



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment

Version 1.6 (revised August 13, 2001)

© SANS Institute 2000 - 2005, Author retains full rights.

Submitted by: Tim Daly

Overview

This assignment is the practical submission for the GIAC GCFW certification. It is composed of 4 sub-assignments that can be summarized as follows:

1. Design the security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.
2. Define the security policy for the external router, primary firewall and VPN used in assignment 1 and provide a tutorial on how to implement one of these policies.
3. Plan, conduct and evaluate a technical audit of the primary firewall described in assignment 1 and 2.
4. Select a previous GCFW practical submission and describe:
 - 3 possible attacks against the primary firewall;
 - a DDOS attack against the network;
 - how you would compromise an internal host.

1 - Security Architecture

Consultation with the management of GIAC Enterprises has resulted in the following business requirements being defined:

- Allow GIAC customers to access and purchase GIAC Fortune Cookie Sayings on-line.
- Allow GIAC suppliers to upload new Fortune Cookie Sayings to the GIAC Fortune Cookie Database server.
- Enable GIAC partners to access required areas of the internal GIAC network.
- Provide mobile and home-based employees with remote access to GIAC's internal network.
- Provide internal GIAC users with the following Internet services:
 - HTTP/S
 - FTP
 - SMTP
- Enable access to GIAC Enterprise's public web server.
- Protect proprietary and sensitive corporate data from unauthorized access, including internal threats.
- All of the above requirements should be realized in a manner so as to minimize the risk posed to GIAC Enterprises on-going operations.

As always, the GIACs financial controller has requested that costs be kept to a minimum. With this in mind and also taking into consideration the current economic climate, the requirement for a fully-redundant architecture has been removed. This decision is expected to be reviewed after the appraisal of GIAC

Enterprises next round of financial results.

In keeping with recognized best practices in network security, the design for GIAC Enterprises security architecture applies security in layers. This design philosophy is known as Defence in Depth and when employed correctly, "can result in an exponential improvement in network security", SANS 2.3, Firewalls 102:Advanced Perimeter Protection and Defence.

Thus the resulting design for GIACs security architecture, shown below in Figure 1, is a combination of the previously stated business requirements and the principles of Defence in Depth.

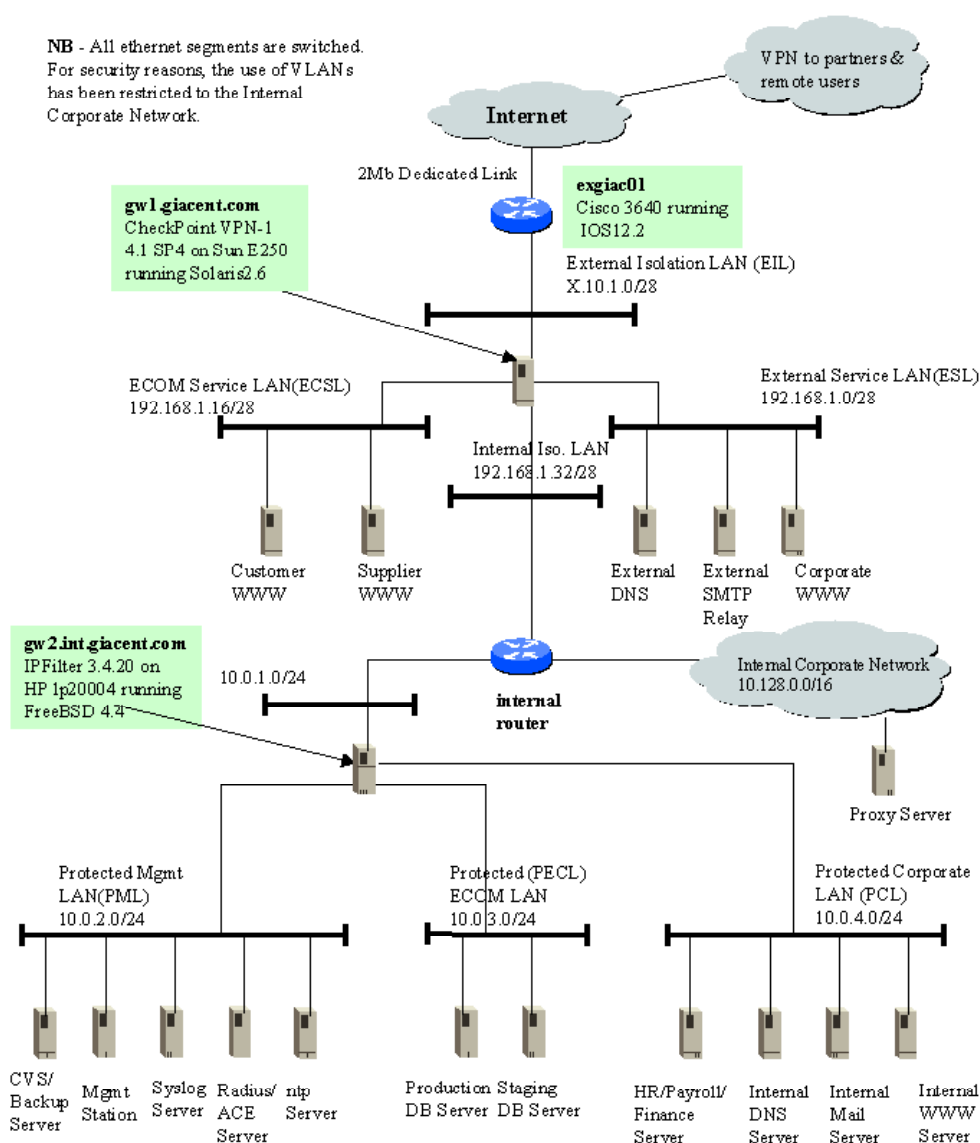


Figure 1

1.1 External Router

The first element to be considered in this security architecture is the external router, **exgiac01**. The specifications of this router are as follows:

- Cisco 3640 running IOS12.2.

This router provides the GIAC Enterprises network with connectivity to the Internet via the serial interface(s0) that connects to the 2MB ISP line. The position of **exgiac01** at the border of GIACs network makes it the first line of defence for protecting internal networks and the first step in the process of developing Defence in Depth. The router implements ingress filtering that:

- protects against spoofed packets(ingress packets that have a source address from an internal network)
- blocks private/RFC1918 addresses
- block source routed packets/packets with IP options set
- blocks some of the more common and well-known attacks before they enter the GIAC network(eg. netbios and rpc scans).

The router also implements egress filtering to minimize the risk of GIAC resources being used for malicious purposes and allow GIAC Enterprises to be considered a "good 'net neighbour".

See section 2.1 for details.

1.2 External Firewall

The next element in the security architecture is the primary/external firewall **gw1.giacent.com**. The hardware specifications of this firewall are as follows:

- Sun Microsystems Enterprise 250 with:
 - Fastest processor available
 - CheckPoint VPN-1 Accelerator Card II
 - 2 * 18GB HDD
 - 1024 MB RAM
 - 1 Quad Fast Ethernet card
 - CDROM drive

The OS/software specifications are as follows:

- Hardened Solaris2.6 with latest patch clusters
- CheckPoint VPN-1 4.1 SP4

(NB - after 4.1 SP5 is proven to be stable and robust, it is intended to migrate to Solaris2.8)

The external firewall is the most important element in GIAC Enterprises security architecture as it is the junction where the public internet, service networks and GIAC internal network meet. This positioning enables it to perform the following functions:

- Protect the ECOM Services LAN(ECSL) from unauthorized traffic while allowing:
 - GIAC customers to securely purchase and download Fortune Cookie Sayings via an SSL encrypted link.

- GIAC suppliers to securely upload new Fortune Cookie Sayings via an SSL encrypted link.
- Protect the External Service Network from unauthorized traffic while allowing:
 - name resolution of hosts in the external name zone
 - sending and receiving of Internet based SMTP mail
 - allowing public access to the GIAC public web server
- Protect GIACs internal network from unauthorized traffic originating from the Internet and both service networks.
- Allow the internal proxy server to securely access the Internet.
- Terminating device for both Client and Site-to-Site VPN connections (see sections 1.3 and 1.4 respectively)

1.3 Site-to-Site VPN for Partner Access

The next element in GIAC Enterprises Security Architecture is the VPN connectivity to their partner. GIAC's partner requires connectivity to various hosts and services on the internal GIAC network. This connectivity is achieved by the configuration of an IKE VPN tunnel between the external firewall, **gw1.giacent.com**, and the partners external firewall, **partner-fw**. The partners firewall also a CheckPoint VPN-1 4.1 firewall.

Legal advice should be sought as to whether a connectivity agreement that clearly states the rights and obligations of each connected party should be drafted and signed prior to the establishment of the VPN tunnel.

1.4 Client VPN for Remote Access

Another important element of the security architecture is secure remote access for the mobile/home office workforce. This is provided by the use of CheckPoint's SecureClient VPN software. This leverages the investment in the primary external firewall to also include the provision of client VPN.

All traffic traversing the public Internet will be encapsulated and 3DES encrypted. All Client VPN connections will be assigned an IP address that is routable on the internal GIAC network from a NAT Pool that is defined on the external firewall.

SecureClient includes basic firewalling functionality that enables a split-horizon client VPN connection. For example, only outgoing and encrypted connections are allowed to leave the client for the duration of the existence of the VPN tunnel. This provides some measure of protection against a compromised client VPN host being used as means of unauthorized access to the GIAC internal network.

Client VPN authentication is also enhanced by the use of strong 2 factor authentication (see section 1.6). Two useful references on how to implement this are "Sample FireWall-1 with SecuRemote Configuration", www.phoneboy.com/faq/0318.html and "How to configure Hybrid Mode IKE for SecuRemote Authentication", support.checkpoint.com/kb/docs/public/securemote/4_1/pdf/hybrid-2-10.pdf

1.5 Internal Firewall

The internal firewall, **gw2.int.giacent.com** has the following specifications:

- Hewlett Packard Ip2000r with:
 - Fastest processor available
 - 2 * 18 GB HDD
 - 512MB RAM
 - 1 Adaptec Quad card
 - CDROM drive

The OS/software specifications are as follows:

- Hardened FreeBSD 4.4 (Security Branch)
- IPFilter 2.4.20

The internal firewall is in place to meet the business requirement of protecting sensitive corporate data from both external and internal threats. It does this by controlling the traffic to the Protected ECOM LAN(PEL) and Protected Corporate LAN(PCL). It also controls access to and from the Protected Management LAN(PML).

All of the software used on this firewall is free and open source. It has also been proven to perform extremely secure and robust, even under high traffic loads. This makes it ideal as an inexpensive but highly effective internal firewall.

1.6 Authentication

2 factor strong authentication utilizing 1 time passwords(based on the combination of a Radius server, RSA's SecurID tokens and ACE server) is used wherever possible. This includes authentication for connections to the Supplier website and the establishment of client VPN connections.

This type of strong authentication is designed to mitigate the risk of sniffing and brute force attacks on simple password based authentication mechanisms. It also provides a central point of user administration.

1.7 DNS

GIAC employs a split DNS architecture. This is achieved through the use of an external DNS server on the External Services LAN (ESL) and an internal name server that is only accessible from internal hosts.

The external name server is only responsible for the resolution of GIACs publicly accessible hosts. The external name server is the SOA for **.giacent.com** and is configured to block zone transfers. The external name server is also configured to act as a recursive resolving name server for the internal name server.

The internal name server contains entries for all internal zones/hosts and is only

accessible from internal GIAC hosts. It is configured to forward requests for external zones to the external name server. These requests would typically be coming from the proxy server.

1.6 Management/administration considerations

A strong security architecture design and the subsequent correct implementation are just the beginning. The continued assurance of the security of GIACs infrastructure is dependent on many factors, including:

- Daily review of all security device logs for unusual or suspicious activity. This will be automated as much as possible.
- All administration/management connections are to be strongly encrypted. OpenSSH utilizing version ssh protocol version 2 and key authentication being the preferred method of remote administration and the only acceptable method of remote terminal access. O'Reilly's "SSH, The Secure Shell" by Barrett and Silverman is an excellent reference for all aspects of different SSH implementations and protocols.
- Strict change management procedures with the ability to track and regress all configuration changes quickly and accurately. With this in mind, it is intended that, where possible, all configuration files will be stored in a [CVS repository](#). All changes to a particular configuration file will be committed to the CVS repository(via ssh) before being installed/applied to the relevant device.
- Monitoring of all relevant newsgroups, mailing lists and web sites to keep abreast of latest developments in vulnerabilities, exploits and patches. A good site with links to a lot of security related material is www.infosyssec.net
- Properly defined and tested incident handling and escalation procedures.
- The creation of a Security Team composed of Security Administrators and a Security Officer that are responsible for the above. Proper training for all these staff is essential.

1.7 Other design features/considerations

Some of the important overall design features are as follows:

- Switched ethernet to minimize the effectiveness of hostile sniffers
- All hosts on the ESL, ECSL and PML are hardened to the bastion host level and Solaris hosts have been audited using [Titan](#) and [YASSP](#). Hosts on the Protected Database and Corporate LAN's are hardened as much as possible. (All exposed/valuable servers have TCPWrappers installed and configured to be as restrictive as possible.)
- All HTTP services are provided using Apache 1.3.20
- The use of an internal firewall, that uses a different OS and firewall software from the external firewall increases the depth of defence of this architecture.
- The segregation of servers and services on a functional level minimizes the risks if one or more hosts are compromised.
- A GPS linked NTP server is used to provide time synchronization of all critical hosts/devices to facilitate easier incident analysis
- An "Acceptable Use Policy" will be defined and communicated to all users of

GIAC Enterprises infrastructure.

© SANS Institute 2000 - 2005, Author retains full rights.

ASSIGNMENT 2 - Security Policy

2.1 - Define your security policy

2.1.1 Border Router

The border router, **exgiac01** is a Cisco 3640 running IOS12.2 and utilizes Extended ACL's to implement the defined security policy. The configuration of **exgiac01** will be implemented as follows:

```
! disable clear text password display
service password-encryption
enable secret

! block known undesirable traffic and services
no ip unreachable
no ip direct-broadcast
no service finger
no service tcp-small-servers
no service udp-small-servers
no cdp run
no ip source-route

! log to internal syslog server
logging 10.0.2.10

! usual authorized use banner
banner / UNAUTHORIZED ACCESS PROHIBITED! This system is for the
use of authorized personnel only! /

! block traffic from non-routable addresses
access-list 101 deny ip host 127.0.0.1 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log

! block traffic with spoofed GIAC public net addresses
access-list 101 deny ip X.10.1.0 0.0.0.15 any log

! block well-known scans eg. netbios rpc
access-list 101 deny udp any any eq 135 log
access-list 101 deny tcp any any eq 135 log
access-list 101 deny udp any any eq range 137 138 log
access-list 101 deny tcp any any eq 139 log
access-list 101 deny ip any any eq 445 log
access-list 101 deny ip any any eq 111 log

! allow incoming traffic
access-list 101 permit ip any any

! allow outgoing traffic from GIAC public net and block
! everything else
access-list 102 permit ip X.10.1.0 0.0.0.15 any
access-list 102 deny ip any any log
! apply access lists in appropriate direction
interface serial 0
```

```
ip access-group 101 in
ip access-group 102 out
```

2.1.2 Primary Firewall

The primary firewall is a CheckPoint VPN-1 4.1 SP4 firewall. It consists of a Gateway Module, **gw1.giacent.com** and a Management Module, **fw-mgmt**, located on the PML network. security policy is configured in CheckPoint 's Policy Editor.

The security policy for this firewall is configured from the CheckPoint Policy Editor GUI client that connects to the Management Server. It consists of a Security Policy rule base and Network Address Translation rule base.

No.	Source	Destination	Service	Action	Track	Install On
-	FW1 Module	Any	Any	accept		Gateways
1	fw-mgmt-station	gw1.giacent.com	FireWall1 ssh icmp-proto ident	accept	Long	Gateways
2	Any	gw1.giacent.com	RDP IKE FW1_topo FW1_pslogon	accept	Long	Gateways
3	All Users@Any	clint-vpn-group	client-vpn-services	Client Encrypt	Long	Gateways
4	partner-vpn-access local-vpn-access	partner-vpn-access local-vpn-access	partner-vpn-services	Encrypt	Long	Gateways
5	Any	gw1.giacent.com	Any	drop	Long	Gateways
6	ecom-net ext-services-net exgiac01	ntp-server	ntp-udp	accept	Long	Gateways
7	ecom-net ext-services-net exgiac01	syslog-server	syslog	accept	Long	Gateways
8	int-proxy-server	Any	http ftp https	accept	Long	Gateways
9	Any	ecom-www-customer ecom-www-supplier	http https	accept	Long	Gateways

10	ecom-www-customer ecom-www-supplier	db-prod-server	sqlnet1	accept	Long	Gateways
11	ecom-www-supplier	radius-box	RADIUS	accept	Long	Gateways
12	Any	ext-dns-server	name	accept	Long	Gateways
13	int-dns-server	ext-dns-server	dns	accept	Long	Gateways
14	ext-dns-server	internal-net-10 ecom-net	dns	accept	Long	Gateways
15	Any	ext-www-server	http https	accept	Long	Gateways
16	Any	ext-smtp-server	smtp	accept	Long	Gateways
17	ext-smtp-server	int-mail-server	smtp	accept	Long	Gateways
18	mgmt-boxes	ecom-net ext-services-net exglac01	ssh ident	accept	Long	Gateways
19	Any	Any	Any	drop	Long	Gateways

No.	Original Packet			Translated Packet			Install On
	Source	Destination	Service	Source	Destination	Service	
1	internal-net-10	partner-net	Any	Original	Original	Original	Gateways
2	partner-net	internal-net-10	Any	Original	Original	Original	Gateways
3	ecom-www-customer	internal-net-10	Any	Original	Original	Original	Gateways
4	ecom-www-customer	Any	Any	ecom-www-customer-NAT	Original	Original	Gateways
5	Any	ecom-www-customer-NAT	Any	Original	ecom-www-customer	Original	Gateways
6	ecom-www-supplier	internal-net-10	Any	Original	Original	Original	Gateways
7	ecom-www-supplier	Any	Any	ecom-www-supplier-NAT	Original	Original	Gateways
8	Any	ecom-www-supplier-NAT	Any	Original	ecom-www-supplier	Original	Gateways
9	ext-dns-server	internal-net-10	Any	Original	Original	Original	Gateways
10	ext-dns-server	Any	Any	ext-dns-server-NAT	Original	Original	Gateways
11	Any	ext-dns-server-NAT	Any	Original	ext-dns-server	Original	Gateways
12	ext-smtp-server	internal-net-10	Any	Original	Original	Original	Gateways

13	ext-smtp-server	Any	Any	ext-smtp-server-NAT	Original	Original	Gateways
14	Any	ext-smtp-server-NAT	Any	Original	ext-smtp-server	Original	Gateways
15	ext-www-server	internal-net-10	Any	Original	Original	Original	Gateways
16	ext-www-server	Any	Any	ext-www-server-NAT	Original	Original	Gateways
17	Any	ext-www-server-NAT	Any	Original	ext-www-server	Original	Gateways

2.1.3 Server VPN

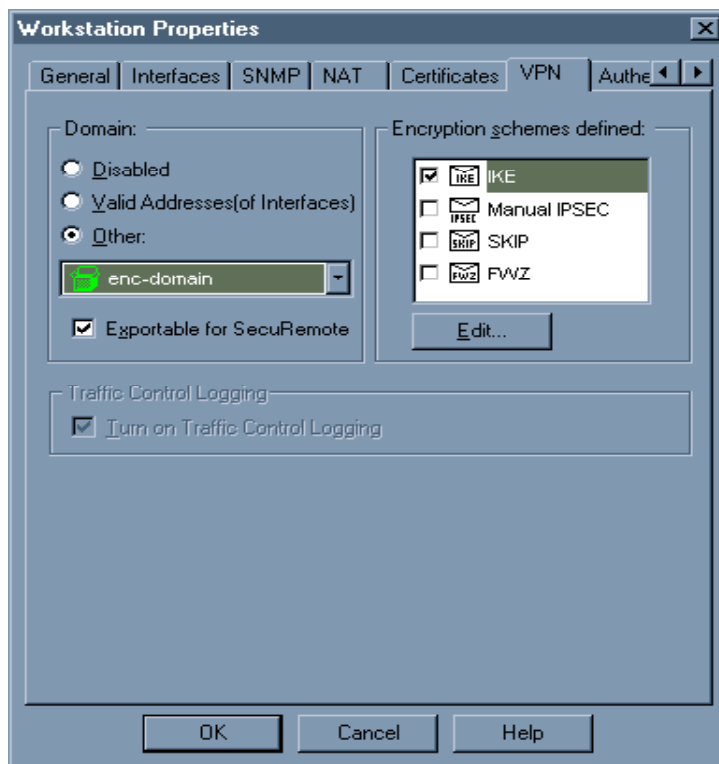
The partner connectivity requirements have been realized through the establishment of an IKE VPN using a pre-shared secret between the VPN-1 firewall, **gw1.giacent.com** and the partner's external firewall, **partner-fw**. The partner's firewall is also a CheckPoint VPN-1 firewall. Fortunately there are no IP address conflicts between the two internal networks and therefore NAT is not necessary.

The parameters for this VPN connection are:

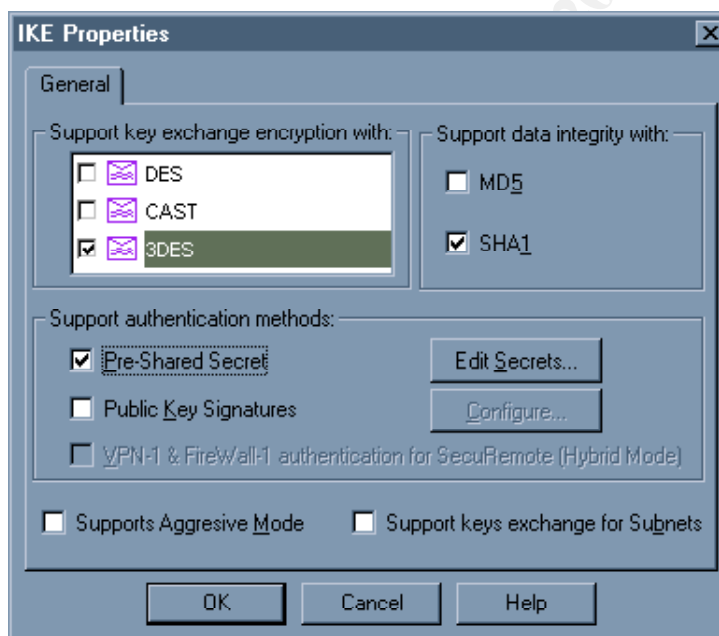
- Primary authentication = pre-shared secret
- Protocol = ESP
- Algorithms = 3DES, SHA-1
- Aggressive Mode is not supported for Phase 1 negotiations (this may be altered if there are issues with establishing/maintaining the connection)
- Perfect Forward Secrecy is implemented.
- Key exchanges for subnets are not supported (this may change if performance is an issue, but the GIAC firewall does have a VPN Accelerator card installed).
- Renegotiate Phase 1 SA every 10080 minutes
- Renegotiate Phase 2 SA every 60 minutes

The following screen shots show the configuration of the above parameters on **gw1.giacent.com** in the CheckPoint Policy Editor.

This screen shot below shows the selection of the IKE encryption scheme and the definition of encryption domain. The encryption domain object needs to contain all objects that need to be accessed over a VPN to this firewall.

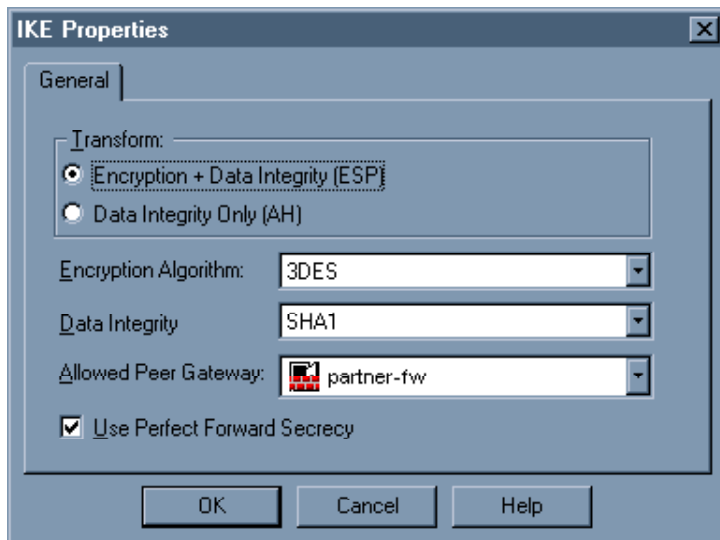


The next screen shot shows the IKE properties screen and the associated



parameters.

The next screen shot shows the Properties of the selected encryption scheme, IKE, of the Encrypt action in rule 4 of the security policy.



2.2: Security Policy Tutorial

This tutorial will focus on the implementation of the security policy on the primary firewall using CheckPoint's Policy Editor. Some important points to note are:

- Packets are compared for with rulebase from the top/first rule down. The first rule that matches is applied to the packet. Therefore the ordering of the rules is extremely important. The syntax of the rule can be seen in the screen shot below:

Source	Destination	Service	Action	Track	Install On	Time
--------	-------------	---------	--------	-------	------------	------

- A match occurs if the **Source**, **Destination** and **Service** fields of the rule equal or include those of the packet. When a match occurs the action that is specified in the **Action** field is carried out. The log entry detail is determined by the **Track** field.
- Firewall-1 is a stateful packet filtering firewall. For more information see Lance Spitzner's paper at <http://www.enteract.com/~lspitz/fwtable.html> for an in-depth discussion of this technology works. There are also quite a number of other papers that relevant to Firewall-1.

2.2.1 Policy Properties

The first action to take in implementing a new security policy on a CheckPoint firewall is to change the default settings in the Policy | Properties window.

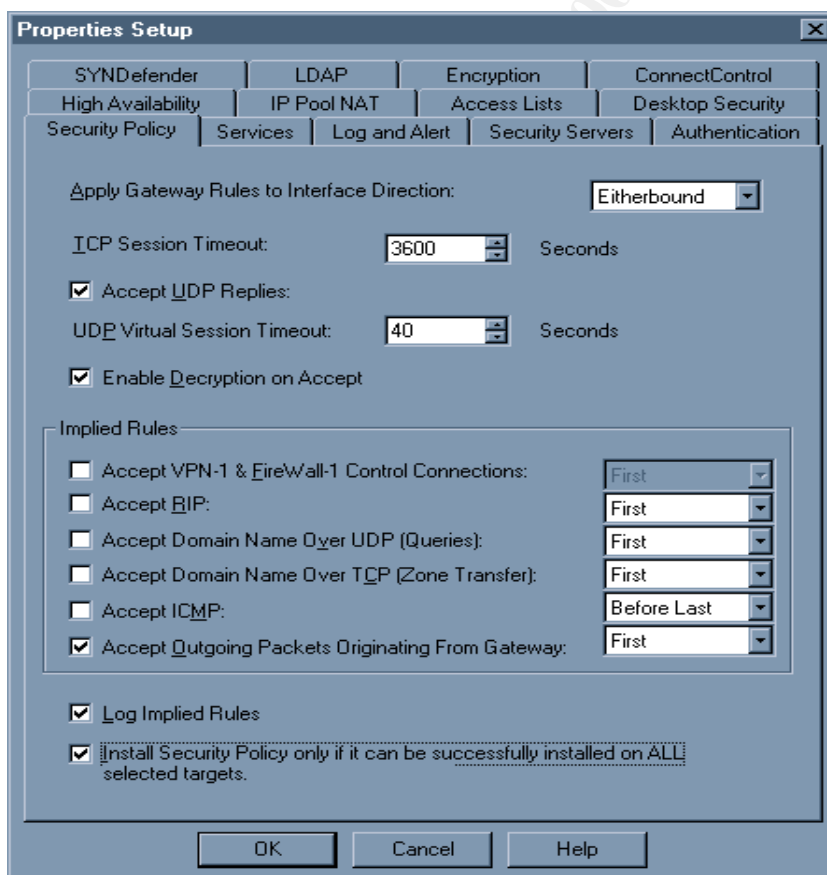
2.2.1.1 Security Policy Tab

The security policy tab contains a number of default settings that enable quite dangerous "Implied Rules" in the security policy. These implied rules can be viewed by selecting Implied Rules from the View pull-down menu.

-	Any	Any	domain-udp	accept	
-	Any	Any	domain-tcp	accept	
-	Any	Any	ICMP	accept	

The above screen shot shows the default implied rules that allows ALL port 53 TCP/UDP and ICMP traffic to traverse the firewall. It is a large security risk to allow unrestricted port 53 and ICMP traffic into and out of your network. The default also accepts FW1 control connections from anywhere and should be disabled. But, ensure that you add a rule that allows you to manage the box or you may lock yourself out. If this happens, add the required management rule and then from the firewall console execute **fw fetch <mgmt stn ip>** to grab the new policy (This is only relevant for configurations that have separated firewall and management stations. For combined installations, it may be necessary to **fw unload localhost** before a new policy can be uploaded, but this has security implications as the firewall is essentially open when the policy is unloaded.)

It is recommended to disable most of these implied rules(as shown in the screen shot below) and manually create rules as required.



2.2.1.2 Services Tab

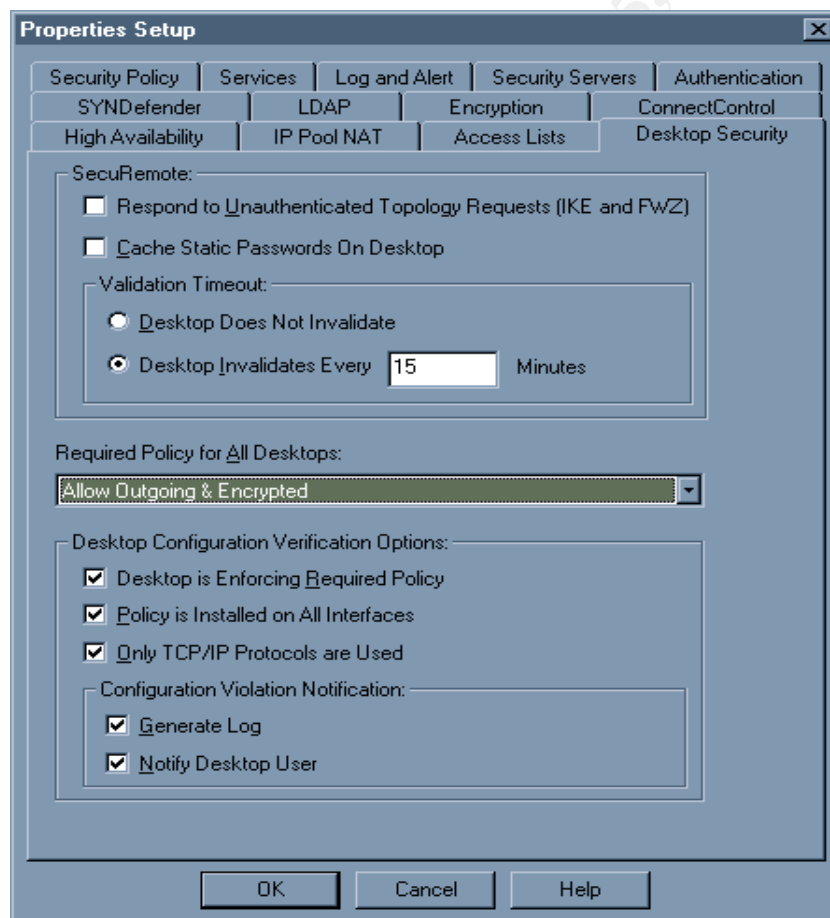
The Services Tab contains checkable 4 options. The first 2 options relating FTP can usually be left enabled and allows the firewall to deal with "protocol bending" nature of Active and Passive FTP connections. The option for RSH and REXEC should be unchecked as these are security risks and should be replaced by SSH. Portmapper and RPC services are also considered dangerous and should not be allowed across an internet firewall.

2.2.1.3 IP Pool NAT

Enable this check box as GIAC will use IP Pool NAT for SecuRemote/Client VPN connections. Set the logging/tracking options to Alert and Log respectively. (NB. The actual NAT Pool network is specified in the NAT tab of the VPN gateway object).

2.2.1.4 Desktop Security Tab

The options in this tab relate to the SecureClient VPN and should be configured as



shown in the screen shot below.

This will ensure that Client VPN hosts do not allow potentially malicious incoming connections while they have a tunnel established to the GIAC internal network.

2.2.1.5 Other Tabs

The default settings on the other tabs are acceptable for the implementation of this policy.

2.2.2 Object Creation

The next step is to determine what objects need to be created in order to implement the security policy. This determination is best carried with a copy of the network architecture and the company's security policy. The objects can then be created using the Policy Editor. The Manage pull-down menu gives access to the Network Objects, Services, Resources, Servers, Users and Time applets that allow the creation of the associated objects.

2.2.3 Rule Creation

After all of the required objects have been created, the process of building the Security Policy Rule Base can begin. A rule can be added to the bottom of the Rule Base using a shortcut button or by selecting Add->Bottom from the Edit pull-down menu. A screen shot of a new rule is shown below:

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	Any	Any	drop		Gateways	Any	

The value of the fields can be changed by right-clicking in the field that you want to change and making an appropriate selection.

When deciding on the order of your rule base, try to place the most frequently matched and most general rules at the top and place the least used and most specific at the bottom.

2.2.4 GIAC Security Policy Rule Base

As the Track and Install On fields are the same for all rules they have been omitted from the following screen shots.

RULE 1: Since we have disabled the Accept FW1 Control Connection in Properties we need to explicitly define a rule that allows us to manage the firewall bastion host.

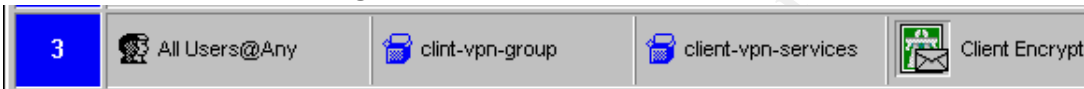
1	fw-mgmt-station	gw1.giacent.com	FireWall1 ssh icmp-proto ident	accept
---	-----------------	-----------------	---	--------

As can be seen, very few ports need to be open for the management connection.

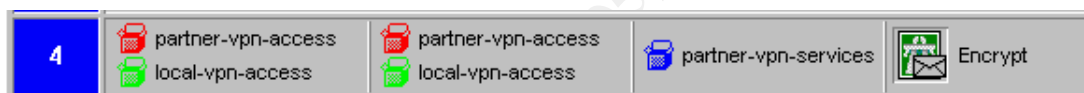
RULE 2: This rule allows the SecureClient VPN clients to download the internal network topology, establish an IPSEC tunnel and download the required desktop policy. A bypass vulnerability has been discovered for the RDP protocol but our configuration is not vulnerable due to patch level and disabling default settings in Properties.



RULE 3: This rule allows Secure Client VPN users to access a limited number of hosts and networks using a limited number of ports and protocols. Tip - As we are using hybrid authentication with radius/SecurID, you only need to create 1 user in the User Database called **generic*** and install it.



RULE 4: This rule allows IPSec VPN traffic between a limited number of hosts/nets on the GIAC and a limited number of hosts/nets on the partner network on a



limited number of ports and protocols.

RULE 5: Protect the firewall bastion host from unauthorized traffic. Sometimes



mistakenly called a stealth rule.

RULE 6: Allow service network hosts and the external router to access the stratum 1 ntp server. This rule could be considered dangerous as it allows traffic initiated from the external service networks into the internal network. There have also been remote root exploits for the xntpd daemon recently. Therefore this traffic will be



closely monitored.

RULE 7: Allow service network hosts and the external router to dump logs on the internal syslog server. As with rule 6, it allows traffic initiated from the external



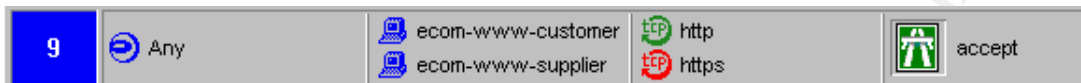
service networks into the internal network and therefore warrants careful monitoring.

RULE 8: Allow the internal proxy server to access the public internet for standard



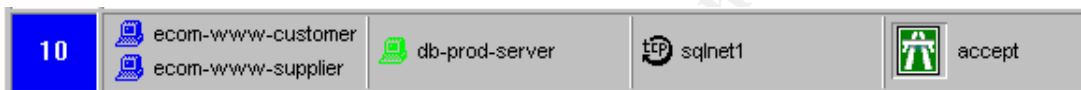
internet services.

RULE 9: Allow all to access the ECOM web servers on TCP ports 80 and 443. This still leaves the web servers open to data driven and buffer overflow attacks that



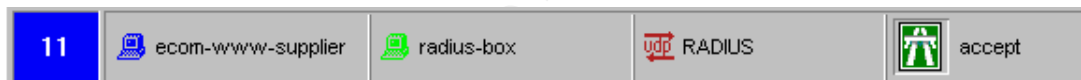
utilize these ports/applications as a transport.

RULE 10: Allow the ECOM web servers to access the backend database server. This is potentially one of the most dangerous rules as it allows exposed web servers to initiate connections to the extremely valuable/sensitive production database



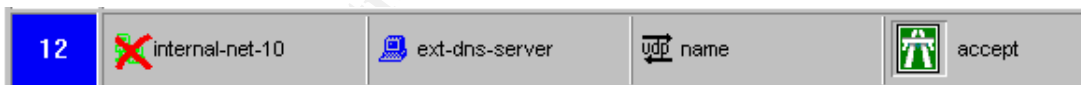
server.

RULE 11: This allows strong authentication of the GIAC suppliers before they are allowed to access the supplier web site. It should be noted that the SecurID one

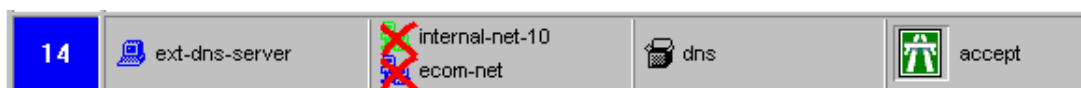


time password is encapsulated within the radius authentication packet.

RULE 12: Allow external UDP DNS requests to the external DNS server.



RULE 13: Allow internal DNS server to use the external server as a resolving server.

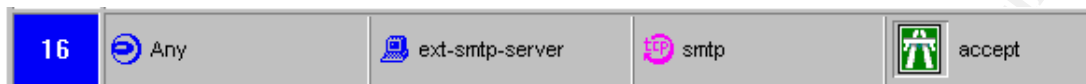


RULE 14: Allow external DNS server to resolve external names.



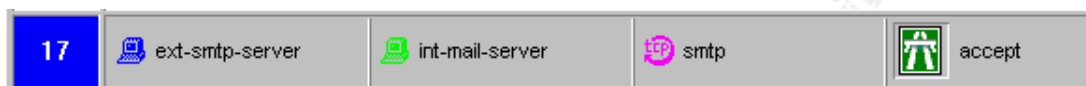
RULE 15: Allow access to the GIAC public web server on TCP ports 21,80 and 443.

RULE 16: Allow SMTP mail to be dumped on the external mail relay. The external SMTP relay is running a Postfix mail server that is hardened against relaying/spam



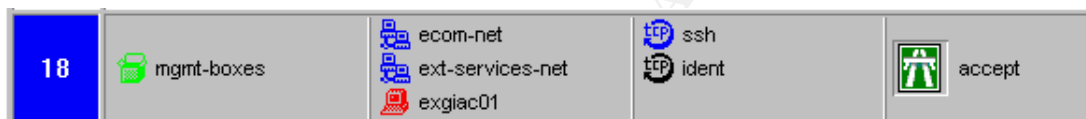
etc.

RULE 17: Allow external mail relay to deliver incoming SMTP mail to the internal



mail server.

RULE 18: Allow management hosts to access external service networks and external router. As can be seen, only ident and ssh are used. Although ident is not



completely trustworthy, it is interesting to see the user name in the connection logs.

RULE 19: Explicit Deny/Drop everything/Clean up rule.



NOTE: It is also important to correctly configure anti-spoofing on all of the firewall's interfaces. These settings can be found in Security Tab of the interface Properties dialog box. These can be tricky and require much careful thought and testing, especially when NAT and VPNs are being used.









2.2.5 GIAC Network Address Rule Base

Although you can configure objects so that NAT rules are generated automatically, it is better to create them yourself so that you understand/know exactly what is happening. Also, each public IP address that is used for a NAT'd host must have a published arp entry on the firewall's external interface or a static route configured on the external router pointing to the firewall.

RULEs 1 & 2: These 2 rules are to ensure that traffic destined for the VPN tunnel with GIAC's partner is encrypted and not translated. Although this rule is not strictly necessary at the moment it is a good to have this in the rule base in case more NAT rules that may affect the partner VPN are added.

No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	 internal-net-10	 partner-net	 Any	 Original	 Original	 Original
2	 partner-net	 internal-net-10	 Any	 Original	 Original	 Original

RULEs 3,4 & 5: These rules prevent NAT from occurring when an internal host accesses the ECOM customer web server, but NAT the ECOM customer web server to a publicly accessible IP address when it accessed by an external host.

3	 ecom-www-customer	 internal-net-10	 Any	 Original	 Original	 Original
4	 ecom-www-customer	 Any	 Any	 ecom-www-customer-NAT	 Original	 Original
5	 Any	 ecom-www-customer-NAT	 Any	 Original	 ecom-www-customer	 Original

RULEs 3,4 & 5 are essentially repeated for:

- 6,7 & 8 → NAT of ecom-www-supplier
- 9,10 & 11 → NAT of ext-dns-server
- 12,13 & 14 → NAT of ext-smtp-server
- 15, 16 & 17 → NAT of ext-www-server

2.2.6 Test 3 Rules

Rules 12, 16 & 17 could be tested by sending an email to/from a yahoo/hotmail account to/from a GIAC mail account. This will test domain resolution of the MX record for GIAC external domain. This will verify that rule 12 is working correctly. It will also test if SMTP mail can be sent and received externally which will verify that rules 16 and 17 are working.

ASSIGNMENT 3: Audit Your Security Architecture

3.1 Audit methodology for Primary Firewall

As per the white paper [Auditing Your Firewall Setup](#) by Lance Spitzner,

There are two parts to auditing your firewall setup. First, you want to test the firewall itself. As a critical system in your security plan, you want to ensure this is secure. Second, you want to test the rulebase, what traffic can pass through the firewall? The whole purpose of the firewall is to control traffic, you want to verify it is doing its job.

The first part of the audit will be on the firewall bastion host itself and will be carried out as follows:

Action	Description	Time/Expertise	When	Cost
A.1	Check physical security of firewall bastion host.	1 hour/engineer	Any	80 euro
A.2	OS & other services check	2 hours/senior engineer	Weekend/ Change window	300 euro
A.3	Firewall software check (config & patch level)	1 hours/senior engineer	Any	150 euro
A.4	Nmap scan of firewall from all directly connected subnets	5 hours/engineer	Any	400 euro

The second part of the audit will validate whether the firewall is correctly implementing the security policy and what is actually accessible through the firewall.

Action	Description	Time/Expertise	When	Cost
B.1	Nmap scan of all known internal networks scan from EIL.	6 hours/engineer	Weekend/ Change window	480 euro
B.2	Confirm Client VPN authentication is working correctly by using incorrect auth credentials	0.5 hour/engineer	Any	40 euro
B.3	Confirm that Client and Site VPN traffic is actually encrypted by sniffing traffic on Internet Isolation LAN	1 hour/engineer	Any	80 euro
B.4	Nessus vulnerability scan of all hosts detected by nmap scan	3 hours/engineer	Weekend/ Change window	240 euro

B.5	Complete review of architecture	3 hours	Any/ Architect	600 euro
-----	---------------------------------	---------	-------------------	-------------

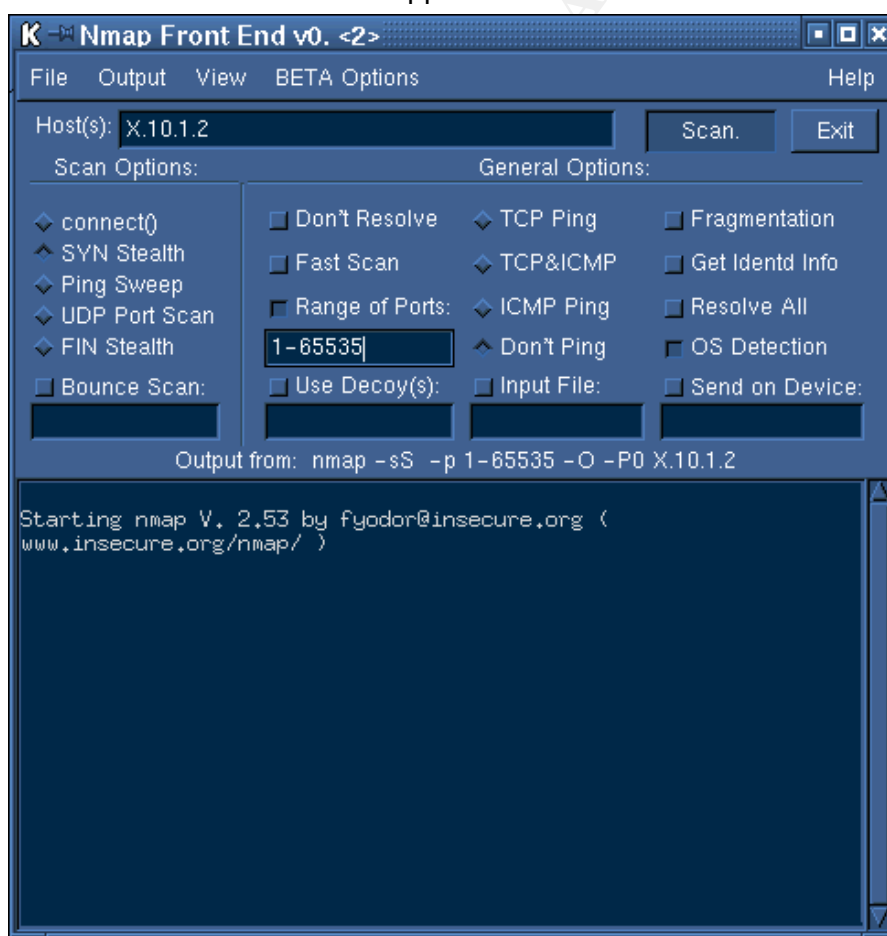
3.2 Conduct the Audit

A.1 Review of physical security - physical access controls in place for building access. ID Badge must be displayed at all times. Limited access to server room based on authorized ID Badge, but a helpful employee held open the door for the audit engineer without requiring identification. Cabinets housing the firewall and connected switches were locked and secure.

A.2 Firewall is appears to be correctly secured to the bastion host level. The only listening services on the firewall services are ssh and FW1/VPN related services. This is expected as the firewall OS has been built from a Core Solaris install and packages added as needed. Titan and YASSP were then run over the install to ensure that nothing extraneous was left running.

A.3 The firewall is running version 4.1 SP4 . Although SP5 has just been released, the release notes do not point to any serious security fixes. Therefore news groups and mailing lists will be monitored for another week or so to ensure that there are no serious issues with this release. All of the dangerous default settings of Firewall-1 have been disabled the rule base appears to be secure.

A.4



The previous screen shot show the GTK front end to nmap about to conduct a stealthy scan, without ping test, of all 65535 TCP ports on the public interface of the firewall. It also attempts to identify the operating system. This is being done from the Internet Isolation LAN. This deliberately bypasses the router ACL so as to test security layer by layer. This scan is exhaustive and will take quite some time.

A full UDP scan using **nmap -sU -p 1-65535 -O -P0 X.10.1.2** was conducted.

The above two scans were conducted against all interfaces of the firewall from a laptop with a valid IP address on directly connected networks. The results of the scans are shown on the table below.

```
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
Interesting ports on (X.X.X.X):
(The 65548 ports scanned but not shown below are in
state: filtered)
Port      State      Service
22/tcp    open       ssh
113/tcp    open       auth
256/tcp    open       rap
257/tcp    open       set
258/tcp    open       yak-chat
259/tcp    open       esro-gen
264/tcp    open       bgmp

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

Only the expected VPN related ports(259 &500) were found to be open in the UDP scan.

The scan results were the same from all subnets and therefore will not be repeated.

B.1 The only hosts detected were the 5 hosts on the service networks.

B.2 Client Authentication was confirmed to be working correctly as incorrect and reused login credentials were all rejected.

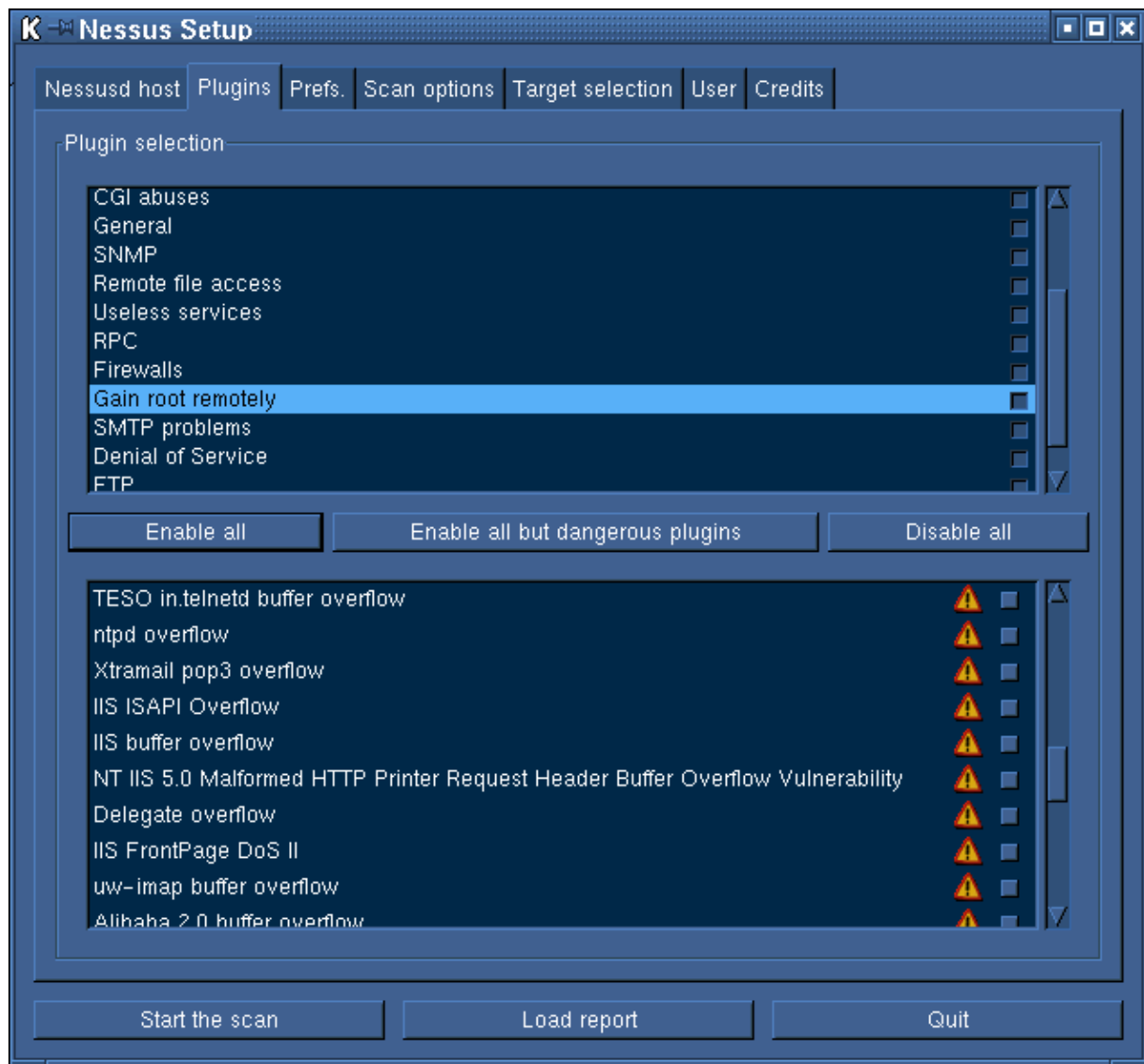
B.3 VPN traffic was captured using tcpdump and Ethereal. All traffic was confirmed to be encrypted and unreadable. The firewall logs also showed encryption and decryption taking place successfully.

B.4 The [nessus](#) daemon and scan client are both installed on the scanning host laptop. All of the latest nessus plug-ins were downloaded and installed. The next screen shot shows some of the possible scan options.

The nessus scan resulted in only various "Security notes" such thing as:

"We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult"

No security vulnerabilities were uncovered by the nessus scans.



3.3 Audit Evaluation and Recommendations

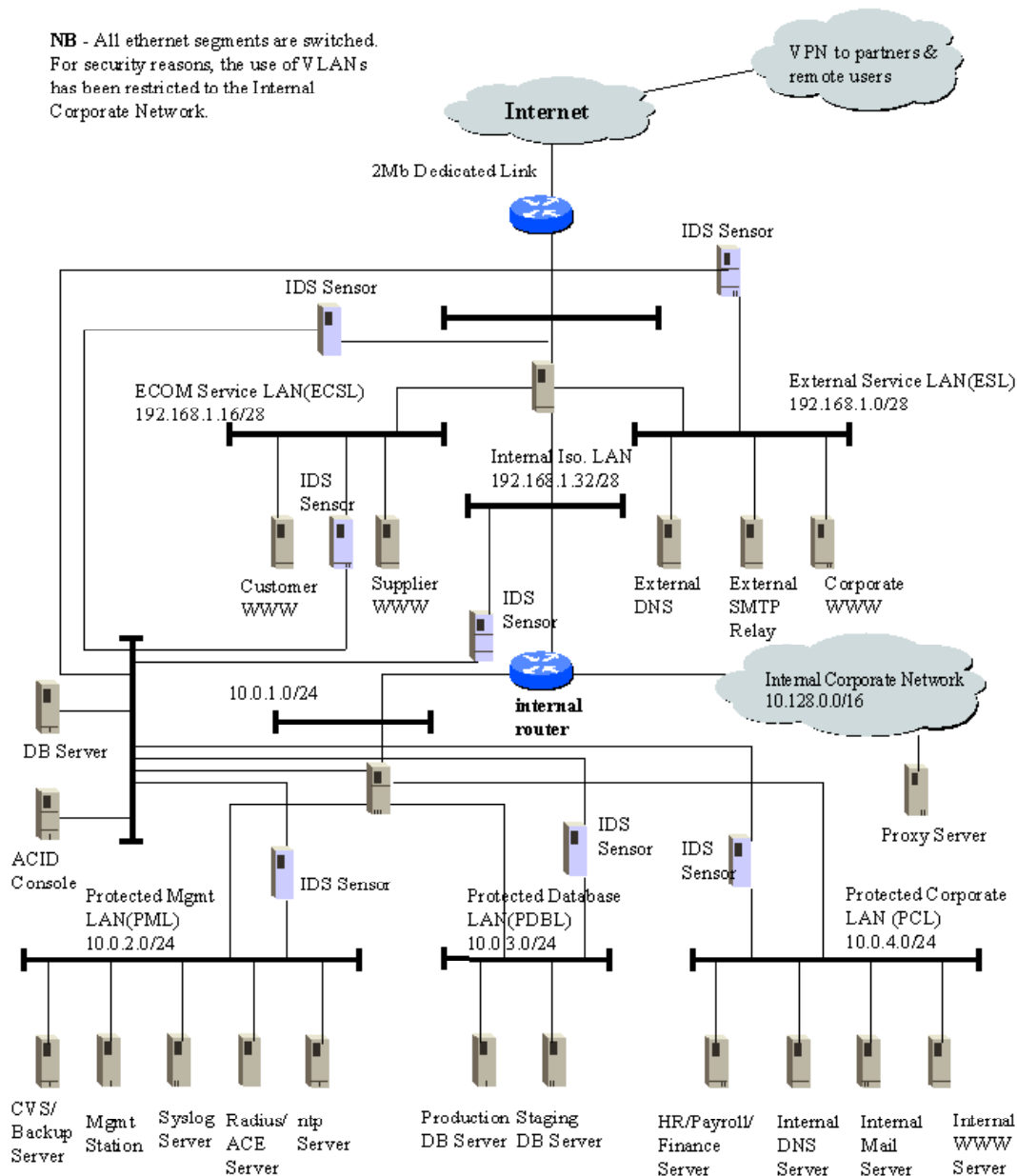
In general the audit results were positive with regard to the state of GIAC Enterprises network security. All of the scans were logged by the firewall. A review of ports required for FW1 management is recommended. It would be better to allow specific required ports rather than using the "Firewall1" service group.

The architectural review resulted in the following recommendations:

- IDS Implementation - A serious limitation of this architecture is the lack of an network intrusion detection capability. This really is a necessity if a pro-active approach is to be taken to incident detection and response. It is recommended that the GIAC Security Team initiate a pilot utilizing using the freely available [Snort](#) IDS software. The next screen shot shows a possible architecture. It should be noted that all IDS sensors have 2 interfaces. The "listening" interface should have no IP address and be patched to a "spanning" port on the switch so that it can sniff all the data on the wire. The second interface is used for reporting/alerting and management of the sensor. This will have the immediate benefit of increased situational awareness with regard to the GIAC network as well as giving an insight into the particular challenges and difficulties of implementing, tuning and maintaining an IDS system.
- Content Scanning should be implemented to try and stop malware entering the GIAC network. It should be implemented on all incoming HTTP and FTP traffic. SMTP traffic should be scanned in both inbound. One possible solution would be the implementation of a TrendMicro VirusWall on the External Services LAN(ESL).
- There are a number of single points of failure should be addressed:
 - implementation of HA/redundant internal and external core routers using HSRP.
 - HA/redundant primary firewall using the [StoneBeat](#) Full Cluster solution
 - Implementation of HSRP for internal IPFilter firewall (this will require significant internal development) so a cold-standby option may be a quick fix.

© SANS Institute 2000 - 2005, All rights reserved.

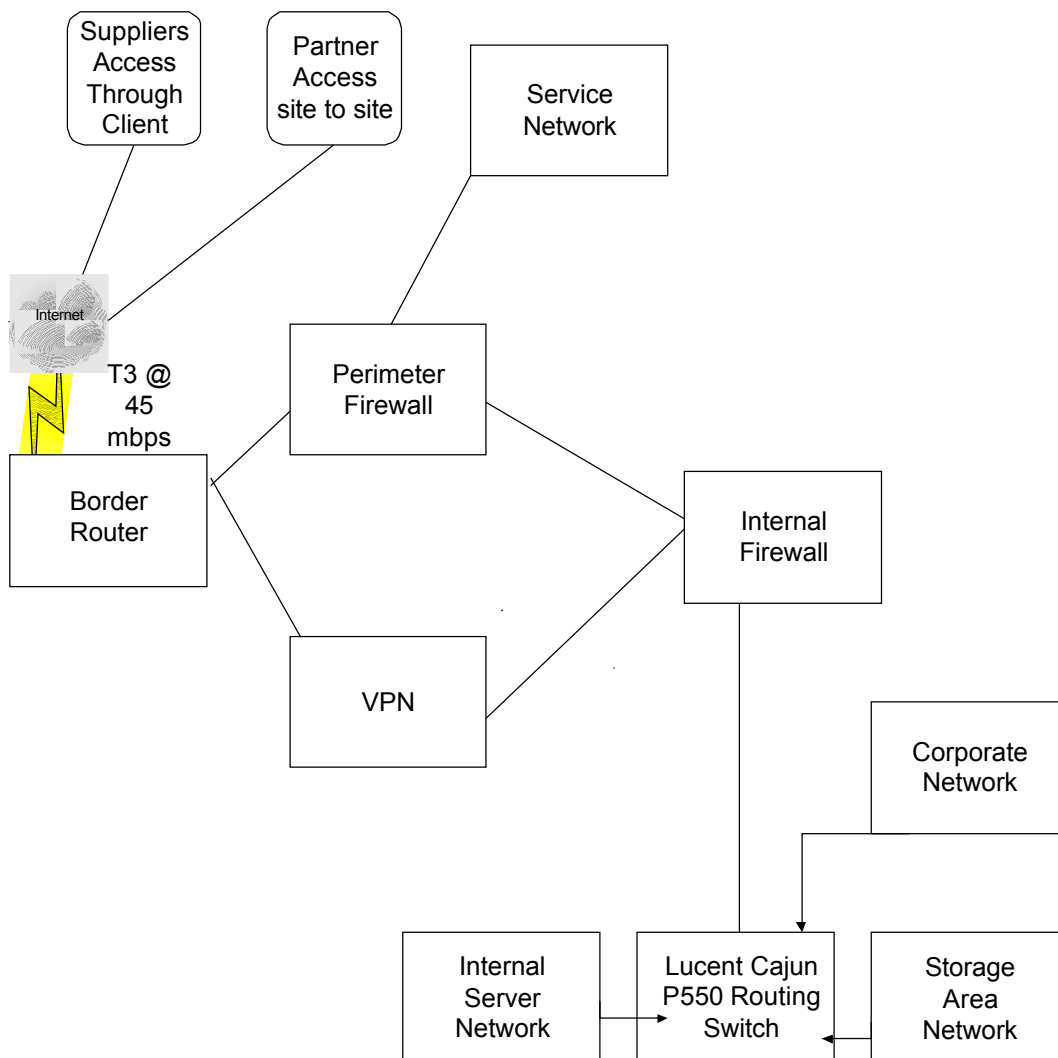
NB - All ethernet segments are switched.
For security reasons, the use of VLANs has been restricted to the Internal Corporate Network.



Architecture with proposed IDS implementation

ASSIGNMENT 4 - Design Under Fire

For this part of the, the practical from Justin Ginsberg, available at www.sans.org/y2k/practical/Justin_Ginsberg_GCFW.zip will be used. The architecture of this submission is shown below.



The perimeter and internal firewalls are both MS NT4 SP6 system running CheckPoint Firewall-1 4.1 SP6(?). This may be just "future-proofing" against attack, but at the time of the writing of this paper CheckPoint had just released SP5. For the purposes of this assignment it is will be assumed that the incorrect patch has

been applied and that the running firewall installations are default 4.1 installs.

4.1 Attacks on primary firewall

ATTACK 1: Check Point Firewall-1 RDP Header Firewall Bypassing Vulnerability

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

ATTACK 2: IP Fragmentation Vulnerability CVE-2000-0482

Description: "Check Point Firewall-1 allows remote attackers to cause a denial of service by sending a large number of malformed fragmented IP packets" from cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0482

ATTACK 3: Fastmode Vulnerability

Description: "Check Point VPN-1/FireWall-1 4.1 SP2 with Fastmode enabled allows remote attackers to bypass access restrictions via malformed, fragmented packets" from cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0082

ACTUAL ATTACK:

The actual attack will be to exploit the IP Fragmentation vulnerability. This will be done using the Jolt2 tool. The result of the attack will be a sustained 100% CPU utilization on the firewall and a complete DOS on the external firewall until the Firewall-1 is restarted.

4.2 DDOS Attacks

50 compromised Cable/DSL hosts running DDOS such as Trinoo all directing large ICMP packets at the external firewall should be enough to basically completely cut off GIACs internet access even though GIAC has a T3 connection. This is because the Firewall allows ICMP traffic by default and there is no rule protecting the firewall itself. Therefore it will attempt to process and respond to allow these ICMP packets.

For more information on DDOS, please see Dav Dittrich's papers that are available from <http://www.cac.washington.edu/People/dad/>

4.3 Compromise an internal host

As stated on p.29 of the Justin Ginsbergs practical submission:

=====

The following are the control properties for Firewall -1. The Control Properties dialog box is where you set the properties that make up the security policy for Firewall -1. These are the control policies for both the Internal and external firewalls that GIAC has deployed.

Security Policy

1. Apply Gateway Rules to interface Direction = Inbound
States that rules will apply on all inbound connections.
2. TCP Session Timeout = 3600
3. Accept Firewall-1 connections = on
#Used so that the two firewalls can communicate
4. Accept UDP Replies = on
Creates a reply channel between the source host and the destination Host.
5. Reply timeout = 40
6. Accept Outgoing Packets = on Last
Accepts outgoing packets from the firewall.
7. Enable Decryption on Accept = off
The firewall is not using Encryption.
8. Accept RIP = on
RIP maintains information about reachable systems.
9. Accept Domain Name Queries (UDP) = on first
Allows Domain Name queries (UDP)
10. Accept Domain Name Queries (TCP) = on First
Allows zone transfers
12. Accept ICMP = on Before Last
Enables you to use ICMP. In this case all ICMP traffic from the inside going out will be answered. The border router or Service Network host will answer all ICMP

=====

As per points 9 & 10, port 53 for both TCP and UDP is open from Any to Any and is placed First in the rulebase. This means that all of GIAC Enterprises internal network are open to port 53. The internal IP space being used by GIAC is not specified so we will assume it routable.

Therefore we will initiate a scan of the internal network looking for hosts running a name service. The submission did not state the type or version of DNS software used on the internal DNS servers. For the purposes of this assignment, it will be assumed that they are running a vulnerable version of BIND 8.x. The vulnerability that will be exploited is listed below:

From the www.cert.org database:

VU#196945 - ISC
BIND 8 contains buffer overflow in transaction signature (TSIG) handling code

During the processing of a transaction signature (TSIG), BIND 8 checks for the presence of TSIGs that fail to include a valid key. If such a TSIG is found, BIND skips normal processing of the request and jumps directly to code designed to send an error response. Because the error-handling code initializes variables differently than in normal processing, it invalidates the assumptions that later function calls make about the size of the request buffer.

Once these assumptions are invalidated, the code that adds a new (valid) signature to the responses may overflow the request buffer and overwrite adjacent memory on the stack or the heap. When combined with other buffer overflow exploitation techniques, an attacker can gain unauthorized privileged access to the system, allowing the execution of arbitrary code.

Exploitation of this vulnerability with appropriate code would allow us to get root access and thereby compromise an internal host. The box would be "rooted" using our favourite root kit from www.rootshell.com, preferably a Kernel Loadable Module such as [KNARK](#). From here, the possibilities for further intrusion are virtually endless, but I guess our next port of call would be the now unprotected, but highly valuable Fortune Cookie Saying database on the SAN.

© SANS Institute 2000 - 2005, Author retains full rights.