Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment Version 3.0

By Georgios Sagos

02-08-2004

Table of contents

Assignment 1 – Security Architecture

1 Introduction

GIAC enterprises is a newly started, fast expanding company that today employs 400 people world wide. The core business of the GIAC enterprises is an e-business which deals in online sale of fortune cookie sayings. The main office is based in Copenhagen Denmark, and 350 of the 400 employees is based here, the rest is sales persons worldwide, also there is a lot of worldwide wide partners who translate the fortune cookies into native languages and work closely together with the sales responsible person(s) in that respectable country. Today there is only one remote sales office based in the US, and the rest of the sales force are working more or less independently from their home or on the road, but other remote sales offices is on the drawing board to create bases for the busy sales force.
The main focus and guidelines giving by the management is accessibility and availability, so therefore redundancy is a big issue.

1.1 Access requirements

Following is the access requirement and restrictions for each "group":

1.1.1 Costumers/General Public:

Connects via http to browse the GIAC enterprises website, if they intent to buy a fortune cookie, they will have to create an account were they supply username and password among others witch is stored in a database.
The transaction will be encrypted with SSL/TLS. When the transaction is complete the customer will be redirected to a page were they can download there fortune cookie(s). If more that one fortune cookie is purchased they will be available packed in a bulk file for download. After the download is complete the page will expire. It is also possible to subscribe for fortune cookies, where the costumers can buy a month or a year subscription, the costumers will then be able to connect to the site for the given period and download the cookies.
Ports: HTTP (TCP port 80) HTTPS (TCP port 443), Restrictions made on web server. Inbound rules on firewall.

1.1.2 Suppliers:

Connects to a SSH version 2 server were they will upload their fortune cookies using secure copy. Due to the number and the rapid change in suppliers the format of the cookie saying varies, that's why the cookies will be revised by the GIAC enterprise approval team witch will upload the cookies in the right format to the GIAC enterprise web server for sale to the public.
Ports: SSH (TCP port 22) Restrictions made on the SSH server. Inbound rules on firewall.

1.1.3 Partners:

Connects via VPN tunnels site to site from the partner's hardware, because it's a very trusted partner alliance, and the criteria of becoming a partner is very strict, business wise and security wise.
Ports: IKE (UDP port 500) ESP (protocol 50) AH (protocol 51). Terminates in firewall cluster modules and restricted to IP addresses (objects).

1.1.4 Internal GIAC enterprise employees:

Connects outbound by an any/allow rule (management net negated), and is NATed on the firewall by a hide behind address rule, On the border gw routers, the following outbound ports are blocked and logged, except NetBIOS UDP port 137 witch is very noisy: telnet TCP port 23, EndPointMapper TCP/UDP port 135, NetBIOS UDP port 138, NetBIOS TCP port 139, NetBIOS TCP/UDP port 445, RPCbind TCP/UDP port 111, NFS TCP/UDP port 2049.
Traffic that's illegal according to GIAC Enterprise security policy is blocked outbound on the FW cluster, traffic like: peer2peer, eDonkey, GNUtella, ident, KazaA, MSN, Napster……new ports and protocols will be added continuously.
They connect to the DHCP server via BOOT relay on the firewall cluster modules, and for domain logon and internal DNS to the internal server segment by an any rule. Ports covers amongst others: Domain Name System (DNS) (UDP port 53), Kerberos authentication (TCP port 88), Windows Time Synchronization Protocol (NTP) (TCP port 123),
EndPointMapper (TCP/UDP port 135), Lightweight Directory Access Protocol (LDAP) (TCP/UDP port 389), Server message block (SMB) for Netlogon, LDAP conversion and distributed file system discovery (TCP port 225), LDAP to global catalog servers (TCP port 3268), restrictions are made on the individual servers.
All users have Norton antivirus installed on their desktops and laptops.
This all applies to the "regular" users, server rights may vary depending of witch department the users are connecting from. All mail (SMTP port 25) in and out goes via Checkpoints CVP (Content Vectoring Protocol) to be scanned by a Clearswift Mailsweeper running Sophos antivirus.
Other than that Internal users are divided into 3 sub groups:

1.1.4.1 IT-operation group:

Can connect to any segment using checkpoint user authentication and SecureID tokens (ACE server).
All connection to any network device will be handled via SSH v2 to the terminal server (Cisco 3640) were authentication again will be forced by the SecureID tokens (ACE server) via the AAA server, were the IT-operation group have write access.

1.1.4.2 IT-support group:

Can connect to any segment using checkpoint user authentication and secure ID tokens (ACE server), But are somewhat restricted by server rights. They can also connect to the terminal server in the management section but only with read access, ass well as the Checkpoint firewall manager were a monitor only user has been configured, and again they are restricted in this segment, management, by server/application rights.

1.1.4.3 GIAC enterprise approval team (super users):

Can connect to the GIAC web cluster, SQL DB, and the SSH2 server in the external server segment by an any rule via Checkpoint user authentication, with some server server/application restrictions.

1.1.5 GIAC Enterprises Remote sales office:

Is setup in a Checkpoint Gateway-to-Gateway (MyIntranet) configuration.
The Remote sales office has the same rights as the regular users on the GIAC Enterprise LAN.
Ports: IKE (UDP port 500) ESP (protocol 50) AH (protocol 51), Checkpoint Gateway-to-Gateway (MyIntranet) configuration. See Internal GIAC Enterprise employees, regular users for more details.

1.1.6 GIAC Enterprise Remote/Home users:

All Users in GIAC Enterprise will have the option to work from home; they connect as the sales road offices with Checkpoint secure client, and are authenticated with RSA tokens (ACE server). Once successfully authenticated they have the same privileges on the GIAC Enterprise LAN as the internal users.
Ports: IKE (UDP port 500) ESP (protocol 50) AH (protocol 51), Checkpoint Secure Client/Policy server configuration. See Internal GIAC Enterprise employees, regular users for more details.

1.2 architecture

Drawing 1 describes the network architecture of GIAC Enterprises, all important components is redundant, and placed in 2 different server rooms if possible, servers that can, have 2 interfaces one is connected to the switch (invisible on the drawing) connected to fwgw1 and the other interface to the switch that is connected to fwgw2. The reason that there are 2 (double) IDS icons on each segment is also that they are connected to the 2 invisible switches (Cisco 2950) on each segment, to simplify an otherwise very detailed drawing these switches are invisible. Each switch pair on each segment is connected to each other by a 1000mb link. In the 3 server segments the servers/network components MAC addresses are locked on the switch ports. The networks connecting the 2 routers and the fw sync on the firewalls are also invisible on the drawing.

The 2 border gw routers are running BGP, with own AS number assigned by RIPE, up against 2 different ISPs witch doesn't share the same backbone. One router is running in fibre, and the other by radio link to their respectable ISPs, and both connections are 8mbit. The BGP is handling traffic so that one router takes care of national traffic, and the other international. The lines on the 2 routers will soon be upgraded; we currently have some offers on the table concerning 150mbit ATM lines, because we see already see peaks around 8mbit and costumer revenue is expected to rise dramatically.

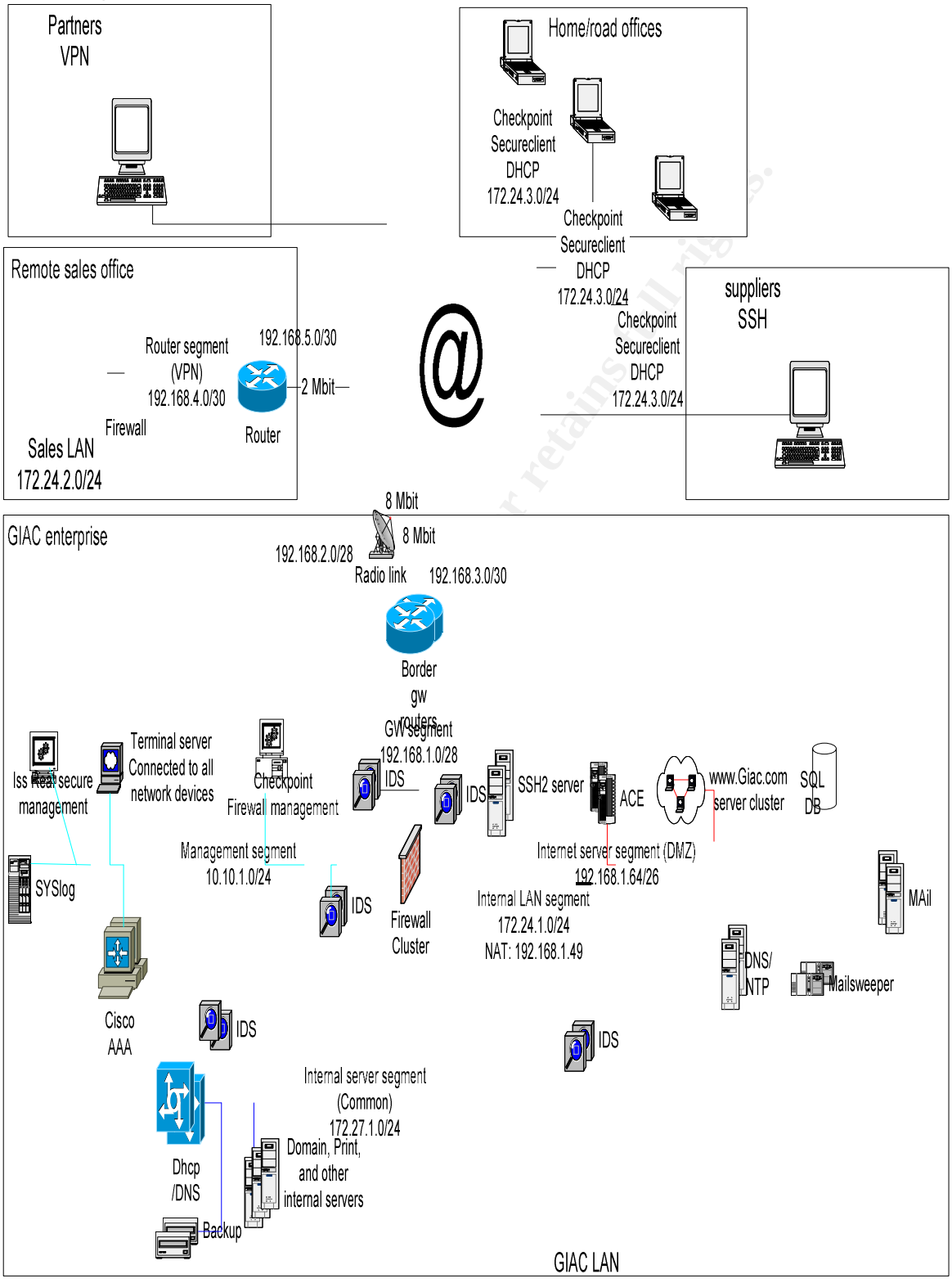
A wireless network for i.e. meeting rooms are being planned as an external network, were the users will be handled like remote users, with VPN and RSA SecurID authentication.

Other future plans, due to the rapid growth of the company, includes VLANs to separate each floor/department in the GIAC Enterprise building, as the GIAC LAN segment is one flat network today, to ease management for network administrators and to have some more redundancy on the network by cabling 2 VLANs into every user segment switch. When The company started up there were only 100 employees and we expected to employ 100 more within the 1st year, but things has gone so well and fast that the network planning couldn't keep up, that's why projects has been planed to put the above mentioned plans into life within a period of 6 moths to cope with the growing revenues.

All non RFC1918 or routable addresses in table 1/drawing 1 has been substituted with the 192.168.x.x range to somewhat protect/cloak GIAC Enterprises real routable addresses for security reasons.

1.2.1 Tables and drawings

Network diagram:



Drawing 1 (Visio)

Net	Usage	First addr.	Last addr.	Subnet bits	# of IP addr.	Comments
0	Network Giac enterprise AS	192.168.1.0	192.168.1.127	25	128	Official/internet routable/RIPE BGP
0.1	Network	192.168.1.0	192.168.1.63	26	64	Subnet of net 0
0.1.1	GW segment	192.168.1.0	192.168.1.15	28	16	Subnet of net 0.1
0.1.2	Spare	192.168.1.16	192.168.1.31	28	16	Subnet of net 0.1
1.1.3	Spare	192.168.1.32	192.168.1.47	28	16	Subnet of net 0.1
1.1.4	NAT segment	192.168.1.48	192.168.1.51	30	4	Subnet of net 0.1
1.1.5	Router loopbak	192.168.1.52	192.168.1.55	30	4	Subnet of net 0.1
1.1.6	Link 1 between routers	192.168.1.56	192.168.1.59	30	4	Subnet of net 0.1
1.1.7	Link 2 between routers	192.168.1.60	192.168.1.63	30	4	Subnet of net 0.1
0.2	Internet server segment (DMZ)	192.168.1.64	192.168.1.127	26	64	Subnet of net 0
1	Outside Border gw router 1	192.168.2.0	192.168.2.15	28	4	Official/internet routable/ISP (is subnetet into 4 /30 nets for serial interfaces)
2	Outside Border gw router 2	192.168.3.0	192.168.3.3	30	4	Official/internet routeble/ISP
3	Management segment	10.10.1.0	10.10.1.255	24	256	RFC 1918
4	Internal server segment	172.27.1.0	172.27.1.255	24	256	RFC 1918
5	GIAC LAN	172.24.1.0	172.24.1.255	24	256	RFC 1918 (DHCP scope)
6	Secure client/policy server	172.24.3.0	172.24.3.255	24	256	RFC 1918 (DHCP scope)
7	Remote sales office outside router	192.168.5.0	192.168.5.3	30	4	Official/internet routeble/ISP
8	Remote sales office router segment	192.168.4.0	192.168.4.3	30	4	Official/internet routeble
9	Remote sales office LAN	172.24.2.0	172.24.2.255	24	256	RFC 1918
10	FW sync.	10.10.10.0	10.10.10.3	30	4	RFC 1918

Table 1 IP Address plan (Excel)

Network Component/brand:	interfaces and IP addresses:	Description:
Border gw router 1 Cisco 7206 VXR router	interface Loopback 0 ip address 192.168.1.53/32 no ip directed-broadcast Description: Used In BGP interface FastEthernet0/0 ip address 192.168.1.2/28 no ip redirects no ip directed-broadcast full-duplex standby priority 100 standby preempt standby ip 192.168.1.1 standby track Serial3/0 10 standby track Serial3/1 10 standby track Serial3/2 10 Description: Primary HSRP routers internal interface interface POS1/0 bandwidth 155000 ip address 192.168.1.57/30 no ip directed-broadcast clock source internal Description: Link 1 between border gw routers used in BGP/OSPF interface POS2/0 bandwidth 155000 ip address 192.168.1.61/30 no ip directed-broadcast clock source internal Description: Link 2 between border gw routers used in BGP/OSPF interface Serial3/0 bandwidth 2048 ip address 192.168.2.2/30 no ip directed-broadcast encapsulation ppp Description: External 2mb modem connection to ISP1 via radio link interface Serial3/1	Software: Cisco IOS version 12.2T This is the primary border gw router in the HSRP (hot router standby protocol) setup, its running BGP (border gateway protocol) to ISP 1 via a radio link connection. The BGP protocol handles the traffic so this router handles all international traffic because the ISP 1 is cheaper than ISP 2 regarding international traffic. Although this is the primary router in the HSRP setup, traffic can still be routed through the POS (Packet over sonnet) interfaces to the secondary router via OSPF. The reason the fairly expensive POS interfaces has been chosen is that the 2 gw routers are placed some distance from each other in 2 separate server rooms. All logs are forwarded to the syslog server (see other components for details). To connect, connect to the terminal server (see other components for details) via ssh2 authentication with RSA SecurID token.

	bandwidth 2048 ip address 192.168.2.6/30 no ip directed-broadcast encapsulation ppp Description: External 2mb modem connection to ISP1 via radio link interface Serial3/2 bandwidth 2048 ip address 192.168.2.10/30 no ip directed-broadcast encapsulation ppp Description: External 2mb modem connection to ISP1 via radio link interface Serial3/3 bandwidth 2048ip address 192.168.2.14/30 no ip directed-broadcast encapsulation ppp Description: External 2mb modem connection to ISP1 via radio link	
Border gw router 2 Cisco 7206 VXR router	interface Loopback0 ip address 192.168.1.54/32 no ip directed-broadcast Description: Used In BGP interface FastEthernet0/0 ip address 192.168.1.3/28 no ip redirects no ip directed-broadcast full-duplex standby priority 65 standby preempt standby ip 192.168.1.1 standby track Serial3/0 10 Description: Secondary HSRP routers internal interface interface POS1/0 bandwidth 155000 ip address 192.168.1.58/30 no ip directed-broadcast clock source internal Description: Link 1 between	Software: Cisco IOS version 12.2T This is the secondary border gw router in the HSRP (hot router standby protocol) setup, its running BGP (border gateway protocol) to ISP 2 via a fiber link connection. The BGP protocol handles the traffic so this router handles all national traffic because the ISP 1 is cheaper than ISP 2 regarding international traffic. Although this is the secondary router in the HSRP setup, traffic can still be routed through the POS (Packet over sonnet) interfaces to the secondary router via OSPF. The reason the fairly expensive POS interfaces have been chosen is that the 2 gw routers are placed some distance from each other in 2 separate server rooms. All logs are forwarded to the log server (see other components for

	border gw routers used in BGP/OSPF interface POS2/0 bandwidth 155000 ip address 192.168.1.62/30 no ip directed-broadcast clock source internal Description: Link 2 between border gw routers used in BGP/OSPF interface Serial3/0 bandwidth 8192 ip address 192.168.3.2/30 no ip redirects no ip directed-broadcast no ip proxy-arp encapsulation ppp ip route-cache flow framing g751 dsu bandwidth 8000 Description: External interface to ISP2 via fiber.	details). To connect, connect to terminal server (see other components for details) via ssh2 authentication with RSA SecurID token.
IDS 1-10 Nokia IP 350	All IDS boxes from 1-10 is configured with 2 interfaces, 1 on the management segment with respectable IP addresses, and 1 in promiscuous mode on the segment each box is configured to detect intrusions. 10.10.1.10-19/24	Software: IPSO 3.8 Build039 and ISS RealSecure 7.0 for Nokia On each Network sensors the following policy is installed: Attack detector, an Attack detector is a default policy in ISS RealSecure, but modified by GIAC enterprise. Using this policy, an ISS RealSecure sensor focuses on network attacks only. This policy is appropriate for Security Administrators who want to know only about the most severe network events, according to RealSecure. The attack detector include a verity of the following attacks: Denial of service, DNS, Email, File sharing, Finger, Firewall, FTP, HTTP, ICMP, Ident, Evasion, IMAP, IP, IRC, NFS, NNTP, POP, Scanners, SNMP, Sun RPC, Telnet, UNIX remote, Windows, SQL. RS kill is enabled on several of the above services so that harmful

		connections are “killed”. It’s very interesting/knowledgeable to monitor the 2 IDS boxes on gw segment outside the firewall, and compare the traffic to the boxes on the inside and visa versa to see what traffic that has been filtered out by the firewall.
RealSecure Console (management) IBM X335	The 2 network connections have been pared/teamed up, and nic1 is connected to switch 1 in the management segment, and NIC2 is connected to switch 2. 10.10.1.20/24	Software: Windows 2003, ISS management console 7.0, MySQL DB server. The IBM X335 is the general choice of server in GIAC enterprises, due to relatively low cost and flexibility. The 2 disks are mirrored with the integrated RAID-1 configuration. All servers in the GIAC enterprise network has Realsecure server sensor installed and configured according to witch OS and applications that server is running. The RealSecure management Console is monitored and fine tuned all the time, when new threats are observed it will be tuned to deal with them, i.e. the SQL Slammer and others.
FWgw1 (FWGWcluster) Nokia IP 1220	IP interfaces: eth-s1p1 100 Mbit Full Duplex External On 192.168.1.5/28 eth-s1p2 100 Mbit Full Duplex Internet_segment On 192.168.1.66/26 eth-s1p3 100 Mbit Full Duplex Internal_LAN On 172.24.1.2/24 eth-s1p4 100 Mbit Full Duplex Internal_server_segment On 172.27.1.2/24 eth-s2p1 100 Mbit Full Duplex	Software: IPSO 3.8 Build039 and Checkpoint R55 3.8 wrapper; VPN1 Pro and Policy server. FWgw1 is set up in a VRRP (Virtual router redundancy protocol) cluster with FWgw2 with equal properties. This cluster is the centre of the GIAC enterprise network, all traffic comes through here. All VPN tunnels are terminated in the cluster, site-to-site as well as client-to-site, Partners, Remote Sales office, Home and Road offices. DHCP scope for secure client users is handled by the GIAC Enterprise DHCP server. All traffic to the GIAC web site will come through the fwcluster modules

	Management_segment On 10.10.1.2/24 eth-s2p2 100 Mbit Full Duplex FW_SYNC On 10.10.10.1 VRRP: External 1 100 2 192.168.1.4 Internet_segment 2 100 2 192.168.1.65 Internal_LAN 3 100 2 172.24.1.1 Internal_server_segment 4 100 2 172.27.1.1 Management_segment 4 100 2 10.10.1.1	where the Checkpoint connect control module will share the traffic between the 3 WEB servers based on load via a load-balancing algorithm. A Load Measuring agent installed on each of the 3 web servers reports the servers status concerning cpu and disk load, and compares the content of the web pages to a file to see if they match, if they don't match, or the cpu/disk or web load exceeds a given limit, the servers agent will report it to the Connect control module based on the fw cluster modules, and traffic will be redirected to another server. The Connect control Module sends ICMP echo requests to each web server in the cluster to see if the servers are up and running, and asks for the servers health on default UDP port 18212. The GIAC enterprise LAN is NATed on the FW cluster with a Hide NAT rule. Checkpoint Smart Defense also helps protection against network and application level attacks and web intelligence to protect the web servers. Boot P relay set on LAN interface to DHCP requests to the DHCP server on the internal server segment. Connections to the IPSO Voyager are restricted to SSL connections, and consol connections via SSH2 to the terminal server.
FWgw2 (FWGWcluster) Nokia IP 1220	IP interfaces: eth-s1p1 100 Mbit Full Duplex External On 192.168.1.6/28 eth-s1p2 100 Mbit Full Duplex Internet_segment On 192.168.1.67/26 eth-s1p3 100 Mbit Full Duplex Internal_LAN On	Software: IPSO 3.8 Build039 and Checkpoint R55 3.8 wrapper; VPN1 Pro and Policy server. See FWgw1 (above) for details.

	172.24.1.3/24 eth-s1p4 100 Mbit Full Duplex Internal_server_segment On 172.27.1.3/24 eth-s2p1 100 Mbit Full Duplex Management_segment On 10.10.1.3/24 eth-s2p2 100 Mbit Full Duplex FW_SYNC On 10.10.10.2 VRRP: External 1 100 2 192.168.1.4 Internet_segment 2 100 2 192.168.1.65 Internal_LAN 3 100 2 172.24.1.1 Internal_server_segment 4 100 2 172.27.1.1 Management_segment 4 100 2 10.10.1.1	
FW mgmt station 1 and 2 IBM X335	The 2 network connections have pared/teamed up, and nic1 is connected to switch 1 in the management segment, and NIC2 is connected to switch 2. 10.10.1.21-22/24	Software: Windows 2003 and Checkpoint R55 with Hotfix HFA 8 Smart Centre and Smart Console. There is 1 PC in the IT department that can connect to the firewall management station with Smart console.
Remote sales office router Cisco 1703 router	interface Ethernet0 ip address 192.168.5.2/30 Description: external interface Ethernet1 ip address 192.168.4.1/30 Description: internal	Software: Cisco IOS version 12.2 The Remote Sales office router has a direct Ethernet link from the ISP. Connect to the router via SSH2
Remote sales office FW	eth-s1p1 10 Mbit Half Duplex	Software: IPSO 3.8 Build039 and Checkpoint R55 3.8 wrapper; VPN1

Nokia IP120	External On 192.168.4.2/30 eth-s2p1 100 Mbit Full Duplex LAN On 172.24.2.1/24	Pro and Policy server. The Remote Sales Office fw module is managed from the GIAC Enterprise fw management server. All traffic to GIAC enterprise is encrypted In a intranet VPN tunnel, all regular internet traffic such as web goes directly through this box and the whole LAN segment is NATed behind the fw modules external IP address with Hide NAT. DHCP addresses is coming from the DHCP server scope in GIAC enterprise main site, so BOOT P relay is set on the FW, to forward the requests. All connections to the fw module are via SSH2 and SSL for voyager with the use of RSA tokens.

Table 2

1.2.2 Other Components

Other components Includes:

- RSA SecurID ASE server with including RSA soft/hard tokens used to validate and authenticate Checkpoint SecureClient, user authentication, and login to terminal server and the remote sales router and firewall module.
- Cisco AAA server used to authenticate IT staff and control at what level they have access to network components via Tacacs+.
- SYS log server on BSD platform that collects syslog information from all network components.
- Cisco 3640 router (terminal server) with console connections to all network devises, only open for SSH2 connections.
- Clearswift MAILsweeper 4.3 cluster with a Sophos antivirus engine installed on to scan all mail in and out of GIAC Enterprise.

1.2.3 Defence-in-Depth

Many people still see a firewall as a box or a peace of hardware or software, but as I see it, a firewall is a concept, layers of security, like defence in depth, a collection of protection methods protecting the “crown jewels” of the company. I have seen it being compared to an onion with layers, where each layer represent a layer of protection, like a firewall box and router ACL for perimeter protection like the outer shell of the onion, and anti virus, host based firewall software and so on for inner layers. And for the hart

of the onion is patching and applying hot fixes and keeping software appliances and applications up to date.

Assignment 2 - Security Policy and Component Configuration

2 GIAC enterprise border routers

Following is the general security setup and ACL's for the GIAC Enterprise routers. The main security policy is in the Nokia IP 1220 Check Point Cluster, the routers ACL's are designed to protect the routers and only take the worst of passing traffic so we can monitor and get the most of the traffic on the Nokia IP 350 ISS RealSecuce 7.0 network sensors before it hits the fw cluster modules and compare it to traffic seen on the IDS censors on the inside of the cluster, and visa versa, and learn from that, and use the knowledge to adjust the security policies on the fw cluster and on the IDS.

2.1.1 GIAC Enterprise routers general security setup

This is the general security setup for the 3 GIAC enterprise border routers, "!" marks description:

```
Current configuration:
no service pad
! Describtion: don't allow pad  service
service tcp-keepalives-in
! Describtion: generates keepalive packets on idle incoming network connections
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
! Description: Time-stamp debugging and log with date and time, milliseconds and
! timezone
No service password-encryption
! Description: -is less secure, Ciscos advice is to use enable secret instead
service internal
! Desciption: Allows more debugging and commands
logging buffered 64000 debugging
! Description: 64kb buffer for debugging messages
logging console notifications
! Description: Level 5 tty (console) syslog messages
aaa new-model
! Description: enable access control via Cisco AAA server
aaa authentication fail-message ^CLogin incorrect^C
! Description: login failure banner message
aaa authentication username-prompt "login: "
! Description: displays "login:" in username prompt
aaa authentication login default tacacs+ line
! Desciption: login method is tacacs+
```

```
aaa authentication enable default enable
! Desciption: determines if a user can access privileged command level
aaa accounting exec default start-stop tacacs+
! Description: specifies accounting information for user exec on terminal sessions and
! Sends a start accounting notice at the beginning of the process and a stop at the end
aaa accounting commands 0 default start-stop tacacs+
aaa accounting commands 1 default start-stop tacacs+
aaa accounting commands 2 default start-stop tacacs+
aaa accounting commands 3 default start-stop tacacs+
aaa accounting commands 4 default start-stop tacacs+
aaa accounting commands 5 default start-stop tacacs+
aaa accounting commands 6 default start-stop tacacs+
aaa accounting commands 7 default start-stop tacacs+
aaa accounting commands 8 default start-stop tacacs+
aaa accounting commands 9 default start-stop tacacs+
aaa accounting commands 10 default start-stop tacacs+
aaa accounting commands 11 default start-stop tacacs+
aaa accounting commands 12 default start-stop tacacs+
aaa accounting commands 13 default start-stop tacacs+
aaa accounting commands 14 default start-stop tacacs+
aaa accounting commands 15 default start-stop tacacs+
! Description: accounting information is captured for user exec modes at indicated privilege
! level 1-15
aaa accounting system default start-stop tacacs+
! Description: to receive session termination after reboots
enable secret 5 $1$QABb$FtNMEC.o5/qDLb7l9ylEV
! Description: MD5 hash of enable password
clock timezone MET 1
! Description: timezone
clock summer-time MET-DST recurring last Sun Mar 2:00 last Sun Oct 2:00
! Description: specifies summer time
ip subnet-zero
! Description: enables subnet zeros to be configured on the router
no ip source-route
! Description: discards packets that can’t specify route
ip cef
! Description: Cisco Express Forwarding remembers the result of a lookup in the routing
! table in memory
no ip bootp server
! Description: disable bootp server
no cdp run
! Description: disable Cisco discovery protocol
no ip classless
! Description: no classless routing
no ip http server
! Description: shutdown routers web server
logging facility local0
! Description: enable logging
```

```
logging 10.10.1.11
! Description: logging to syslogserver
logging source interface fastethernet0/0
! Description: send logging from internal interface
tacacs-server host 10.10.1.12 key $1$QABb$FtNMEC.o5/qDLb7l9ylEV
! Description: Cisco AAA server key
line con 0
 no exec
 exec-timeout 5 0
 transport input none
! Description: line con 0 is connected to the terminal server
line aux 0
exec-timeout 0 1
login local
no exec
! Description: service is disabled
 line vty 0 4
 access-class 10 in
! Desciption: line vty 04/telnet disabled on the GIAC Enterprise border GW routers, ACL
! used for the remote sales office router
ntp clock-period 17180013
! Description: compensate for error in system clock
ntp update-calendar
! Description: update calendar over network time protocol
ntp server 172.27.1.5 version 1
ntp server 192.168.1.68 version 1
! Description: NTP servers
end
```

2.1.2 GIAC Enterprise router ACL's

Following is the router ACL's:

ACL on external interfaces marked "in" on interface:

```
ip access-list extended Ingress-filter

 deny ip  10.0.0.0 0.255.255.255 any log
 deny ip  172.16.0.0 0.15.255.255 any log
 deny ip  192.168.0.0 0.0.255.255 any log
! Description: block private RFC 1918 addresses
 deny ip  127.0.0.0 0.255.255.255 any log
 deny ip  0.0.0.0 0.255.255.255 any log
 deny ip  host 255.255.255.255 any log
! Description: block loopback and broadcast addresses
 deny ip  169.254.0.0 0.0.255.255 any log
! Description: deny end node autoconfig
 deny ip  192.0.2.0 0.0.0.255 any log
! Description: deny test-net
```

```
 deny ip  224.0.0.0 15.255.255.255 any log
! Description: deny class D (multicast)
 deny ip  240.0.0.0 7.255.255.255 any log
! Description: deny class E (reserved for future use)
 deny ip  248.0.0.0 7.255.255.255 any log
! Description: deny net 248-255
 deny ip 192.168.1.0 0.0.0.129
! Description: deny internal ip range incoming on external interface (192.168.4.0 .0.0.0.3
! for remote sales office)
 deny   tcp any any eq 23 log
! Description: deny telnet
 deny   tcp any any eq 135 log
 deny   udp any any eq 135 log
! Description: Block NetBIOS (TCP and UDP 135)
 deny   udp any any eq 137
! Description: Block NetBIOS (UDP 137) - Don't log
 deny   udp any any eq 138 log
! Description: Block NetBIOS (UDP 138)
 deny   tcp any any eq 139 log
! Description: Block NetBIOS (TCP 139)
 deny   tcp any any eq 445 log
 deny   udp any any eq 445 log
! Description: Block NetBIOS for Windows 2000 (TCP and UDP 445)
 deny   tcp any any eq 111 log
 deny   udp any any eq 111 log
! Description: Block portmap/rpcbind (TCP and UDP 111)
 deny   tcp any any eq 2049 log
 deny   udp any any eq 2049 log
! Description: Block NFS (TCP and UDP 2049)
 deny 53 any any log
 deny 55 any any log
 deny 77 any any log
 deny 103 any any log
! Description: Cisco vulnerability
permit ip any any
! Description: permit every port and every one else.
```

ACL on internal interfaces on the GIAC Enterprise border gw routers, marked “in” on interface:

ip access-list standard egress-antispoof:

```
 deny   tcp any any eq 22 log
! Description: deny ssh
 deny   tcp any any eq 23 log
! Description: deny telnet
 deny   tcp any any eq 135 log
 deny   udp any any eq 135 log
```

```
! Description: Block NetBIOS (TCP and UDP 135)
 deny   udp any any eq 137
! Description: Block NetBIOS (UDP 137) - Don't log
 deny   udp any any eq 138 log
! Description: Block NetBIOS (UDP 138)
 deny   tcp any any eq 139 log
! Description: Block NetBIOS (TCP 139)
 deny   tcp any any eq 445 log
 deny   udp any any eq 445 log
! Description: Block NetBIOS for Windows 2000 (TCP and UDP 445)
 deny   tcp any any eq 111 log
 deny   udp any any eq 111 log
! Description: Block portmap/rpcbind (TCP and UDP 111)
 deny   tcp any any eq 2049 log
 deny   udp any any eq 2049 log
! Description: Block NFS (TCP and UDP 2049)
 permit 192.168.1.0 0.0.0.129
 permit  10.10.1.0 0.0.0.255
! Description: allow internal address range in on internal interface (192.168.4.0 0.0.0.3
! for remote sales office)
 deny   any log
! Description: deny all other ip addresses and log them.
```

ACL on line vty 0 4 (Telnet)

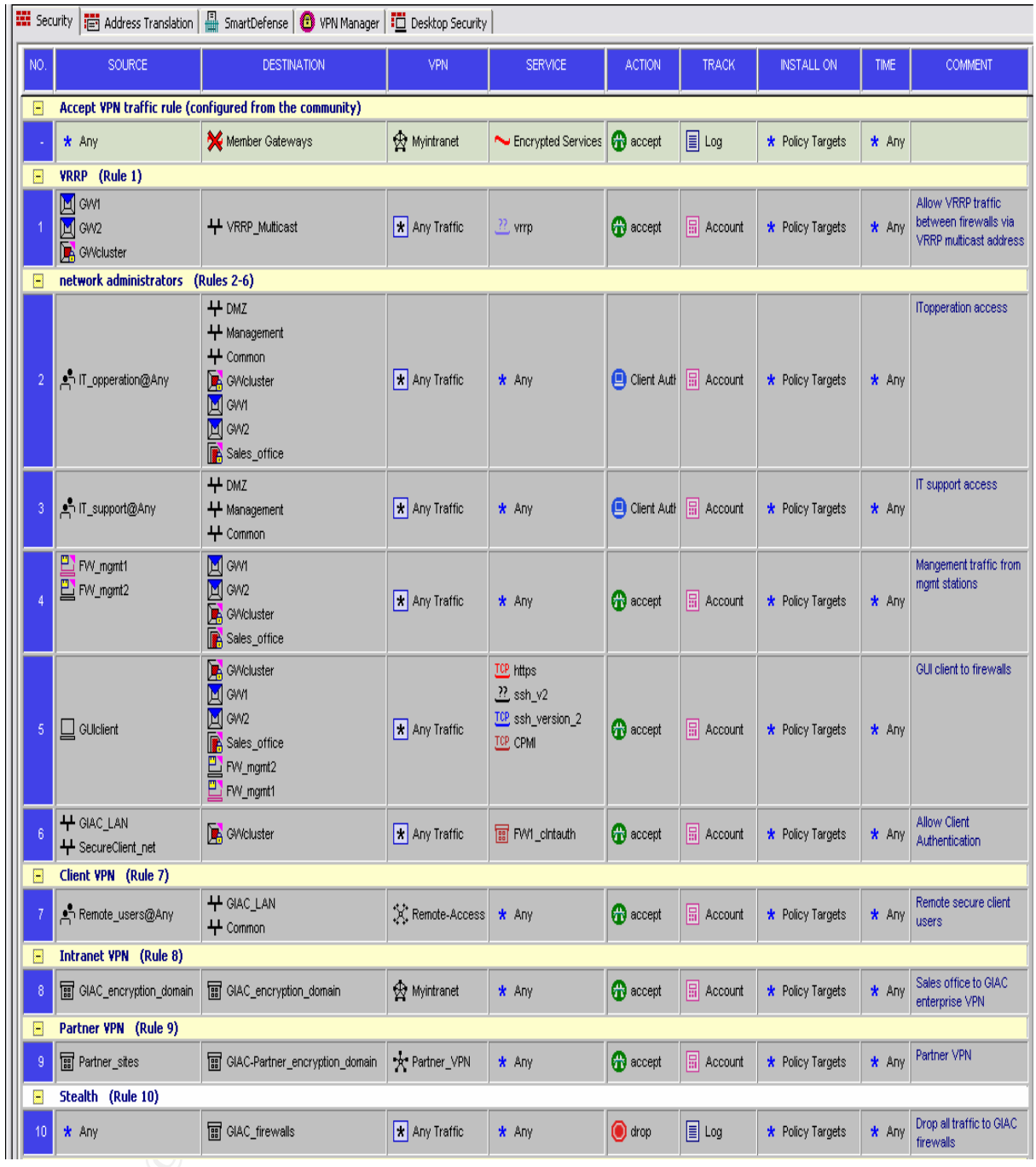
```
 access-list 10 deny any log
! Description: deny all access via telnet (access-list 10 permit 192.168.4.0 0.0.0.3 for
! remote sales office) and log.
```

2.2 GIAC Enterprise Nokia Checkpoint Firewall boxes

Following is the Security policy, NAT policy, and VPN´s, on the GIAC Enterprise fw gw cluster and on the remote sales firewall box, the main policy enforcers.

2.2.1 Security policy

This is the GIAC Enterprise Checkpoint security policy:



Security | Address Translation | SmartDefense | VPN Manager | Desktop Security

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Accept VPN traffic rule (configured from the community)								
-	* Any	Member Gateways	Myintranet	Encrypted Services	accept	Log	* Policy Targets	* Any	
	VRRP (Rule 1)								
1	GW1 GW2 GWcluster	VRRP_Multicast	* Any Traffic	vrrp	accept	Account	* Policy Targets	* Any	Allow VRRP traffic between firewalls via VRRP multicast address
	network administrators (Rules 2-6)								
2	IT_opperation@Any	DMZ Management Common GWcluster GW1 GW2 Sales_office	* Any Traffic	* Any	Client Auth	Account	* Policy Targets	* Any	ITopperation access
3	IT_support@Any	DMZ Management Common	* Any Traffic	* Any	Client Auth	Account	* Policy Targets	* Any	IT support access
4	FW_mgmt1 FW_mgmt2	GW1 GW2 GWcluster Sales_office	* Any Traffic	* Any	accept	Account	* Policy Targets	* Any	Mangement traffic from mgmt stations
5	GUIclient	GWcluster GW1 GW2 Sales_office FW_mgmt2 FW_mgmt1	* Any Traffic	TCP https ssh_v2 TCP ssh_version_2 TCP CPMI	accept	Account	* Policy Targets	* Any	GUI client to firewalls
6	GIAC_LAN SecureClient_net	GWcluster	* Any Traffic	FW1_clntauth	accept	Account	* Policy Targets	* Any	Allow Client Authentication
	Client VPN (Rule 7)								
7	Remote_users@Any	GIAC_LAN Common	Remote-Access	* Any	accept	Account	* Policy Targets	* Any	Remote secure client users
	Intranet VPN (Rule 8)								
8	GIAC_encryption_domain	GIAC_encryption_domain	Myintranet	* Any	accept	Account	* Policy Targets	* Any	Sales office to GIAC enterprise VPN
	Partner VPN (Rule 9)								
9	Partner_sites	GIAC-Partner_encryption_domain	Partner_VPN	* Any	accept	Account	* Policy Targets	* Any	Partner VPN
	Stealth (Rule 10)								
10	* Any	GIAC_firewalls	* Any Traffic	* Any	drop	Log	* Policy Targets	* Any	Drop all traffic to GIAC firewalls

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Network mangament and services (Rules 11-14)								
11	Network_devises	SYSlogserver	Any Traffic	UDP syslog	accept	Account	Policy Targets	Any	Network devises to syslog server
12	Network_devises	CiscoAAA	Any Traffic	TCP TACACSplus	accept	Account	Policy Targets	Any	Network devises to AAA server
13	CiscoAAA	ASE_server	Any Traffic	securid UDP RADIUS	accept	Account	Policy Targets	Any	AAAserver traffic to ASE server
14	Management	Internal_DNS-DHCP-NTP_server	Any Traffic	ntp dns	accept	Account	Policy Targets	Any	Management net to DNS, NTP.
	Suppliers (Rule 15)								
15	Suppliers	SSH2_server	Any Traffic	ssh_v2 TCP ssh_version_2	accept	Account	Policy Targets	Any	Supplier to ssh2 server
	WEB (Rule 16)								
16	Any	WEB_cluster	Any Traffic	TCP http TCP https	accept	Account	Policy Targets	Any	Traffic to web servers
	DMZ (Rules 17-20)								
17	Any	Mailcluster	Any Traffic	smtp->MAILsweepe	accept	Account	Policy Targets	Any	SMTP traffic to mailcluster via MAILsweeper
18	Mailcluster	Any	Any Traffic	smtp->MAILsweepe	accept	Account	Policy Targets	Any	SMTP traffic from mailcluster via MAILsweeper
19	Any	External_DNS-NTP_server	Any Traffic	dns ntp	accept	Account	Policy Targets	Any	Traffic to external DNS/NTP server
20	External_DNS-NTP_server	Any	Any Traffic	dns ntp	accept	Account	Policy Targets	Any	Traffic from external DNS/NTP server
	Common servers (Rule 21)								
21	BACKUPserver	DMZ Management	Any Traffic	Any	accept	Account	Policy Targets	Any	Backupserver
	Internal super users (Rule 22)								
22	SuperUsers@Any	WEB1 WEB2 WEB3 DBserver SSH2_server	Any Traffic	Any	Client Auth	Account	Policy Targets	Any	Superusers to DMZ
	Internal users (Rules 23-25)								
23	Sales_office_LAN GIAC_LAN	Any	Any Traffic	Illigal_services	drop	Log	Policy Targets	Any	Block unwanted services out
24	GIAC_LAN	Common	Any Traffic	Any	accept	Account	Policy Targets	Any	Accept traffic from GIAC LAN to common net
25	GIAC_LAN Sales_office_LAN	GIAC_NET	Any Traffic	Any	accept	Account	Policy Targets	Any	GIAC lan to internet
	Drop (Rule 26)								
26	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clean up rule - block all other connections

Table 3 (Checkpoint console)

Comments:
All accept/authentication rules are accounted, and all drop rules are logged.

Rule 0: automatic generated VPN rule (Implied rule) when My intranet VPN was made.

Rule 1: allow VRRP (IP protocol 112) traffic from fw gw´s to VRRP multicast net 224.0.0.18

Rule 2: allow Client authentication for IT operation team to fw gw´s and to protected networks. All users in the IT operation user group authenticate with RSA soft/hard token via SecurID ASE server.

Rule 3: allow client authentication for IT support team to protected networks. All users int it support user group authenticate with RSA soft/hard token via SecurID ASE server.

Rule 4: allow all traffic from the 2 fw mgmt stations to all the fw modules.

Rule 5: allow SSH2, SSL, and Checkpoint mgmt interface (TCP port 18190) from GUI station to fw mgmt servers and to fw modules.

Rule 6: allow client authentication (telnet port 259, and http port 900) from GIAC enterprise LAN and Secure Client net to fw gw cluster.

Rule 7: allow remote users (SecureClient users) to GIAC Enterprise encryption domain via Remote Access community.

Rule 8: allow all encrypted traffic from GIAC Enterprise main site encryption domain to Remote sales office encryption domain and visa versa via meshed VPN community.

Rule 9: allow encrypted traffic from partner sites to GIAC Enterprise encryption domain via star community VPN domain.

Rule 10: deny everything to GIAC Enterprise fw gw modules.

Rule 11: allow syslog (UDP port 514) traffic from all network devises to syslog server.

Rule 12: allow tacacs+ (TCP port 49) traffic from all network devises to AAA server.

Rule 13: allow securID service (securidprop tcp port 5510, securid –udp udp port 5500, radius udp 1645) from Cisco AAA server to SecurID ASE server.

Rule 14: allow NTP and DNS service (UDP and TCP port 123 and 53) from management net to internal DNS/NTP server.

Rule 15: allow suppliers IP addresses to access the SSH 2 servers with SSH2 protocol.

Rule 16: allow anyone to connect to the logical web object (web cluster) with http and SSL.

Rule 17-18: Allow SMTP traffic with resource via CVP server – Clearswift MAILsweeper in and out of GIAC Enterprise mail cluster.
Rule 19-20: allow NTP and DNS traffic in and out of external DNS/NTP server.

Rule 21: allow any traffic from GIAC backup server to DMZ and mgmt net.

Rule 22: allow any traffic to web servers, DB server and SSH2 server with client authentication from super users witch authenticate with RSA Seruid tokens on ASE server.

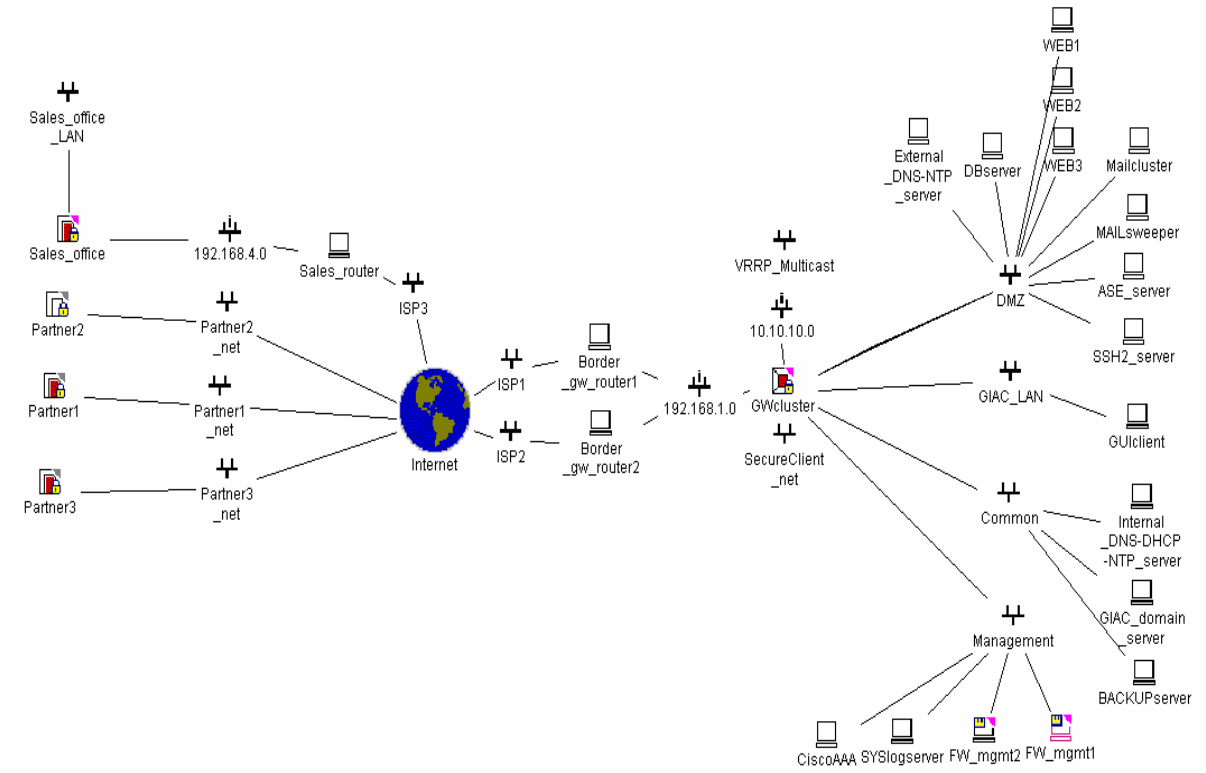
Rule 23: deny unwanted traffic from internal LANs (traffic that's illegal according to GIAC Enterprise security policy, traffic like: peer2peer, eDonkey, GNUtella, ident, KazaA, MSN, Napster……new ports and protocols will be added continuously.

Rule 24: allow all traffic from GIAC LAN to common net/common server and services.

Rule 25: allow Internal LANs to the internet, all GIAC nets have been negated.

Rule 26: Drop everything (for log purposes).

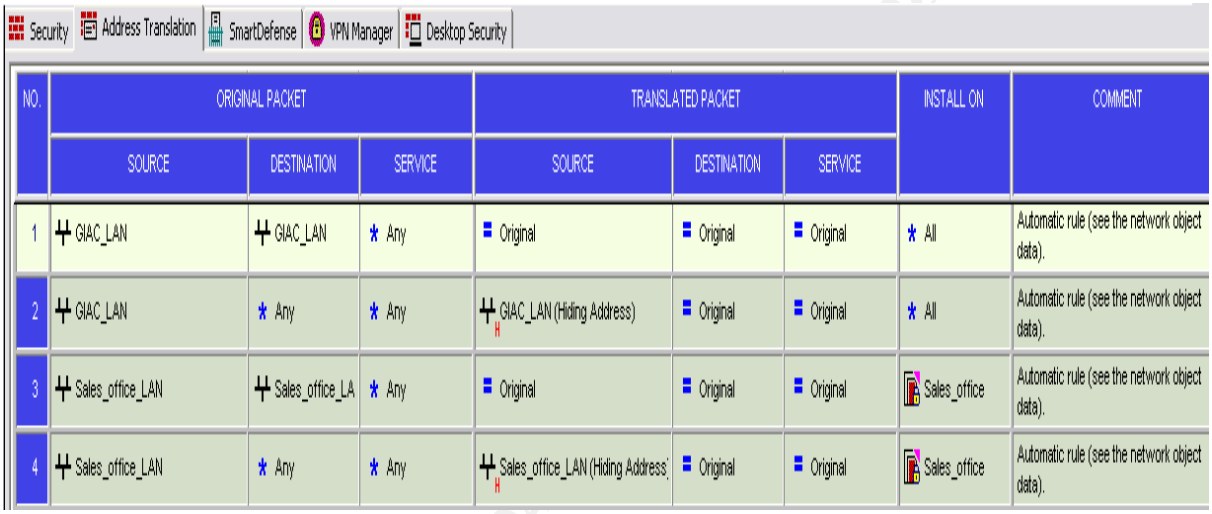
Network seen form Checkpoint point of view:



Drawing 2 (Checkpoint management console)

2.2.2 NAT table

This is the NAT table as seen on the Check Point mgmt station, rule 1-2 are the rules for hiding the GIAC LAN behind NAT address. Rule 3 and 4 are the rules for hiding the Remote sales office LAN behind the FW GW module external interface address. We have found and seen some peculiar behaviour concerning the automatic NAT rules witch is used here, so they will be changes to manual configured NAT rules instead in the near future.



NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	GIAC_LAN	GIAC_LAN	Any	Original	Original	Original	All	Automatic rule (see the network object data).
2	GIAC_LAN	Any	Any	GIAC_LAN (Hiding Address)	Original	Original	All	Automatic rule (see the network object data).
3	Sales_office_LAN	Sales_office_LA	Any	Original	Original	Original	Sales_office	Automatic rule (see the network object data).
4	Sales_office_LAN	Any	Any	Sales_office_LAN (Hiding Address)	Original	Original	Sales_office	Automatic rule (see the network object data).

Table 4 (Checkpoint management console)

2.2.3 Smart defence

Smart defence is enabled for active network defence against DOS attacks, IP/ICMP sanity, TCP verifier and Fingerprint scrabbling. Application intelligence protects HTTP protocol, scripting on web servers, SMTP protocol, FTP protocol and file sharing, enforce DNS UDP.

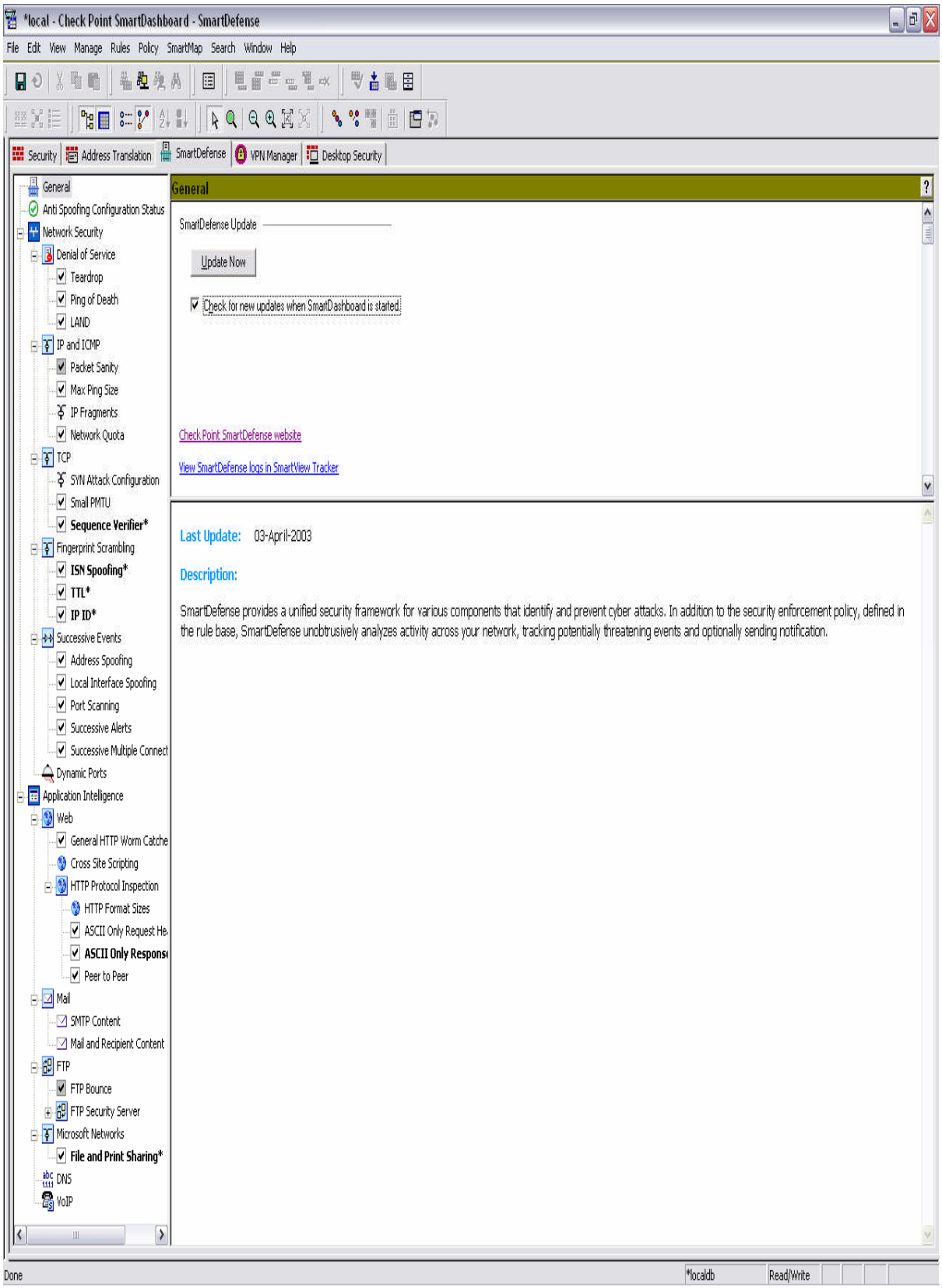


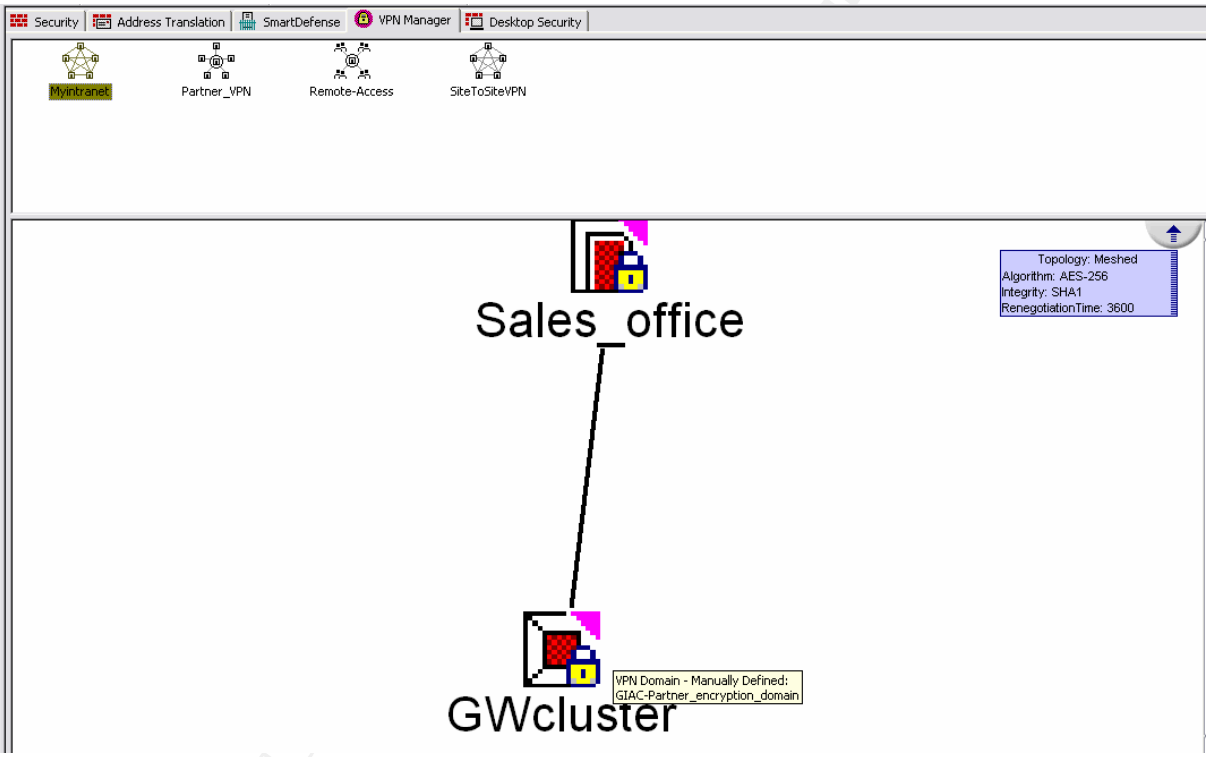
Table 5 (Checkpoint management console)

2.2.4 VPN configurations

We have 2 different types of site-to-site VPN´s, the intranet VPN that's fully meshed, even though there are only 2 sites in the VPN domain now, but as mentioned earlier, new remote sales offices are on the way. And the partner VPN that is set up like a hub-and-spoke where the satellite offices can connect to the main site but not with each other.

2.2.4.1 Intranet VPN

The intranet VPN is setup as certificate VPN, a certificate is configured on each of the participating gw´s. Also on each gw object in the Checkpoint management console is configured the encryption domains, the network(s) inside the GWs witch should be included in the VPN tunnel.



Drawing 3 (Checkpoint management console)

Accept all encrypted traffic, and no excluded services:

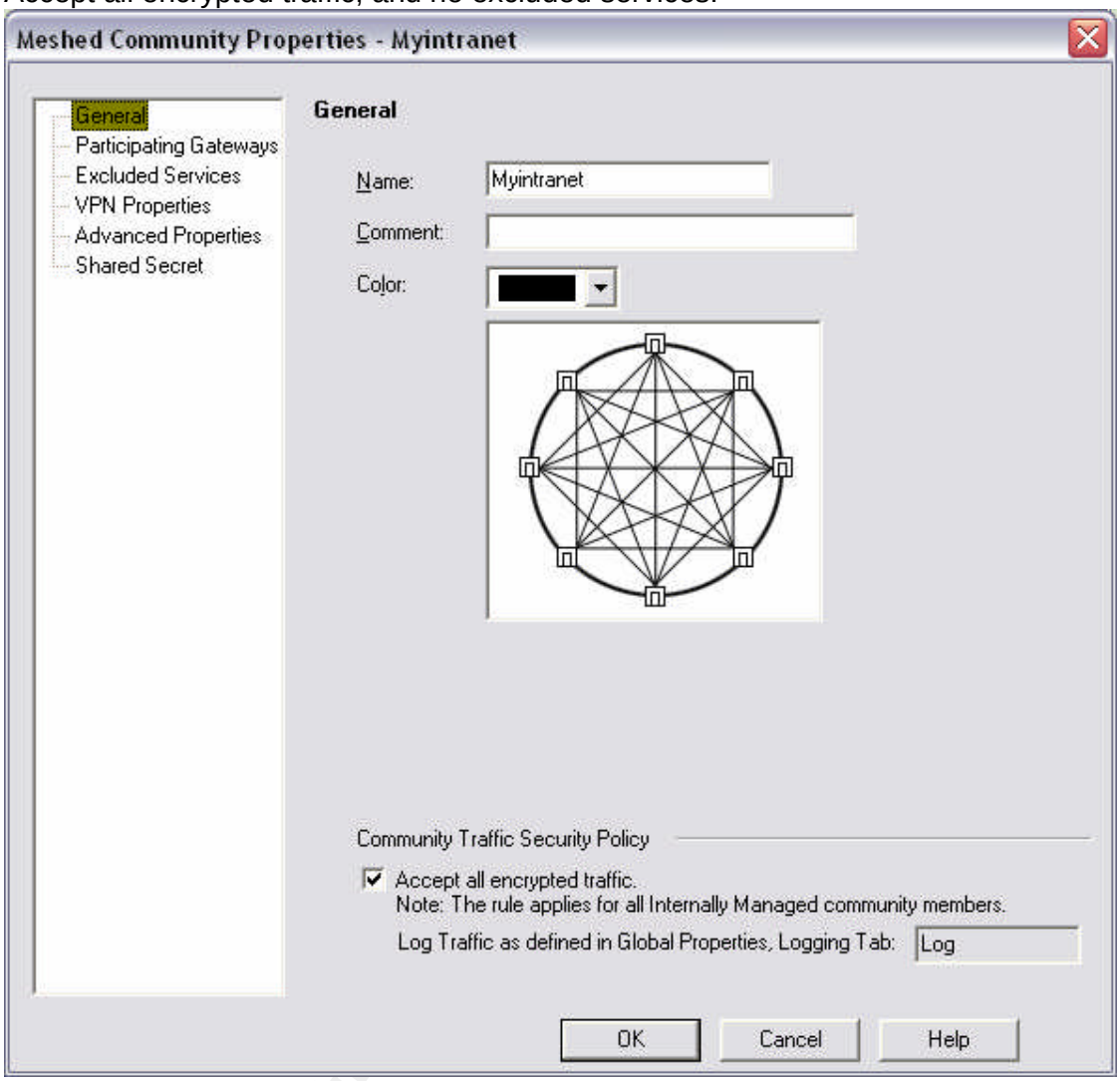


Table 6 (Checkpoint management console)

Participating GW´s is the remote sales office fw module and the GIAC Enterprise module.

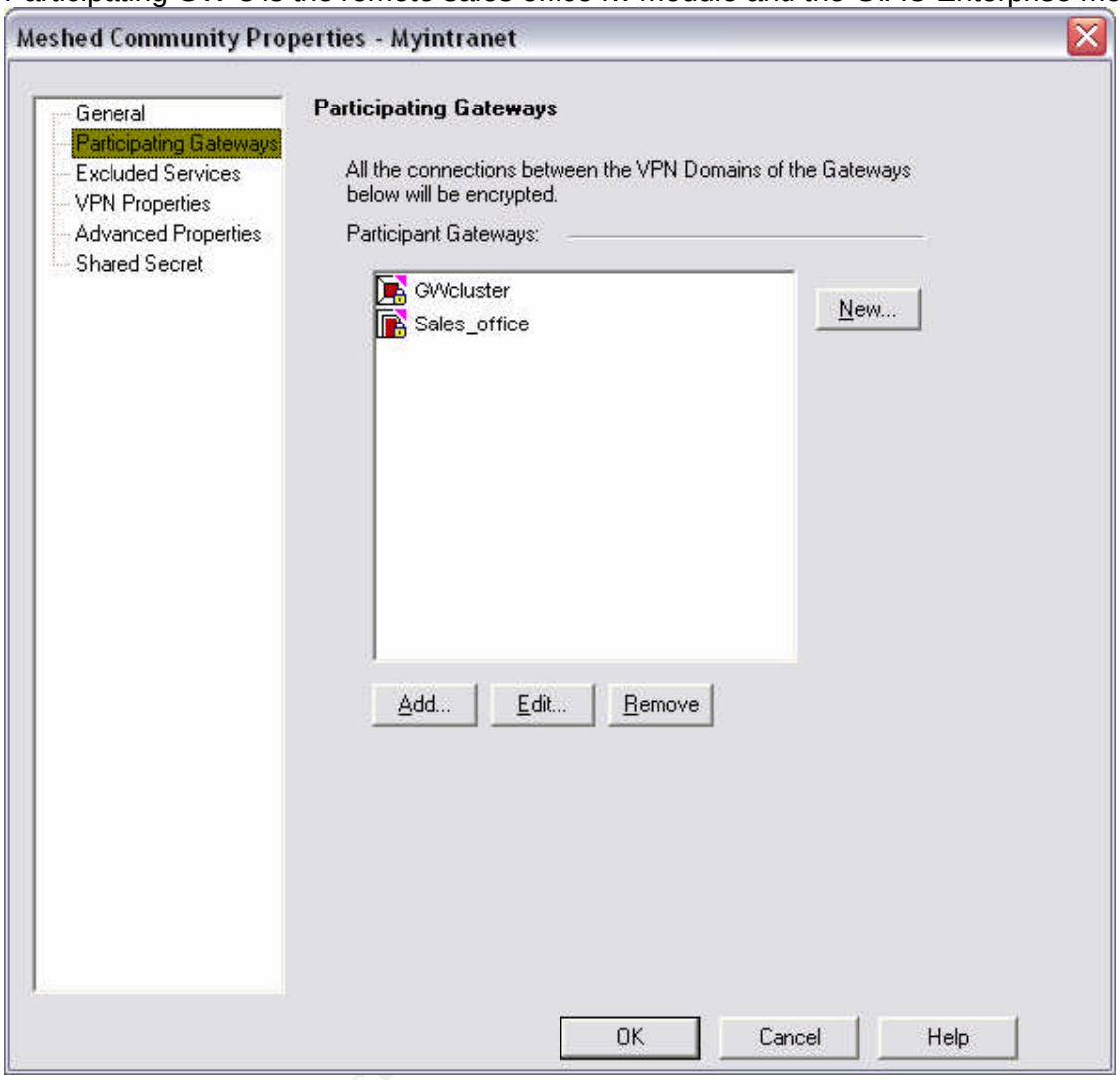


Table 7 (Checkpoint management console)

VPN properties include AES-256 SHA1 for phase 1, and the same strong encryption for phase 2:

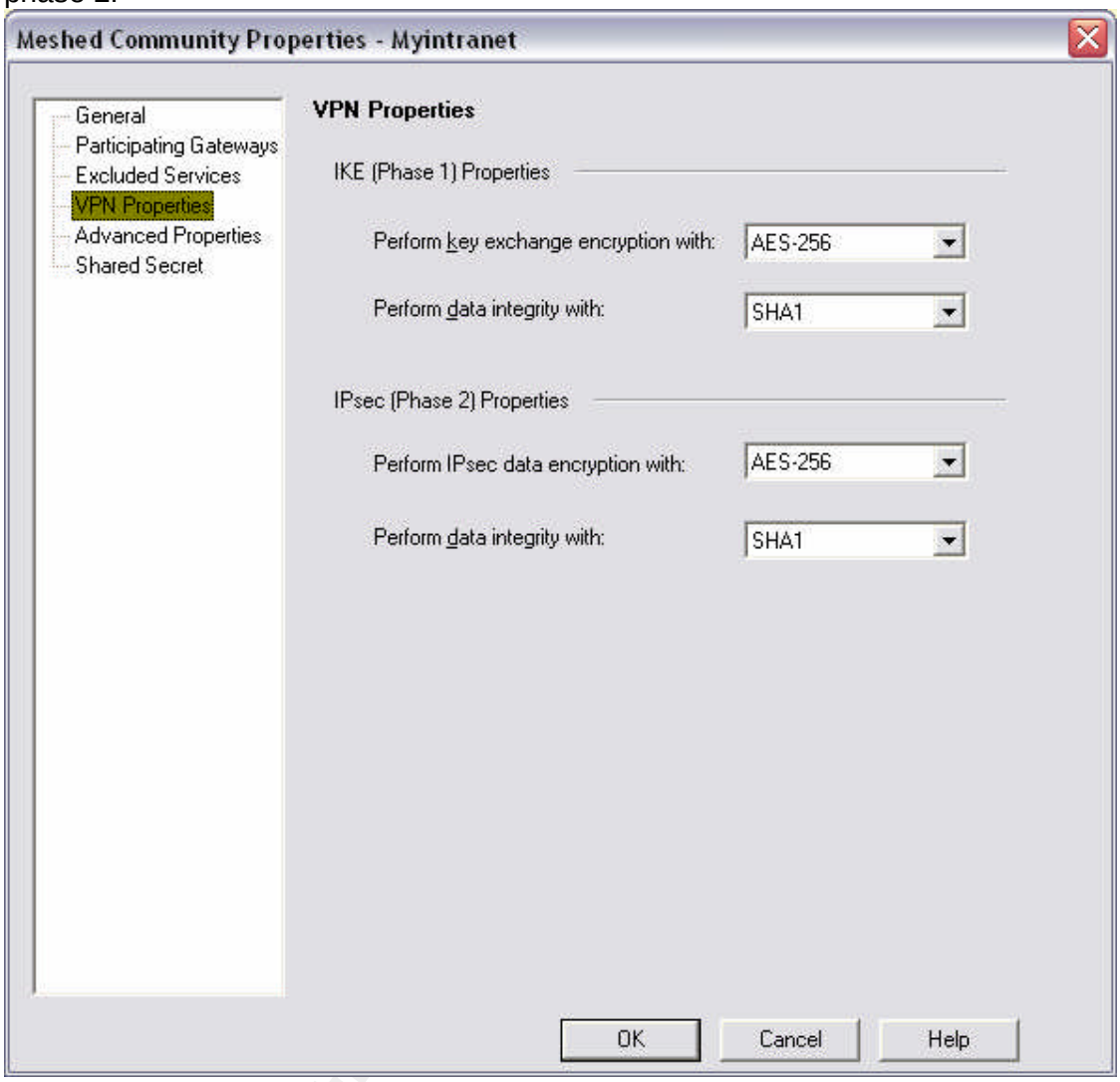


Table 8 (Checkpoint management console)

Advance properties, includes phase 1 aggressive mode to negotiate IKE with 3 packets instead of 6 turned off, and perfect forward secrecy on phase 2 turned on, using the strong Diffie-Hellman encryption scheme. The DIffie-Hellman group 2 1024 bit encryption has been chosen. NAT is disabled inside VPN domain:

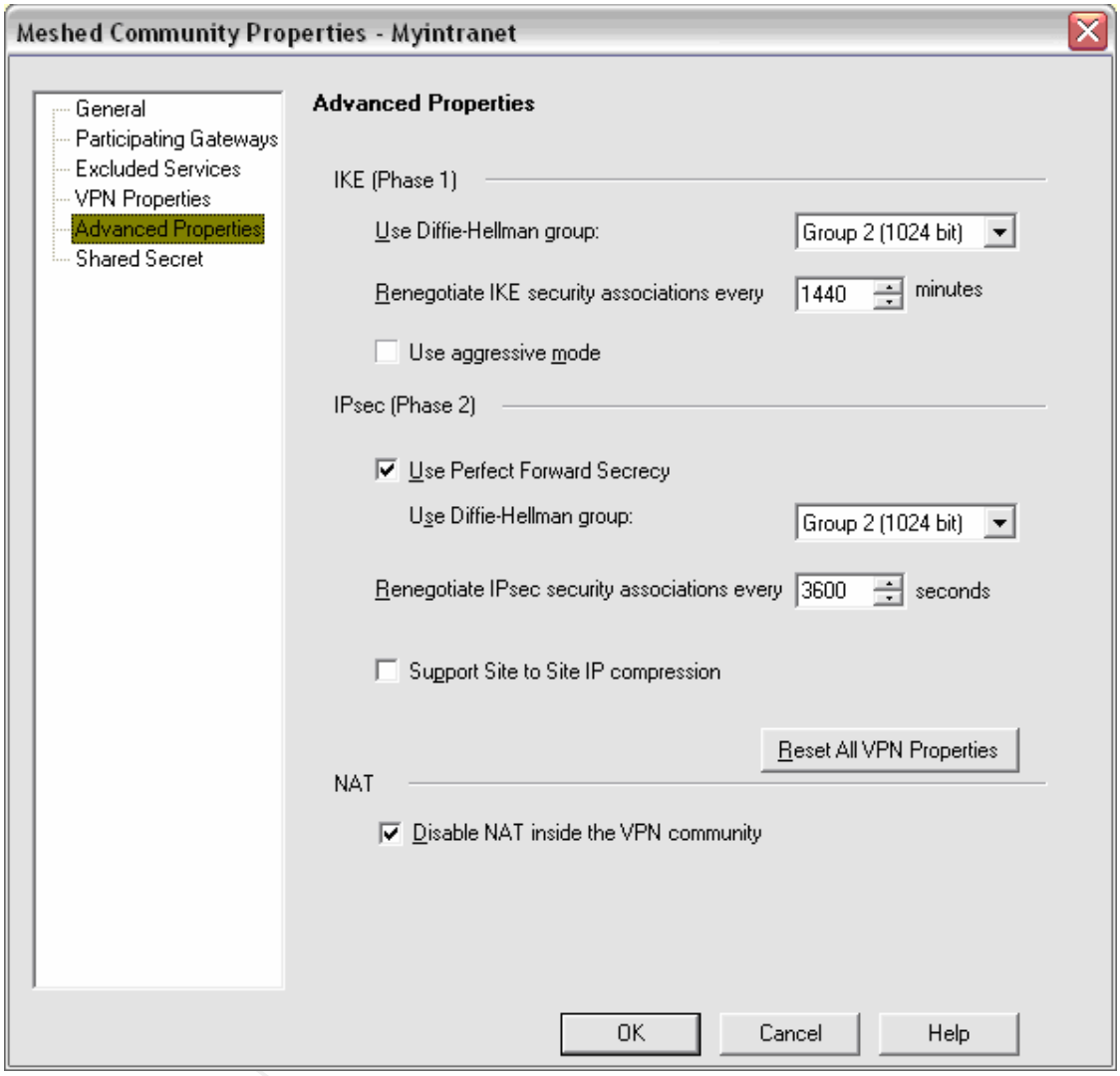
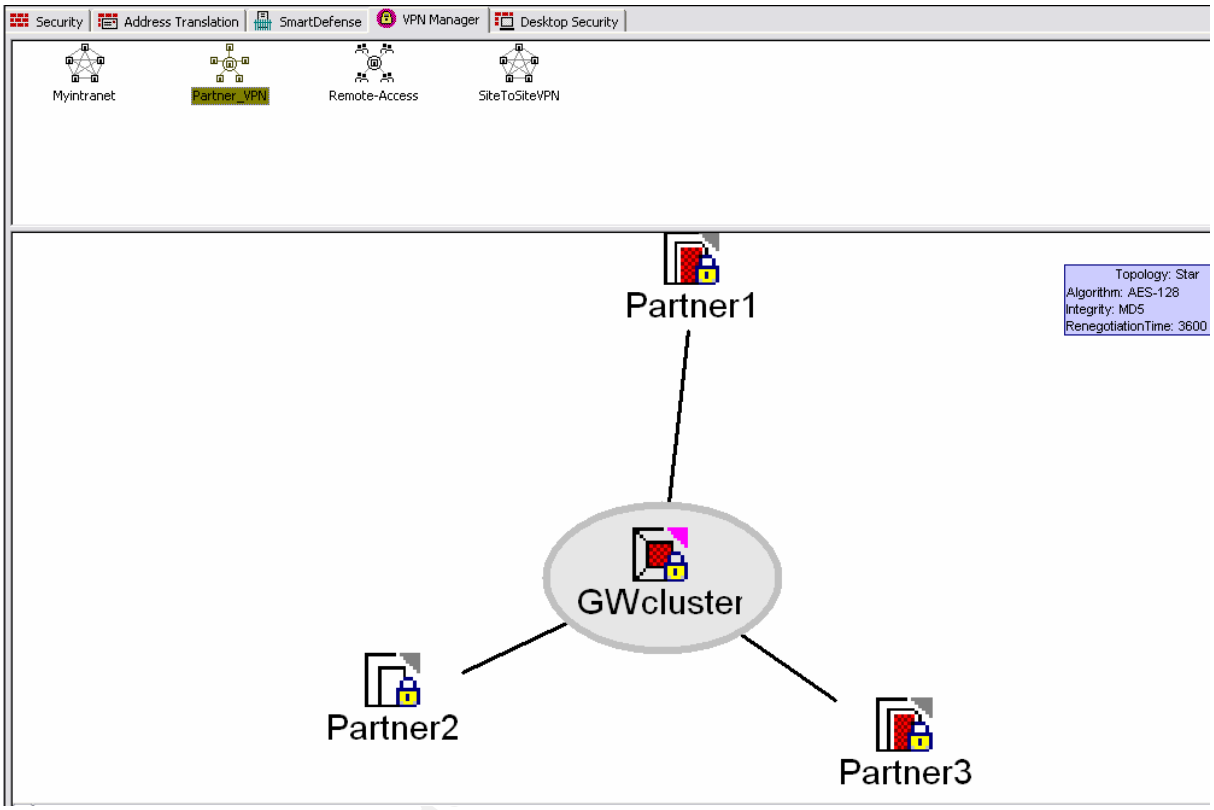


Table 9 (Checkpoint management console)

2.2.4.2 Partner VPN

The Partner VPN´s is also based on certificates, but is setup as a star VPN configuration. Each gw object in the Checkpoint management console is defined as a externally managed object. Encryption domains has been setup on the modules:



Drawing 4 (Checkpoint management console)

The Central gw of the hub and spoke VPN is the GIAC Enterprise gw cluster:

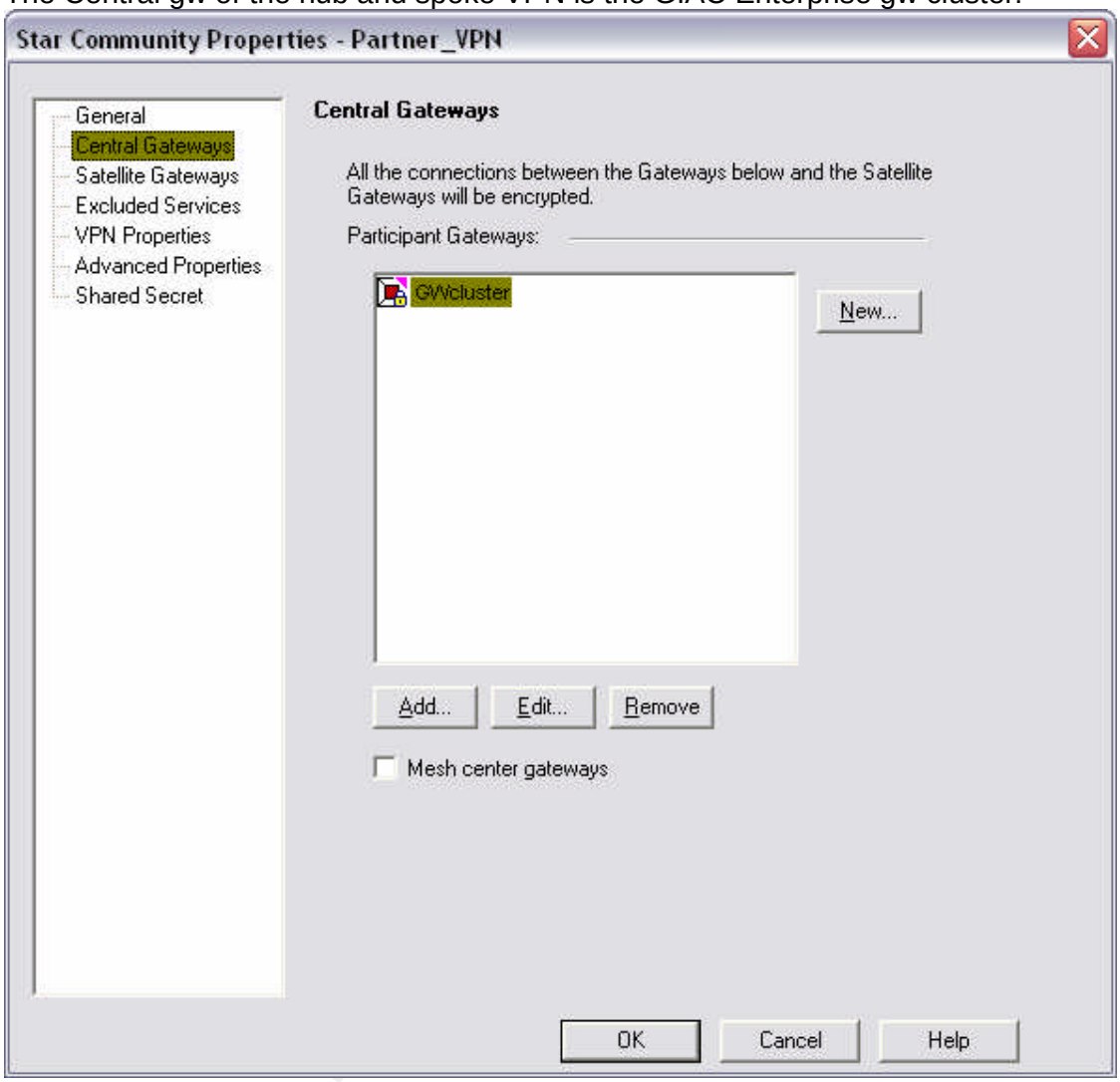


Table 10 (Checkpoint management console)

The 3 satellite partner GW´s:

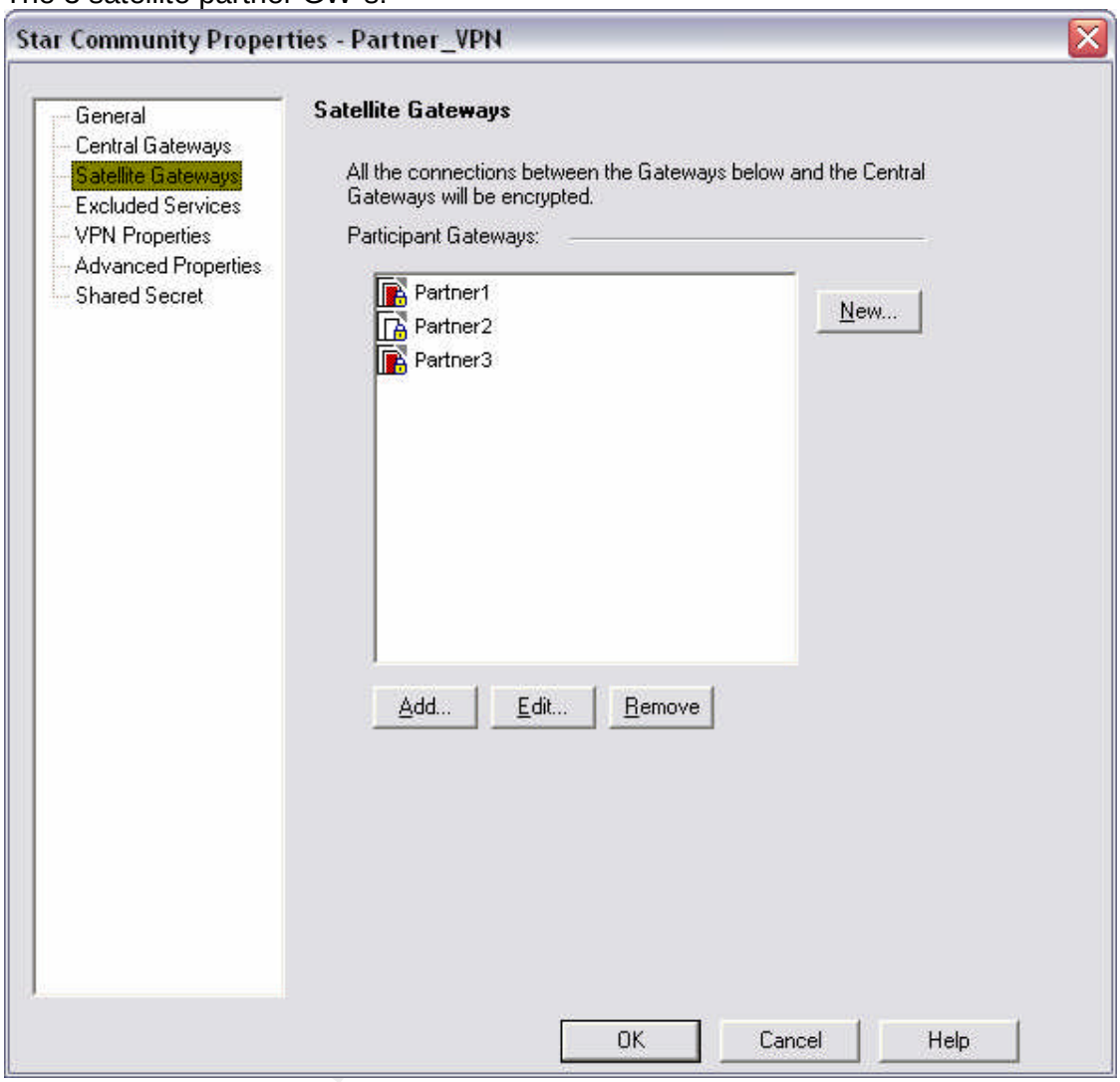


Table 11 (Checkpoint management console)

Excluded services that we don't want to pass through the VPN tunnels from our partners and in to GIAC Enterprise LAN:

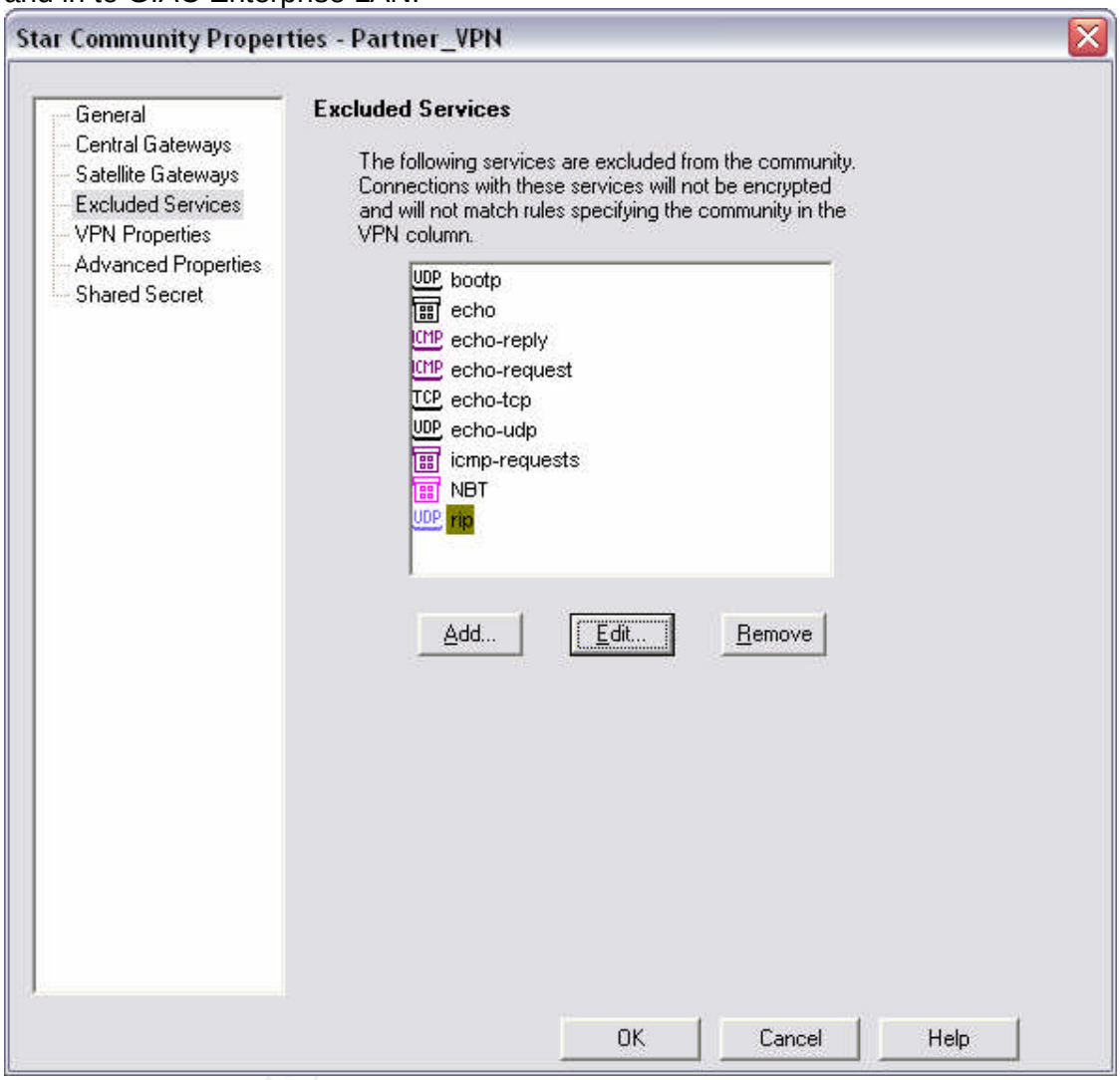


Table 12 (Checkpoint management console)

Phase 2 is set to AES-128 and MD5, this is the minimum specs for partner VPN according to GIAC Enterprise security policy, because its difficult to set hardware/software standards for a partner companies, and you cant dictate how they set up their GW´s, so that's why the minimum specs were made.

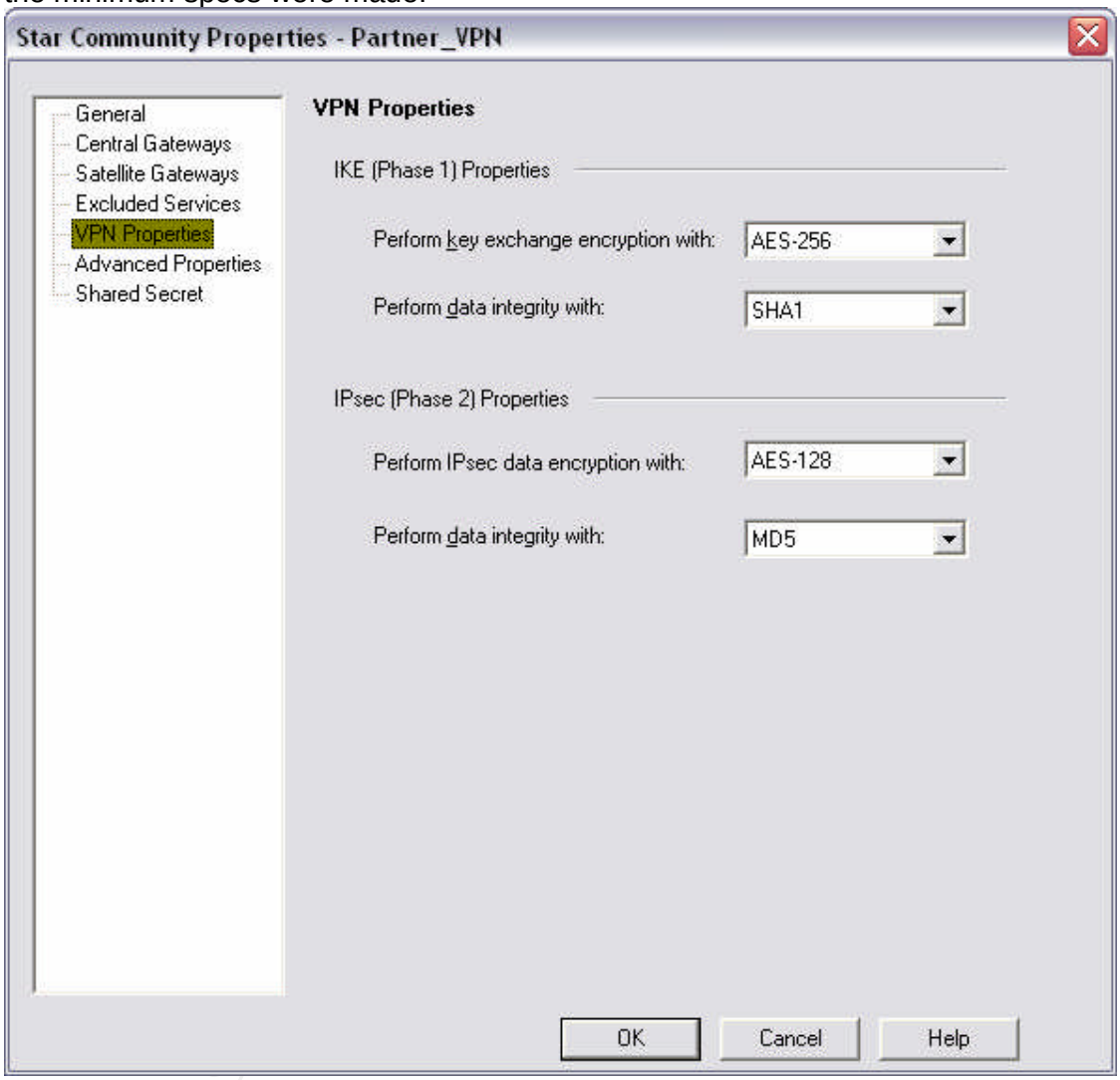


Table 13 (Checkpoint management console)

Again we see no aggressive mode and no perfect forward secrecy due to that we don't know what partners are capable of in terms of hardware/software.

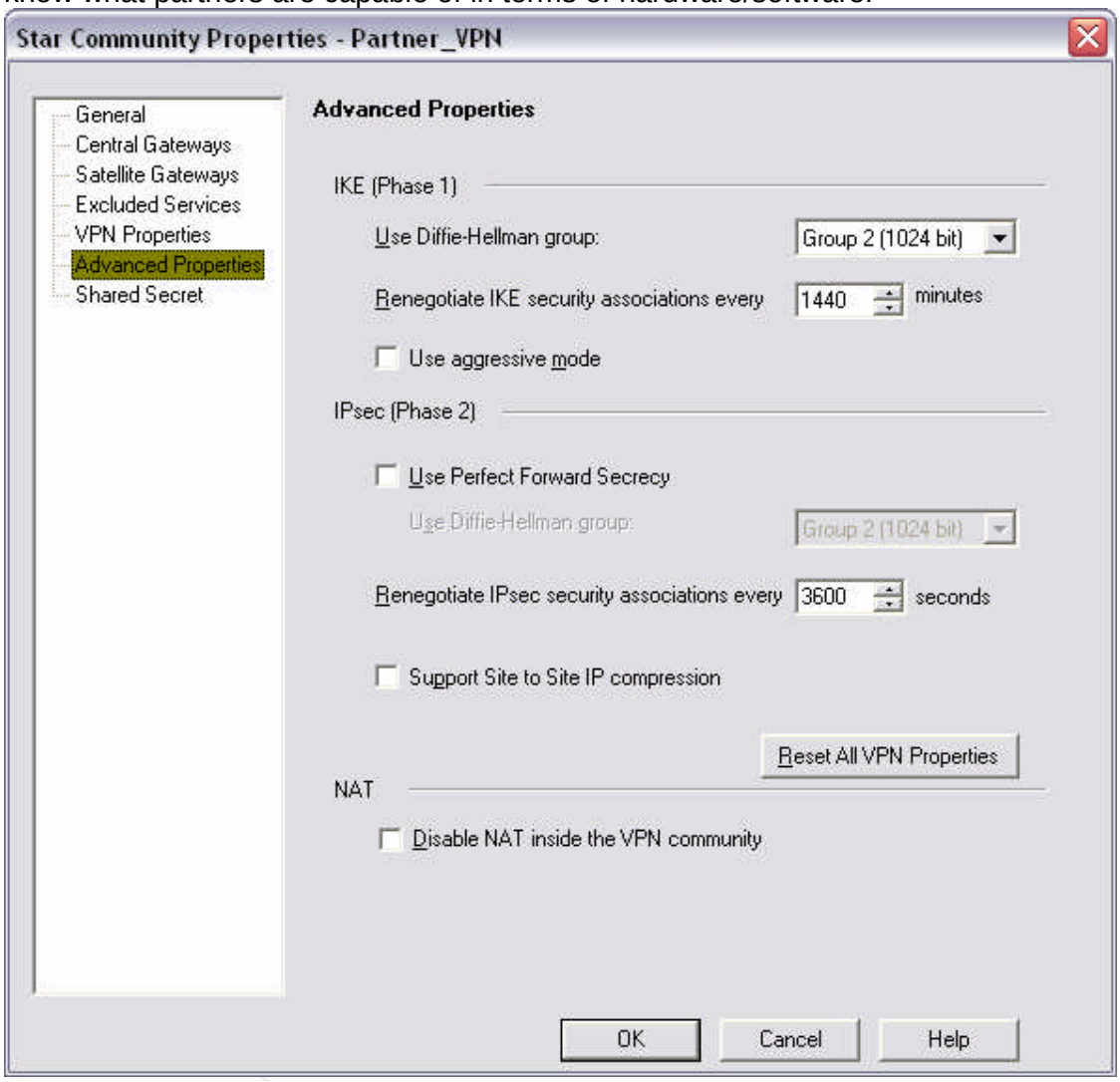
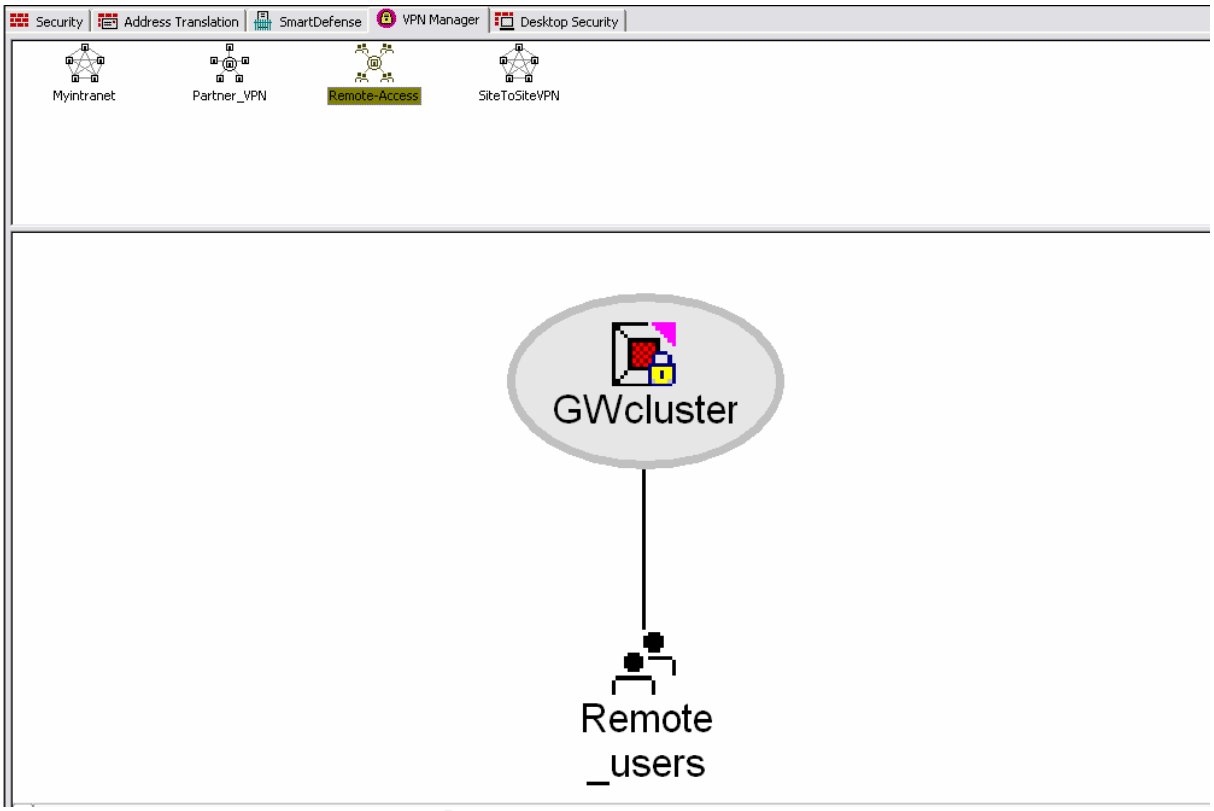


Table 14 (Checkpoint management console)

2.2.5 Secure Client configuration

All secure client users authenticate via soft/hard SecurID tokens via ASE server.

Remote users/Secure Client users all terminate in the GIAC Enterprise cluster policy server.



Drawing 5 (Checkpoint management console)

Desktop security policy:
Rule 1: Block all connections to user's laptop.
Rule 2: allow encrypted traffic to GIAC Enterprise encryption domain.
Rule 3: Block all other traffic.

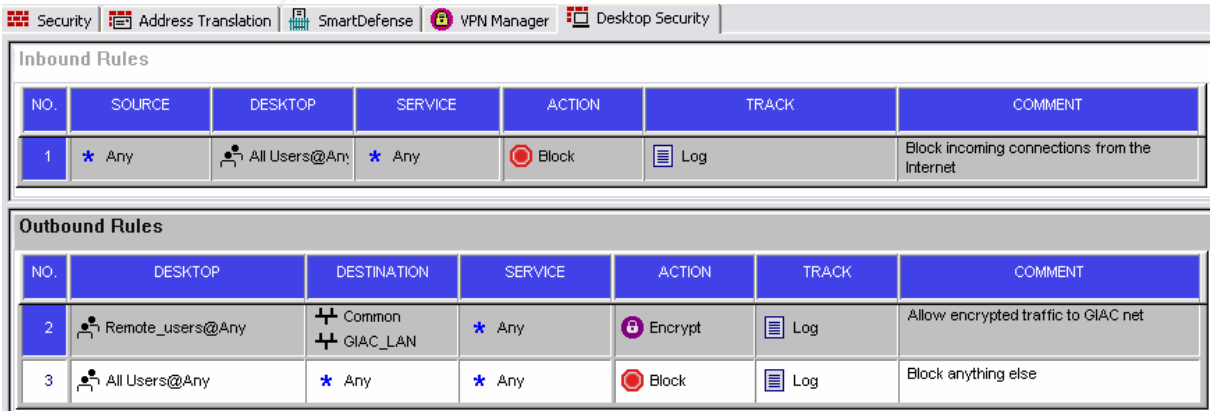


Table 15 (Checkpoint management console)

Remote access properties on the GW cluster UDP NAT traversal enabled, while Visitor mode is disabled:

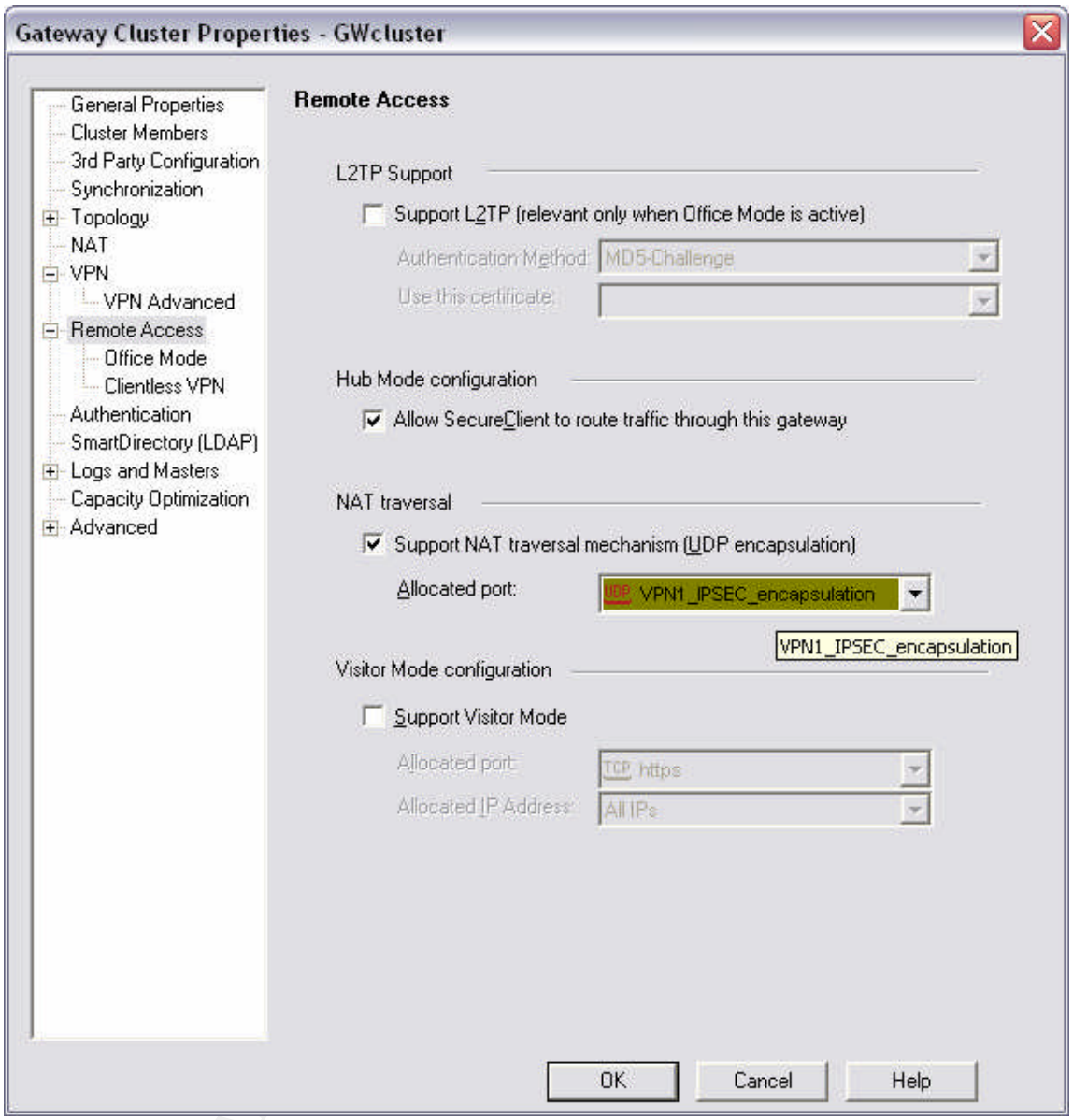


Table 16 (Checkpoint management console)

Allow office mode to all users, and let the internal DHCP server handle the DHCP scope for Secure Client users. Anti-spoofing turned on for office mode addresses and the DHCP server has been given a virtual IP address in the secure client IP scope, the DHCP lease duration is set to 15 min.:

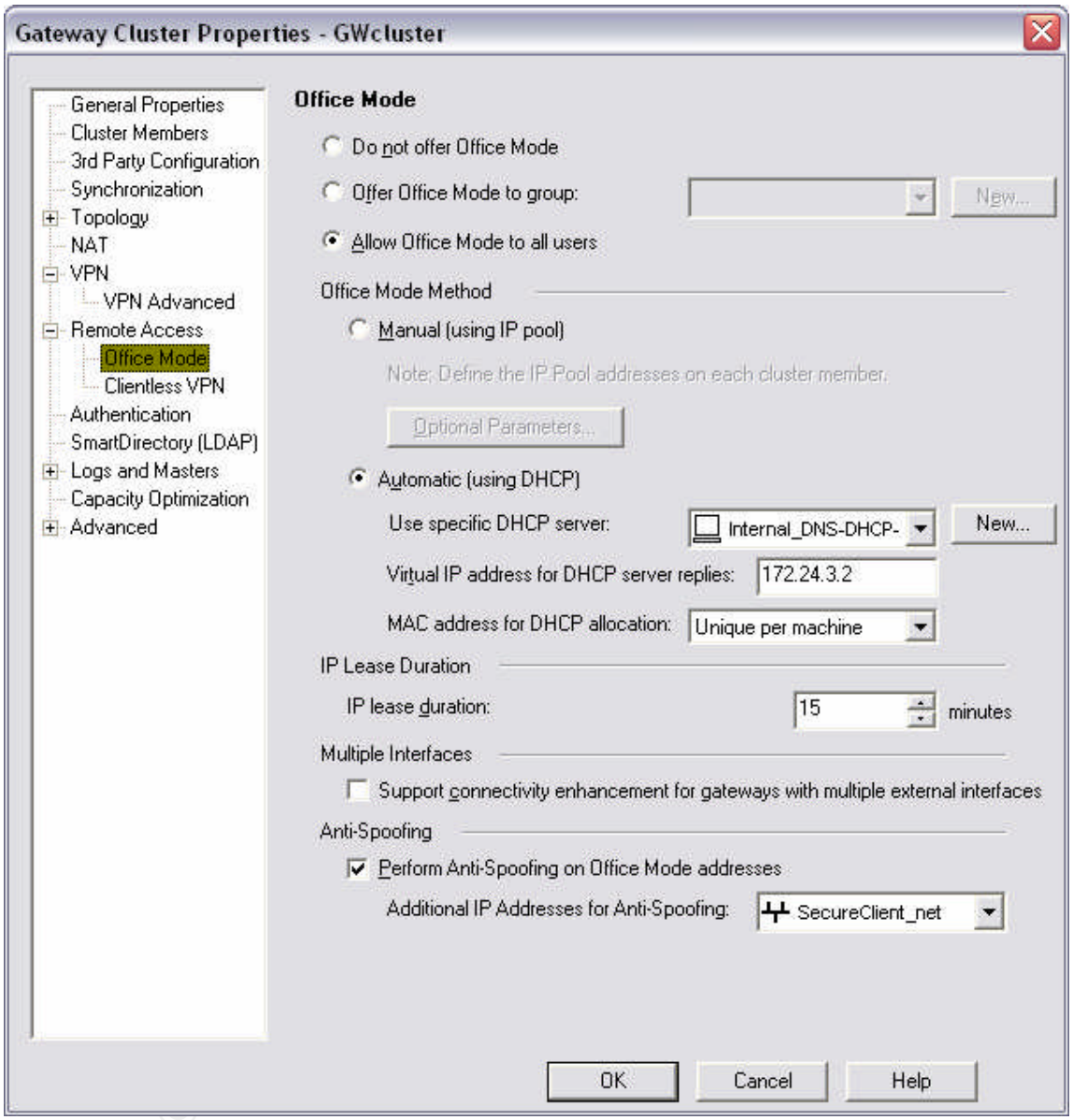
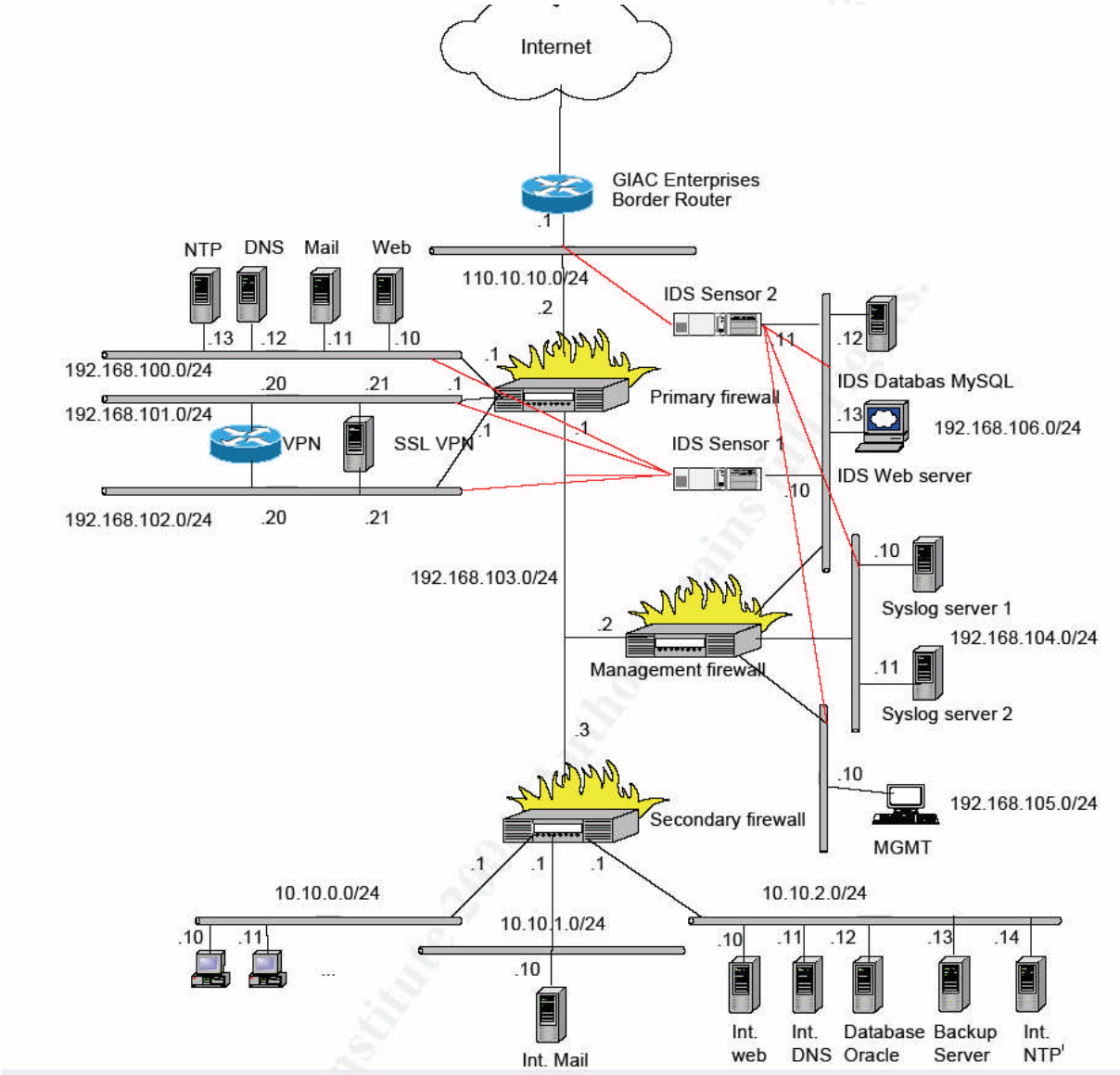


Table 17 (Checkpoint management console)

Assignment 3 - Design under fire

3 Network diagram

Jasmir Beciragic practical from June 24th 2004 was chosen for this assignment:



Drawing 6 (Jasmir_Beciragis_GCFW.pdf)

3.1 Performing reconnaissance

The goal here is to gather as much information about the site we want to attack. We will try to gather enough information about GIAC Enterprise network to scan the net, compromise an internal system, and gain access to the web server since this it's the crown jewels of GIAC Enterprise whose core business is web sales.
The only thing I know so far is that I'm going to attack a web company called GIAC Enterprise, so what can we do…?
Visit the GIAC website; gather all information about contacts, addresses, phone numbers and mail addresses.
DNS look-ups on all possible FQDN resemblance i.e. www.giac.com-net-* , and gather all IP addresses. Visit www.ripe.net and www.internic.net use their whois databases and gather all information. Social engineering would be worth trying, calling the sales office, they are always willing to talk, maybe set up a fake sales meeting concerning a purchase of large amount of bulk fortune cookies for resell, usually sales offices are always patched up so if I bring a laptop and get some fake sales slides with some unimportant figures on, tell them that I need an internet connection, hook up do a quick scan of the network with some batch files running in the background, but it must be fast, 15min. at the most, it will probably take avail for the security admins to react to the suspicious traffic patterns on their IDS sensors, and find me. We could use the efficient mapper technique to scan the network fast. Ping the broadcast address of the network to have all addresses to reply and save it to a file.
After that we could sit in the parking lot for a while trying to connect to their WLAN to see how good its protected, if its just protected by WEP, we could try to gather enough packages using Airsnort to break the key, and scan the network some more. Maybe we will find a badly configured WLAN access point put up by a regular user, and so we did, and I can even get my hands on a desktop connected to the WLAN that poped up in my windows network neighbourhood. I'm in!

3.2 Network scan

I already know some of the internal address range from "the sales meeting" and from the wlan information.

We will now try to conduct a NMAP scan from the internal desktop, first we will install NMAPNT, and then we will run it:

nmapnt -sS -P0 -v -v -O 10.10.0.0/24

-sS TCP SYN stealth port scan (best all-around TCP scan)
-P0 Don't ping hosts – to try to reduce packages.
-v Verbose. Its use is recommended. Use twice for greater effect.
-O Use TCP/IP fingerprinting to guess remote operating system

Output:
Initiating SYN half-open stealth scan against (10.10.0.0/24)
Adding TCP port xxx (state open).

Adding TCP port xxx (state open).
The SYN scan took 3600 seconds to scan 20000 ports.
For OSScan assuming that port xxx is open and port xxxx is closed and neither are firewalled
For OSScan assuming that port xxx is open and port xxxx is closed and neither are firewalled
For OSScan assuming that port xxx is open and port xxxx is closed and neither are firewalled
Interesting ports on (10.10.0.0/24):
(The 20000 ports scanned but not shown below are in state: filtered)

Port	State	Service
xxx/tcp	open	xxxx
xxx/tcp	open	xxxx
xxxx/tcp	closed	xxxx
xxx/tcp	open	xxxx
xxx/tcp	open	xxxx
xxxx/tcp	closed	xxxx
xxx/tcp	open	xxxx
xxx/tcp	open	xxxx
xxxx/tcp	closed	xxxx
xxx/tcp	open	xxxx
xxx/tcp	open	xxxx
xxxx/tcp	closed	xxxx

…..

TCP Sequence Prediction: Class=xxxx
Difficulty=xxx (Good luck!)

Sequence numbers: xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
No OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
TSeq(Class=TR)
T1(Resp=Y%DF=N%W=xxxxx%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=N%W=xxxxx%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Nmap run completed -- 256 IP address (x host up) scanned in 3600 seconds

Note: this is not the real out put of the scan, the real "simulated" scan gave more results, the out put is just to show how nmapnt output looks like, the "x"s represent numbers.

I find a number of computers amongst them some running Linux OS. I have download a program called rlogin v1.00 that I install on the machine I'm on, and try rlogin to all of them with a verity of passwords, most of the machines have rlogin turned off, but suddenly I guess right and get access via rlogin to a Linux machine. I will now use the rlogin vulnerability to become root - http://www.cert.org/advisories/CA-1997-06.html.

3.3 Compromise system

Still in the GIAC Enterprise parking lot.

I found the following script on:
http://metalab.uniten.edu.my/~uwe/resources/HOWTOs/VNC-Pusher.html

---

```
#!/bin/sh
# chkconfig: 35 77 21
# description: initiates and keeps vncserver plus reverse ssh up
# starts a new vnc when the ssh-link to the viewer is down
#  either on demand, on boot, or as cron-job, or remote ('reset')
#
# on demand: ./remterm start (stop, restart)
#
# on boot: in /etc/init.d/ respectively /etc/rc.d/init.d/
#  to be used with chkconfig
# as cron-job: add 'remterm check' as a cronjob
#  when the link to the remote user is down; either due to link
failure
#  or intentionally (remote user kills the child of sshd for that
session)
#  the associated vncserver and ssh are killed locally and
restarted
# Uwe Dippel
# udippel@uniten.edu.my
# 10-06-2003
RUNASUSER=user_on_REMOTE
VNCID=3                          # must be between 1 and 9 !!
SCREENDEFS="-depth 16 -geometry 1024x768"
REMUSER="user_on_LOCAL@host.domain.com"
SSHQ=`ps -ax | grep -m1 590$VNCID:localhost:590$VNCID \
                  | grep -v 'grep' | cut -c1-5`
VNCSERVER=/usr/bin/vncserver
SUDO=/usr/bin/sudo
SSH=/usr/bin/ssh
# source function library.
if [ -f /etc/init.d/functions ] ; then
  . /etc/init.d/functions
elif [ -f /etc/rc.d/init.d/functions ] ; then
  . /etc/rc.d/init.d/functions
```

```
else
  exit 0
fi
# Avoid using root's TMPDIR
unset TMPDIR
# Source networking configuration.
. /etc/sysconfig/network
# Check that networking is up.
[ ${NETWORKING} = "no" ] && exit 0
RETVAL=0
test -x $VNCSERVER || exit 1
test -x $SUDO      || exit 1
test -x $SSH       || exit 1
start()
{
       if [ -f /var/run/remterm.pid ] ; then
              echo "remote terminal already started" && exit 0
       fi
       action $"Starting vncserver $VNCID : \
              " $SUDO -H -u $RUNASUSER $VNCSERVER :$VNCID
$SCREENDEFS
       RETVAL=$?
       sleep 3
       echo -n "Starting revers ssh link: "
       daemon $SUDO -H -u $RUNASUSER \
              $SSH -2 -f -N -R 590$VNCID:localhost:590$VNCID
$REMUSER
       RETVAL=$?
       echo
       sleep 3
       ps -ax | grep -m1 590$VNCID:localhost:590$VNCID \
              | grep -v 'grep' | cut -c1-5 > /var/run/remterm.pid
}
stop()
{
       if [ -f /var/run/remterm.pid ] ; then
       action $"Stopping vncserver $VNCID : \
              " $SUDO -H -u $RUNASUSER $VNCSERVER -kill :$VNCID
       RETVAL=$?
       rm -rf /tmp/.X11-unix/X$VNCID
       sleep 3
       echo -n "Stopping ssh link: "
       killproc remterm
       RETVAL=$?
       echo
       sleep 3
       else
              echo "no remote terminal running !" && exit 0
       fi
```

```
}
restart()
{
	stop
	sleep 5
	start
}
check()
{
	if [ "$SSHQ" != "" ] ; then
		echo "Remote terminal running ($SSHQ)" && exit 0
else
		restart
	fi
}
# See how we were called:
case "$1" in
	start)
		start
		;;
stop)
		stop
		;;
restart)
		restart
		;;
check)
		check
		;;
*)
		echo $"Usage: $0 {start|stop|restart|check}"
		exit 1
esac
exit $?
```

What it basically does is connect to my home pc via SSH, opening a SSH tunnel, in witch we can tunnel the VNC remote terminal witch is installed on the Linux machine in server mode in a little while, and on my home PC in viewer mode.

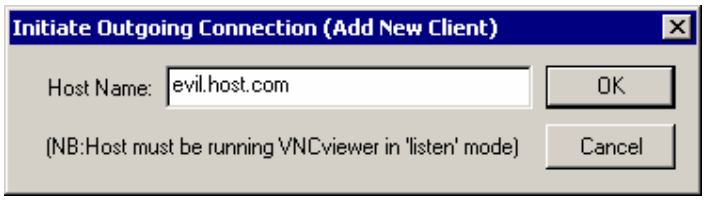
The proposed script remedies these situations:

1. The *link* can be initiated automatically
2. The script can restart **vncserver** (and the *link*) if desired
3. The *link* can be checked regularly and re-initiated automatically if need arises
4. Killing the **sshd** on LOCAL forces a restart of **vncserver**

(Taken from http://metalab.uniten.edu.my/~uwe/resources/HOWTOs/VNC-Pusher.html*)*

After that I also install Ultra VNC server on the windows desktop I´m working from (for backup)

Configure it to connect to my home PC were, as mentioned before, I have a VNCviewer in listening mode:



Drawing 7 (Ultra VNC)

After that I take of in a hurry!

3.4 Gain access to system

Now I have gained access to a system, internal Linux workstation, by compromising the rlogin and installing VNC and a little script, but that was from the inside, now I have to check if my work has paid off. I first check if the VNC from the Windows machine is connecting to my VNC viewer, its not working!!!
Then I check the SSH tunnel, and it works, fortunately, because I hadn't tested it before.

But my real goal was the web server, and the only thing I know so far is the externally IP address, and that it could be NATed. So what now, I will try a Nessus scan from the inside.

Running Nessus:
(Taken from http://www.nessus.org/demo)

1. Add user:
   nessus-adduser

Addition of a new nessusd user

Login : admin
   Authentication (pass/cert) [pass] : pass
   Password : password

   User rules
   ----
   nessusd has a rules system which allows you to restrict the hosts
   that admin has the right to test. For instance, you may want
   him to be able to scan his own host only.

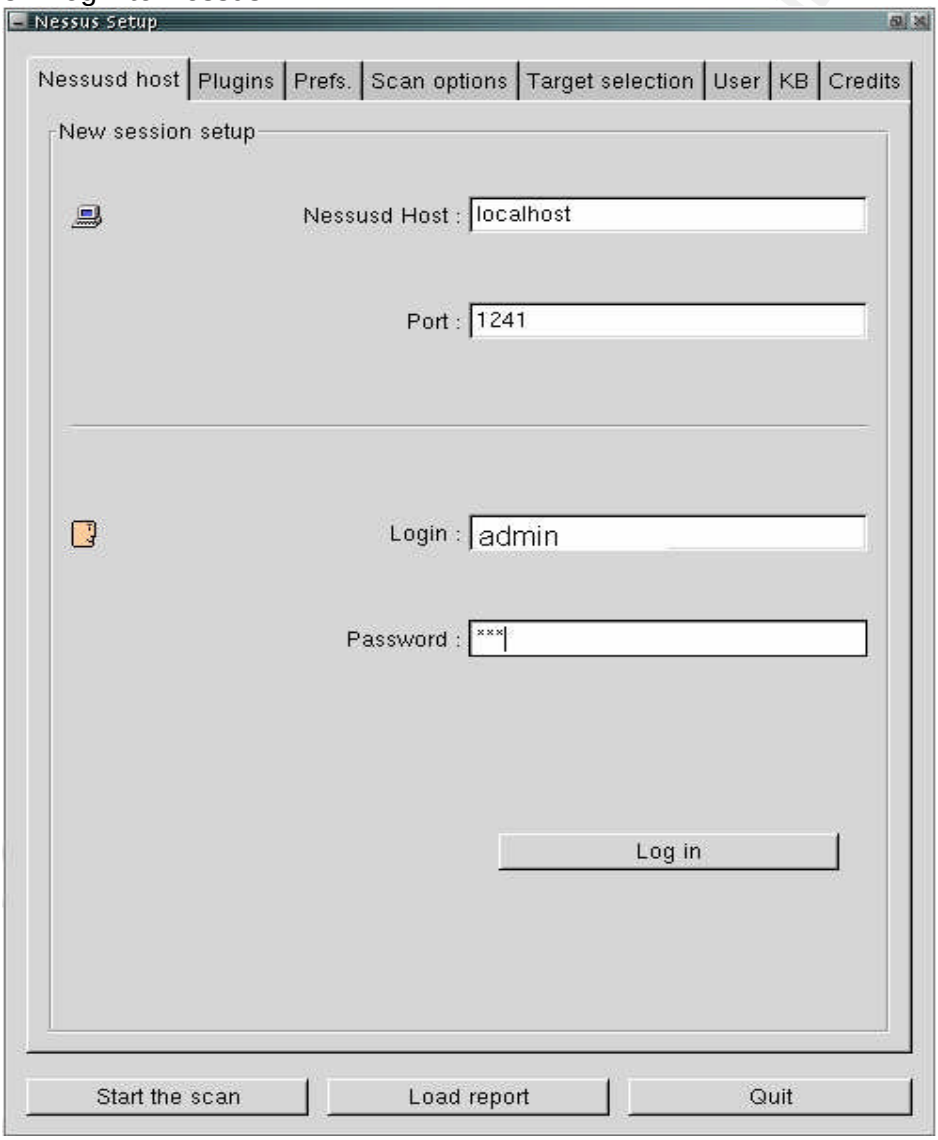
   Please see the nessus-adduser(8) man page for the rules syntax

   Enter the rules for this user, and hit ctrl-D once you are done :
   (the user can have an empty rules set)

Login : admin
Password: password
DN :
Rules :
accept my IP
default deny
Is that ok (y/n) ? [y] y
user added.

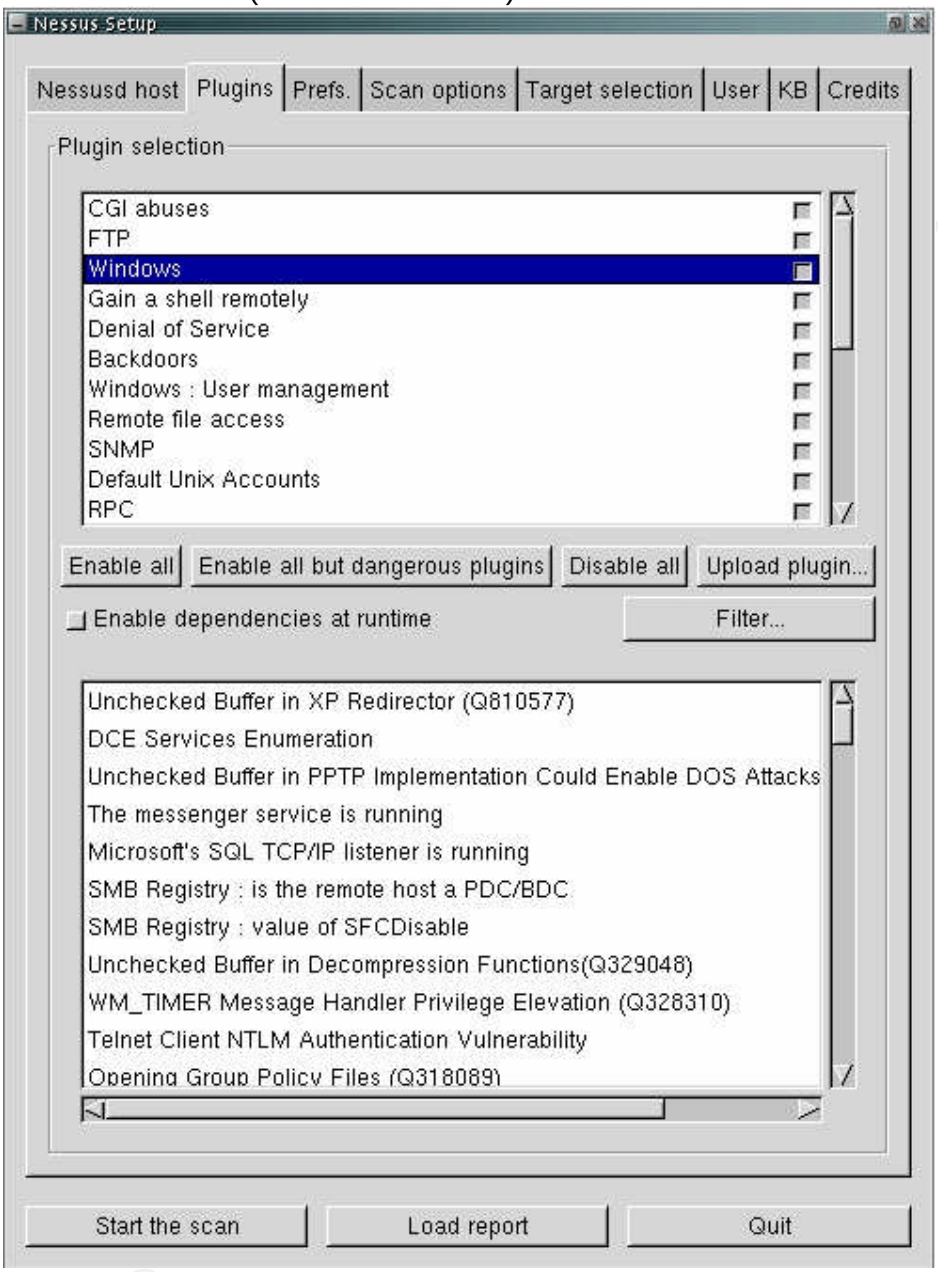
2. Start Nessus:
   nessusd -D

3. Log into Nessus:



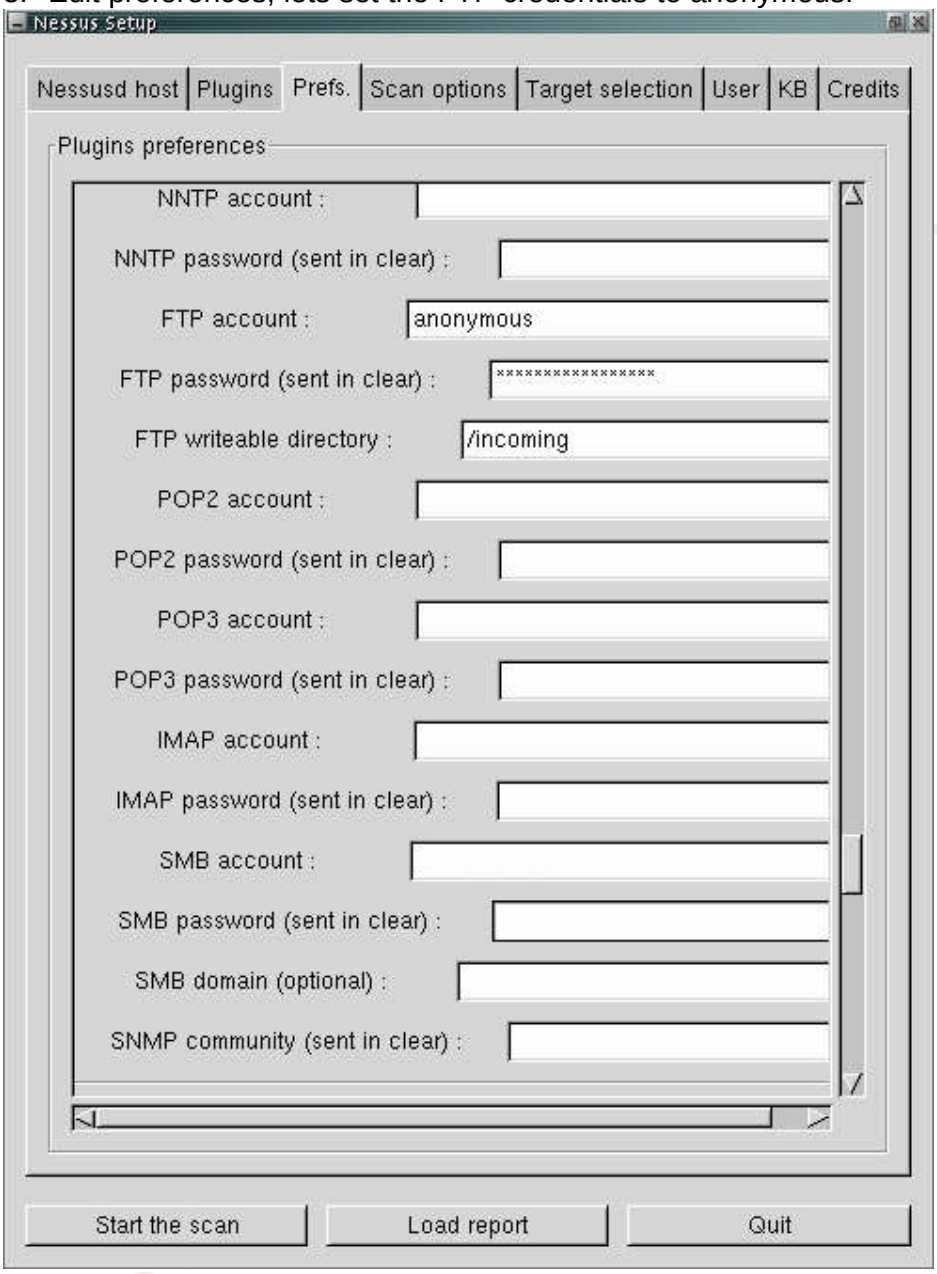
Drawing 8 (Nessus)

4. Select Checks (lets check them all)



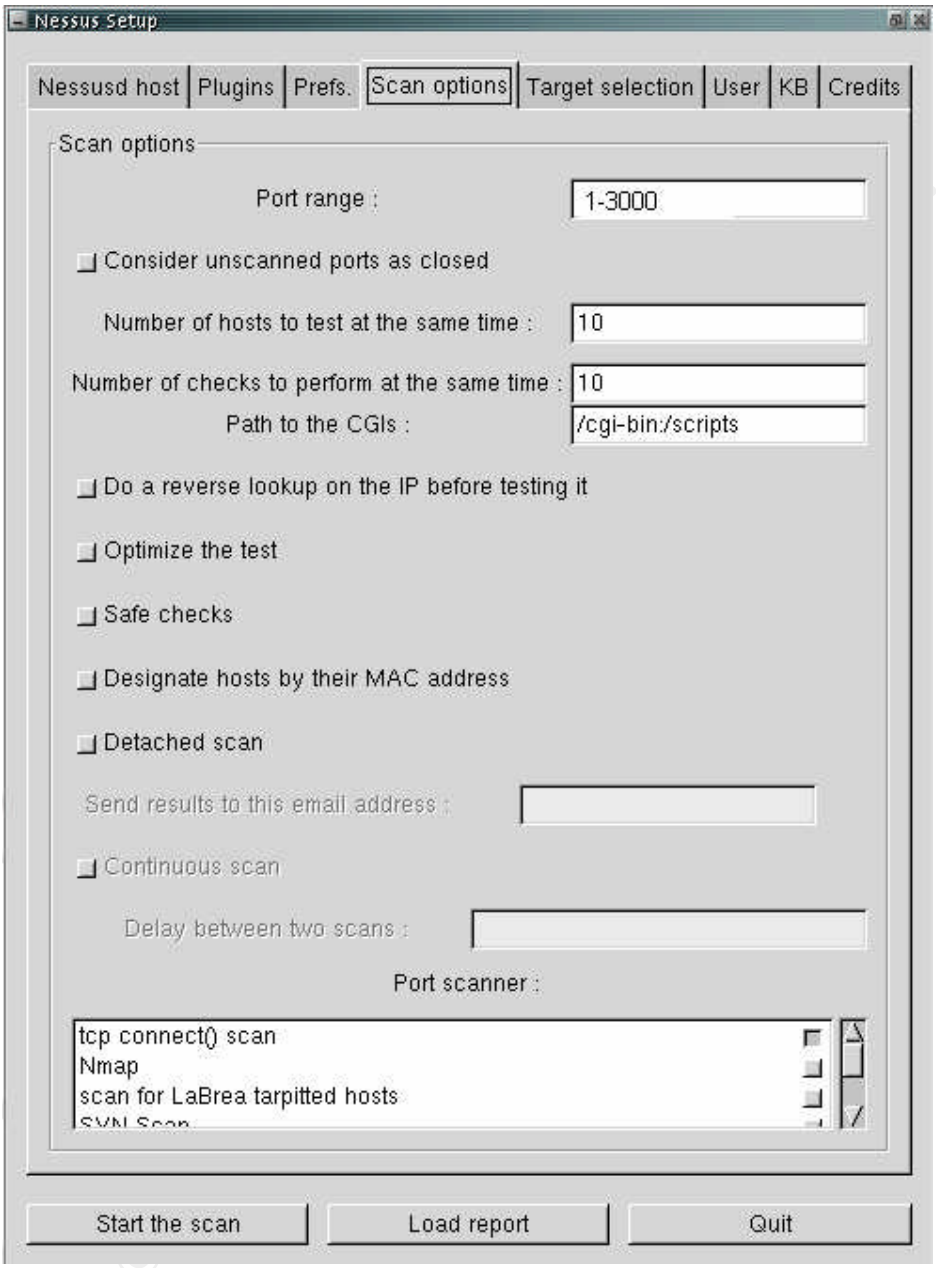
Drawing 9 (Nessus)

5. Edit preferences, lets set the FTP credentials to anonymous:



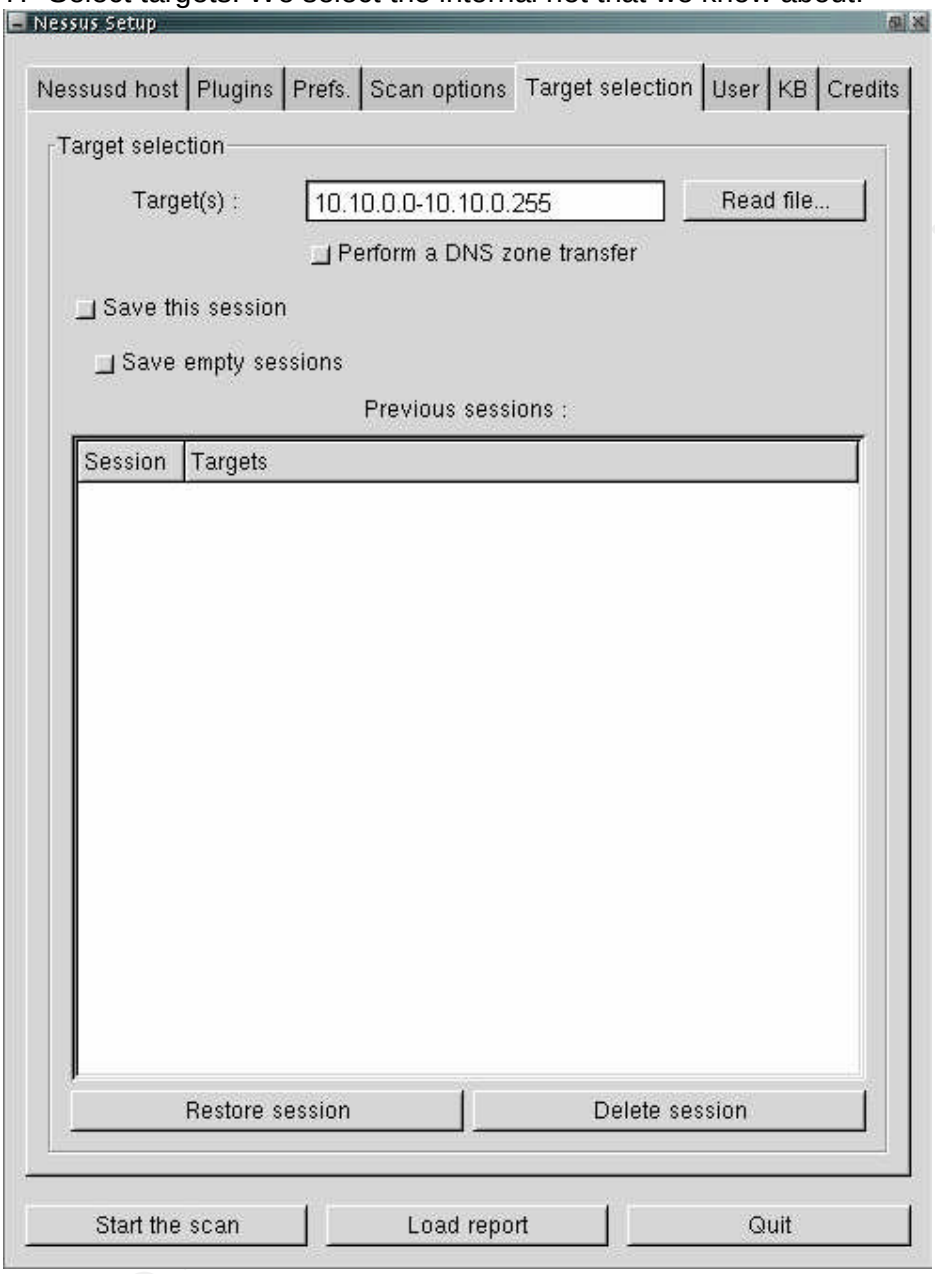
Drawing 10 (Nessus)

6. Scan options, Lets scan ports 1-3000, 10 host at the time using tcp connect scan, as we want to connect to the web server:



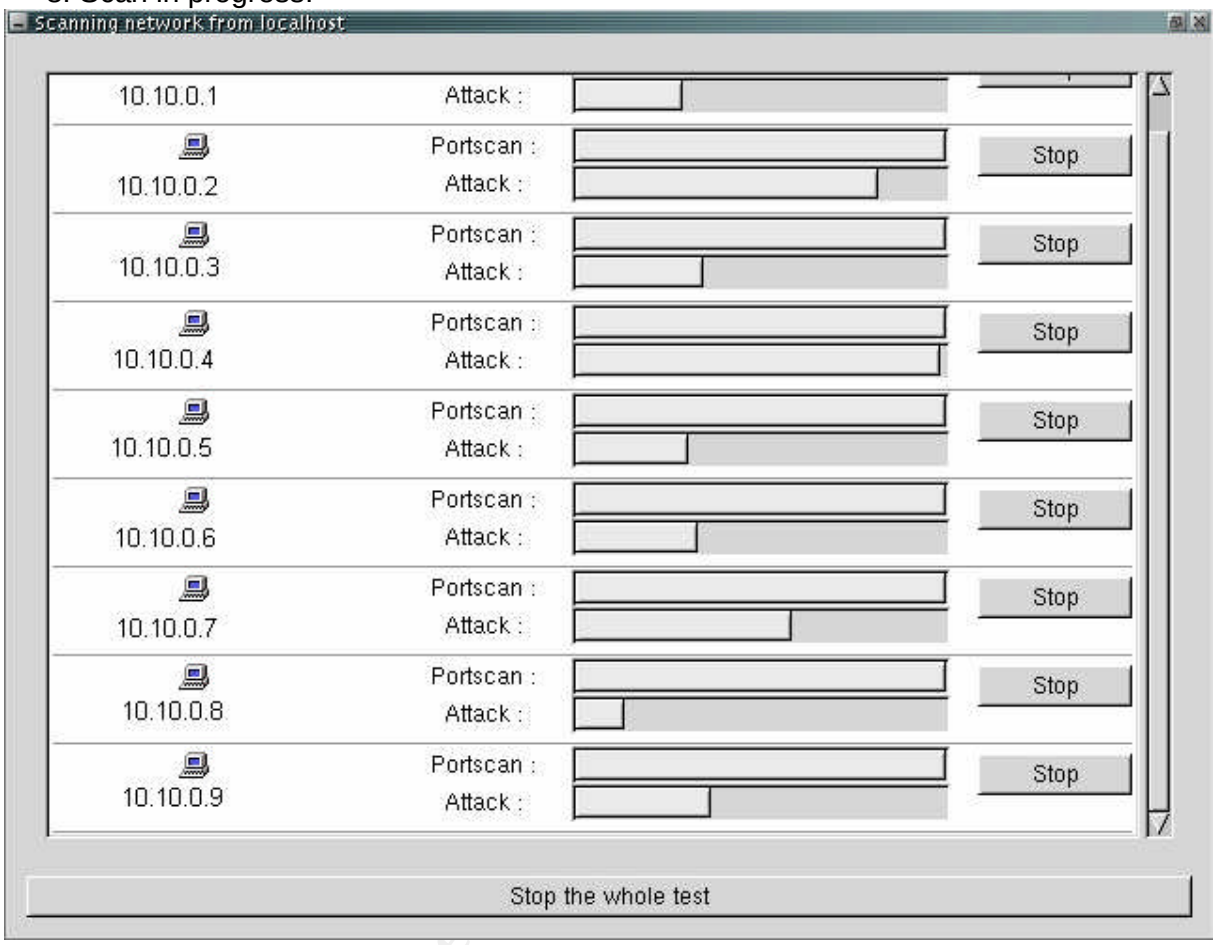
Drawing 11(Nessus)

7. Select targets. We select the internal net that we know about:



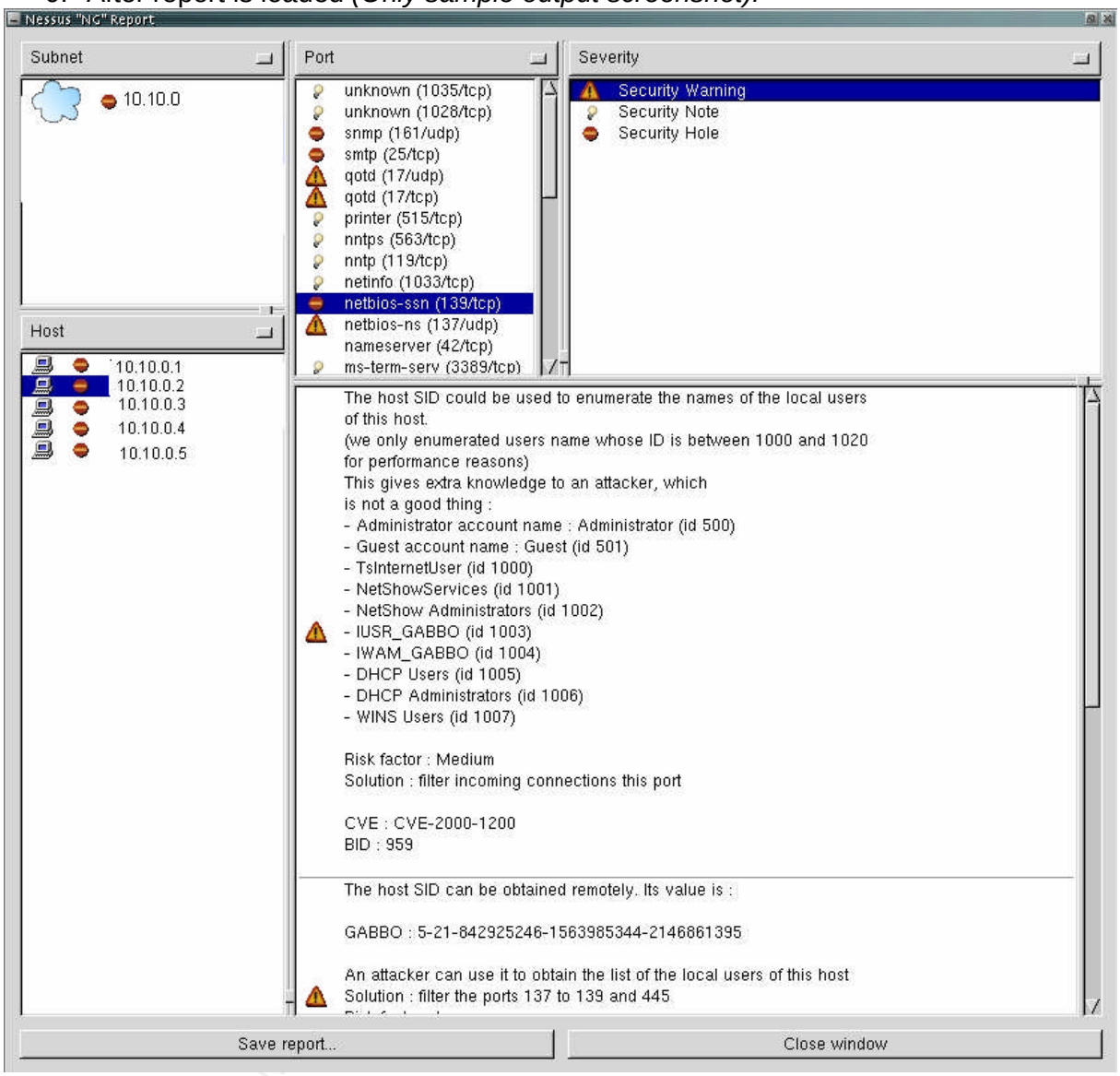
Drawing 12 (Nessus)

8. Scan in progress:



Drawing 13 (Nessus)

9. After report is loaded *(Only sample output screenshot):*



Drawing 14 (Nessus)

The results was inconclusive, even though I got a lot of information and some vulnerabilities on other machines, I didn't get anything that could help me connect or compromise the web server from the inside, but I could try to check for if any of the vulnerabilities I found on the other machines could be used as a leap board.
Ups….what happened I got disconnected to the Linux machine on the inside……..
After a while…..still nothing the script I put on there should have restarted the connection!

Let's try the Nessus from the outside on the official routed addresses this time using NMAP as port scanner……nothing!

After waiting a week or so and I still haven't received any connections from the Linux machine, I give up. Either they are on to me and blocked the ports, traced me in their IDS, or they have shut down or reinstalled the machine, or cleaned it from the script. The attempt failed!

3.5 Countermeasures

It didn't state if there was WLAN access or not on Jasmir Beciragic practical, so I made up the rouge user implemented WLAN access point, not unrealistic that some users experiment with different gadgets, they might have asked the IT department and been told that it's against company security policy or a solution is on the way. I've seen it before. In the past there was a lot of focus on rouge modems, but now I think we must move on and look at today's technologies.

- Unplug all unused network patches.
- Regularly scan of rouge WLAN access points.
- Block outbound SSH (might be impossible for management reasons)
- Block outbound VNC connections (very difficult as VNC can be altered to run on another port.

Assignment 4A - Future state of security technology

4 IKE/IPSEC vs. SSL

The following will describe the pros and cons with using IKE/IPSEC and SSL, I will try to compare the 2, is one better than the other? Is one stronger/weaker than the other? Witch one should I use when making VPN tunnels to my network?
For a while now IKE/IPSEC has been used to securing VPN tunnels to our networks, we trust the integrity and the security of these tunnels, and SSL has been used to secure i.e. payment over the internet through our browsers as a little key lock at the lower right corner.
The IPSEC VPNS has been standard for a long time implemented by Cisco, Nokia, Checkpoint and many others, but recently Nokia, Checkpoint and others has implemented SSL VPN as a secure tunnel to our networks in form of NSAS (Nokia Secure access server) and Conectra amongst other SSL VPN gateways/terminators. This paper will however not look so much at the vendor's solutions, but more at the IPSEC and SSL protocols in general and how they are used.

4.1 IKE/IPSEC, history and facts

Let's start by looking at the history and facts of the 2, and briefly how they work.

IPsec is a standard made up of a set of protocols that adds secure services on the network and is used for VPN (Virtual Private Network) tunnels; IPsec is very flexible and robust. The Protocol includes AH authentication header described in RFC 2402, IP protocol 51, that takes care of connectionless integrity, authentication and protect against replays.

ESP, Encapsulating Security Payload described in RFC 2406, IP protocol 50, adds different security services to the IP protocols, and works in conjunction with AH described in RFC 2401. If IKE Internet Key Exchange described in RFC 2409 TCP/UDP port 500 is used with IPsec it will take care of negotiation and creation of the SA´s (security associations) between the IPsec peers to protect the network. IPSEC (IP security) document roadmap described in RFC 2411 by R. Thayer from Sable Technology Corporation, N. Doraswamy from Bay Networks, R. Glenn from NIST, from November 1998.
IKE is a central part of IPSEC, as briefly mentioned before it takes care of creating SA´s. SA´s is a set of policies and keys used to identify each IPSEC connection witch Includes the following: SPI, Security Parameter Index, IP addresses, AH or ESP protocol.
IKE is a hybrid protocol based on ISKMP, Internet Security Association and Key Management Protocol, described in RFC 2408, used for implementing a key exchange protocol. Oakley described in RFC 2412 and skeme, described in the IKE RFC 2409 used for key exchange protocol, Skeme uses rapid key refreshments. Oakley, within IKE, uses by default the Diffie-Hellman algorithm described in RFC 2631 for the authenticated key exchange.
IKE consists of 2 phases.
Phase 1: The peers negotiate and establish a secure connection that will be used for phase2, witch is called ISAKMP SA. ISAKMP defines phases, and OAKLEY defines modes. There are 2 modes in phase 1, main mode witch exchanges 6 packages is slower but more secure, and aggressive mode witch exchanges 3 packages is faster.
Phase 2: The SA´s is negotiated and created in Quick mode. In Phase 2 PFS, Perfect Forward Secrecy can be used to make Phase 2 stronger but slower with the use of Diffie-Hellman key exchange algorithm.
IKE uses tunnelling mode encryption, witch basically means that it encrypts the entire IP packet including the IP header and adds its own header to the new encrypted packet. Encryption algorithms used with IKE includes DES, Triple DES, CAST cipher and AES 128-256. Authentication Algorithms includes MD5 and SHA-1.

4.2 SSL v3, history and facts

SSL, Secure Socket Layer described in http://wp.netscape.com/eng/ssl3/draft302.txt is actually a TLS Transport Layer Protocol described in RFC 2246 by T. Dierks and C. Allen from Certicom in 1999. SSL originates from Netscape to secure web/browser traffic to and from Netscape Navigator v 1.0. Today SSL is widely used with HTTP to secure different web transactions (HTTPS).
SSL provides privacy and integrity between 2 applications thus SSL is application layer based.
SSL handshake protocol works like this:
When the SSL client connects to a server, they first have to agree upon SSL version, Cryptographic algorithm, authenticate each other and generate shared secrets.

Client Server

ClientHello -------->
ServerHello
Certificate*

```
                                  ServerKeyExchange*
                                 CertificateRequest*
                      <--------      ServerHelloDone
  Certificate*
  ClientKeyExchange
  CertificateVerify*
  [ChangeCipherSpec]
  Finished                 -------->
                                  [ChangeCipherSpec]
                      <--------           Finished
  Application Data         <------->     Application Data
```

* Indicates optional or situation-dependent messages that are not always sent.

(Note: taken from http://wp.netscape.com/eng/ssl3/draft302.txt*)*

The Client starts with sending a “hello” to the server, the hello includes Client SSL version, session ID, Cipher suites and compression methods. The server then reply with a server “hello”, where it acknowledges the suggested containments of the clients hello, directly followed by the servers certificate that must match the selected cipher suite. The server can optionally request a certificate from the client if needed. Then comes a server hello done message. If the server requested a client certificate, this will now be send by the client according to the cipher suit proposed in the initial hello from the client, other than that if diffie-hellman certificates are used the clients cert must match the server specified parameters. Then follows the client key exchange message depending on witch public key algorithm has been selected, could be RSA, FORTEZZA or Diffie-hellman public value. At last a finish message to verify all above, the finish message is the first packet to go through the established SSL tunnel.
Encryption algorithms used with SSL includes RC2, RC4 and Triple DES. Authentication methods includes: MD5 and SHA1.

4.3 IKE/IPSEC pros and cons

Let’s look at the pros and cons about IKE/IPSEC based on the information in the above section 4.1 and other source information.
First of all IKE/IPSEC has been used to make VPN tunnels for ages now, so I should think that all techniques are well tested and documented by now. After reading a lot of stuff articles, RFCs and other references it’s become clear to me that I’m looking at a dilemma, some of the pros are actually cons and visa versa, and that concerns section 4.4 as well, but there must be some obvious flaws and weaknesses as well, let’s take a look.
When connecting using IKE/IPSEC to a VPN server, client software must be installed, witch is actually good because you can validate the client like Checkpoint SCV Secure Client Verification. But seen from the users view, he’s tied to the unit that the client is installed on witch I see as a security feature, but it limits the user’s freedom of choice when travelling etc. and limited support for all platforms, PDA´s (Personal Digital Assistant). The client has to be ported. Also SCV checks gives the possibility to control anti virus and other software on the client machine, and at the same time it demands that all users is able to configure and in some cases even install the client themselves, although vendors is trying

to help this issue like Checkpoint has the Secure Client packaging tool to help the administrators in some degree pre configure a client for the users. Another good thing about the client software is that it in some cases offers host based firewall software on the computer it's installed on.
As IKE/IPSEC is network based it gives transparent network access for all applications, but since its network based it can also cause trouble with Firewalls, NAT, overlapping address schemes and X-DSL connections. Again vendors is trying to overcome this i.e. by implementing connectivity enhancements like NAT traversal tunnelling mechanisms; IKE over TCP and Force UDP Encapsulation. Also the possibility to offer an internal address range via DHCP to the clients.
An IKE/IPSEC solution seems to be a little more expensive than an SSL VPN solution, but many already have the hardware to support IKE/IPSEC in form of some kind of firewall box, so all they need is basically the licenses needed to "turn on" the IKE encryption in order to establish the IKE/IPSEC VPN tunnels.
A couple of years ago weaknesses in the IKE aggressive mode (see section 4.1) was found, usernames were passed in clear text, but vendors addressed this problem fairly quickly, i.e. Checkpoint came up with the Hybrid mode were authentication schemes are supported.
Weaknesses in IKE/IPSEC VPN implementations seem rather limited as far as I can read. I found this Power point presentation on IKE/IPSEC where I copied this table from witch I think summons up pretty good weaknesses in IKE/IPSEC:

EFFECT MECHANISM	ATTACK	INDUCED ACTIVITY	IMPLICATION
Exhaustion of processing capacity	Initiate many IKE negotiations by sending many fake requests in a short time period (flooding).	Responder spends processing capacity by computing expensive DH modular exponentiations or parsing vast amount of payloads of each request.	Decreases performance of computer. Responder is unable to serve legitimate users.
Exhaustion of memory capacity	Initiate many IKE negotiations by sending many fake requests in a short time period (flooding).	Responder reserves memory by creating a state for each half-open connection (in a similar way like in TCP SYN flooding attack).	Decreases amount of available physical memory. When the physical memory runs out, virtual memory (disk memory) is used which causes swapping and a radical decrease in computer's performance.
Exhaustion of disk storage capacity	Initiate many IKE negotiations by sending many fake requests (flooding).	Responder writes error logs of abnormal events, e.g. of timed connections.	Decreases amount of disk storage. Disk quota of process may exceed.
Exploit of implementation flaw	Send a specially fabricated packet.	Responder crashes (e.g. because of a buffer overflow).	Responder becomes unavailable.
Exploit of implementation flaw	Send a specially fabricated packet.	Responder jams because it loops endlessly using all the available processing capacity.	Responder becomes unavailable. Also other services of a computer, which have lower priority than the Responder has, become unavailable.

Table 18 (taken from http://keskus.hut.fi/opetus/s38310/03-04/kalvot03-04/muittari_180504.ppt)

4.4 SSL pros and cons

Even though the IKE/IPSEC VPN´s have been in place for a while, the SSL/TLS have been here longer, tested by millions and millions of people all over the globe in different environments, it needs no extra software such as a client, it has in place client, the web browser, even though there are some SSL gateways/servers that need ActivX or Java to be installed to activate different features or to get access to specific applications, and not all public computers allow for applet download. When you don't have control over the client you are subsequent to the flaws and weaknesses in them. Another example of this from: http://www.thoughtcrime.org/ie-ssl-chain.txt

```
========================================================================
Exploit

So what does this mean?  This means that as far as IE is concerned, anyone
with a valid CA-signed certificate for ANY domain can generate a valid
CA-signed certificate for ANY OTHER domain.

As the unscrupulous administrator of www.thoughtcrime.org, I can generate
a valid certificate and request a signature from VeriSign:

[CERT - Issuer: VeriSign / Subject: VeriSign]
-> [CERT - Issuer: VeriSign / Subject: www.thoughtcrime.org]

Then I generate a certificate for any domain I want, and sign it using my
run-of-the-mill joe-blow CA-signed certificate:

[CERT - Issuer: VeriSign / Subject: VeriSign]
-> [CERT - Issuer: VeriSign / Subject: www.thoughtcrime.org]
   -> [CERT - Issuer: www.thoughtcrime.org / Subject: www.amazon.com]

Since IE doesn't check the Basic Constraints on the www.thoughtcrime.org
certificate, it accepts this certificate chain as valid for
www.amazon.com.

Anyone with any CA-signed certificate (and the corresponding private
key) can spoof anyone else.

========================================================================
```

SSL seems a little weaker than IKE/IPSEC, as most browsers by default only supports 128 bit cipher strength, in IKE/IPSEC its much more granular plus it supports AES-256, and you have to use token or certificate instead of password in SSL to raise the security level or other kind of 2 factor authentication.
Some vendors like http://www.rainbow.com/ offers a solution were you get the SSL gateway and iKey USB tokens for authentication, hardware based authentication, witch off cause requires USB slots on the PC you connect from, but these days most if not all computer have USB.
The users can connect from anywhere were there is a browser with SSL, the airport, the library, internet cafes on the PDA, cellular,….etc. If the client comes from unknown un-

trusted machines, some SSL gateways like Nokia´s NSAS and Checkpoints Contectra will grant limited access. A set of demands that has to be fulfilled in order for the client to gain different "levels" of access. I.e. if you have this version of antivirus engine and that virus definition update and are running a host based firewall (cooperate laptop) you have access to upload files, but if it doesn't detect any of the above you are only able to read mail – differential granular access to applications and easy access to web based applications.
Maybe its just me being paranoid but I don't like the idea of un-trusted machines connecting to my network, but I guess it works and it gives incredible freedom and space for users and affect how and where we can work. A problem could be if sensitive or confidential information was left on public computers if connecting from one of these, certificates and maybe even files the user can download unknowing that it will be left on that public PC.
I found this article on:
http://www.internetweek.com/allStories/showArticle.jhtml?articleID=16700677
In August 2003, for example, The New York Times reported a story about a man who had installed keystroke logging software on Internet terminals at Kinko's copy stores around New York City. According to the report, the man harvested personal information on 450 people who had used the kiosks. The crime was only uncovered when one of the victims actually saw his computer being controlled by a remote user.
This is a big security issue, and it's very hard or impossible to control these things.
SSL users suffers from a great level of exposure with no host based firewall protection, but off cause you can overcome this by installing firewall software, and it is even possible to get central managed protection, but then we are back to tying the user to 1 unit and limiting his roaming ability.
It can be difficult to get all proprietary applications implemented successfully, but still from an administrators point of view it's hard enough to secure internal computers
SSL is obviously more scalable and cheaper than IKE/IPSEC, and especially if you are from a smaller company.

4.5 Conclusion

So let's try to summon this up and make some conclusions, what is best? Well I guess it depends on several different factors; what you want, what suits your company/security policy, what do you protect, how critical, sensitive or confidential is your data, how big is your network, do you already have some hardware to support either solution, and so and so forth. It's very difficult/impossible to make a chart on when you would choose one over another.
Do you want the strongest level of security and encryption then I would definitely chose IKE/IPSEC, where you have some degree of control over the client, and were the users only can connect from 1 unit witch is installed by the IT department and runs cooperate antivirus solutions.
If you have a dynamic work force that travels a lot and you want them to access the core applications from any ware, and any unit at any time or if you don't want the administration hassle with installing and managing clients, SSL VPN could be the solution.
A unique thing about SSL is the ability to get access from any devise i.e. PDA´s witch a lot of us have, its very handy to access what you need very fast, without powering up the laptop, you have the access possibility right by you hand. If you don't want problems with users who can mess up or can't install the client, or have incompatible hardware/software or OS platform SSL would probably also be the answer.

But with these fairly new products based on well known technology such as Nokia´s NSAS and Checkpoint´s Conectra and others, were we have the ability to make granular checks on the users "clients" and differentiate access ability based on these checks, and the use of 2 factor authentication such as RSA, is the security levels of IKE/IPSEC and SSL really that far from each other? I think we will see a great deal of mix of the 2 solutions in the future.
My conclusion is that I think both IKE/IPSEC and SSL VPN will survive, the SSL VPN gateways are still fairly new as mentioned above, but as far as I can tell it's of from a good start. You can ask yourself if it's fair to possible fall victim to a "client" such as a browser that you have no control of; browser type, version, encryption scheme.
Witch one would I chose? I would probably combine the 2, so I could connect from my cellular and PDA with restricted access, and still have IKE/IPSEC as my main remote access scheme, but who knows what the future will bring. Witch solution would you choose?

References

5 Books

- SANS Institute track 2 course material books 2.1 – 2.6
- Check Point NG AI management II and III course material books (CCSE and CCSE+)
- Cisco CCIE study guide book

5.1 Links

Nokia support web:
http://www.nokia.com/nokia/0,8764,163,00.html

Checkpoint knowledgebase:
https://secureknowledge.checkpoint.com/sk/public/intro.jsp

Cisco:
https://www.cisco.com

ISS RealSecure (IDS):
http://www.iss.net/

Clearswift (MailSweeper):
http://www.clearswift.com/

Security solutions:
www.dubex.dk

Cisco vunerability:
http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Internic whois:
http://www.internic.net/whois.html

Ripe whois:
http://www.ripe.net/db/whois/whois.html

NMAP:
http://www.insecure.org/nmap/nmap_download.html

VNC script:
http://metalab.uniten.edu.my/~uwe/resources/HOWTOs/VNC-Pusher.html

WEB crack:
http://www.wi-fiplanet.com/tutorials/article.php/2106281

Rlogin:
http://homepage.eircom.net/~djkoshea/network/rlogin.html

Rlogin vulnerability:
http://www.cert.org/advisories/CA-1997-06.html

NEWT (nmap to windows)
http://www.tenablesecurity.com/newt.html

WLAN sniffer:
http://airsnort.shmoo.com/

NESSUS (screenshots):
http://www.nessus.org/demo/first.html

IP Security document roadmap:
http://www.faqs.org/rfcs/rfc2411.html

IPsec info:
http://en.wikipedia.org/wiki/IPSec

IPsec protocol overwiev:
http://www.freesoft.org/CIE/Topics/141.htm

SSL/TLS:
http://wp.netscape.com/eng/ssl3/ssl-toc.html

SSL vulnerability:
http://www.thoughtcrime.org/ie-ssl-chain.txt

Cisco IKE/IPSEC vulnerability:
http://www.oar.net/notices/workshop465.html

Old Checkpoint fw1 4.1 IKE/IPSEC vulnerability:
http://www.checkpoint.com/techsupport/alerts/ike.html
Article on IPSEC vs. SSL:
http://www.internetweek.com/allStories/showArticle.jhtml?articleID=16700677

Rainbow SSL solution:
http://www.safenet-inc.com/products/igate/igate.asp

SSL history:
http://developer.netscape.com/misc/developer/conference/proceedings/cs2/sld004.html

IKE RFC:
http://www.ietf.org/rfc/rfc2409.txt

ISAKMP RFC:
http://www.faqs.org/rfcs/rfc2408.html

OAKLEY RFC:
http://www.faqs.org/rfcs/rfc2412.html