Global Information Assurance Certification Paper

GCFW Practical Assignment
Version 1.5e

Track 2: Firewalls, Perimeter Protection, And Virtual Private Networks

(SANS 2001 Baltimore)

Done by
Last Name : Tan
First Name : MeauHuat

CONTENT

Assignment 1 - Security Architecture

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in onl ine 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.

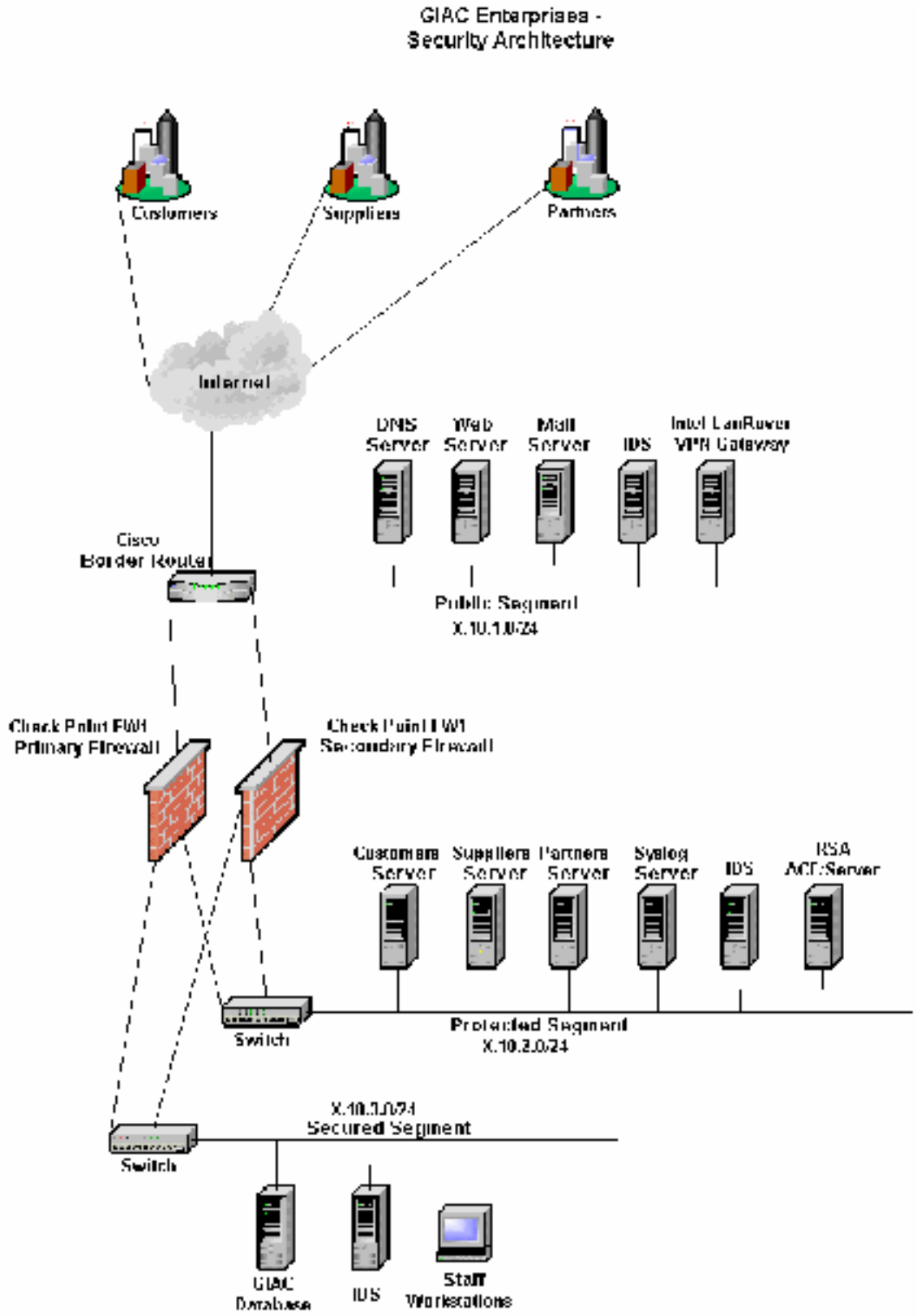
You must consider and define access for:

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

==========

GIAC Enterprises Architecture

GIAC Enterprises' network consists of 3 main segments, namely Public, Protected and Secured Segment (refer to the following diagram).



Public Segment
Public Segment consists of:

DNS Server: To resolve address. Sensit ive servers like IDS, database servers, firewalls etc will not be listed.

Web Server: To provide information for the public about GIAC Enterprises.

Mail Server: To provide email function for staff. Anti -virus software will be installed on it.

Intel Lan Rover VPN Gateway: This is the VPN device used by GIAC Enterprises.

IDS: Snort (version 1.7, www.snort.org) is use as intrusion detection system for detection of suspicious traffic and monitoring of network traffic. Si gnatures selected for this Public Segment will focus mainly on DNS, web, and SMTP attacks and some other general traffic patterns.
If the IDS is connected to a switch, be sure port mirroring is configured on that port so that it could analyze all the traff ic passing through the switch. This applies to all the others IDS.

Protected Segment
Protected Segment consists of:

Customers Server: Customers database. Only existing customers will be given remote access to it.

Partners Server: Partners database. Only existing partners will be given remote access to it.

Suppliers Server: Suppliers database. Only existing suppliers will be given remote access to it.

Syslog Server: Centralized log server. All servers will send a copy of their log to it. Swatch (ftp://ftp.stanford.edu/general/security -tools/swatch) will be used to analyze the log for intrusion and fault detection. The log can also be aid in forensics if any of the servers had been compro mised and had their log removed.

IDS: Snort will focus on monitoring and detecting suspicious traffic to and from the servers.

RSA ACE/Server : RSA (http://rsa.com) ACE/Server, together with RSA SecurID, will be able to provide centralized, strong, two -factor authentication services for the servers in all the three segments.

Secured Segment
Secured Segment consists of:

GIAC database : Database containing GIAC Enterprises sensitive data.

IDS: Snort is deployed to monitor mainly internal traffic.

Staff workstations : This is where staff will have their workstations connected. Administrators accessing servers, routers and firewalls should only be originated from this segment.

General Policies And Procedures

All servers run either a hardened Sun Solaris or Redhat Linux. Before actual deployment, all necessary patches will be applied and only services needed by the server's operation will be opened. Security sites such as CERT (www.cert.org), SANS (www.sans.org) and SecurityFocus (www.securityfocus.com) will be searched for any vulnerability on the applications and operating system that are deployed. Nessus (version 1.0.8, http://www.nessus.org) will be use to scan and counter check on all servers before deployment.

Bastille Linux (http://bastille-linux.sourceforge.net) will be use to secure servers running Redhat Linux.

For hardening Solaris, the following 2 sources are useful: YASSP: Hardening Script for Solaris (http://www.yassp.org) and Titan (http://www.fish.com/titan).

All remote access by the administrators is done via openssh (version 2.9, http://openssh.org). Tcp_wrappers (ftp://ftp.porcupine.org/pub/security/index.html#software)will be installed to further restrict where the servers are allows to be connected from. By default, servers are only allows to be connected from the Secured Segment.

ACE client will be installed on all applicable servers allowing the use of SecurID for remote log in to improve security. PIN for the token will be set to allow 6 -8 alphanumeric characters in length.

Administrators are given access to servers strictly base on their operation needs. No shared account will be allowed.

Main Perimeter Defence Components

Border Router

The border router is a Cisco 3640, running IOS version 12.1. Besides the primary function of routing, the border router will also act as GIAC Enterprises first layer of perimeter defense (don't ignore free security). Elimination of the most basic of attacks can be performed at this entry point. Well-known exploits such as sunrpc (tcp 111) and netbios (tcp, udp 137 -139) can be blocked here. More details will be discussed on part 2 of the assignment.

The connection to the Internet is via a 2MB link.

Firewalls

A pair of Check Point FW1 (version 4.1 SP3) (http://www.checkpoint.com) which run on Nokia 440 (IPSO 3.3) (http://www.nokia.com/securitysolutions/platforms/440.html) is use as the firewalls. Check Point FW1 provides easy of management (easy to use GUI) and has

stateful inspection engine. There exist popular mailing lists (E .g. fw-1-mailinglist@beethoven.us.checkpoint.com) and web sites (E.g. www.phoneboy.com) for problem discussion and information sharing.

The Nokia is a hardened box and is easy to deploy and manage. The IPSO has a VRRP (Virtual Router Redundancy Protocol) monitored circuit configuration. This method of setting up VRRP between two or more Nokia firewalls eliminates the creation of asynchronous routes th at occurs when there is only a single interface failure.

"Monitored Circuit will have a firewall let go of its priority over IP addresses associated with its active network interfaces when a single network interface loses its link state. This results in the secondary firewall taking on all of these IP addresses". [URL 2]

The protocol may have some problem working in switch environment. [URL 5] MAC address caching on the switch in front of the firewalls should be set to 0 (arp timeout 0).

Virtual Private Network
The VPN device is a hardware, Shiva LanRover VPN Gateway (ShivICE Version 6.70p5) (http://support.intel.com/support/si/vpn/lanrover) capable to support up to 300 tunnels. The LanRover is easy to install, deploy, and configure using its Shiva VPN Manager (GUI based configuration and monitoring software).

"It supports 2 type of encapsulation, Shiva Smart Tunneling (SST) Encapsulation and Encapsulating Security Payload (ESP) Encapsulatio n. ESP is the security portion of the IPSec standard. ESP should be used when you communicate with another non -Intel VPN device (such as a firewall or router) that has implemented the ESP portion of the IPSec standard." [URL4]

Shiva VPN Client (the clien t software) can be use by remote users to established secure connection to the VPN Gateway.

Remote Access

Access For Customers
Customers are the companies that purchase bulk online fortunes. They should have secure web connection (using SSL) to access the Customers Server for making purchases, querying, information updates etc.

Only selected source addresses from the customers are allowed access to the server.

Access For Suppliers
Suppliers are the authors of fortune cookie sayings that connect to su pply fortunes. They will be provided with the VPN client or they could use ssh (scp for file transfer) to upload the fortunes and update database.

Since authors may not have fixed source address, SecurID (token) will be provided to them for any remote acc ess to improve security.

Access For Partners
Partners are the international partners that translate and resell fortunes. Their access to the Partners Server will be done over VPN connection.

Only few selected source addresses from the partners are allow ed access to the server.

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".

==========

Router Configuration

Although router's main function is to do routing, it can be used as the first layer of defense for GIAC Enterprises' network. The router should tighten and be configured not to give out information to outsiders. Unnecessary services will be turned off. Both ingress and egress filters will be added to the router.

This is not a complete router setup. It is mainly dealing with the security aspect of the setup.

Administrative Access

An access list is added to restrict administrative remote login. Only IP from Secured Segment (X.10.3.0/24) are allow telnet access:

```
# Create a rule in access-list "20" to allow access from X.10.3.0/24 (Secured
# Segment)
router(config)# access-list 20 permit X.10.3.0 0.0.0.25
# Setting the vty to apply the ACL to
router(config)# line vty 0 4
# Apply the created ACL to the inbound direction
router(config-line)# access-class 20 in
```

Trying to telnet from other network could test this access rule. Access will be denied.

Banner Message

A banner message for login stating that it is illegal to access or attempt to access the router without any proper authorization. "^C" is a delimiter for the message.

```
router(config)# banner login ^CWARNING: For AUTHORIZED Personnel Only^C
```

A "WARNING: For AUTHORIZED Personnel Only" message will be shown upon getting a login prompt from the router.

Enable Logging

Router's logging will be turn on and will be logging to the syslog server.

```
# Enable logging to all supported destinations
router(config)# logging on
# Define logging will be sent to the Syslog Server
router(config)# logging syslog_server
```

Login to the Syslog Server and check the messages log (assuming default setting for /etc/syslog.conf) and check for messages from the router.

Encrypt Passwords

All passwords on the router will be encrypted and hashed.

```
router(config)# service password-encryption
# permanent MD5 hashing on password
router(config)# enable secret
```

Enter "show configuration" on the router, the once clear text passwords are now encrypted.

Disable Unnecessary Services
Cisco IOS provided some services and features which will not be used and will be disabled/removed. This will help to prevent undiscovered vulnerability that could be use to bypass or penetrate the router.

```
# Disable UDP services like echo, discard, chargen,   bootps, snmp
router(config)# no service udp -small-servers
# Disable TCP services like echo, discard, daytime, chargen
router(config)# no service tcp -small-servers
# Disable finger service as it could provide outsiders with user login information
router(config)# no service finger
```

Use nmap to do a port scan on the router, all the above mentioned services will not be shown opened.

The following are others services and features that will be disabled:

```
# Disable Cisco Discovery Protocol.
router(config)#  no cdp run
# Disable simple network management protocol.
router(config)# no snmp -server
# No bootp service needed.
router(config)# no ip bootp server
# No Dynamic Host Configuration Protocol (DHCP) service needed.
router(config)# no service dhcp
# No packet assembler/disassembler (PAD) service needed.
router(config)# no service pad
# Disable classless forwarding.
router(config)# no ip classless
# Disable direct-broadcast which could be use to prevent denial of service problem
router(config)# no ip d irect-broadcast.
# Prevent DNS queries
router(config)# no ip domain -lookup
# Disable web server.
router(config)# no ip http server
# Drop packet using source routing. This is because source route can be used to
# deliver  malicious packets to destina tions that can not normally be reached due to
# access lists.
router(config)# no ip source route
# Disbale sending of ICMP redirects messages.
router(config-if)# no ip redirects
# Disable ICMP unreachables messages will prevent the router from sendin  g out
# network information.
router(config-if)# no ip unreachables
```

Blocking Invalid IP Addresses – Ingress 1
The next few sections are on ingress and egress filters using the ACL. Extended Access List will be used here as it offers greater degree of conf iguration flexibility.

The following consists of 2 sets of addresses we want to block from entering into GIAC Enterprises' network. The first set is private/loopback address that should not travel across the Internet. The other is GIAC Enterprises' own network address (for preventing address spoofing).

Packets that used those IP as their source IP coming into GIAC Enterprises' network are up to malicious act. This section on Ingress 1 and next section on Ingress 2 will combine to form an access list "110".

```
# Invalid IP
router(config)# access-list 110 deny ip host 0.0.0.0 any
# Private IP
router(config)# access-list 110 deny ip 10.0.0.0 0.255.255.255 any
# Loopback IP
router(config)# access-list 110 deny ip 127.0.0.0 0.255.255.255 any
# Private IP
router(config)# access-list 110 deny ip 172.16.0.0 0.15.255.255 any
# Private IP
router(config)# access-list 110 deny ip 192.168.0.0 0.0.255.255 any

# Public Segment IP
router(config)# access-list 110 deny ip x.10.1.0 0.255.255.255 any
# Protected Segment IP
router(config)# access-list 110 deny ip x.10.2.0 0.255.255.255 any
# Secured Segment IP
router(config)# access-list 110 deny ip x.10.3.0 0.255.255.255 any
```

Testing can be done by configuring snort to alert for these IP addresses in the Public Segment and use a packet generator program like hping2 (http://www.eaglenet.org/antirez/hping2.html) to construct a normal SYN packets using these IP as their source IP from outside GIAC Enterprises' network. Snort should not have any alert for these packets which are created, as the router will deny them from entering the network.

However, this filter can be by -pass if the packet created has other flags like ACK or FIN set. This is the limitation of the extended access list.

Blocking Unwanted Services – Ingress 2

The following are used to block off some common services that should not enter into GIAC Enterprises network over the Internet. Some of them have history of known exploits. These rules formed the second part of the rules for access -list 110 from the previous section.

```
# "Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd
# (Calendar Manager), and rpc.statd that allow immediate root compromise." [URL1 ]
router(config)# access-list 110 deny tcp any any eq sunrpc log
router(config)# access-list 110 deny udp any any eq sunrpc log

# "Global file sharing and inappropriate information sharing via NetBIOS and
# Windows NT ports 135 ->139 (445 in Windows2000), or UNIX NFS exports on port
# 2049." [URL1]
```

```
router(config)# access-list 110 deny tcp any any range 135 139 log
router(config)# access-list 110 deny udp any any range 135 139 log
router(config)# access-list 110 deny tcp any any eq 445 log
router(config)# access-list 110 deny udp any any eq 445 log
router(config)# access-list 110 deny tcp any any eq 2049 log
router(config)# access-list 110 deny udp any any eq 2049 log
router(config)# access-list 110 deny tcp any any eq 4045 log
router(config)# access-list 110 deny udp an y any eq 4045 log

# The following are ports usually use by X windows and could be exploitable.
router(config)# access-list 110 deny tcp any any range 6000 6063 log
router(config)# access-list 110 deny udp any any range 6000 6063 log
```

Lastly, the following rules are added at the end of the ACL. Although IOS has an invisible terminating rule of "deny any any", it is better to add an additional "deny any any" to act as a reminder.

```
router(config)# access-list 110 permit ip any any
router(config)# access-list 110 deny ip any any
```

Doing a nmap to any of the machine behind the router and the above ports will be shown being filtered.

Apply access-list 110 to the serial "in" interface of the router.

```
router(config)# interface serial 0/0
router(config) # ip acce ss-group 110 in
```

Allowing Valid Outgoing IP – Egress 1

The following egress filter is added to the out interface to prevent any possible of spoofed IP routing out of GIAC Enterprises' network.

```
router(config)# access-list 120 permit ip x.10.1.0 0.255.255.2 55 any
router(config)# access-list 120 permit ip x.10.2.0 0.255.255.255 any
router(config)# access-list 120 permit ip x.10.3.0 0.255.255.255 any
router(config)# access-list 120 deny any
```

If servers or workstation in GIAC Enterprises could connect outside the LAN, then this rules is working. However, double check by trying to spoof packets out to the Internet by using hping2. Connect an IDS to the router and mirror the outgoing interface to check whether did the spoof packets being successful send out by th e router.

Firewall Configuration

The firewall is the main perimeter defense device. Much attention is needed to ensure the configuration is done properly or else it will only present a false sense of security.

This is not a complete firewall setup. It is mainly dealing with the security aspect of the setup.

Tightening the Firewall
Download a copy of ssh from www.f-secure.com for Nokia's IPSO [URL3] to replace telnet for remote accessing the firewall.

Using the Nokia's voyager (for web configuration), clicks on "Config -> Network Access and Services" and turns off the following services and restricts access.

Network Access:	
Allow FTP access:	No
Allow TELNET access:	No
Allow admin network login:	No
Allow com2 login:	No (Modem Configuration)
Allow com3 login:	No (Modem Configuration)
Voyager Access:	
Allow Voyager web access:	No
Voyager port number:	(defaults to 80)
Note: Use the 'voyager' command to re -enable web access.	
Services:	
Enable 'echo' service:	No
Enable 'discard' service:	No
Enable 'chargen' service:	No
Enable 'daytime' service:	No
Enable 'time' service:	No

Policy Editor And Rulebase
Policy Editor is one of the components of the Check Point Management Client. This is the tool for setting up the rules for the firewall and other security properties.

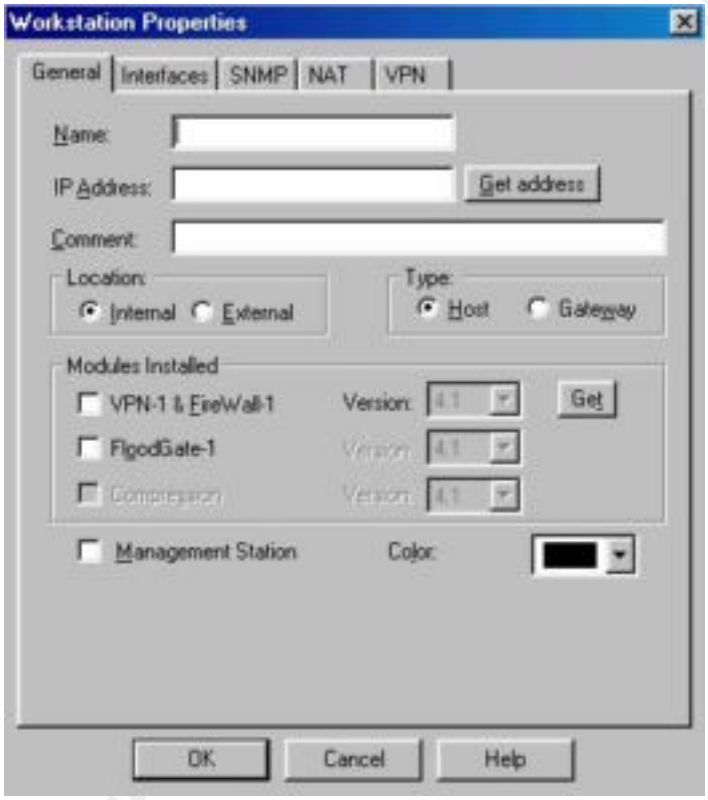
Upon successfully login to the Policy Editor, the current rulebase will be shown.

The rulebase is make up of many individuals rules and each rule has the following format:

- **No.**: The rule number. The execution of rules is from top to bottom and by first match condition. This means the ordering of the rules is very important. The most commonly fired rules are advice to be placed higher (having smaller numbe r) to improve performance.
- **Source**: The source IP of the packet to be checked.
- **Destination**: The destination of the IP to be checked.
- **Service**: The destination port of the packet to be checked.
- **Action**: What the firewall should do with the packet if the rule matches. Possible actions include Accept, Drop, Reject, User Auth, Client Auth, Session Auth, Encrypt and Client Encrypt.
- **Track**: What should be done to track that this rule had been fired. Possible tracks include Short (short logging), Long (long logging) , Account, Alert, Mail, Snmp Trap and UserDefined.

- **Install On**: Which firewall(s) should this rule be installed on.
- **Time**: The time for what this rule is valid.
- **Comment**: For adding any comment needed. Can serve as a reminder or inform other administrator wh y this rule is added.

Network Objects
All equipment is configured as network objects (Manage ->Network Objects) in FW1. The following 2 diagrams shown the most commonly used objected in the rulebase, Workstation and Network. The friendly GUI made configur ation of these objects simple.



By clicking "help" button, it will provide the following explanation for each of the field:

Name – the object's name.

IP Address – a 32-bit address that uniquely identifies a single host connection on an Internet network

Get Address - Click on this button to resolve the object's name to an IP address.

Comment - descriptive text. This text is displayed on the bottom of the Network Object window when this item is selected.

Color - the color of the object's icon. Selec t the desired color from the drop -down list.

Location: Internal/External - relevant for FireWalled objects only. Only Internal objects appear in the System Status View.
A FireWalled object is internal to its own Management Station and external to other Management Stations.
You cannot install a Security Policy on an object from a Management Station where the object is defined as external.

Type: Host/Gateway - whether this object is a host or gateway

Modules Installed - Specifies the Check Point Modules in stalled on this workstation, and their version numbers. The Policy Editor installs policy on a workstation compatible with the Module version on the workstation. You can also click on the Get button to fetch the version number.

Management Station – whether a Management Server is installed on this object.
Member of Gateway Cluster – whether the gateway is a member of a gateway cluster. Gateway clusters are used to implement high availability. A FireWall -1 Management Station cannot be a member of a gateway cluster. If you check this property you must also select a gateway cluster object from the drop -down list.

By clicking "help" button, it will provide the following explanation for each of the field:

Name – the object's name.

IP Address – a 32-bit address that uniquely identifies a single host connection on an Internet network

Net Mask - If the network is a standard Class A, B, or C network, the Net Mask does not need to be specified.

Comment - descriptive text. This text is displayed on the botto m of the Network Object window when this item is selected.

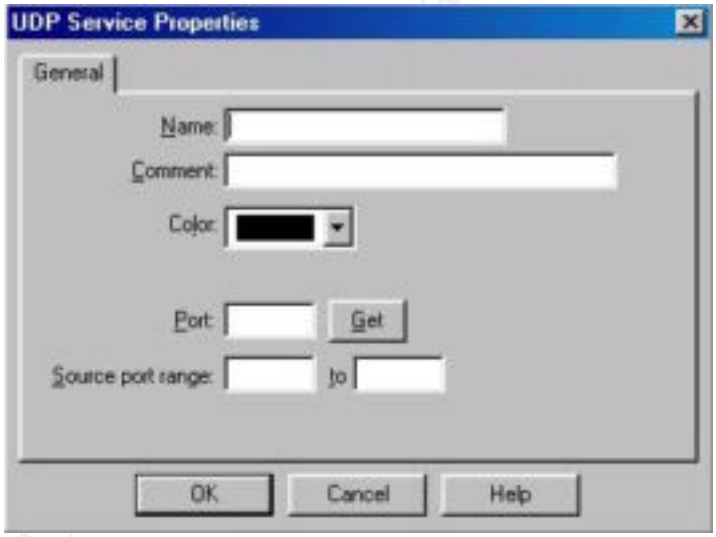
Color - the color of the object's icon. Select the desired color from the drop -down list.

Location: Internal/External - Valid for FireWalled objects only.

Broadcasts: Allowed/Disallowed - allows you to specify whether to consider the network's broadcast IP address as being in the network. If this is set to Allow, then in rules which allow access (that is, rules whose Action is neither Reject nor Drop) and in which this network object is either th e Source or the Destination, the last address in the network is considered to be part of the network.

Services

Services can be configured at Manage ->Services. Below shown the most commonly used services, UDP and TCP, that can be configured using the GUI.



By clicking "help" button, it will provide the following explanation for each of the field:

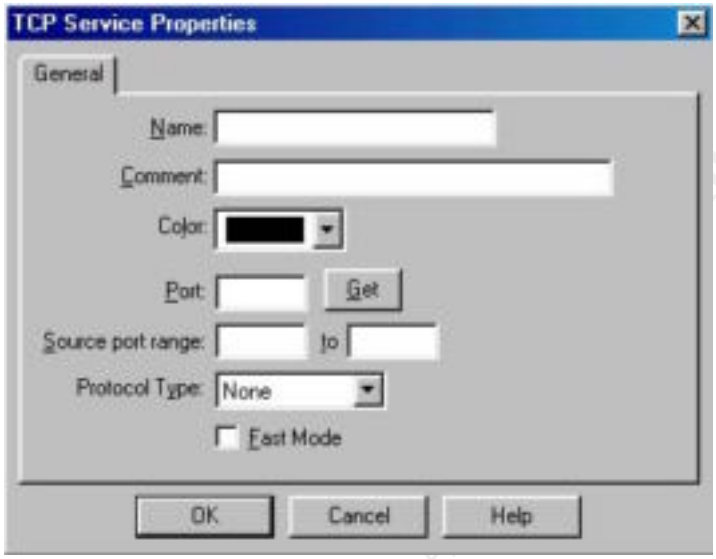
Name - the service's name. The name assigned here should be identical to the server service name (as it appears in the services file, so that FireWall -1 will be able to retrieve some properties automatically. If NIS is being used, FireWall -1 will automatically retrieve the information from the NIS.

Comment - descriptive text. This text is displayed on the bottom of the Services window when this service is selec ted.

Color - the color of the service's icon. Select the desired color from the drop -down list.

Port - the number of the port used to provide this service

Source Port Range - a datagram whose source port field is in this range is considered to belong to this service.



By clicking "help" button, it will provide the following explanation for each of the field:

Name - the service's name. The name assigned here should be identical to the server service name (as it appears in the services file, so that FireWall-1 will be able to retrieve some properties automatically. If NIS is being used, FireWall -1 will automatically retrieve the information from the NIS.

Comment - descriptive text. This text is displayed on the bottom of the Services window when this service is selected.

Color - the color of the service's icon . Select the desired color from the drop -down list.

Port - number of the port used to provide this service. To specify a port number.

Get - Retrieves information about the service's port.

Source Port Range - you may specify a range of port numbers available on the client side of the service. If specified, only those Source Port Numbers will be Accepted, Dropped, or Rejected when inspecting packets of this service. Otherwise, Source Port Number is not inspected.

Protocol Type - specifies which protocol type is associated with the service, and by implication, the Security Server that enforces Content Security and Authentication for the service.

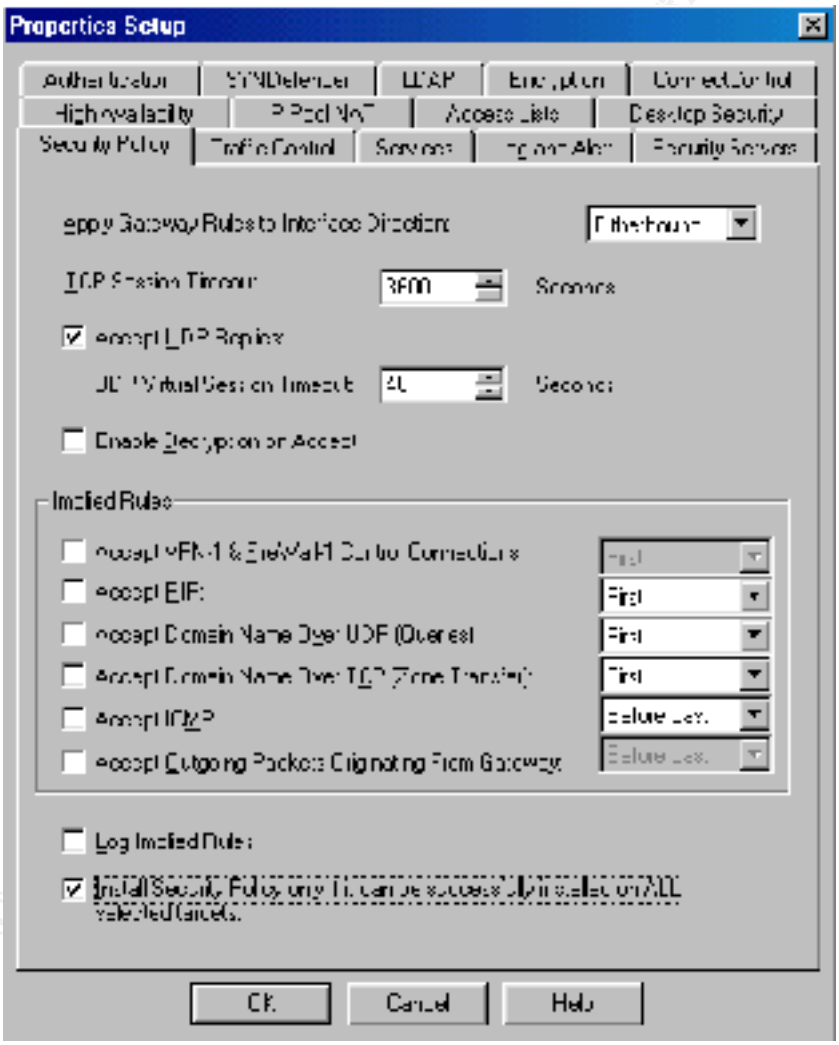
Fast Mode – Use the FASTPATH feature for this service, which speeds inspection. If Fastpath is enabled, the following FireWall -1 features cannot be used:

- Encryption – Encryption cannot be used because key information is stored in the connections table.

- Accounting – Accounting requires the connections table and therefore cannot be used.

Fast Mode eliminates TCP connections from your connections table. However, this could introduce additional security issues. [URL6]

Security Policy Properties
Bring up the following setup screen through Policy ->Properties under Policy Editor.



Unchecked all the boxes under implicit rules group. Implicit rules will not show up at the rulebase by default. Sometimes administrator might miss the implied rules and mis - interpreted the rulebase. Rather, it is a good pract ice to add in a replacement rule(s) for them so that the rulebase will show the complete rules and the ordering can be more flexible (no longer restrict to First, Last and Before Last).

To view the implied rules, click on View ->Implied Rules.

Check on the box "Install Security Policy only if it can be successfully installed on ALL selected targets" as the same rulebase will be loaded onto both firewalls. This is to ensure that both firewalls have the same rulebase in case the Primary Firewall has interfa ce failure and the Secondary Firewall took over.

Rulebase
The following diagram shows the rule that is being implemented. The following colour scheme had been adopted when creating Network Objects to aid in reading the rulebase.

Red: Firewall related n etwork objects.

Green: Network objects from Secured Segment.

Yellow: Network objects from Protected Segment.

Black: Network objects not protected by the firewall.

Rule 1: Allow selected workstations from Secured Segment to access and configure the firewalls

Rule 2 and 3: Needed for VRRP Monitored Circuit and both firewalls to communicate.

Rule 4: Stealth rule for the firewall.

Rule 5: Allow machine from Public and Secured Segments to syslog to the Syslog Server in Protected Segment.

Rule 6: Allow server from other segments to authenticate through the ACE Server.

Rule 7, 8 and 9 : Allow remote access for customers, suppliers and partners to their respective servers.

Rule 10 : Allow Protects Segment to access different services in the Public Seg ment.

Rule 11 : Allow Secured Segment to access different services to the Internet including Public and Protected Segments.

Rule 12 : Although there is an implicit rule to deny all traffic as the last rule, it is done without any logging. This rule is adde d to enable logging so as to know what kind of traffic had been deny.

There should exist some procedure to keep track of any modification made to the firewall. Information such as who/which department, reason(s) for adding/deleting/modifying the rule, when the rule added, how long will the rule be valid etc should be documented.

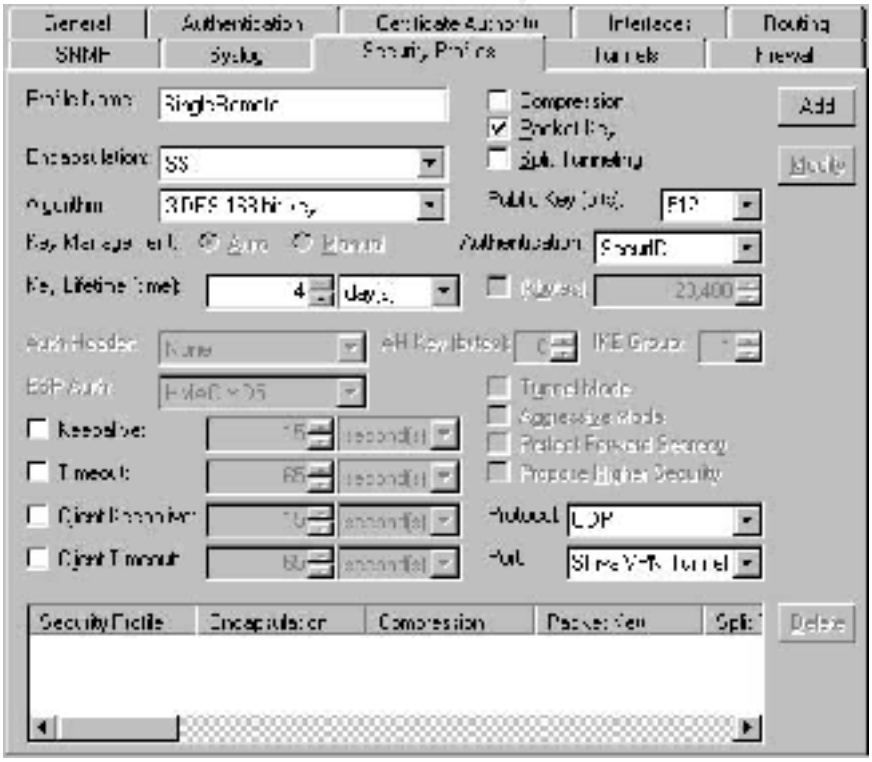
VPN Configuration

The configuration for the VPN device is based on Single Remote User and Site to Site.

This is not a complete VPN setup. It is mainly dealing with the profile setting for the tunnels.

Single Remote User

The following configuration is for single remote user. GIAC Enterprises' staff and suppliers who need this access will be using the Shiva VPN Client.



Profile Name: Something descriptive to reference this sec urity Profile when it is applied to a tunnel.

Encapsulation: Two types of encapsulations are available. Shiva Smart Tunneling (SST) and Encapsulating Security Payload (ESP). SST is chosen for the Single Remote User as it could allow authentication through the use of SecurID.

Algorithm: 3-Des 168-bit key is chosen as it offers better security and is the industrial standard.

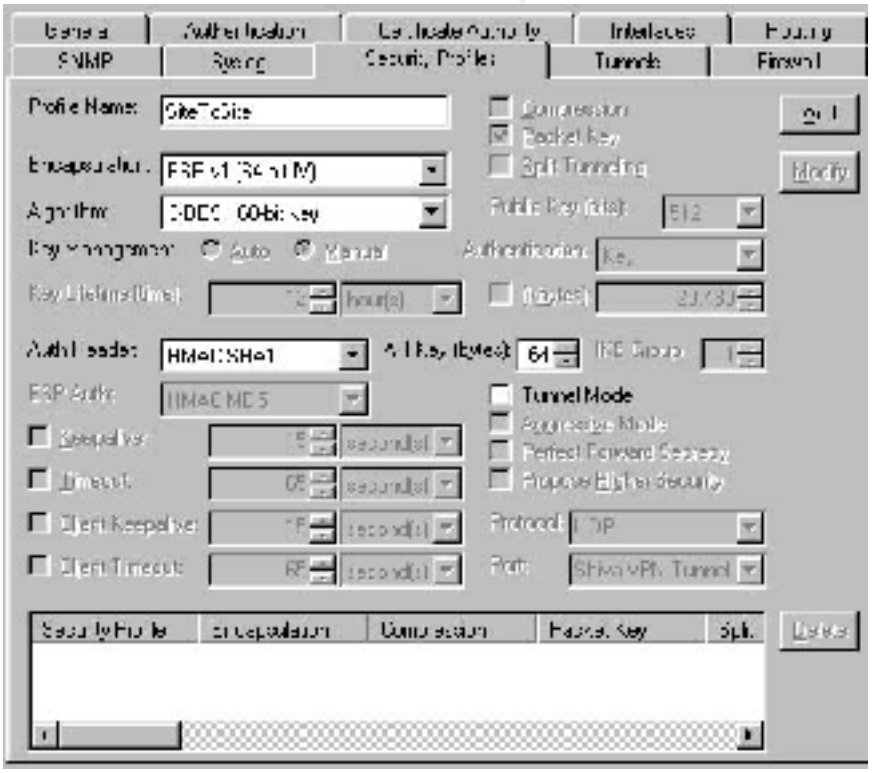
Public Key (bits): Public keys are used during the authentication and session key exchange processes. 512 bits is sufficient in thi s setup.

Key Lifetime (time): This defines how long a session key will be used. 2 weeks is sufficient since remote users are not expected to establish VPN connection back to GIAC Enterprises frequently.

Authentication: SecurID is chosen for authenticatio n since it is more secure than password authentication.

All other value will leave as default. SST is using protocol UDP port 2233.

Site To Site
The following configuration is for Site to Site.



Profile Name: Something descriptive to reference this security Profile when it is applied to a tunnel.

Encapsulation: ESP is selected as is may be used to communicate with other VPN devices. Most VPN has some implementation for the ESP portion of the IPSec standard and this should allow them to communicate .

Algorithm: 3-Des 168-bit key is chosen as it offers better security and is the industrial standard.

Auth Header: HMAC SHA1 is chosen as SHA1 hashing algorithm is slightly more secure than MD5 and HMAC allow up to 64 bytes of AH keys.

AH Key (bytes): This value specifies the length of the key to be used when hashing the packet to produce the authentication header. 64 bytes are selected for better security.

Assignment 3 - Audit Your System 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.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

==========

Planning the Assessment

First and foremost, GIAC Enterprises' management must be informed and agreed to give permission to allow for the assessment to take place. The needs and risks for the assessment should be explained to them.

This assessment will only be carried out by internal staff. The scale of GIAC Enterprises network could be rather costly if the security assessment is being outsource to some auditing/security company. It will also benefit the engineers as they will gain a better understand of the network. Therefore support from network and system department is necessary for the assessment to be successful.

A detailed plan will be discussed and documented with all the necessary engineers (network, system, security etc) involved. Discussion should include the exact assessment procedure, server failure risk (in case server crash due to scanning), expected results from assessment etc. This may take around a day.

The time to carry out the assessment is during the organization's maintenance day. Maintenance day is usually being selected during some off peak period when traffic is low and so is ideal.

Select a maintenance day whereby there will not be much changes being done to the network and system. Assessment will start once the normal maintenance routine is over.

During the assessment, someone from each area should be present to help out and standby for unforeseen incident. Assessment time should kept within the maintenance time frame. Should

any serious incident happen, stop all assessment and remedy it. Consider postponing the assessment to the next maintenance day if remaining time is not sufficient.

Data collected will be analyzed and findings will be presented. Depending on the findings and changes to be made, it could take hours to days.

Implementing The Assessment

Firewall can be audited by checking whether did it deny what it should deny, accept what it should accept, whether logging had been done, the ordering of the rules is correct (wrong ordering of rules or logic will break the security), how secure is the firewall itself etc.

Nmap and snort are selected to carry out the assessment. Snort can be us e to capture the assessment traffic and validate against the scanning.

```
# To test the stealth rule. –P0 option means do not try and ping the host at all
# before scanning. –O option means to activate remote host identification via TCP/IP
# fingerprinting. Use the man page for nmap for more details.
nmap$ nmap –P0 –O Primary_Firewall > PriFW.scan
```

Content of PriFW.scan:

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Warning: OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed TCP port
All xxx scanned ports on Primary_Firewall are: filtered
Too many fingerprints match this host for me to give an accurate OS guess

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

The above result from t he nmap scan shows there is no ports an outsider can connect to the Primary Firewall from the Internet. This is the expected result, as the stealth rule will drop all packets going to the firewall itself (as seen that all scanned port had been filtered).

Do a scan to check what type of traffic the firewall allows into the Protected and Secured segments.

```
# First set up another snort process in the IDS in the Protected and Secured segments
# to capture all packets that the firewall will allow to go through that are generated by
# the nmap host only.
snort$ snort –v host nmap_host > assess-traffic.snort

# Checking what kind of information can be retrieved by doing a scan outside the
# firewalls. -sU option means doing a UDP scans and –sT means to do TCP connect()
# scan.
nmap$ nmap –P0 –sU –sT X.10.2.0/24 > Int-ProSeg.scan
nmap$ nmap –P0 –sU –sT X.10.3.0/24 > Int-SecSeg.scan
```

The content of ProSeg.scan will show that only Suppliers_Server, with its respective Suppliers_Services port(s) opened, is visib le from the Internet. Verify it with assess -

traffic.snort (generated by the IDS in Protected Segment), other snort log and firewall log. The content of ProSeg.scan is as follow:

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
All xxx scanned ports  on  (X.10.2.0.1) are: filtered
All xxx scanned ports on  (X.10.2.0.2) are: filtered
….
Interesting ports on  (Suppliers_Server):
(The yyy ports scanned but not shown below are in state: filtered)
Port                              State      Service
Suppliers_Services_port /t cp  open        Suppliers_Services
….
All xxx scanned ports on  (X.10.2.254) are: filtered
All xxx scanned ports on  (X.10.2.255) are: filtered

Nmap run completed  -- 255 IP addresses (255 hosts up) scanned in zzz seconds
```

Assess-traffic.snort should have p ick up those traffic from the nmap_host to the Suppliers Server with those respective services running. The log file should record some connection log like "nmap_host.src_port -> Suppliers_Server.service_port".

SecSeg.scan will show a result whereby all p orts had been filtered for the whole of X.10.3.0/24 because the firewall rulebase does not have any rule allowing traffic to go into the Secured Segment. The IDS in the Secured Segment will not capture any traffic.

Since it is scanning 2 class C networks and the firewall will be dropping almost all the scanned packets, it will takes hours to finish the whole scan.

Once this has been done, do the same scanning across the 3 different segments with similar procedure. Remember to setup the snort in the respec tive segment during the scanning.

From the Public Segment:

```
nmap$ nmap –P0 –sU –sT X.10.2.0/24 > Pub-ProSeg.scan
nmap$ nmap –P0 –sU –sT X.10.3.0/24 > Pub-SecSeg.scan
```

From the Protected Segment:

```
nmap$ nmap –P0 –sU –sT X.10.1.0/24 > Pro-PubSeg.scan
nmap$ nmap –P0 –sU –sT X.10.3.0/24 > Pro-SecSeg.scan
```

From the Secured Segment:

```
nmap$ nmap –P0 –sU –sT X.10.2.0/24 > Sec-ProSeg.scan
nmap$ nmap –P0 –sU –sT X.10.1.0/24 > Sec-PubSeg.scan
```

All data that are capture during the assessment will be kept for furthe r analysis and storage.

Perimeter Analysis

After the data had been collected, compare them to the expected results that had been previous discuss during the planning stage. The result should be close to the expected result. Should there be any different, it could indicate either some component had been mis -configured or there is mis -understanding (or even not understanding) of the tools, configuration etc.

Verify and make the necessary adjustment and the same/modified assessment should be conducted in a later period if necessary.

The firewall and IDS log should be checked against the scanned results to ensure that all expected logging had been done. Looking through the log might uncover things that are otherwise hidden. All previous log from firewall an d IDS alone could already reveal a lot of what type of traffic are allow/disallow in the network.

An observation is that there is only a single point access from GIAC Enterprises to its ISP. Should the ISP has network problem that will affect the link, GI AC Enterprises' operation will be affected. Getting a second ISP to provide another link to the Internet should be considered.

In the "Blocking Invalid IP Addresses – Ingress 1" section, the limitation of Extended Access List was discussed. IOS also supp orted a better inspection feature, reflexive ACL, that used dynamically created access -control lists which gives router greater control over the flow of traffic. This implementation will take up much more resources than the Extended Access List and might s low down routing. However, it might still worthwhile to explore the feasibility of implemented this added security.

Lastly, GIAC Enterprises' management should be informed of the assessment result and the follow up.

Assignment 4 - Design Under Fire

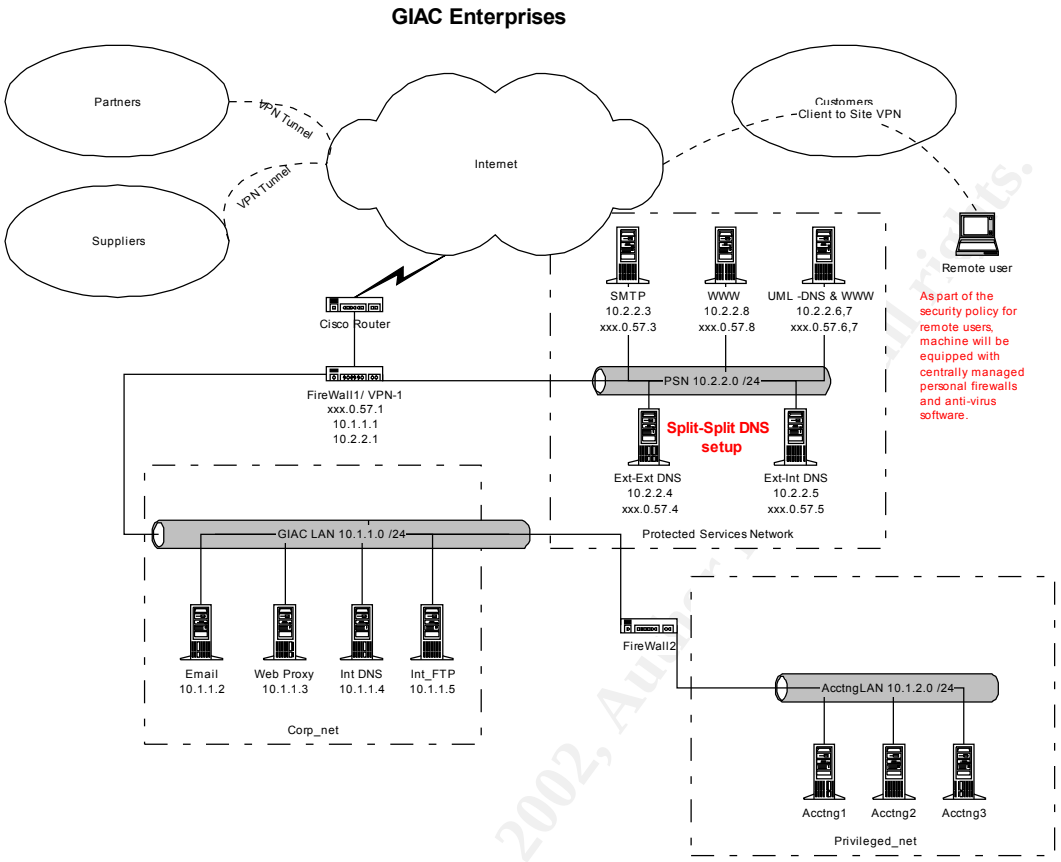
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously post ed 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 i tself. 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 at tack 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 sy stem. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand -waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

I had selected the Brett Gordon's GCFW practical for this assignment (http://www.sans.org/y2k/pra ctical/Brett_Gordon_GCFW.doc) and the following diagram is taken form his practical.



The firewall used is Check Point FW -1 with VPN-1 strong v.4.1 sp2 running on NT4.0 sp6.1

Attack Against the Firewall

A check at http://www.checkpoint.com/techsupport/alerts and www.securityfocus.com for Check Point vulnerabilities shows 2 of them applicable to Brett Gordon's implementation:

1. **Format Strings Vulnerability** , July 11, 2001 [URL7]

"Who is affected:
All installations of VPN -1/FireWall-1 which allow remote GUI connections should be assumed vulnerable to this exploit. It should be noted again that the attack must be made by an authorized and valid VPN -1/FireWall-1 administrator connecting from an authorized GUI client station."

Since there is no mentioned that the "Accept VPN -1 & Firewall-1 Control Connections" is unchecked (check by default) in the Implied Rules under Policy ->Properties, outsider could connect to the firewall as this implied rule is install as "First". This mean the stealth rule will not be able to control who can access the firewall.

FW1 had a default "fwadmin" account for management station. The only thing left is the /$FWDIR/conf/gui-clients file which indicate which IP is a valid GUI client. The chances of doing a brute force password attack is low even if the firewall administrator allows remote GUI client access for convenient purposes.

2. **RDP Communication Vulnerability**, July 9, 2001 (Updated July 12, 2001) [URL8]

No known exploit for this vulnerability reported yet but the following site http://www.inside-security.de/advisories/fw1_rdp_poc.html describe a proof of concept which demonstrate how it can be use to bypass firewall checking.

Denial of Service Attack

The rulebase contain the following rules:

Source	Destination	Service	Action	Track	Description
Internet	PSN_UML_WWW PSN_WWW	Http Https	Allow	Long	Access to webservers.
Internet	PSN_SMTP	TCP 25	Allow	Long	Allow mail to relay.
Internet	PSN_UML_DNS PSN_Ext_ext_DNS	UDP 53	Allow	Long	Allow access to DNS. No zone transfers allowed.

According to http://www.phoneboy.com/faq/0289.html (Increasing Number of Connections Allowed) FireWall-1 will only handle 25,000 simultaneous connections by default.

The above 3 rules allow some of the GIAC Enterprises' services being access from the Internet. Legitimate traffic from within and Internet will always fill up part of the connection table. During peak period of the day, the connection table will be largely fill up. It is possible to launch a denial of service attack by generating enough http, smtp and domain-udp traffic to these servers and fill up the connection table to it 25,000 limit.

Although the firewall does not crashed, it will not be able to accept any more connection. Thus, this denial service attack on the firewall will affect the whole Internet-related operation of GIAC Enterprises.

There are few possible countermeasures:

1. Follow the URL from phoneboy.com mentioned above and tune up the limit of the connection table.

2. Tighten up all these servers and move them out of their current network. Create a new network connected to the router and place them there.

3. Switch to a different firewall that can handle a much bigger connection table.

Compromise An Internal System

The internal system to compromise is the PSN_Ext_ext_DNS since it can resolve query from the Internet. Information inferred from the assignment is that it is running on Linux and therefore it is most probably using Bind.

The following exploits (all in the year 2001) had been found:

1. http://ftp.die.net/mirror/exploits/?M=A
bind8exploit.c (01-Feb-2001)
bind82x.c (07-Feb-2001)

2. http://igloo.its.unimelb.edu.au/Webmail/tips/msg00451.html
http://www.hack.co.za/daem0n/named/t666.c

"Since arbitrary malicious code may be inserted by the exploitation of this bug, there may be an arbitrary number of possible variants. However, the main variant is the "t666.c" code, written by "ADM," and available at http://www.hack.co.za/daem0n/named/t666.c. It uses the bug to create the most important of all hacking tools, a shell running as a priveleged user."

3. http://packetstormsecurity .org/0102-exploits/indexdate.shtml
tsl_bind.c (Feb 9 2001)
"Bind prior to 8.2.3 -REL remote root exploit - Includes instructions for finding the offset on linux."

bind8x.c (Feb 9 2001)
"Bind prior to 8.2.3 -REL remote root exploit - exploits the named INFO LEAK and TSIG bug. Includes shellcode for Linux."

These scripts are trying to exploit the named INFOLEAK and TSIG bug in BIND. For more information see http://www.isc.org/products/BIND/bind -security.html.

All scripts will be used one by one to try to compromise the DNS server. Since no further information regarding which BIND was installed, either the compromise will be unsuccessful or one of them will get a root shell.

REFERENCES

[URL1] SANS Institute. "How To Eliminate The Ten Most Critical Internet Security Threats: The Experts' Consensus", http://www.sans.org/topten.htm

[URL2] Nokia Knowledge Base. "Resolution 1214: Please Explain VRRP Monitored Circuit on IPSO 3.1 and later", https://support.nokia.com/knowledge/frmResolutionView.jsp?ResolutionId=1214 (A login account is needed)

[URL3] Nokia Knowledge Base. "Resolution 1348: Worldwide SSH availability" https://support.nokia.com/knowledge/frmResolutionView.jsp?ResolutionId=1348 (A login account is needed)

[URL4] Intel NetStructure Support."Intel NetStructure Virtual Private Networking Concepts Guide", http://support.intel.com/support/netstructure/vpn/concepts.htm

[URL5] Nokia Knowledge Base. "Resolution 1384:VRRP and Ethernet Switches (Problems with MAC address caching)" https://support.nokia.com/knowledge/frmResolutionView.jsp?ResolutionId=1384 (A login account is needed)

[URL6] Lance Spitzner. "Understanding the FW-1 State Table", http://www.enteract.com/~lspitz/fwtable.html

[URL7] Check Point Alerts Archive. "Format Strings Vulnerability", http://www.checkpoint.com/techsupport/alerts/format_strings.html

[URL8] Check Point Alerts Archive. "RDP Communication Vulnerability" http://www.checkpoint.com/techsupport/alerts/rdp.html

[Book1] Lance Spitzner, Chris Brenton, S. Winter, S. Northcutt. Firewalls 102: Perimeter Protections and Defense, In-Depth