
2.6.4 FW2

This firewall is both a packet and a proxy firewall. Http, https, and ftp are all proxied as the entire either the design or the finance network. The other services are time dependent like CU-seeme and real audio so these are allowed in without the proxy. Between the two networks, only a small set of users on the design network need access to the finance database and no one on the finance network requires access to the design network. Both networks have free access to send anything through this firewall.

Src	Dest	Service	Action
All	Design/Finance	http/https/ftp	Proxy
All	Design/Finance	All	Accept
Ralph Julie Nancy	FinanceDB	ODBC	Accept[6]
Design	Finance	All	Drop
Finance	Design	All	Drop
External	Finance/Design	All	Accept

[Diagram 2.7]

[6] Ralph, Julie, and Nancy are all the people that need access to the finance database from the design network. They only need access via ODBC.



[2.7]

OpenBSD: ifp.rules and ipnat.rules (txp0 is DMZ 2 interface, txp1 is design network and txp2 is the finance network)

```
map txp0 txp1/32 txp2/32 proxy port ftp http https
pass in on txp0 any to any
block in txp2/32 any from txp1/32
block in txp1/32 any from txp2/32
pass in on txp2/32 from 10.0.6.12/32 port = 1527 keep state
pass in on txp2/32 from 10.0.6.13/32 port = 1527 keep state
pass in on txp2/32 from 10.0.6.14/32 port = 1527 keep state
pass out on txp0/32 any from any
```

Assignment 3 – Assessment

3.1 Perimeter defense

The initial assessment of this network would be done from an outside system during a variety of days and times. This should take multiple days to get a valid report of changing rules and will require several man-hours. The hardware costs for this are minimal as the tools used are free and will run on low-end hardware.

The first step in analyzing this network would be via DNS. First, by looking at the whois database for giac.com, the primary name server for giac.com is reveled.

```
cadfael% whois giac.com

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: GIAC.COM
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com
   Name Server: DNSgiac.giac.com
   Name Server: NS1.ISP.COM
   Updated Date: 20-jun-2001
```

From this, an nslookup probe will revel the IP's used:

```
cadfael% nslookup www.giac.com dnsgiac.giac.com
Server:  dnsgiac.giac.com
Address:  123.123.2.2

Name:    www.giac.com
Address:  123.123.2.3

[…]

Name:    wwws.giac.com
Address:  123.123.2.4

Name:    mailgiac.giac.com
Address:  123.123.2.5
```

A traceroute to any of these systems would show where the router is located.

```
> traceroute www.giac.com
traceroute to www.giac.com (123.123.2.3), 30 hops max, 40 byte packets
 1  tenkuu (198.59.115.1)  3 ms  3 ms  1 ms
 2  123.123.123.1 (123.123.123.1)  36 ms *  35 ms
```

The traceroute will not continue beyond the router since the routers ACL's are blocking odd UDP and ICMP on the inbound interface.

The next scan would be an nmap scan against the router and other IP's to see what services might be running. The nmap is done with the –P0 option since it is clear that ICMP is blocked.

```
nmap -sTU -P0 123.123.123.1

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
All 3082 scanned ports on  (123.123.123.1) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 3542 seconds
```

For this router config, nmap is defeated with the –P0 option.

Other scans from within the network can also be done to verify systems running on the servers and confirm firewall settings. Options like the –sA to test for ACK attacks can be used with the nmap scanner.

```
[root@friday sacaske]#  nmap -sA -P0 123.123.1.2

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on fw1.giac.com (123.123.1.2):
(The 1521 ports scanned but not shown below are in state: filtered)
Port            State           Service
264/tcp         UNfiltered      bgmp    [7]
265/tcp         UNfiltered      unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 552 seconds
```

3.2 Areas of concern

There are weaknesses within this network that if exploited could cause a wide degree of problems. The first of these is a DOS attack. There are several ways that you can cause a network to bottleneck, including the new nimda virus that can also open all a web server's http sockets by sending so many http-gets that no legitimate connections can get through. Several other DOS attacks exist and unfortunately, not all can be blocked.

VPN session hijacking via a vulnerability on the external end can also be a high concern. The design of VPN assumes that both ends of the tunnel are protected. If one end is compromised, the exploiter now has an encrypted tunnel into the network, and depending on which VPN system they have accessed, they will have all the services allowed to them available. The only protection for this is constant diligence with regard to securing the external systems.

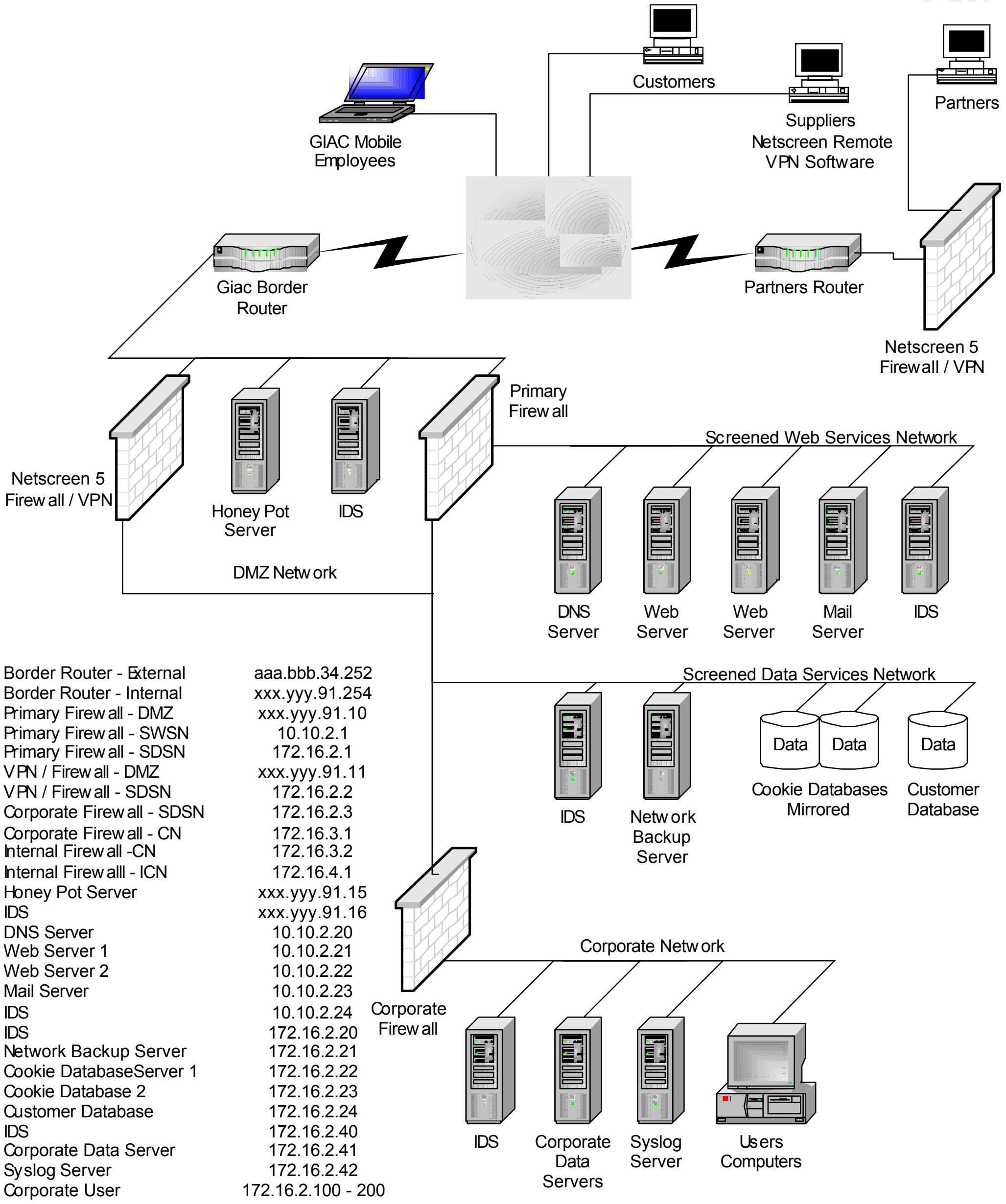
There are two potential areas of compromise based on the network configuration. The first is the email server: since it is located on the external DMZ, someone could potentially find an exploit that would allow them to steal the email still residing on the server. The other area is the

[7] Better look into this to make sure it is not a problem with Firewall-1 or a misconfiguration.

secure web server. If someone were able to gain access to this system completely, they would be able to make ODBC requests through the firewall to the sayings database.

Assignment 4 – Design Under Fire

The system that will be attacked was designed by Phil Hale. This system was selected mostly at random, although the network was an interesting design. His paper is located at http://www.sans.org/y2k/practical/Phil_Hale_GCFW.zip.



Border Router - External	aaa.bbb.34.252
Border Router - Internal	xxx.yyy.91.254
Primary Firewall - DMZ	xxx.yyy.91.10
Primary Firewall - SWSN	10.10.2.1
Primary Firewall - SDSN	172.16.2.1
VPN / Firewall - DMZ	xxx.yyy.91.11
VPN / Firewall - SDSN	172.16.2.2
Corporate Firewall - SDSN	172.16.2.3
Corporate Firewall - CN	172.16.3.1
Internal Firewall -CN	172.16.3.2
Internal Firewalll - ICN	172.16.4.1
Honey Pot Server	xxx.yyy.91.15
IDS	xxx.yyy.91.16
DNS Server	10.10.2.20
Web Server 1	10.10.2.21
Web Server 2	10.10.2.22
Mail Server	10.10.2.23
IDS	10.10.2.24
IDS	172.16.2.20
Network Backup Server	172.16.2.21
Cookie DatabaseServer 1	172.16.2.22
Cookie Database 2	172.16.2.23
Customer Database	172.16.2.24
IDS	172.16.2.40
Corporate Data Server	172.16.2.41
Syslog Server	172.16.2.42
Corporate User	172.16.2.100 - 200

In Phil's design, he is using the Netfilter 1.1.1 on Redhat 7.0 as his primary firewall. He is also using Netscreen 5 as a remote access firewall and VPN solution. Under the Assumptions section, Phil defines the suppliers and partners network as functioning under a network security specified by GIAC. In this specification, he does not specify such requirements for mobile user. There is also no mention of Firewall or any other requirement other then use of VPN for the mobile user to access the corporate network under the Service Access Requirements. (Page 3 of Phil's paper)

Since it is much easier to attack an unprotected Windows PC then a hardened RedHat system, an attack that compromises the mobile PC then exploits the VPN into the corporate network will be used. There are three methods to exploit an unprotected PC's VPN:

1. Steal the key or certificate used for establishing the VPN session from the mobile system and make the connection from a different PC.
2. Use PC control software like Back Orifice installed on the mobile user's system via an email attachment, a browser hole, or even a shared drive; then use the user's PC to connect.
3. Create a Trojan program that will send itself through the VPN and establish a direct connection back to the attacker from the inside. This can succeed even if the user is not on the VPN and the Internet at once.

The network configuration and the configuration of the mobile user's system will decree which of these should be used. All of these attacks are preventable with the use of a firewall on the mobile PC, but in theory, if the VPN key system was also tied to the establishing computer's MAC address, it would prevent a rogue computer from using a stolen key. This could be confirmed by hashing the MAC address in the TCP packet header along with the rest of the key on the VPN system.

How are the mobile systems found? Most large companies provide directories either online or in paper form. Once you have a list of people that work for the various departments, start looking for them on big online areas like AOL. You can then watch for their logins and know when and where to strike. You can even strike up an online friendship with the user and develop enough confidence to make getting a Trojan program installed even easier.

Now, before actually attacking the mobile users system, it would be highly useful to have mapped the network as much as possible using tools like nmap, traceroute and other network mapping tools. This should be done both stealth and loud to reinforce the admin's feeling that an attack would come from the outside. If the honeypot is not well thought out, it would be easy to detect since nothing will be going or coming to it. Give the admin some nice logs to analyze.

In addition to pretending to attack from the outside, a DOS attack against the web servers would do nicely at keeping the admin nice and distracted. For a DOS attack, something new would be fun, so let's attack the two web servers with nimda http messages. The 50 PC's could be configured to focus the attack on just those systems. Since the virus infects on port 80 by sending standard http requests initially, the IDS and the firewall would not notice them as anything odd.

Since GIAC is not using IIS (smart people that they are) nimda will not actually do anything, but it will take up all the sockets and cause the web server to get really sad. This is tough to block as it is so new and uses ports that are also used for legitimate traffic. Several hacks have been done to try to stop these, but the results often cause as much grief. One of these methods was to divert all the http:get requests with bogus stuff to /dev/null. That would have helped, but the SYN and ACK had already been established and the socket would remain open until it timed out. This can use up all available TCP buffers on a server even if the buffer number has been increased in the OS configuration. Another theoretical method to block nimda is to hijack the http:get packet, set the FIN flag, and then pass it along to the web server, closing the socket and allowing legitimate packets through.

Now, back to the VPN hijack, since the poor admin is pulling out his hair worrying about the web servers and watching crazy logs on the IDS system, it is time for the sneak. The VPN tunnel provides a clear path through the firewall and into the corporate network. Here, you can go directly to the Cookie Database with nothing to stop you. There is an IDS on this network, but a cleaver hacker could make the database requests look like they were legitimate – possibly a remote employee modifying something or a partner downloading fortunes. The IDS system may not even worry about a remote user connections to the database system.

The attacker now has all the cookies. Mmmmm.

References:

1. 2.3 Firewalls 102: Perimeter Protection with Firewalls, Sans Institute Presented by Eric Cole, July 2001.
2. 2.4 VPNs and Remote Access, Sans Institute, Presented by Eric Cole, July 2001.
3. Firewall-1 Enterprise Security Management User Guide, Checkpoint Software Technologies, Ltd, September 1998.
4. People that had brains picked:
    a. Paul Caskey[8], pcaskey@swcp.com, WAN manager, ARA.
    b. Mark Costlow, cheeks@swcp.com and Jamii Corely, jamii@swcp.com, owners, SouthWest Cyberport (ISP).
    c. Ron Marr, rhmarr@sandia.gov, database programmer, Technadyne Eng.

[8] Paul would like special credit since he was designing a security plan for his network while I was writing this paper and I caused him much grief by pestering him on all his hardware research.