Global Information Assurance Certification Paper

GIAC Enterprises: Fame, future and fortune

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment - Version 2.0
Challenge Certification

T. Brian Granier
GCIA, CCNA, CCSE, CHP, MCSE (NT4&W2K), MCP+I, N+, A+

Abstract

This document is presented as a practical submission for the GCFW certification. It is based upon GCFW assignment 2.0 and is being presented as a Challenge certification. Assignment one covers business processes, systems analysis, proposed network infrastructure and access requirements for the fictitious company of GIAC Enterprises, an e-business that sells fortune cookie sayings. Assignment two covers the implementation details associated with the designed infrastructure, with a detailed tutorial on installing the central firewall's rule-base on a Checkpoint NG FP3 firewall. Assignment three outlines the steps taken to verify the security infrastructure implemented with heavily utilization of the nmap scanning tool. After the details of the audit are presented, additional defense recommendations are presented to offer methods that the original proposed infrastructure might be improved. The final assignment takes an adversarial view of the Brad Tauer's GCFW practical assignment security implementation. This adversarial view discusses the timeless issue of social engineering and highlights attack methodologies that should be considered when designing a defense in depth perimeter security environment. Specific tools discussed include nmap, TFN2K, netstumbler, BackOrifice, keyloggers, personal firewalls and virus protection.

Assignment 1 – Security Architecture

Introduction

GIAC Enterprises recently obtained a considerable amount of business in their acquisition of their largest competitor, Fortunes For You. As a result of the acquisition, GIAC Enterprises would like to extend its e-commerce capabilities to more effectively deliver its core product, fortune cookie sayings. By strategic partnerships, GIAC Enterprises has managed to maintain rights to their fortune cookie sayings database and has extended their market share by permitting partners to translate and redistribute the sayings in other countries.

1.1 ***External relationships*** – this section gives information about the different relationships that exist external to the organization

1.1.1 **Customers** – *Companies or individuals that purchase bulk online fortunes*

Customers will need to create an account on the company web site with a form on the SSL portion of the site. They will specify their desired username and password in the account request form and will be emailed a confirmation code to activate their account. Subsequent order placement and status checking requests will be performed on the company web server under the SSL portion of the site, after they have logged in. After orders have been processed, customers will be able to download their fortune cookie sayings through the SSL portion of the web site.

1.1.2 **Suppliers** – *Companies that supply GIAC Enterprises with their fortune cookie sayings*

Suppliers will submit their sayings to the DropChute server. They may track the status of the review process and payment details by logging into the SSL portion of their website with an account that is provided to them offline as part of their contract initiation package. Exception reports and remittance advice will be sent via DropChute with email notification that the reports are available.

1.1.3 **Partners** – *International companies that translate and resell fortunes*

Partners will pickup their database of sayings with DropChute. Emails will be sent when a batch of sayings have been uploaded to DropChute, so that they will know to retrieve them. Partners will be provided with a user name and password that they can use to login to the SSL portion of the website to check the status of their requests. Although GIAC Enterprises is not currently accepting the translated text back in association with the original fortune cookie sayings, it is anticipated that this will at some point be desired. DropChute will be available for this purpose.

1.1.4 **General public** – *The general public*
The general public will need to be able to view the web server, as this group includes potential customers who have not yet submitted their application to be a registered user. They will also need to be able to access the DNS server for name resolution and to be able to send and receive mail from GIAC Enterprises.

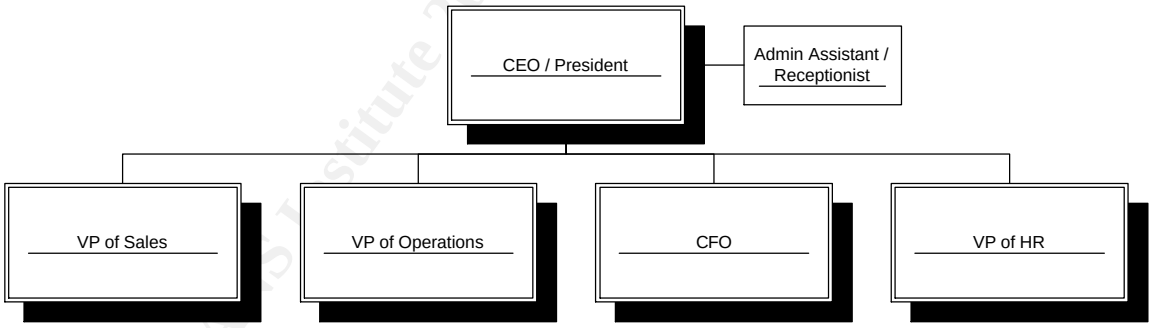
1.1.5 Resulting Connection needs – this specifies the connection needs identified based upon the external relationships**.**

Source	Destination	Protocols	Purpose
Internet	GIAC-WEB	HTTP, HTTPS	Access to the public web server
Internet	GIAC-DNS1	UDP DNS	Access to the DNS server
Internet	GIAC-DNS2	UDP DNS	Access to the DNS server
Internet	GIAC-Imail	SMTP	Ability to send mail to GIAC Enterprises
Internet	GIAC-Dropchute	TCP 2030	Custom port for DropChute delivery
GIAC-Imail	Internet	DNS, SMTP	Send outbound emails

1.2 ***Internal relationships*** – this section identifies internal business units and their needs.

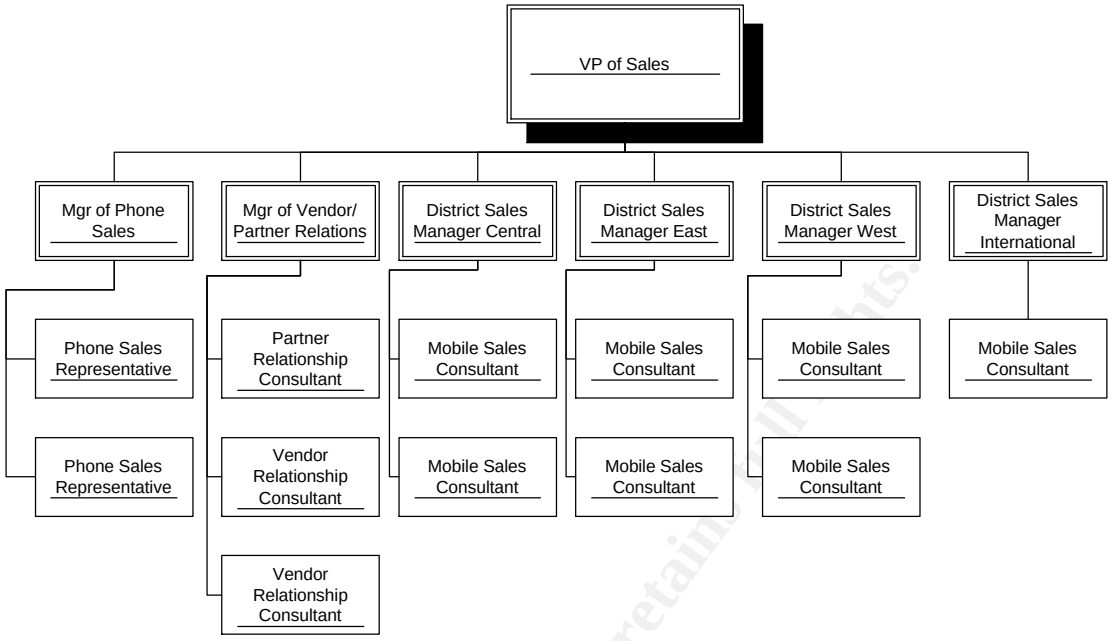
1.2.1 **Organizational Chart** – To understand the functional needs of the employees, it is valuable to review the organizational chart for GIAC Enterprises.

1.2.1.1 Executive Staff



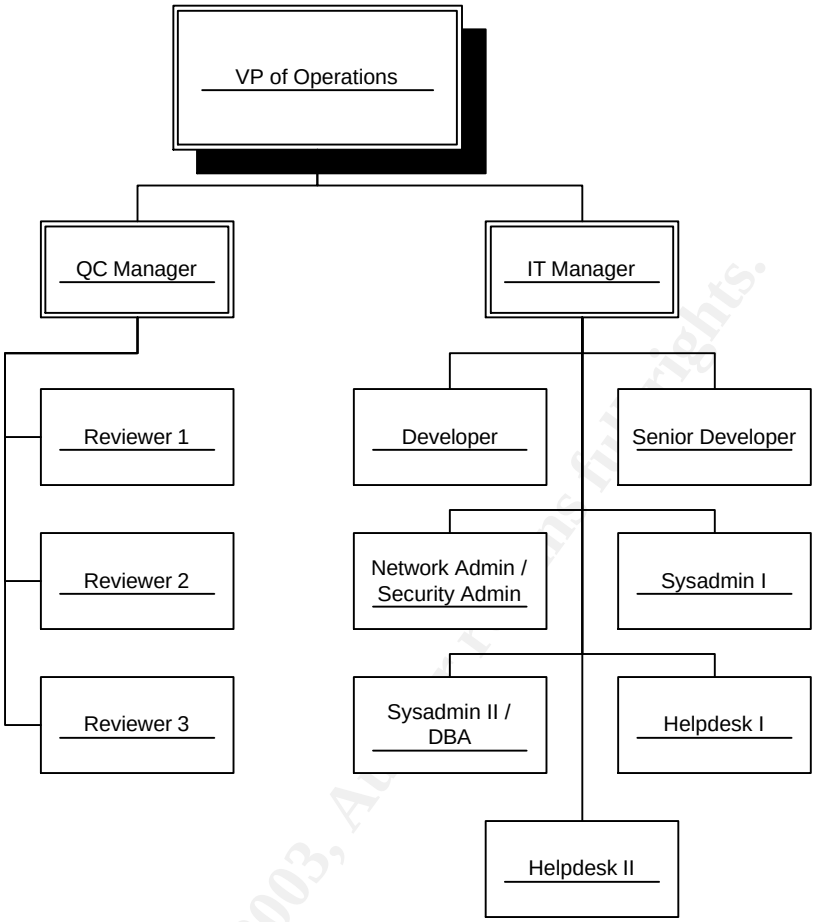
The executive staff rarely interacts with the core functional systems for the business. Their primary needs reside in file sharing on the corporate file server, email and printing.

1.2.1.2 Sales Staff



The sales staff is generally a highly mobile group of individuals. The VP of sales is typically in the office 75% of the time, district sales managers for 50% of the time and mobile sales consultants 10% of the time. The phone sales division is the only group that does not travel. The Manager of Vendor/Partner Relations is in the office 75% of the time and his staff are in the office 90% of the time. This group of individuals interfaces very heavily with the Intranet server for checking the status of orders and payments and to enter new orders. They also make heavy utilization of the mail server and the corporate file server.

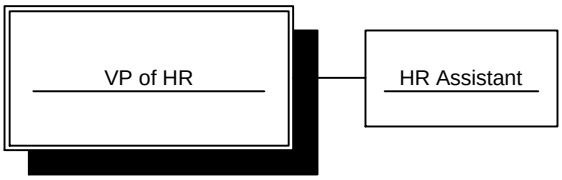
1.2.1.3 Operational Staff



The operational staff is divided into two functional groups. The QC group is responsible for checking for grammatical errors or inappropriate content in the fortune cookie sayings. They will also occasionally enter their own fortune cookie sayings. They are primarily involved in working with the Intranet site and its parsing functionality and updating the status of Vendor and Partner events in the status database. The reviewers also process customer orders that require manual intervention. The QC Manager works from the corporate office, but the three reviewers work from home.

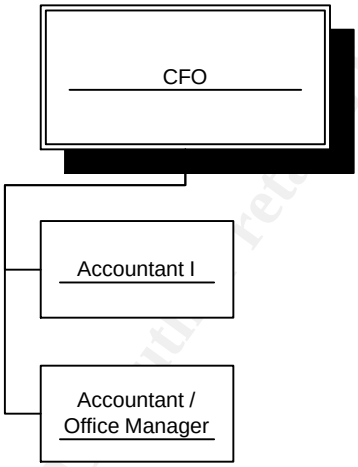
The IT group handles the technical details associated with the core business servers. Two Developers handle the external and internal web site and parsing engine. Two Sysadmins are responsible for the maintenance of the systems, with one of them providing DBA services. The Network Admin/Security Admin maintains the network and security infrastructure. The Helpdesk staff handles internal help requests and assists customers that are having technical problems with their connection. With the exception of the Helpdesk, the IT group has VPN connections available for emergency and off-hours access to address critical problems. The two Developers work from home most of the time.

1.2.1.4 HR Staff



The HR staff makes light utilization of the companies' server infrastructure. They are primarily interested in the corporate file server, email server and printer.

1.2.1.5 Finance Staff



The finance staff regularly audits the status database and manages the accounting server. The accounting server is completely separate from the other operational systems. Besides the finance server and the status database, this group accesses the email server, corporate file server and printer.

1.2.2 **Resulting Connection needs** – This specifies the access needs for the internal employees, both stated and implied

Source	Destination	Protocols	Purpose
Corporate Network	Border Router	SSH	Management of border router
Corporate Network	Screened,Data,Monitor Networks	TCP 3389	Terminal Server for server management
Corporate Network	GIAC-Fin/Payroll	All*	Access to the accounting server
Corporate Network	Internet	HTTP,HTTPS	General web access
Corporate Network	GIAC-Intranet/Parser	HTTP, FTP	Access to the Intranet server
Corporate Network	SnortCenter Console	HTTP, SSH	Snort Management
Corporate Network	GIAC-WEB	FTP	To upload new web sites
Corporate Network	Whatsup Gold	HTTP	Viewing Whatsup Gold site

* Not enough information is currently available in regards to the access needs for Peachtree. After the initial installation, the firewall logs should be reviewed for possibly tightening this access.

1.2.3 Employee VPN access needs – This specifies the VPN access needs for internal employees, both stated and implied.

Sales and Reviewer staff will need the following VPN access:

Destination	Protocols	Purpose
Intranet/Parser	HTTP	Access to the Intranet server
GIAC-Exchange	All	Access to internal email server
GIAC-DC1, GIAC-DC2	All	File sharing and domain resource utilization

Sysadmin/Netadmin will need the following VPN access:

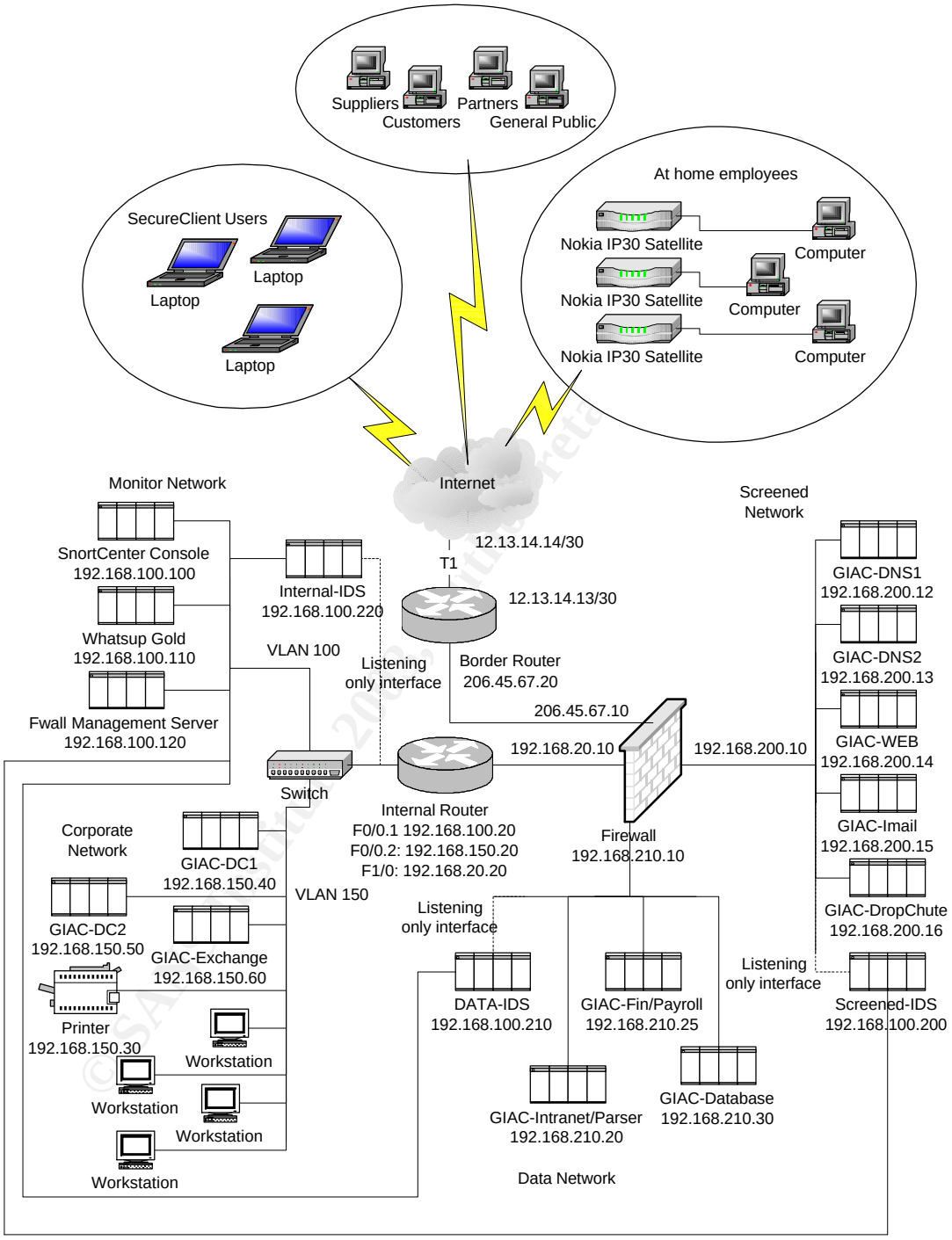
Destination	Protocols	Purpose
Screened,Data,Monitor Networks	TCP 3389	Terminal Server for server management
GIAC-Intranet/Parser	HTTP	Access to the Intranet server
GIAC-Exchange	All	Access to internal email server
GIAC-DC1, GIAC-DC2	All	File sharing and domain resource utilization

Developers will need the following VPN access:

Destination	Protocols	Purpose
GIAC-Intranet/Parser	HTTP, FTP	Access to the Intranet server
GIAC-WEB	FTP	Ability to upload manage the web site
GIAC-Exchange	All	Access to internal email server
GIAC-DC1, GIAC-DC2	All	File sharing and domain resource utilization

1.3 ***Network infrastructure*** – This section covers the network infrastructure designed to achieve the stated goals.

1.3.1 Network Diagram



1.3.2 IP Address Assignments

1.3.2.1 Network List

Network Name	IP Space	Short description
Internal Network	192.168.20.0/24	Used to interface with the firewall for various subnets
Monitor Network	192.168.100.0/24	Used for security and monitor based systems
Corporate Network	192.168.150.0/24	Used for local workstations and internal servers
Screened Network	192.168.200.0/24	Used for hosts directly accessed by the outside world
Data Network	192.168.210.0/24	Used for the critical servers
VPN Network	192.168.220.0/24	Used to NAT SecureClient users
Public Network	206.45.67.0/24	Used for hosts that need publicly routed IPs

1.3.2.2 Internal Network

The internal network is to separate the firewall from the corporate network and the monitor network. The value of this interim network is with intent of adding future branch office, vendor and supplier private internal networks connected with private line circuits. This will allow numerous internal private networks to connect through a single interface in the firewall and will ensure that with proper routing configuration on the routers on this network, all traffic between private networks must go through the central firewall to ensure appropriate access permissions. Alternative methods would require additional network ports in the firewall.

Host Name	IP Address	Description
Firewall	192.168.20.10	Internal side of firewall
Internal Router	192.168.20.20	Firewall facing interface

1.3.2.3 Monitor Network

The monitor network is used for systems meant to monitor the infrastructure from an administrative or security standpoint.

Host Name	IP Address	Description
Internal Router	192.168.100.20	VLAN 100 interface of Internal Router
SnortCenter Console	192.168.100.100	IDS Management System
Whatsup Gold	192.168.100.110	Whatsup Gold monitoring system
Fwall Management Server	192.168.100.120	Firewall management server
Screened-IDS	192.168.100.200	Screened Network IDS Host
DATA-IDS	192.168.100.210	Data Network IDS Host
Internal-IDS	192.168.100.220	Internal Network IDS Host

1.3.2.4 Corporate Network

The corporate network consists of the two domain controllers, printer, internal Exchange server and the local workstations located inside the corporate office.

Host Name	IP Address	Description
Internal Router	192.168.150.20	VLAN 150 interface of Internal Router
Printer	192.168.150.30	Shared Printer
GIAC-DC1	192.168.150.40	Primary Domain Controller
GIAC-DC2	192.168.150.50	Secondary Domain Controller
GIAC-Exchange	192.168.150.60	Internal Exchange Server
DHCP Reserved	192.168.150.128/25	IP reserved space for DHCP

1.3.2.5 Screened Network

The Screened network is intended for hosts that are made available for direct access from systems located outside of GIAC Enterprises firewall.

Host Name	IP Address	Description
Firewall	192.168.200.10	Screened Interface on Firewall
GIAC-DNS1	192.168.200.12	Primary DNS Server
GIAC-DNS2	192.168.200.13	Secondary DNS Server
GIAC-WEB	192.168.200.14	Public Web Server
GIAC-Imail	192.168.200.15	Public Mail Server
GIAC-Dropchute	192.168.200.16	DropChute Server

1.3.2.6 Data Network

The Data network consists of servers that are critical to the core business for GIAC Enterprises and do not have direct access permitted from general hosts on the Internet.

Host Name	IP Address	Description
Firewall	192.168.210.10	Data Interface on firewall
GIAC-Intranet/Parser	192.168.210.20	Hosts the Intranet and Parsing engine
GIAC-Fin/Payroll	192.168.210.25	Hosts the accounting and payroll software
GIAC-Database	192.168.210.30	Stores the cookie sayings database

1.3.2.7 VPN Network

The VPN network is used as a NAT Pool for employees connecting with SecureClient. This is done to prevent any potential IP address conflicts on the internal network. The entire 192.168.220.0/24 subnet is reserved for this purpose.

1.3.2.8 Public Network

The public network is for the purpose of providing IP addresses for hosts or networks that need a publicly routable IP address.

Host/Network Name	Public IP	Internal IP	Description
Firewall	206.45.67.10	N/A	Public interface on firewall
Border Router	206.45.67.20	N/A	Border Router internal IP
GIAC-DNS1	206.45.67.12	192.168.200.12	DNS1 public IP
GIAC-DNS2	206.45.67.13	192.168.200.13	DNS2 public IP
GIAC-WEB	206.45.67.14	192.168.200.14	Web Server public IP
GIAC-Imail	206.45.67.15	192.168.200.15	Imail Server Public IP
GIAC-DropChute	206.45.67.16	192.168.200.16	DropChute Server Public IP
Monitor Network	206.45.67.100	192.168.100.0/24	Hide Nat for Monitor network
SnortCenter Console	206.45.67.101	192.168.100.100	SnortCenter Console
Fwall Mgmt Srvr	206.45.67.120	192.168.100.120	Static NAT for firewall mgmt srvr
Corporate Network	206.45.67.150	192.168.150.0/24	Hide Nat for Corporate network
Data Network	206.45.67.210	192.168.210.0/24	Hide Nat for Data network

1.4 ***Systems Explanation*** – This section covers an explanation of the functional purpose and specification for each system identified in the network infrastructure. The majority of the server infrastructure uses Windows 2000

Server. All of these servers have Service Pack 4 applied with all appropriate security patches applied. Norton Antivirus is installed on the servers.

1.4.1 Border/Internal Router and Internal Switch

The border router will be a Cisco 3725 router with 256 MB of RAM (max) running IOS version 12.3(1). The IOS version to be used is the IP PLUS IPSEC 3DES version and was selected based upon stability and security needs. This will provide ample power to run the access lists that will be configured on this perimeter device and provide a considerable amount of room for growth. As the first line of defense from external attacks, the access lists will be configured to reduce obviously unnecessary traffic in an effort to reduce the amount of noise seen and handled by the central firewall. Backups will be manually performed for the configuration of this router as a part of the change management process.

The internal router will be a Cisco 2621 router with 32 MB of RAM running IOS version 12.0(7)T2 with IP Plus feature-set for VLAN trunking. Since route-map filters will be configured to forward all traffic to the firewall that is destined to traverse between two networks, it is unnecessary to deploy excessive power in this device. This router is a cost-effective solution to provide dual fast-Ethernet access between the VLAN networks and the firewall. It would have been desirable to have used the maximum RAM available (64 MB) and to have used IOS 12.2(17), but due to budgetary restraints it was not possible to do so. The IOS version selected was based upon the desire to select the most recent IOS version with IP Plus feature-set that would run on the 2621 with 32 MB of RAM, since this device was already owned by GIAC Enterprises. An acceptable major release version was not available. Backups will be manually performed for the configuration of this router as a part of the change management process.

The Internal switch will be placed between the Internal router and the Corporate and Monitor network. This switch will be configured for the specified VLAN implementation. It will be an HP4000M with the latest firmware version (currently C.09.16). The selection of this device is based upon making usage of equipment that is already owned and in operation by GIAC Enterprises. Backups will be manually performed for the configuration of this switch as a part of the change management process.

1.4.2 Firewall and Management Server

The central firewall will be a Nokia IP530 running IPSO 3.6 FCS7 (current latest version) with Checkpoint FireWall-1/VPN-1 FP3 with the latest hotfix roll-up package. The selection of this particular Nokia platform was based upon a desire to provide 4 integrated network cards as part of the base unit and capable of supporting the desired version of IPSO. Although this system is likely more powerful than needed for current and long-term future growth needs, it is the minimum Nokia platform available to meet the requirements. The next available platform down that supports this version of IPSO (IP330) would have no room for growth as the available expansion port would be used immediately to provide the

additional required local network ports. Although the next version of Checkpoint is available (AI), the lack of a tested IPSO version supporting this platform and the newness of the version release make it unwise to deploy this version at this time. The need for a VPN-1 accelerator card to improve VPN performance was evaluated, but based upon the limited VPN needs and the limited amount of bandwidth available, it would be unnecessary to do so at this time.

Since IPSO is specifically designed as a secure platform for running Checkpoint FireWall-1/VPN-1, additional patches should be unnecessary, but future releases of IPSO versions should be reviewed for potential OS level security fixes. No direct backup would be necessary on the firewall.

The Management Server is a CheckPoint function that is used to configure and deploy the security policy to the firewall. Although this function could reside on the firewall itself, due to the desire to maintain the logs off the firewall and to manage configuration changes separate from the core firewall function, we have chosen to separate this function onto another system. The Firewall Management Server will be running on the Monitor Network on a system running Windows 2000 Server. GIAC Enterprises will be making utilization of an existing server for this purpose. This system is a Compaq Proliant 1850R with dual PII 450 MHz processors and 512 MB of RAM. The hard drives consist of a mirrored 9 GB system partition and a 36 GB drive. The 36GB partition is used for storage of log files. Although it would be possible for hardware failure to cause GIAC Enterprises to lose their logs, the likelihood of failure is considered acceptable. The firewall configuration information will be backed up to tape nightly using an internal tape drive on the system. Firewall logs will be archived to tape and zipped on the local hard drive as part of the nightly backup process once they are one week old. When they are one month old, they will be purged from the system.

1.4.3 DropChute server

The DropChute server runs the DropChute Enterprise 3.02 software. Information about this application can be found at http://www.hilgraeve.com/dropchute/enterprise/index.html. This system will be running Windows 2000 Server as the operating system. The Enterprise version is required in order to automate processes to occur based upon the receipt of incoming files and to prepare files for auto-delivery. DropChute provides an encrypted delivery methodology with strong authentication based upon digital certificates created from the DropChute server. Suppliers and Partners will be provided with DropChute Pro (http://www.hilgraeve.com/dropchute/pro/index.html) for approximately $200 to connect with the GIAC Enterprise DropChute server. Note that by default, a DropChute Enterprise server will attempt to connect to an external server (ldap.dropchute.com) on port 389 for ldap services. This is unnecessary and undesired in this configuration, so it should be disabled. To do so, follow the instructions at http://www.hilgraeve.com/dcplus/dcfirewall.html. GIAC

Enterprises will change the default port from 23 to 2030 for purposes of this connection to provide additional obscurity. Each vendor and supplier will have a unique user account with a unique certificate for purpose of connecting to this server. As part of the DropChute configuration, each of these users will have a unique directory that is only viewable by the configured user account. The Intranet/Parsing engine will have ftp access to this system in order to make files available for partners. This system will have ftp access to the Intranet/Parsing engine in order to deliver received files from suppliers as part of the inbox automation process. Since incoming data is immediately moved to the parsing server and outbound data is able to be recreated from the core database, the normal backup routine should suffice for this system.

1.4.4 Imail Server

The Imail server is the public facing mail server. This system will be running Windows 2000 Server. It is used to send and receive mail from the Internet. The Intranet/Parsing engine and Web server will use this server to send notification emails to customers, vendors and suppliers. The internal Exchange server will send all of its outbound mail through this server. The virus filtering functionality will be enabled on this system by usage of Declude and F-Prot. Information about Declude can be found at http://www.declude.com/Virus/index.html. Information about F-Prot can be found at http://www.f-prot.com/products/home_use/dos/. Upon receipt of inbound mail, messages will be scanned for viruses and then forwarded to the internal Exchange server for final delivery. More information can be obtained from http://www.ipswitch.com/products/imail_server/index.html. Since inbound mail is immediately forwarded to the internal Exchange server and outbound mail is completed after delivery, backups are not critical on this system. The normal backup routine should suffice.

1.4.5 DNS Servers

The primary and secondary DNS servers will be running on a DNSOne appliance. Since DNS queries to these hosts are not expected to exceed the size limit for UDP queries, only UDP DNS queries will be permitted through the firewall to this host. This system is managed via SSL. More information can be found at http://www.infoblox.com/. This system was chosen for its ease of management and security management process available from the manufacturer. With no Linux/Unix administrators on staff and with a lack of desire to run public DNS services on a Windows system, the cost/benefit analysis suggests that relying upon the vendor to maintain the security of these systems with regularly updated patches is the better economic solution. These systems will serve as a live backup for each other.

1.4.6 Web Server

The public web server is running Windows 2000 Server. It is running IIS 5.0 with careful attention paid to security patches. This system has limited access to the user database and status database located on the internal web server. An SSL

certificate is installed on this system for encrypted access to the web based application that is used to manage user profiles and retrieve information in regards to the placement and status of orders. After order forms have been filled out, they are sent to the Intranet/Parser for automatic or manual processing via ftp. Fulfilled customer orders are uploaded to this system from the Intranet/Parser after they have been processed to make them available for download by the customer. Backups are performed according to the regular backup schedule as the content rarely changes.

1.4.7 Database

The internal database server runs on Windows 2000 Server with SQL Server 2000 and all applicable patches. The Web server will have limited access to this database for purpose of comparing the hashed password for users logging in and allowing them to edit their user profiles. Additionally, the web server access will permit for status request information to be processed and delivered to customers, suppliers and partners from the SSL site. The Intranet/Parsing engine will have less restrictive user based access to permit updating the core Fortune Cookie sayings database and updating the status and user database through the Intranet management pages. This is a very critical system. As such, it will be running on Hardware RAID 5 with a hot spare hard drive. The backup routine will be reviewed for minimal exposure in case of a loss of data. A duplicate additional reduced data set database exists on this system for the sole purpose of development.

1.4.8 Intranet/Parser Server

The Intranet/Parser system runs Windows 2000 Server. It is running IIS 5.0 with careful attention paid to security patches. Access to this system is restricted to internal employees as it is used for the purpose of managing the content of the Fortune Cookie Database, updating the status of Customer purchases, managing the review and status of Supplier entries, and processing Partner requests and Customer orders. A separate site instance exists on this system for development purpose that is pointed at the development database on the central database server. This system receives files from the DropChute server via ftp and places files for Partners onto the DropChute server. It also sends notification emails to the Imail server to notify Customers, Suppliers and Partners of status changes. The Parser/Intranet server is also responsible for fulfilling customer orders by sending the fortunate cookie sayings in csv format to the web server so that customers may retrieve them over the public SSL site. Completed order forms are received from the web server for processing via ftp. This system accesses an online credit card authorization service over https in an attempt to provide automated fulfillment. More information on the product used can be found at http://www.mbankcard.com/. Orders that fail to be automatically placed are marked for manual completion by one of the Reviewer staff. Backups of this system are important, although the exposure is limited since the core application changes infrequently. The backup routine for the system for this system needs

to be carefully reviewed to minimize downtime and loss of data in the event of a failure according to the risk acceptance of GIAC Enterprises.

1.4.9 Finance/Payroll System

The Finance/Payroll system is used by the CFO and accountants for managing the accounting database. This server runs Windows 2000 Server. This system runs Peachtree Complete Accounting 2004 and maintains a modem for connection to ADP to send payroll instructions. The phone line that is attached to this system is provisioned for outbound calls only. Additionally, the system is configured not to answer any inbound calls.

1.4.10 Domain Controllers

The domain controllers provide the file server function for GIAC Enterprises. These systems are running Windows 2000 Server. The primary domain controller acts as the print server to connect to the HP 4500 printer. The secondary domain controller serves the function of being the Norton Antivirus Corporate Edition management server. Note that since the GIAC Enterprise internal Windows domain will be in Active Directory native mode, the concept of primary and secondary domain controller is irrelevant. These terms are used for conceptual reasons only. These systems are backed up according to the risk acceptance analysis for the file server functionality.

1.4.11 Exchange Server

The internal Exchange Server houses the user mailboxes and maintains the calendaring for internal employees. It is running Windows 2000 Server with Exchange 2000. It also uses the Exchange plug-in for Norton Antivirus Enterprise Edition. This system should be backed up regularly.

1.4.12 IDS systems

The IDS system infrastructure involves Snort sensors deployed with a listening only interface on the network it watches and a connection on the monitor network. These systems are deployed in accordance with the document located at http://www.superhac.com/docs/snort_enterprise.pdf. The SnortCenter console will also run syslog, ftp and ntp for the border router.

1.4.13 Whatsup Gold

The Whatsup Gold system is used to monitor the availability of systems on the network. It sends alert emails to the Imail server for notification of critical events. This system runs on Windows 2000 Professional with Service Pack 4. Information about Whatsup Gold can be found at http://www.ipswitch.com/Products/WhatsUp/index.html.

1.4.14 Corporate Workstations

Corporate workstations are running Windows 2000 Professional with Service Pack 4 and the latest security patches applied. They are running Norton

Antivirus Corporate edition, which is centrally managed from the secondary domain controller.

1.4.15 Mobile Laptop

Mobile laptops are running Windows 2000 Professional with Service Pack 4 and the latest security patches applied. They have SecureClient installed with virus filtering in accordance with the standard mobile user configuration. These systems are used by the mobile sales staff, system administrators and the network admin.

1.4.16 Home Users

Home users are given systems very similar to internal employee workstations. They are running Windows 2000 Professional with Service Pack 4 and the latest security patches applied. They have virus filtering installed on them. These users have a broadband connection to the Internet with an IP30 Satellite device for VPN functionality. The IP30 device is managed by the Firewall Management Server. The default "High Security" policy for outbound access will be applied to these systems. The VPN is certificate based to accommodate for systems that may require a dynamic IP address. Although more concise control can be obtained of these systems with regards to modifying the default policy sets with SofaWare, this would require installing backwards compatibility mode on the Firewall Management Server. Since this is not a recommended configuration and the High Security mode provides adequate protection, these systems are instead managed through the SSL management interface. More information about this appliance can be found at http://www.checkpoint.com/products/choice/platforms/nokiaip30.html.

1.4.17 Resulting Connection Needs

In addition to the connection needs identified in relation to external and internal relationships, an analysis of the purpose and function of each of the servers provides this chart of access requirements:

Source	Destination	Protocols	Purpose
GIAC-Imail	213.220.100.3	HTTP, FTP	F-Prot antivirus updates
GIAC-Intranet/Parser	64.94.118.66	HTTPS	Credit card authorization
Whatsup Gold	All	SNMP, icmp	Monitoring
GIAC-WEB	GIAC-Database	TCP1433 (ODBC)	Database queries
GIAC-DC1, GIAC-DC2, GIAC-Exchange	GIAC-DNS1, GIAC-DNS2	DNS	Dns queries
Screened,Monitor,Data Networks	GIAC-DNS1,GIAC-DNS2	DNS	Dns queries
Corporate Network	GIAC-DNS1, GIAC-DNS2	HTTPS	Managing DNS Server
GIAC-Intranet/Parser	GIAC-DropChute, GIAC-WEB	FTP	Transferring files
GIAC-Imail	GIAC-Exchange	SMTP	Sending mail
Screened,Monitor,Data Networks	Firewall	TCP: 259,900	User authentication for temporary access

Fwall Mgmt Srvr	Firewall	TCP: 18191, 18192, HTTPS, SSH	Firewall control connections
GIAC-Exchange, GIAC-Intranet/Parser	GIAC-Imail	SMTP	Sending mail
GIAC-DC1, GIAC-DC2	Internet	SNTP	Time synchronization
GIAC-DC2	Internet	TCP2847	Norton virus definitions updates
Screened,Monitor,Data Networks	Internet	SNTP	Time synchronization
Screened,Monitor,Data Networks	Internet	HTTP, HTTPS, FTP	Used with user authentication to download patches by admins
GIAC-DNS1, GIAC-DNS2	Internet	DNS	Dns queries
GIAC-DropChute	Internet	TCP: 2030	Custom port used by GIAC for DropChute
Fwall Mgmt Srvr	Internet	TCP: 981	SSL over TCP 981 for IP30 management
GIAC-Imail	Internet	SMTP	Sending mail
Border Router	SnortCenter Console	NTP, Syslog, ftp	Enables logging and time synchronization from border router
GIAC-DropChute, GIAC-WEB	GIAC-Intranet/Parser	FTP	Transferring files

1.5 ***Physical Security*** – This section discusses the physical security of GIAC Enterprises.

The physical security of the network infrastructure is an important element of the overall security posture for GIAC Enterprises. All server class systems, routers and switches are expected to be stored in a suitable environment (humidity, temperature and power controlled) with restricted access to only the personnel that need physical access to fulfill their job role.

Assignment 2 – Security Policy and Tutorial

2.1 *Internal Router configuration*

The entire configuration for the internal router is found in Appendix A. Since many of the configuration details are similar between the border router and the internal router, I will only cover the aspects of the configuration that are unique and interesting to the internal router. The purposes for the other commands that are common to the internal and border router are explained in the next section.

2.1.1 VLAN configuration

```
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 192.168.100.20 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 150
 ip address 192.168.150.20 255.255.255.0
!
```

The “encapsulation” command specifies the VLAN that is associated with the interface. This provides the layer 2 separation of the Corporate and Monitor network.

2.1.2 Route-map filter

```
!
interface FastEthernet0/0.1
  ip policy route-map filter
!
interface FastEthernet0/0.2
  ip policy route-map filter
!
access-list 50 permit 192.168.100.0 0.0.0.255
access-list 50 permit 192.168.150.0 0.0.0.255
route-map filter permit 10
 match ip address 50
 set ip next-hop 192.168.20.10
!
```

The effect of this configuration is that any traffic inbound from F0/0.1 and F0/0.2 that are coming from 192.168.100.0/24 or 192.168.150.0/24 will be automatically forwarded to the firewall at 192.168.20.10. The access-list 50 specifies the subnets that are automatically forwarded and the next-hop specifies where the traffic will be forwarded to. Note that this configuration bypasses the routing engine on the router. This prevents hosts on the 192.168.100.0/24 network from communicating with hosts on the 192.168.150.0/24 network without passing through and being permitted by the firewall and vice versa. Essentially, this takes the responsibility of access lists off of the router and gives it to the firewall instead.

2.1.3 Null route

```
ip route 0.0.0.0 0.0.0.0 Null0
```

This configuration essentially specifies that if the network is not directly attached, then the router will not be able to pass traffic to it. Since all connections that are intended to pass **through** this router are to or from the 192.168.100.0/24 or 192.168.150.0/24 networks and routing for these networks to other networks is handled by the route-map filter, there is no reason for the core routing engine to have a default route. Utilization of the core routing engine on this router would be evidence of unintended and potentially malicious traffic; therefore we send it to Null0 where it will be dropped.

2.2 Border Router Configuration

The complete configuration is shown in Appendix B. I'll cover the details of the configuration that were applied for the purpose of providing additional security.

2.2.1 Time synchronization

```
clock timezone CDT -6
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
ntp authentication-key 6767 md5 0058202327692E3224047510 7
ntp authenticate
ntp trusted-key 6767
ntp server 206.45.67.101 key 6767
```

The service timestamps commands will ensure that logs will be shown with the appropriate timestamp. The ntp configuration will setup the router to receive its time configuration from the SnortCenter console via it's statically NATted public IP address. The time synchronization traffic will be checked for authenticity to ensure it came from the expected host in order to prevent tampering with the time on the border router.

2.2.2 Logging

```
logging buffered 16384 debugging
no logging console
!
logging trap debugging
logging facility local5
logging 206.45.67.101
!!
int <interface>
 ip accounting access-violations
!
exception core-file GE-Border
exception protocol ftp
exception dump 206.45.67.101
!
ip ftp username rooter
ip ftp password 7 12090404011C03162E8
```

The “logging buffered” command sets up a logging buffer on the router. “no logging console” will turn off logging to the console which could flood the port and reduce performance. Next, we establish the SnortCenter console host as the destination to send the log files. On the interfaces, we turn on “ip accounting access-violations” in order to log packets that failed the access-list and were not routed. Finally, the remaining commands are used to ftp a core-dump file in the event of router crash to the SnortCenter console so that it can be analyzed in this unlikely and disastrous event.

2.2.3 SNMP configuration

```
access-list 20 remark SNMP ACL
access-list 20 permit 206.45.67.100
access-list 20 deny   any log-input
!
snmp-server community makeithardtoguess RO 20
snmp-server enable traps tty
```

SNMP should be enabled with careful consideration due to its potential for information gathering. In this case, we have established an access-list that will only respond to SNMP queries coming from the NATted public address of the Monitor network. Additionally, the community name should not be configured with the default of “public” or “private” and should be difficult to guess.

2.2.4 Login configuration

```
enable secret 5 $1$EAje$2gZvU3p7P9n579eVQCYH0.
!
username giacsa password 7 13151601181B0B382F
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
aaa session-id common
!
ip ssh source-interface FastEthernet0/0
!
radius-server authorization permit missing Service-Type
!
access-list 90 permit 206.45.67.150 log-input
access-list 90 deny   any log-input
!
line con 0
 exec-timeout 15 0
line aux 0
 exec-timeout 0 10
 no exec
line vty 0 4
 access-class 90 in
 exec-timeout 15 0
 transport input ssh
!
```

The “enable secret” command sets the privileged password. The “username” command sets the username and password permitted access to the router. All of

the commands starting with “aaa” relate to setting up a local authentication function to be used for logging into the router. The “ip ssh” turns on the ssh server on the router, which is more secure than the default telnet, and configured it to listen on the IP address configured on the F0/0 interface. Note that a “crypto key generate rsa” command must be issued for this to work. The “radius-server” command is automatically entered as part of the “aaa” commands. Finally, access-list 90 combined with the “line vty 0 4” configuration will specify that the only remote access permitted will be from the public NATted address for the Corporate LAN over ssh.

2.2.5 Null routes

```
ip route 0.0.0.0 254.0.0.0 Null0
ip route 2.0.0.0 255.0.0.0 Null0
…
ip route 198.18.0.0 255.254.0.0 Null0
ip route 223.0.0.0 255.0.0.0 Null0
```

These null routes will drop traffic destined for IP space that is not assigned according to IANA. By routing it to Null0, the traffic will be effectively dropped. Details can be found at http://www.cymru.com/Bogons/index.html.

2.2.6 Egress filter

```
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq smtp
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq www
access-list 110 permit udp 206.45.67.0 0.0.0.255 any eq domain
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq domain
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 443
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 2030
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 123
access-list 110 permit udp 206.45.67.0 0.0.0.255 any eq ntp
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 981
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 2847
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq ftp
access-list 110 permit udp 206.45.67.10 0.0.0.0 any eq 500
access-list 110 deny   ip any any log-input
```

This egress filter will be applied on traffic that is initiated from an internal host. It will permit traffic to pass through the router if it originates from GIAC Enterprises assigned public address space and is using a protocol that is expected to be coming from this address space. All other traffic is dropped and logged.

2.2.7 Ingress filter

```
access-list 120 deny   ip 0.0.0.0 1.255.255.255 any log-input
access-list 120 deny   ip 2.0.0.0 0.255.255.255 any log-input
…
access-list 120 deny   ip 223.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 224.0.0.0 31.255.255.255 any log-input
!
access-list 120 deny   ip 206.45.67.0 0.0.0.255 any log-input
access-list 120 permit tcp any host 206.45.67.14 eq www
access-list 120 permit tcp any host 206.45.67.14 eq 443
access-list 120 deny   tcp any any eq www
access-list 120 deny   tcp any any eq 443
```

```
access-list 120 deny   tcp any any eq 1433
access-list 120 deny   tcp any any eq 1434
access-list 120 deny   tcp any any eq 445
access-list 120 deny   udp any any eq netbios-ns
access-list 120 deny   udp any any eq netbios-dgm
access-list 120 deny   tcp any any eq 139
access-list 120 permit ip any 206.45.67.0 0.0.0.255
access-list 120 deny   ip any any log-input
```

The first part of the ingress filter looks for traffic coming from the IANA unassigned address space and drops it. It's the same list as used in the null route section for the same reason. Next, we deny traffic coming in from the Internet that is sourced with an IP address that should be on the local network; thus preventing an externally initiated land attack. Next, we want to drop obviously unnecessary and noisy traffic that make the bulk of unwanted traffic. To do so, first we must permit http and https to our internal web server and then block traffic to any host using the noisiest list of ports. This list is a matter of opinion and experience for the most part and is likely to change over time. To obtain a list of the most recent noisiest ports on the Internet, visit http://www.dshield.org. Next we permit the remaining traffic destined for a host on GIAC Enterprises public IP space. The last line in the access-list will drop and log whatever is left.

2.2.8 Services explicitly turned on

```
service nagle
service password-encryption
```

"nagle" will turn on congestion control that can help against over-utilization of your bandwidth. Additional information on this service can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt3/frf012.htm#1019552. "password-encryption" will ensure that passwords are stored in a hashed format.

2.2.9 Commands explicitly turned off

```
no service pad
no service dhcp
no ip source-route
no ip bootp server
no ip http server
no ip http secure-server
no cdp run
```

Basically, none of these services are needed or used. The most important services to note here is source-route and cdp. Turning off source-route will prevent potential intruders from specifying a source-route in their packet that could enable them to appear to come perform a man in the middle attack or to successfully hijack a connection or other malicious activity. Turning off cdp is a good idea. It's a protocol used by Cisco devices to learn about and announce the presence to other Cisco devices within the same collision domain. There's no reason to use it for GIAC Enterprises.

2.2.10 Interface settings

```
no ip redirects
no ip unreachables
no ip proxy-arp
```

"no ip redirects" will ensure the router does not send information about potentially better routes. "no ip unreachables" will silence the router from notifying a source host when a system it is trying to connect to can't be reached. "no ip proxy-arp" will ensure the router does not pretend to be an IP address it is not.

2.2.11 The unstated

There were many configuration commands that were entered into the router, but do not show up in the configuration. This is because they are the default value for the version of IOS that is in use. Examples include "no ip direct-broadcast" and "no service tcp-small-servers". A very useful template for starting the configuration of a secure router can be found at http://www.cymru.com/Documents/secure-ios-template.html. Other sources of information are http://www.sans.org/rr/papers/38/242.pdf and http://www.sans.org/rr/paper.php?id=794.

2.3 IP30 Configuration

2.3.1 Basic configuration

The IP 30 devices are configured based upon the configuration document found at http://support.checkpoint.com/kb/docs/public/sofaware/pdf/DAIP_Support.pdf. The IP30 device is permitted access through the VPN tunnel based upon the VPN configuration in the firewall policy. See the firewall policy section for details. Here is a quick list of steps that must be taken to configure the IP30:

- Configure the internal network
- Configure the external network (varies based upon ISP)
- Create a certificate file from the Firewall Management Server and upload it to the IP30 device
- Configure the "firewall" object as a VPN gateway device
- Enable SSL management and configure 206.45.67.120 as an authorized management host
- Specify the "High Security" policy

2.3.2 Internet access rules

In regards to general access to the Internet, the IP30 devices are deployed with the High Security default policy, which is as follows:

Source	Destination	Service	Action	Track
Any	Any	dns, DHCP	Accept	No_Tracking
Home_network	Any	http, https, pop-3, smtp, imap, ftp	Accept	No_Tracking
Home_network	Any	Any	Reject	Long_Tracking
Any	Any	NBT	Drop	No_Tracking

Any	Any	Any	Drop	Long_Tracking

Without implementing backwards compatibility mode on the firewall management server, it is not possible to change this configuration in a centralized manner. The first rule provides for permitting dns and DHCP traffic. DHCP is likely used on the external side for the firewall to achieve its dynamic address from the ISP. DNS resolution is also permitted in the first rule, both from internal hosts and the firewall itself to resolve IPs for use in its logs. In the second rule, the internal network is permitted general basic access to the Internet. It is likely unnecessary to permit pop-3, smtp, imap and ftp, but this provides very limited risk since the connections permitted are outbound only. The third rule will reject (send a Reset) any other connections originating from the internal network. Next, any NBT traffic is blocked without logging so the log files don't get too burdened with this traffic. The final rule ignores and logs any traffic not fitting one of the previous rules.

2.3.3 Implicit rules

The traffic that allows for remote management of the IP30 (TCP981) and the traffic that permits for the VPN tunnel to be established (IPSEC) is implicitly permitted as part of the IP30 configuration. The IP30 device is configured to accept TCP 981 for remote management only from the firewall management systems public NATted IP address (206.45.67.120).

2.4 SecureClient configuration

The SecureClient configuration is controlled from the Policy Server. In the tutorial, the Policy Server is placed on the firewall, but in the real production network, it might be better to put the policy server on the management server. Since the complete rule base for SecureClient users is provided at the very end of the "Firewall security policy/ VPN policy tutorial" section, I will not repeat it here. However, I will outline the purpose for each of the rules.

2.4.1 The rules

Rules 1, 3, 4, and 5 basically are a reiteration of the VPN rules already stated in the firewall policy. The purpose for these rules is covered in more detail in the next section.

Rule 2 is intended to block any inbound access not related to the VPN connection. That is to say, general hosts on the Internet are blocked from connecting directly to the SecureClient host.

Rule 6 permits SecureClient users to connect to general systems on the Internet over http, https and dns. It also provides for ping packets to be sent as a method to test connectivity. This is considered the appropriate minimum access to the Internet for the mobile sales staff.

Rule 7 will block any traffic not defined as allowed as part of the VPN and not permitted for general Internet access under rule 6.

2.4.2 Additional information

The SecureClient users authenticate to the firewall using S/Key, they will need to have an S/Key calculator loaded on their system or use one freely available on the Internet. It is the responsibility of GIAC Enterprises to make a policy in regards to this. Note that due to the configuration of the firewall, SecureClient users will not have the ability to download their topology information. This is an intentional design consideration. It is necessary to temporarily permit this access to the firewall to create a topology file that will then be used in a SecureClient Packaging Tool deployment. This is done with intent to make it difficult for a potential intruder to learn about internal network designs in order to perform an informed attack. It is also advisable to configure SecureClient so that it will not connect to your firewall unless the virus application on the host is running. This helps mitigate against hosts that are infected by virtue of their general connection to the Internet later connecting through the VPN to your internal network and propagating a worm or virus that would have otherwise been stopped by your perimeter defenses.

2.5 Firewall policy

Since the specific rules are provided near the end of the next section, I will not repeat them here. Instead, I will discuss the rule base and the purpose for the rules. It might be useful to print the 3 pages that contain the rules to reference as you read through this section.

2.5.1 SmartDefense

Not shown in the tutorial section is the configuration of SmartDefense. This provides additional protection against some obviously illegal traffic, performs some limited content scanning (such as looking for Code Red), and protects against SYN flood attacks among other things. For this implementation, I have turned on all SmartDefense options with default configuration. This should be done with care as the default values may not be appropriate for every environment.

2.5.2 About ordering

Checkpoint FireWall-1/VPN-1 applies rules in the order in which they are presented. Therefore, it is important to consider the placement of rules to maximize security, performance and the intended access rights. To better facilitate the ordering of these rules, I have specified sections separated with section titles in order to keep the rule sections in an appropriate order. I'll review each of the section titles and discuss why they are placed in the order they are before discussing each rule.

2.5.3 Firewall Access Rules

The security of the firewall itself is critical to the successfulness of your perimeter defenses. Therefore, it's desirable to block any and all access to the firewall as soon as possible. However, there is some traffic that needs to be permitted to the

firewall. Therefore, we will identify connections that require direct access to the firewall first in order to block the remaining traffic to the firewall.

Rule 1 is required for VPN users to connect and SecureClient users to download their policies. If the designed implementation were shown with a separate Management Server, then the Policy Server would reside on this host. This would require this rule to be changed to accommodate for the Policy Server traffic to be permitted to the Management Server instead of the firewall.
Rule 2 is required for the Client Auth rules to work. Administrators will establish a connection on these ports to manually authenticate themselves and open temporary access to the Internet.
Rule 3 is required for the Management Client to be able to connect to the Management Server on the firewall object for the purpose of modifying and installing the policy base. This rule would be drastically different if the Management Server were in the original designed implementation. Specifically, this rule would provide for TCP 18191, TCP 18192, SSH and HTTPS access.

2.5.4 Client Auth Rules

The Client Auth rules are put above the stealth rule because they require connection to the firewall as a part of the way they work. The Client Auth rules are used by administrators to open temporary Internet access from hosts that otherwise would have no outbound access with the specific intent of providing the facility by which they can download patches for servers on these networks.

Rules 4, 5 and 6 are the rules that grant access to the Internet from the Screened, Monitor and Data networks respectively. They are special purposes rules used to allow IT sysadmins to download and install patches to the systems on these networks without leaving the access open at all times, which could pose a security risk if these systems were to become compromised or infected with a virus or trojan.

2.5.5 Stealth Rule

With the first two groups out of the way, we can now block any and all remaining access directly to the firewall.

Rule 7 blocks all access to the firewall. This helps to reduce the risk of fundamental OS compromise of the firewall itself.

2.5.6 VPN Connections

We select VPN connections next because they should be processed quickly for performance reasons and because subsequent block rules could interfere with permitted VPN connectivity if we put it lower in the rule base.

Rule 8 grants any authorized SecureClient user to access the domain controllers and Exchange server over their VPN connection as specified in the VPN needs.

Rule 9 grants the same group of users the ability to open a web connection to the Intranet/Parser system.
Rule 10 permits IT sysadmins the ability to terminal service into servers on the Screened, Data and Monitor network for purpose of being able to administer these systems remotely.
Rule 11 is similar to rule 8, except that it is applied to users connected through an IP30 device.
Rule 12 grants ftp access to the developers so that they can update the content of the Intranet and Web servers.

2.5.7 Internet Inbound

Since the majority of illegitimate traffic in terms of volume is expected to come from the Internet, we want to handle these connections first so we can allow what is permitted and quickly drop the rest. By having these rules high in the rule base, we improve the overall performance of the firewall by dropping illegitimate traffic from the Internet as soon as possible.

Rule 13 gives the outside world the ability to perform DNS queries against GIAC's public DNS servers. Note that only udp queries can be performed. Due to the small size of all expected dns queries, tcp dns queries are unnecessary.
Rule 14 permits general access to the DropChute server over the custom port that GIAC Enterprises has selected for their DropChute connections.
Rule 15 allows the receipt of mail from the outside world.
Rule 16 permits the general public to view the public web server.
Rule 17 provides for the border router to be able to send logs and update its time to the SnortCenter Console.
Rule 18 will drop any traffic that hasn't fit a rule definition as specified above that originated from outside the firewall.

2.5.8 Internet Outbound

Now that we've handled permitted traffic originating from the Internet and dropped the illegitimate traffic, it's now time to do the same for traffic destined for the Internet from internal hosts for the same reason.

Rule 19 allows the specified source devices to synchronize their time with a time server on the public Internet.
Rule 20 gives the Firewall Management system the ability to connect to the SSL management site on IP30 devices so they can be remotely managed.
Rule 21 allows the secondary domain controller to update its virus definitions for Norton in order to redistribute them to internal hosts.
Rule 22 gives the public dns servers the ability to perform outbound dns queries for the purpose of being able to fulfill internal dns queries.
Rule 23 gives the DropChute server the ability to connect to an external DropChute server that has been configured with the non-standard port for purposes of receiving files from GIAC Enterprises.

Rule 24 provides a method for the public mail server to send mail to the outside world.
Rule 25 allows the public mail server to update its F-Prot virus definitions.
Rule 26 allows for the Intranet/Parser system to perform credit card authorizations.
Rule 27 gives users on the corporate network the ability to connect to the border router in order to manage it.
Rule 28 gives users on the corporate network the ability to browse the internet to view http and https based web sites.
Rule 29 allows for the Whatsup Gold monitoring system to monitor any internal host, with the exception of the firewall. It is placed here as any lower would block access to the border router.
Rule 30 will reject any other connections destined for hosts outside the firewall. The usage of "reject" is important here. This means the firewall will send a reset packet back, allowing the internal host to close the half-open session; thus preventing the utilization of excessive system resources.

2.5.9 Pre-block/Management Rules

These rules are used for internal IT management functions. They are placed here in the rule base as subsequent blocking can hinder the ability for these functions to work.

Rule 31 gives users on the corporate network the ability to terminal service to servers on the Data, Screened or Monitor network for remote administration.

2.5.10 Internal traffic to Data network

Now that we've handled the bulk of the traffic, it's time to deal with internal connections. We handle connections to the data network first since this is the network where the most valuable internal resources reside. It's important to block unintentional access as soon as possible so that incorrect rule changes elsewhere are less likely to hinder the security of this network.

Rule 32 gives the web server the ability to access the database on the internal database server in order to populate web requests as permitted based upon the ODBC connection and the internet application.
Rule 33 provides for the DropChute server to transfer files received from suppliers to be processed and for orders entered via the public web server to be transferred for processing as well.
Rule 34 permits users on the corporate LAN to connect to the finance server. This rule should be reviewed for the ability to provide a stricter rule definition.
Rule 35 allows http access to the Intranet server for general business purposes. The ftp access it grants is for developers to be able to change the content of this site when they are working from the office.
Rule 36 will reject the remainder of traffic destined for the data network. "Reject" is used for the same reason here as it was in rule 28.

2.5.11 Internal traffic from Data network

Again, we deal with connections on the Data network, this time with traffic that is sourced from the data network so that we can explicitly block the remaining traffic.

Rule 37 provides for the Intranet/Parser to send completed orders to the DropChute and Web servers in order to complete business transactions.
Rule 38 gives internal hosts the ability to send DNS queries to the public DNS server.
Rule 39 will reject the remaining traffic originating from the data network. “Reject” is used, again, for the same reason as in rule 28.

2.5.12 Remaining rules

Finally, we deal with the other required rules not specified in any of the previous sections.

Rule 40 provides a method for the internal mail server to receive mail from the outside world through the public mail server.
Rule 41 allows for developers to upload new web content to the public web server when they are in the office.
Rule 42 gives IT sysadmins the ability to administer the DNSOne appliances.
Rule 43 gives IT sysadmins the ability to view snort alerts and to connect to administer the SnortCenter Console system.
Rule 44 permits IT staff to view the Whatsup Gold system via the web interface.

2.5.13 Cleanup Rule

The cleanup rule is important. Although the firewall will drop any traffic not explicitly permitted, it does so without logging the data. The cleanup rule explicitly blocks any remaining traffic with logging turned on. Since it blocks any traffic it sees, it should be placed last as any subsequent rules are irrelevant.

Rule 45 provides the function described in the paragraph above.

2.6 Firewall security policy / VPN policy tutorial

The central firewall for GIAC Enterprises is the most critical security infrastructure device. It is responsible for the implementation of the majority of the security access policies and is the VPN gateway for the Enterprise. This tutorial will give a step by step implementation guide for the configuration of the firewall security policy.

Important: Please note that due to resource limitations, I was unable to exactly implement the firewall infrastructure as designed for the purpose of GIAC Enterprises. The important difference is that I deployed the Checkpoint FireWall-1/VPN-1 Enforcement module and Management Server on a single system running Windows 2000 Server. The system that was identified as the

Management Server in the network design was instead a Management Client used to modify the security policy. The impact this change in configuration would have in an actual implementation is one of performance, OS security for the enforcement module and stability of the firewall application.

This tutorial begins assuming the following tasks have been accomplished:

- Base operating system installed on the enforcement module and management server with appropriate security patches.
- IP routing has been enabled in the enforcement module.
- Appropriate modules have been installed (SVN Foundation, FireWall-1/VPN-1, Management/Log Server, Policy Server).

2.6.1 Setting up the global configuration for the firewall

First, we need to add routes for the 192.168.100.0/24 and 192.168.150.0/24 networks to the enforcement module. The route should point to 192.168.20.20. On Windows 2000, you would enter the following commands:

```
route –p add 192.168.100.0 mask 255.255.255.0 192.168.20.20
route –p add 192.168.150.0 mask 255.255.255.0 192.168.20.20
```

In the designed architecture, this would be done on the Nokia platform and would be done through Voyager in the Static Routing management page.

Next, we will ensure that the Management client has the ability to access the Management Server for purposes of modifying the rules and pushing the policy to the firewall. To do so we need to go to the Checkpoint Configuration NG. From the command line on the management server, type “cpconfig”. Select the “Management Clients” tab and enter the host IP of 192.168.100.120 into the “remote hostname” box and select “Add ->”. This will permit the management client system at 192.168.100.120 to connect to the management server for modifying and pushing policies.

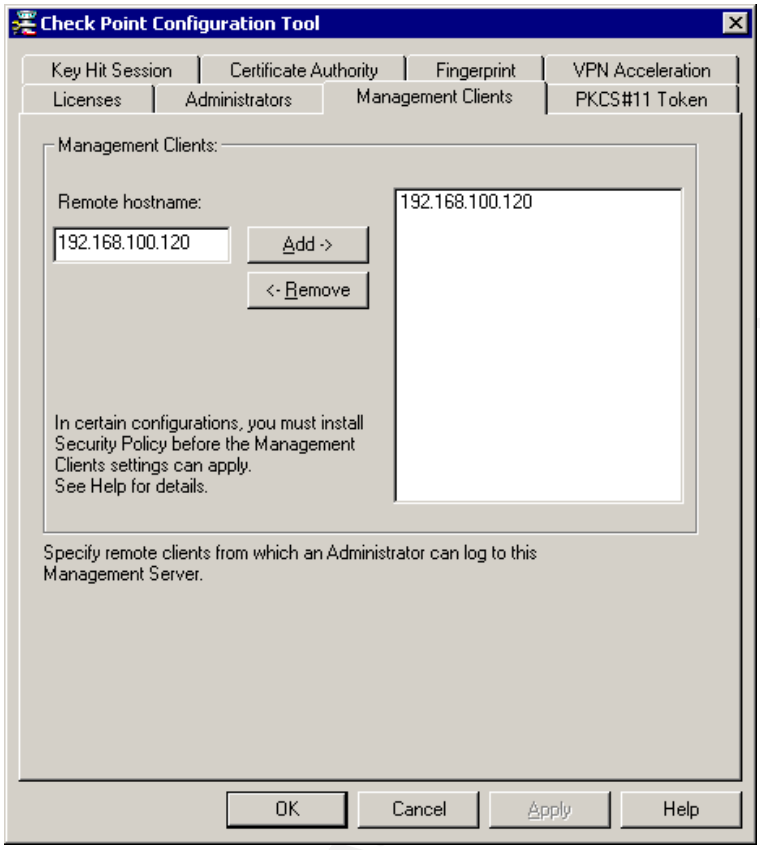


Figure 1

Now all access to modify the firewall configuration should be accessible from the Management Client. This step would be unnecessary with a separate Management Server as originally designed.

After the Smart Client tools have been installed on the management client, you can access the policy editor by entering the user name and password and host IP of the Management server from SmartDashboard as follows:

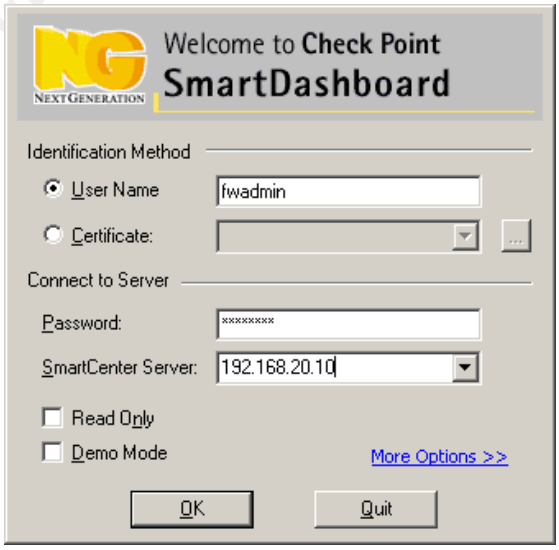


Figure 2

You will be presented with a fingerprint. You should ensure that this fingerprint matches the one provided as part of the initial installation of checkpoint. If it is, then select “Approve”.

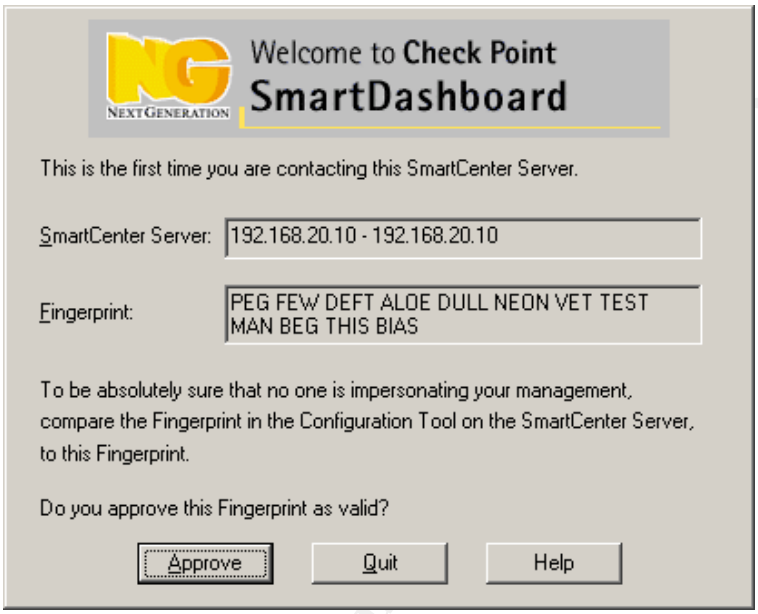


Figure 3

The starting screen will look as follows:

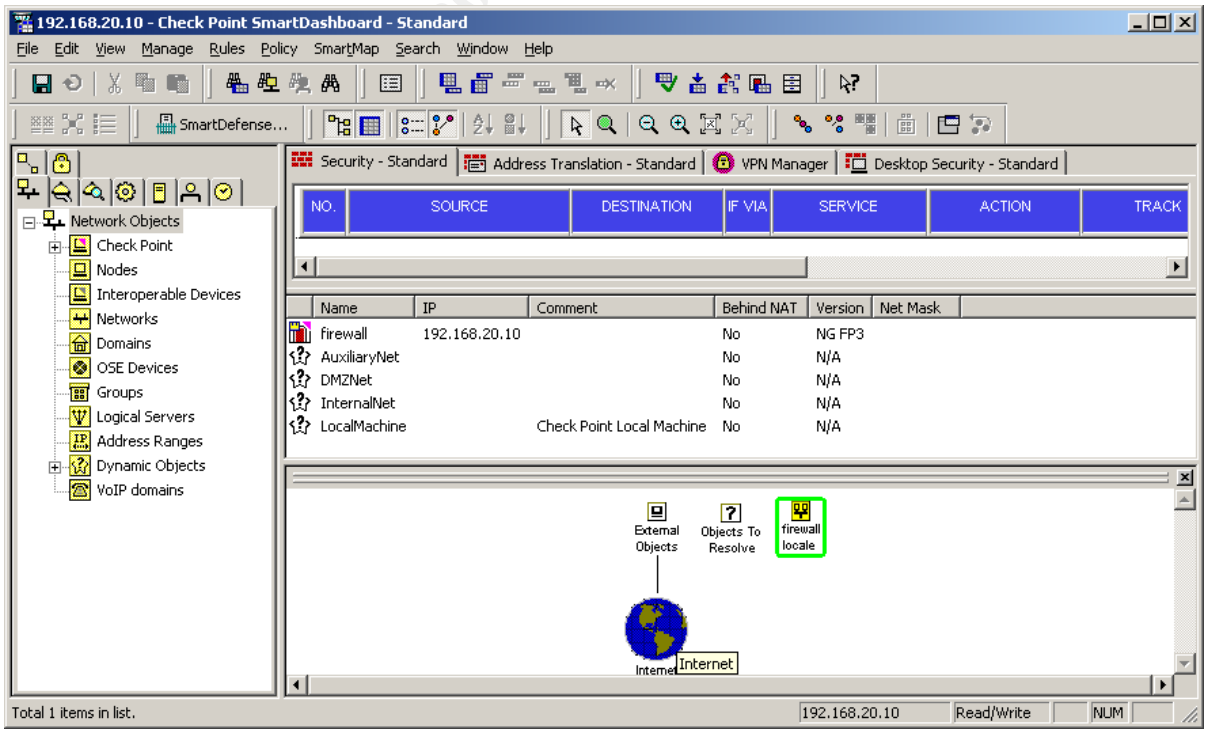


Figure 4

The basic configuration of the firewall object is very important. Before we can begin with this configuration, however, we must configure a few network objects to be used in the firewall object configuration. The following networks must be configured:

Network Name	IP Space	Short description
SN_Internal	192.168.20.0/24	Used to interface with the firewall for various subnets
SN_Monitor	192.168.100.0/24	Used for security and monitor based systems
SN_Corporate	192.168.150.0/24	Used for local workstations and internal servers
SN_Screened	192.168.200.0/24	Used for hosts directly accessed by the outside world
SN_Data	192.168.210.0/24	Used for the critical servers

Here are the instructions for configuring the SN_Internal object. The other subnets can be configured by repeating these instructions and modifying the appropriate information. From the screen displayed in figure 4, in the left pane, right click on “Network” and select “New Network”. Fill in the resulting box as follows:

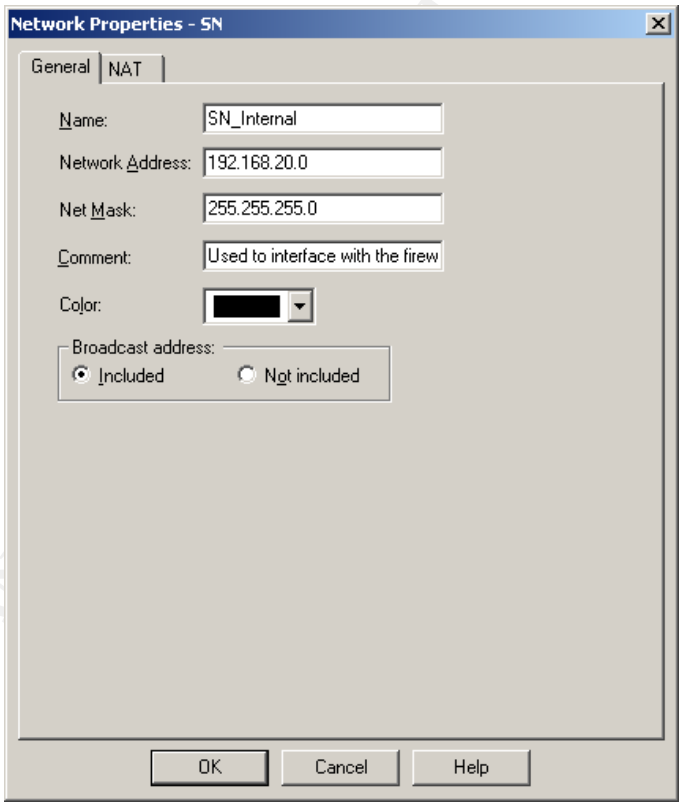


Figure 5

Select “OK” and you’re done. Repeat these steps for the other subnets. When you are finished, you should see something like the following figure on your screen:

	Name	IP	Comment	Behind NAT	Version	Net Mask
	SN_Internal	192.168.20.0	Used to interface with t...	No	N/A	255.255.255.0
	SN_Monitor	192.168.100.0	Used for security and ...	No	N/A	255.255.255.0
	SN_Corporate	192.168.150.0	Used for local workstati...	No	N/A	255.255.255.0
	SN_Screened	192.168.200.0	Used for hosts directly ...	No	N/A	255.255.255.0
	SN_Data	192.168.210.0	Used for the critical ser...	No	N/A	255.255.255.0

Figure 6

Since there are multiple subnets that interface with the 192.168.20.10 interface on the firewall, we'll need to create a group for use with the appropriate subnets to be used in the anti-spoofing configuration of the firewall. On the screen displayed in Figure 4, right click on "Group" and select "New Groups -> Simple Group…" Fill in the information as follows:

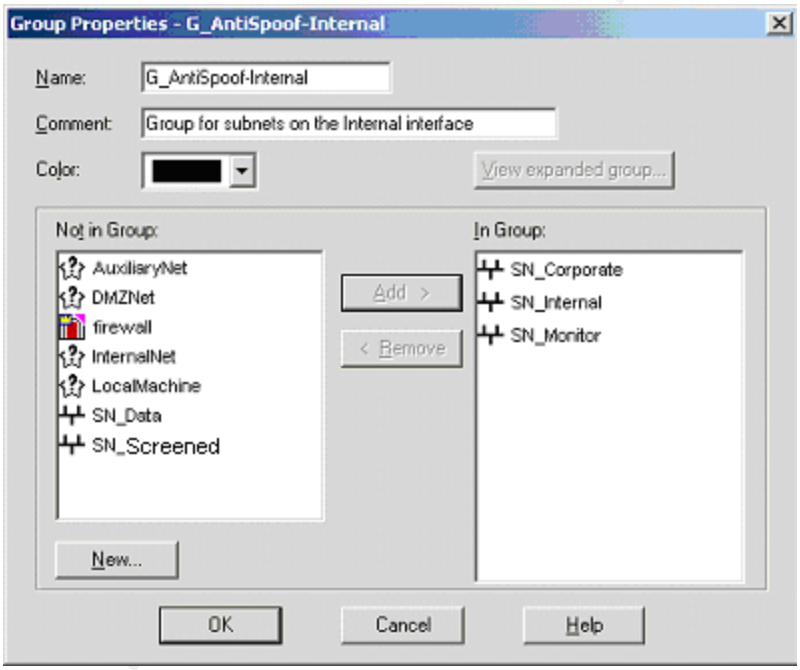


Figure 7

Select "OK" Now we should be ready for configuring the firewall object itself.

Double click on the "firewall" icon or the icon that represents the enforcement module in your policy and select topology. You will need to modify the configuration here to configure anti-spoofing rules. Follow these instructions:

- Highlight the interface with 206.45.67.10 as the IP address. Select edit and go to the topology tab. Select "External" and then click on "OK"
- Highlight the interface with 192.168.200.10 as the IP address. Select edit and go to the topology tab. Under the "Internal" section, select "Specific" and select "SN_Screened" from the drop down box and click "OK".

- Highlight the interface with 192.168.210.10 as the IP address. Select edit and go to the topology tab. Under the “Internal” section, select “Specific” and select “SN_Data” from the drop down box and click “OK”.
- Highlight the interface with 192.168.20.10 as the IP address. Select edit and go to the topology tab. Under the “Internal” section, select “Specific” and select “G_AntiSpoof-Internal” from the drop down box and click “OK”,

The resulting configuration should look as follows (interface names may differ):

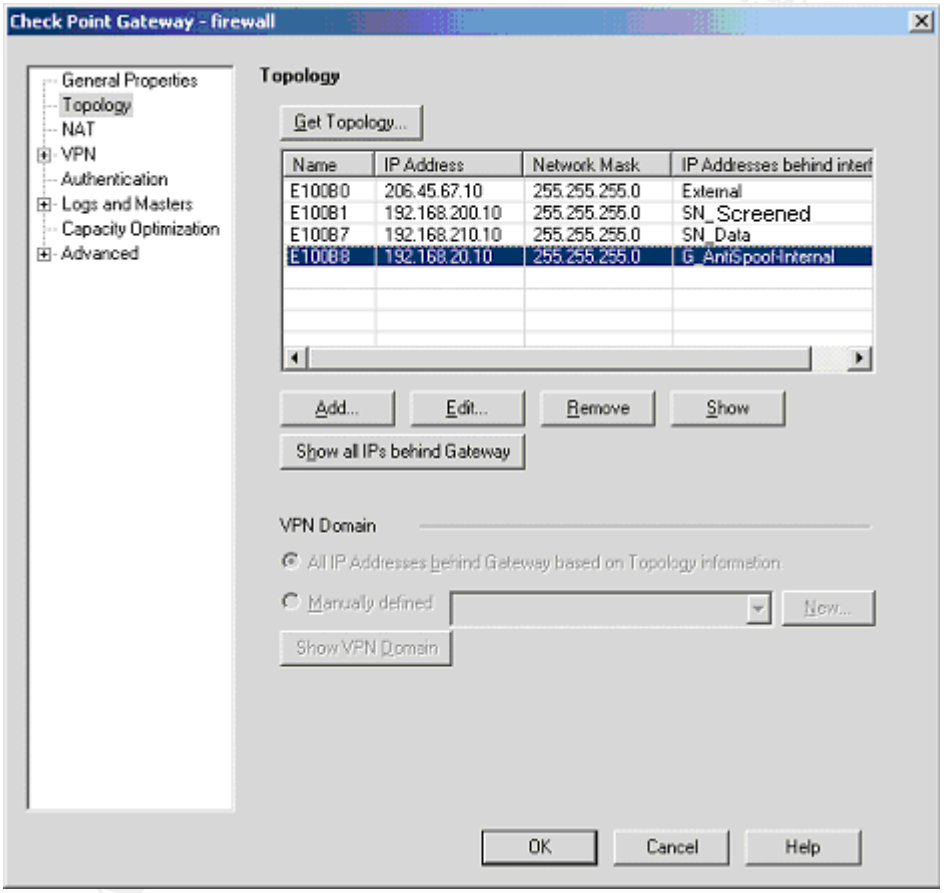


Figure 8

Next, let’s prepare the firewall module for the authentication methodology that will be used for VPN and authenticated connections. In the screen shown in figure 8, select “Authentication” from the left hand pane. In the “Enabled Authentication Schemes:” section, change it so that “S/Key” and “VPN-1 & FireWall-1 Password” are the only options selected. S/Key is selected for the VPN authentication parameter because there was a stated desire to provide one time passwords, but there was no desire to spend any money to provide this capability. Given these requirements S/Key is the best alternative since S/Key calculators can be freely obtained and no additional licensing cost would be

required. GIAC Enterprises will need to select what S/Key calculator they will use for the SecureClient users. Select “OK” and you’re finished with the configuration of the firewall object.

The “Global Properties” for the firewall should be addressed next. These configuration parameters affect some settings that can affect how the firewall handles some administrative functions with regards to dealing with potentially bad traffic and permitting certain controls. To access the global properties, select “Policy -> Global Properties” from the top of the window shown in figure 4. In the initial screen, we want to change the configuration so the only the “Log implied rules” option is turned on. Since we are building a restrictive firewall, we do not want any hidden rules to be enforced. Instead, we want to explicitly define all connections that are permitted. Although this theoretically makes the need to log implied rules unnecessary, it’s still good practice to log whenever possible. The resulting configuration should like as follows:

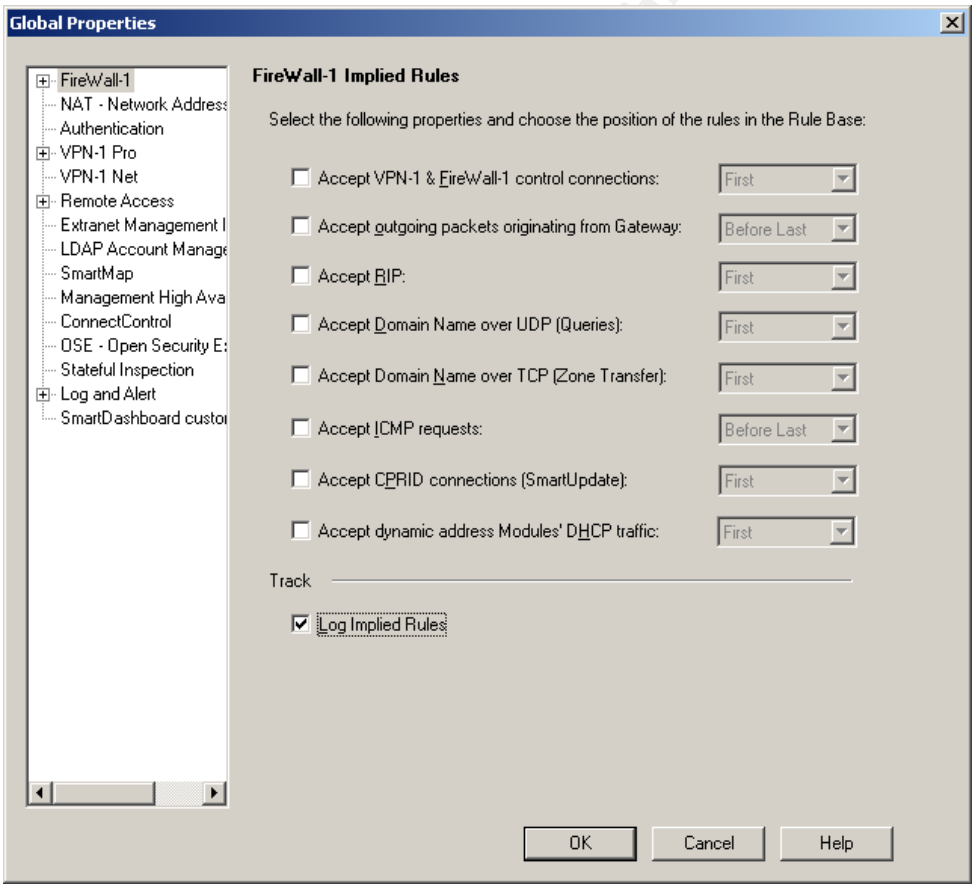


Figure 9

In the “NAT – Network Address Translation” section we need to select the box that says “Enable IP Pool NAT…” so that we will be able to apply a NAT translation for SecureClient users in order to prevent potential IP address conflicts. Also, select log for the two subsections beneath this configuration.

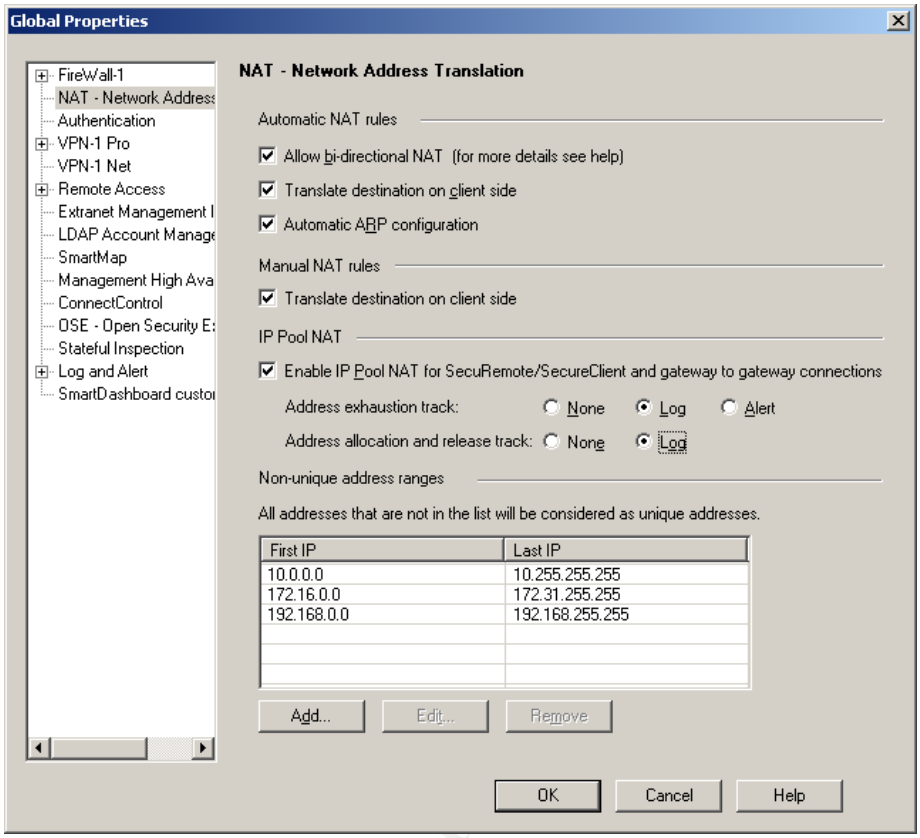


Figure 10

All of the other default global properties should be acceptable.

2.6.2 Network object definitions

In order to apply the security policy appropriately, we must have the appropriate network objects configured. First, let's handle the host objects. This table identifies the host objects that must be defined:

Host Name	IP Address	Description
Border_Router	206.45.67.20	Border Router
Ext_CCAuth	64.94.118.66	Credit Card Authorization Host
Ext_Fprot	213.220.100.3	F-Prot Antivirus update server
FW_Mgmt_Client	192.168.100.120	Firewall management client
GIAC-Database	192.168.210.30	Stores the cookie sayings database
GIAC-DC1	192.168.150.40	Primary Domain Controller
GIAC-DC2	192.168.150.50	Secondary Domain Controller
GIAC-DNS1	192.168.200.12	Primary DNS Server
GIAC-DNS2	192.168.200.13	Secondary DNS Server
GIAC-Dropchute	192.168.200.16	DropChute Server
GIAC-Exchange	192.168.150.60	Internal Exchange Server
GIAC-Fin_Payroll	192.168.210.25	Hosts the accounting and payroll software
GIAC-Imail	192.168.200.15	Public Mail Server
GIAC-Intranet_Parser	192.168.210.20	Hosts the Intranet and Parsing engine

GIAC-WEB	192.168.200.14	Public Web Server
SnortCenter_Console	192.168.100.100	IDS Management System
Whatsup_Gold	192.168.100.110	Whatsup Gold monitoring system

To configure these host objects, right click on the “Nodes” icon from Figure 4 in the left pane and select “New Nodes -> Host”. Fill in the appropriate information. The first host will look as follows:

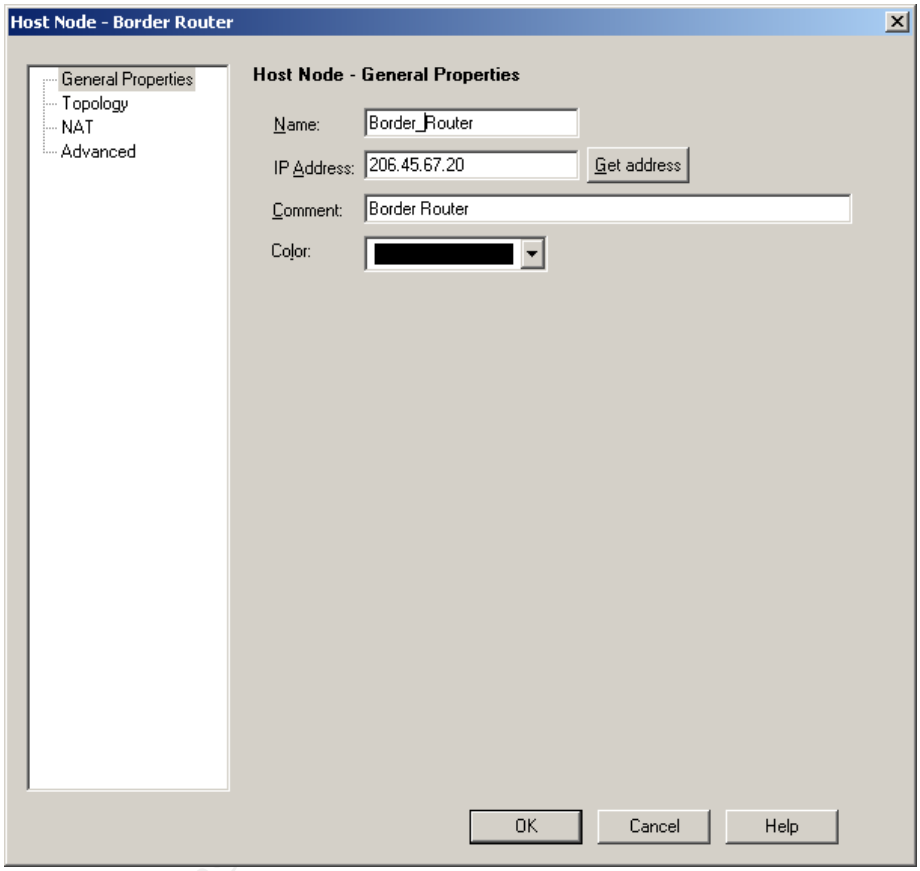


Figure 11

The rest of the host entities will work the same, filling in the values from the table above. When you are done, the host list should look as follows:

Name	IP	Comment	Behind NAT	Version	Net Mask
Border_Router	206.45.67.20	Border Router	No	N/A	
Ext_CCAuth	64.94.118.66	Credit Card Authorization Host	No	N/A	
Ext_Fprot	213.220.100.3	F-Prot Antivirus update server	No	N/A	
FW_Mgmt_Client	192.168.100.120	Firewall managment client	No	N/A	
GIAC-Database	192.168.210.30	Stores the cookie sayings database	No	N/A	
GIAC-DC1	192.168.150.40	Primary Domain Controller	No	N/A	
GIAC-DC2	192.168.150.50	Secondary Domain Controller	No	N/A	
GIAC-DNS1	192.168.200.12	Primary DNS Server	No	N/A	
GIAC-DNS2	192.168.200.13	Secondary DNS Server	No	N/A	
GIAC-Dropchute	192.168.200.16	DropChute Server	No	N/A	
GIAC-Exchange	192.168.150.60	Internal Exchange Server	No	N/A	
GIAC-Fin_Payroll	192.168.210.25	Hosts the accounting and payroll software	No	N/A	
GIAC-Imail	192.168.200.15	Public Mail Server	No	N/A	
GIAC-Intranet_Pa...	192.168.210.20	Hosts the Intranet and Parsing engine	No	N/A	
GIAC-WEB	192.168.200.14	Public Web Server	No	N/A	
SnortCenter_Cons...	192.168.100.100	IDS Management System	No	N/A	
Whatsup_Gold	192.168.100.110	Whatsup Gold monitoring system	No	N/A	

Figure 12

The required subnet network objects have already been defined as part of the firewall object configuration. All that's left in this section is one additional group object and a NAT pool. Follow the instructions from the firewall object configuration information in regards to creating a group and create a group called G_InternalNets with all subnet entities as members. To create the pool of addresses for SecureClient users, right click on address ranges from the left pane in figure 4 and select "New Address Range". Configure the object as follows:

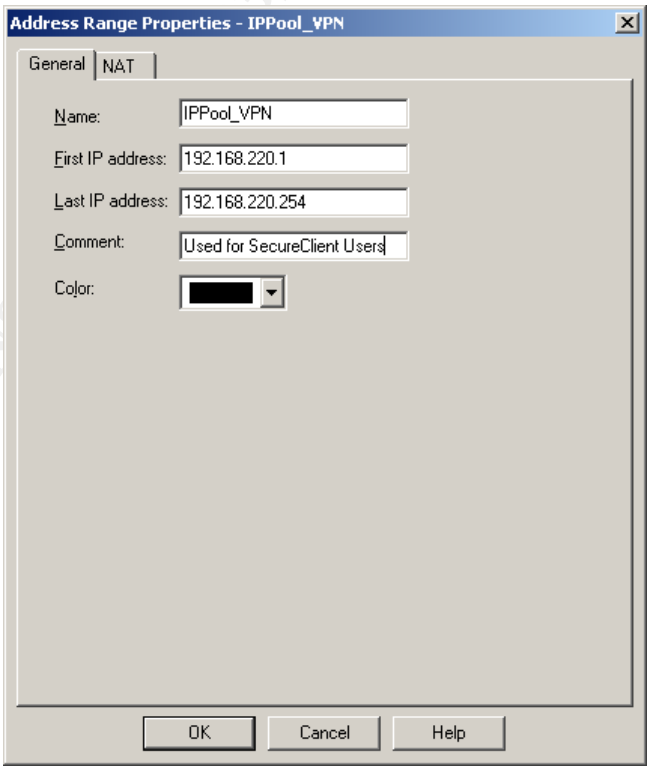


Figure 13

To specify this IP Pool for use by SecureClient users, edit the firewall object and select the VPN tab. Make it look as follows:

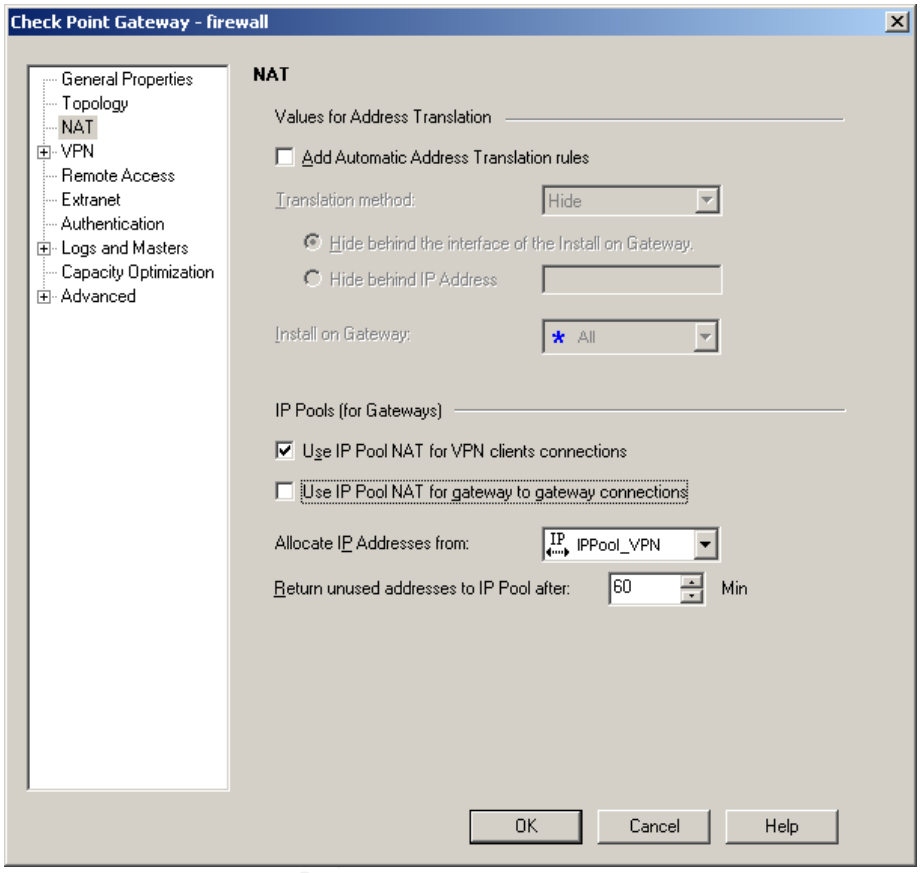


Figure 14

Note: If these objects are not configurable, ensure the “VPN-1 Pro” is selected under “General Properties” for the firewall object.

Now that we have completed the creation of the all the network objects, it’s time to apply the NAT configuration. First, let’s deal with the static NAT configurations. Static NATs apply to address translations that map one external IP to one internal IP address and are used whenever a connection is initiated from the outside to the inside. The following table outlines the static NATs that must be applied:

Host Name	Public IP	Internal IP
GIAC-DNS1	206.45.67.12	192.168.200.12
GIAC-DNS2	206.45.67.13	192.168.200.13
GIAC-WEB	206.45.67.14	192.168.200.14
GIAC-Imail	206.45.67.15	192.168.200.15
GIAC-DropChute	206.45.67.16	192.168.200.16
SnortCenter_Console	206.45.67.101	192.168.100.100
FW_Mgmt_Client	206.45.67.120	192.168.100.120

To apply the static NAT configuration, edit the associated network object and select NAT in the left hand pane. Modify the configuration by checking the “Add Automatic Address Translation rules” checkbox, select “Static” in the “Translation Method” and entering the associated public IP address in the “Translate to IP Address” text box. When you are done, click on “OK”. The following image shows the configuration for GIAC-DNS1.

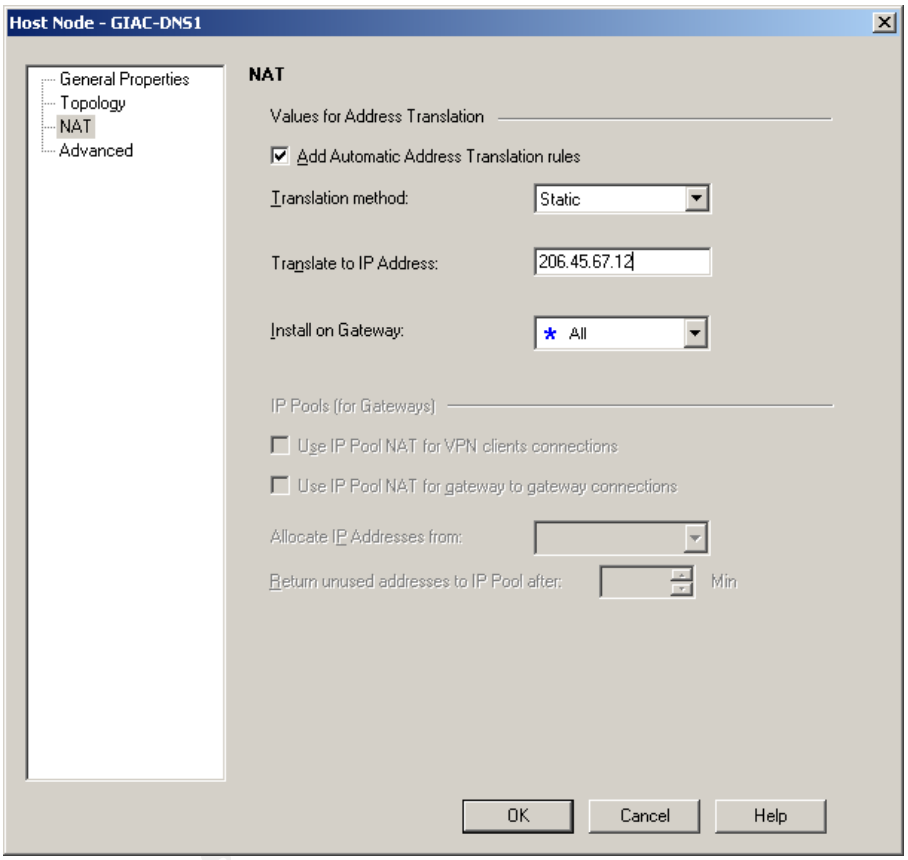


Figure 15

Next, we must specify the Hide NAT configurations. Hide NAT is used whenever connections are initiated from an internal host to an external host. This is basically a proxying configuration whereby many internal hosts can “hide” behind one public IP address. Hide NATs are typically applied to subnet entities. The following table outlines the necessary Hide NATs:

Network	Public IP	Internal IP
SN_Monitor	206.45.67.100	192.168.100.0/24
SN_Corporate	206.45.67.150	192.168.150.0/24
SN_Data	206.45.67.210	192.168.210.0/24

To apply the Hide NAT configuration, edit the associated network object and select NAT in the left hand pane. Modify the configuration by checking the “Add

Automatic Address Translation rules" checkbox, select "Hide" in the "Translation Method" and entering the associated public IP address in the "Hide behind IP Address" text box. When you are done, click on "OK". The following image shows the configuration for SN_Monitor:

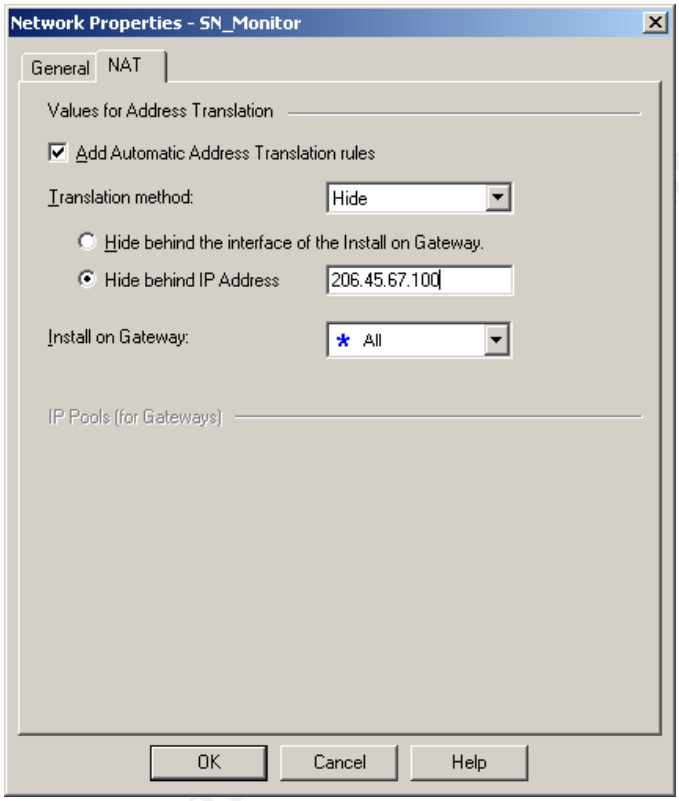


Figure 16

The final step is to create a negate NAT for internal communication. That is to say, whenever traffic travels from one internal network to another internal network, we want to avoid using NAT. To do this, select the "Address Translation" tab at the top of figure 4. Then click on the  icon at the top of the screen to add a new NAT rule to the top of the list. Right click in the "Source" column on the left and select "Add". Find and highlight the G_InternalNets group from the drop down box and click on "OK". Do the same for the destination column. The resulting configuration will prevent potential problems that occasionally result from your firewall NATting when it may not be necessary. It will also provide a clearer view of potential intrusion attempts that originate from internal hosts in your IDS systems.

NO.	ORIGINAL PACKET			TRANSLATED PACKET		
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
1	G_InternalNets	G_InternalNets	Any	Original	Original	Original

Figure 17

2.6.3 Creating Users and User Groups

Next we must create the users and user groups that will be used for authentication for VPNs and for conditional access. The following table specifies the users that we will need to configure:

User name	Auth Type	Purpose for account
authna1	VPN-1/FW-1 Passwd	Special access account for Network/Security Admin 1
authsa1	VPN-1/FW-1 Passwd	Special access account for Sysadmin 1
authsa2	FW-1/VPN-1 Passwd	Special access account for Sysadmin 2
centralcon1	S/Key	Mobile sales consultant 1 Central VPN Account
centralcon2	S/Key	Mobile sales consultant 2 Central VPN Account
dsmgrcentral	S/Key	District Sales Manager Central VPN Account
dsmgreast	S/Key	District Sales Manager East VPN Account
Dsmgrintl	S/Key	District Sales Manager International VPN Account
dsmgrwest	S/Key	District Sales Manager West VPN Account
eastcon1	S/Key	Mobile sales consultant 1 East VPN Account
eastcon2	S/Key	Mobile sales consultant 2 East VPN Account
intlcon1	S/Key	Mobile sales consultant 1 International VPN Account
mgrvendpr	S/Key	Mgr of Vendor/Partner Relations VPN Account
netadm1	S/Key	Network/Security Admin VPN Account
prcon1	S/Key	Partner relations consultant 1 VPN Account
sysadm1	S/Key	Sysadmin 1 VPN Account
sysadm2	S/Key	Sysadmin 2 VPN Account
vencon1	S/Key	Vendor relations consultant 1 VPN Account
vencon2	S/Key	Vendor relations consultant 2 VPN Account
vpofsales	S/Key	VP of sales VPN Account
westcon1	S/Key	Mobile sales consultant 1 West VPN Account
westcon2	S/Key	Mobile sales consultant 2 West VPN Account

To configure a user, select the  icon from the left pane of Figure 4. Then right click on “User” and select “New User -> Default”. Fill in the login name specified above.

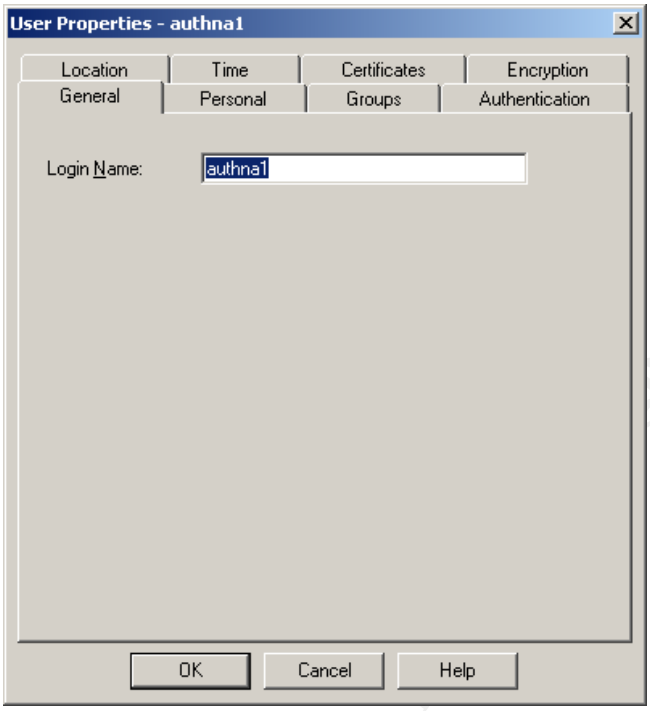


Figure 18

Next, click on the personal tab and fill in the information from the “purpose for account” table above into the comment field.

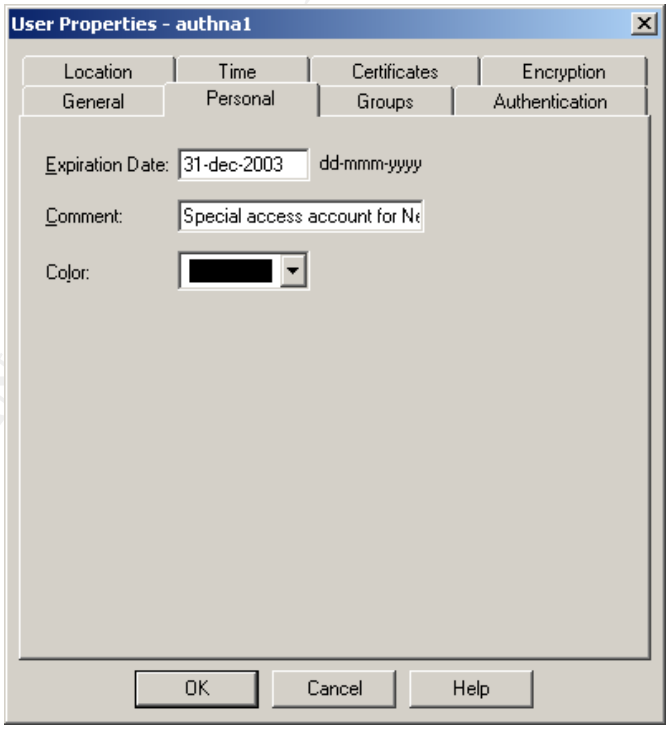


Figure 19

On the “authentication” tab, select the authentication type specified in the table above in the “authentication scheme” drop down box. For VPN-1/FW-1 password, click on “Change Password” and enter the desired password for the specified account.

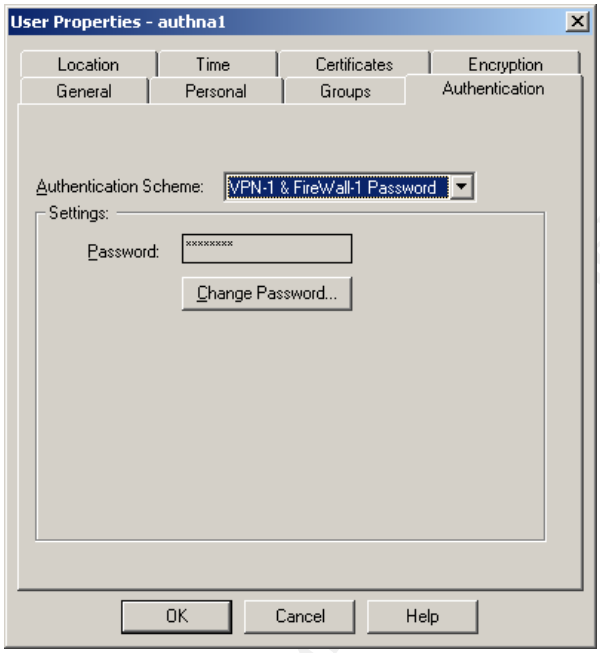


Figure 20

For S/Key users, leave the seed field alone. The secret key is the password the user will need to know. The length field is the number of time the user can use the specified password. You should select the firewall object in the “Installed on” section. Select “MD5” under method. When everything has been filled in, click on “Generate”. A completed screen looks as follows:

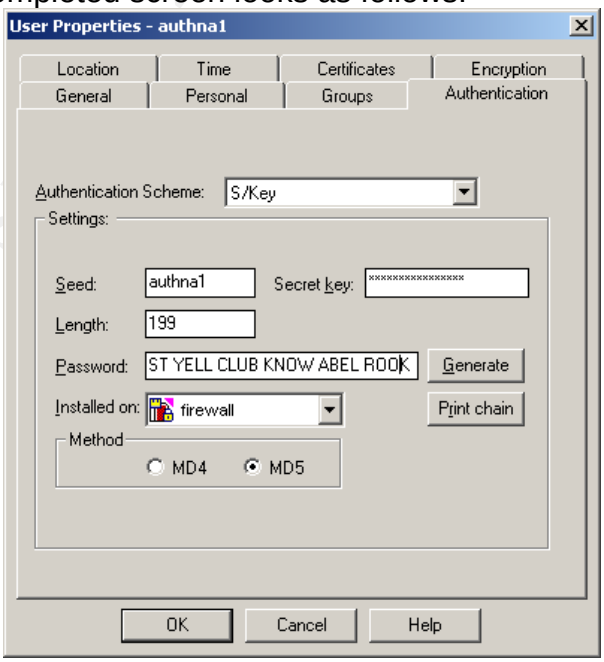


Figure 21

Next, go to the Encryption tab and select the “IKE” box and select “Log” in the authentication track area.

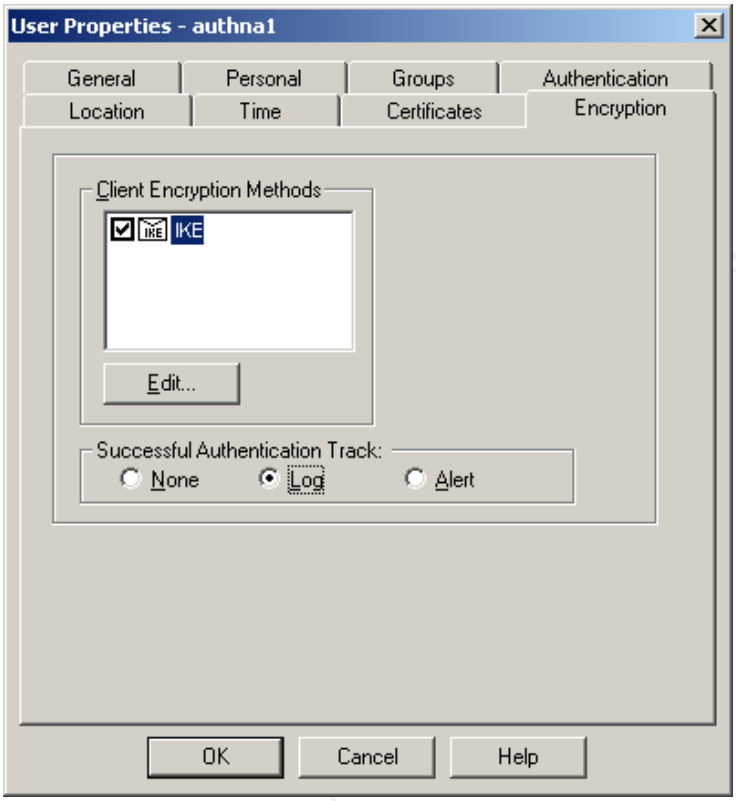


Figure 22

Click on “OK” and you’re done. Repeat this process for all of the users in table above. Now it’s time to make the user groups. The following table specifies the required user groups and the members:

Group	Members	Purpose
Auth_Admin	authna1, authsa1, authsa2	Permit special access for web utilization
VPN_Admin	sysadm1, sysadm2, netadm1	VPN group for IT admins
VPN_General	centralcon1, centralcon2, dsmgrcentral, dsmgreast, dsmgrintl, dsmgrwest, eastcon1, eastcon2, intlcon1, mgrvendpr, netadm1, prcon1, vencon1, vencon2, vpofsales, westcon1, westcon2	VPN group for mobile sales
VPN_All	All users except authna1, authsa1, authsa2	Group used for Policy Server config

To configure a group, select the  icon from the left pane of Figure 4. Then right click on “Groups” and select “New Group”. Fill in the group name specified above and populate the “Comment” text box with the information in the purpose field from the table above. Last, move all of the members specified from the table

above from the list on the left to the list on the right. Here is an example of the "Auth_Admin" group:

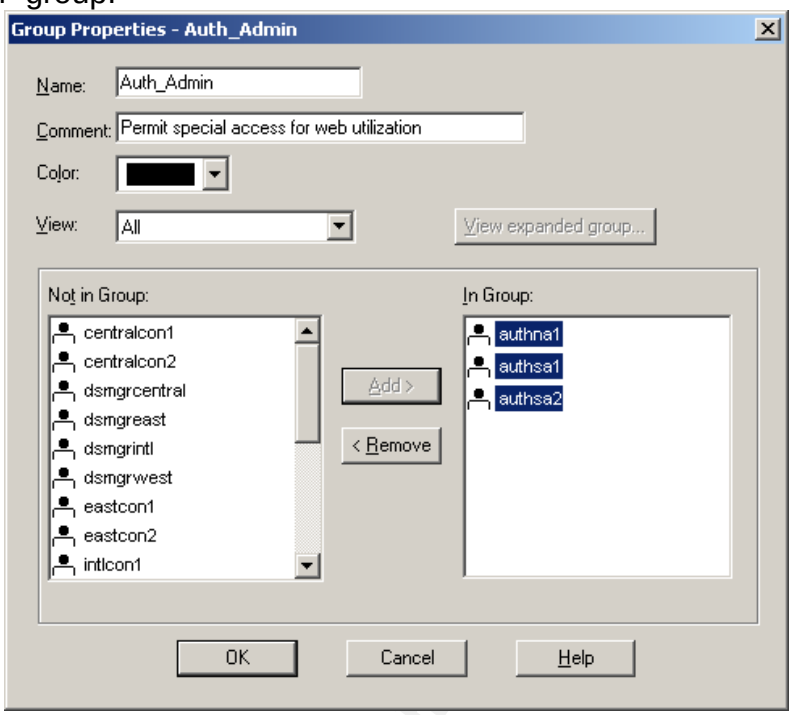


Figure 23

2.6.4 Service definitions

Next, we'll need to create a few services that weren't already included in the service database as part of the Checkpoint install. Specifically, we'll need to create TCP services for the following ports: 981, 2030, 2847, 3389. To create a service, click on the  icon at the top left of figure 4. Right click on "TCP" and select "New TCP". Enter "TCP<portnumber>" for the name, and then enter the port number in the "Port" text box.

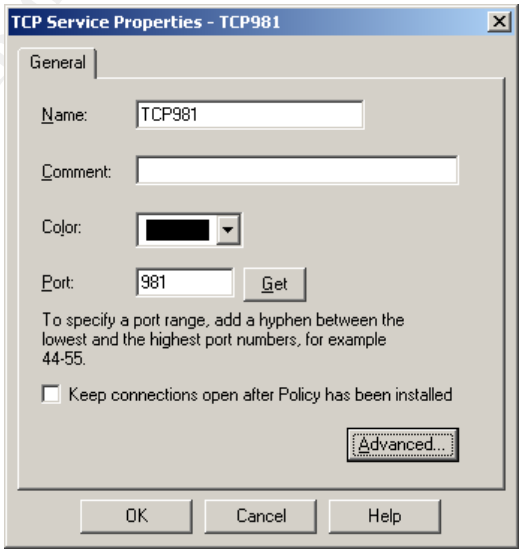


Figure 24

Click on “OK” and you’re done.

2.6.5 VPN Community preparation

Now it is time to prepare the VPN communities for connection with the IP30 Satellite devices. First we need to create subnet entities for the home network of the five employees who have IP30’s deployed to work from home. Create subnet entities according to the instructions shown above with the following table:

Name	Network IP Space	Comment
SN_Rev1	192.168.30.0/24	Reviewer 1 home network
SN_Revn2	192.168.31.0/24	Reviewer 2 home network
SN_Rev3	192.168.32.0/24	Reviewer 3 home network
SN_Dev1	192.168.33.0/24	Developer home network
SN_SnrDev1	192.168.34.0/24	Senior Developer home network

Next, we’ll need to create Checkpoint objects for each of the remote IP 30 devices. We’ll configure all of the IP30 gateways with dynamic addresses. The impact of this configuration is the certificates must be used for the VPN configuration and VPN tunnels will always be initiated from the remote side.

The following devices will need to be configured:

Gateway Name	Comment
GW-Rev1	Reviewer 1 home network
GW-Rev2	Reviewer 2 home network
GW-Rev3	Reviewer 3 home network
GW-Dev1	Developer home network
GW-SnrDev1	Senior Developer home network

Right click on “Check Point” in the left pane of the screen shown in figure 4. Select “New Check Point -> Gateway”. Accept the default “Classic Mode” and click on “OK”. Fill in the name box with the information from the table above. Select “Dynamic Address” to specify that the gateway has its public IP address dynamically assigned. Fill in the “Comment” text box with the information from the table. The resulting configuration should look as follows:

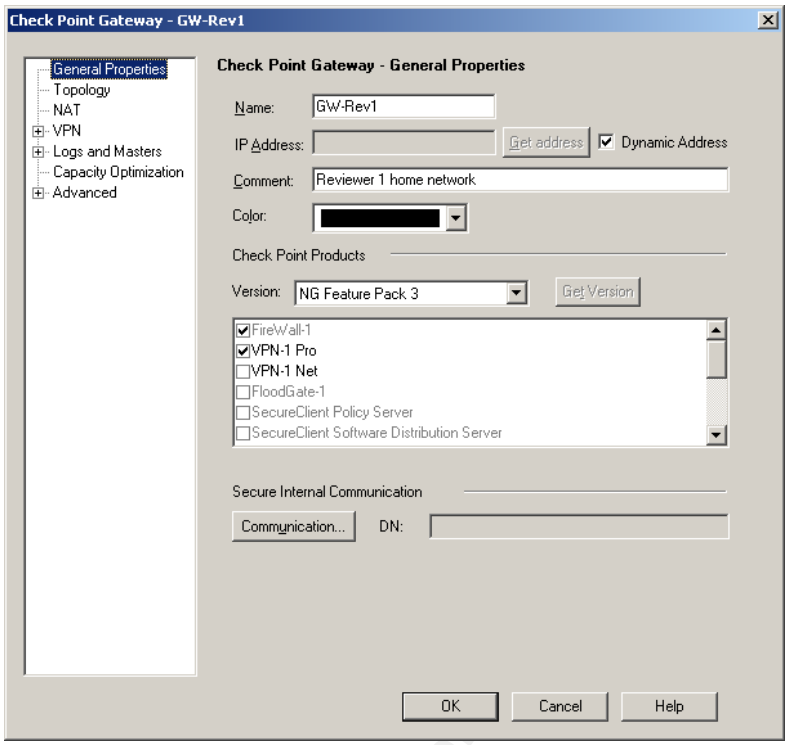


Figure 25

Next, click on the “Topology” selection from the left pane in figure 24. Click on “Add” to add an interface to this device. Enter “External” in the name box and select the “Dynamic IP” check box.

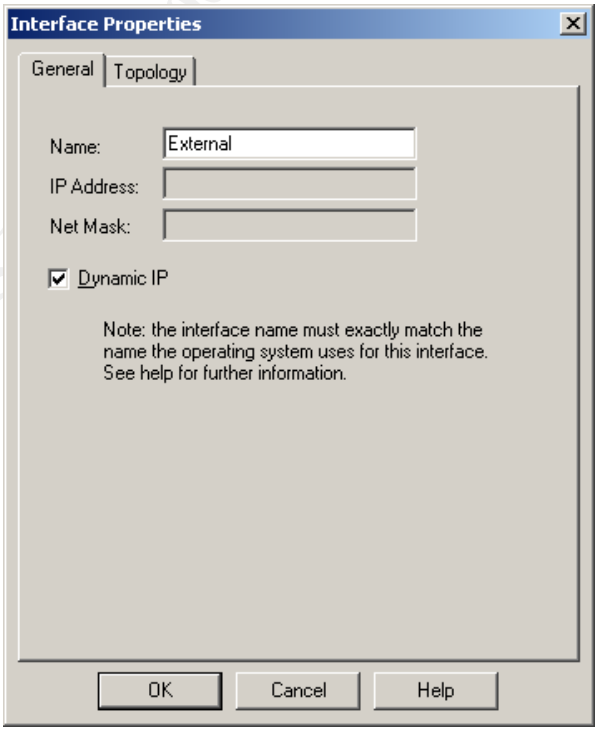


Figure 26

Click on the “Topology” tab and check the “Perform Anti-Spoofing based on interface toplogy” check box.

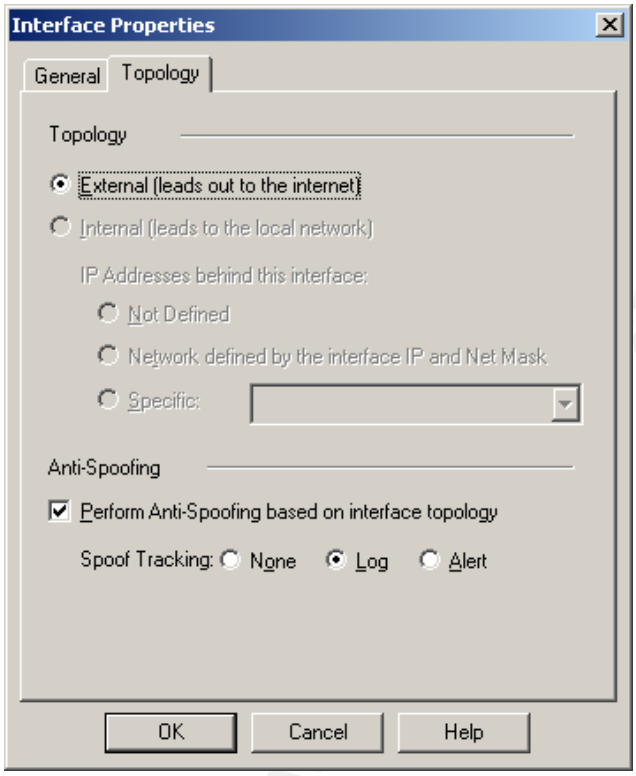


Figure 27

Click on “OK”. Click on “Add” again and specify “Internal” in the name field. Specify the internal network to match the private network behind the specified gateway.

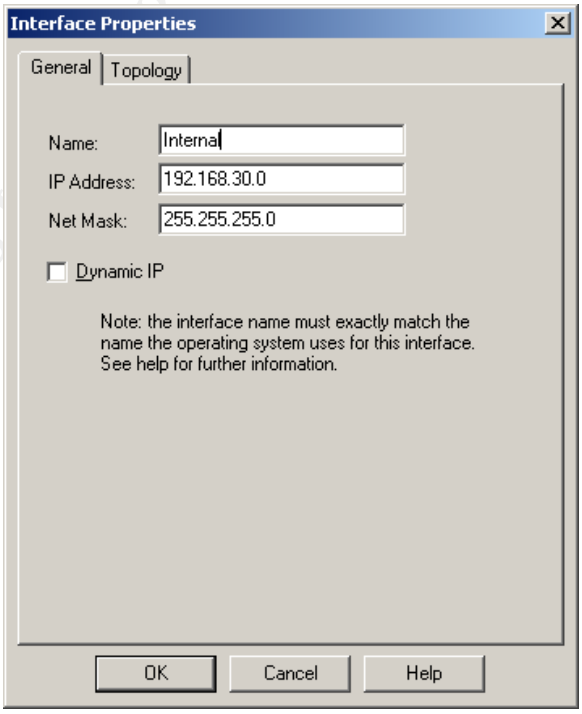


Figure 28

Select the topology tab and select the “Specific” radio button. Select the appropriate network that is behind the specified device in the drop down box.

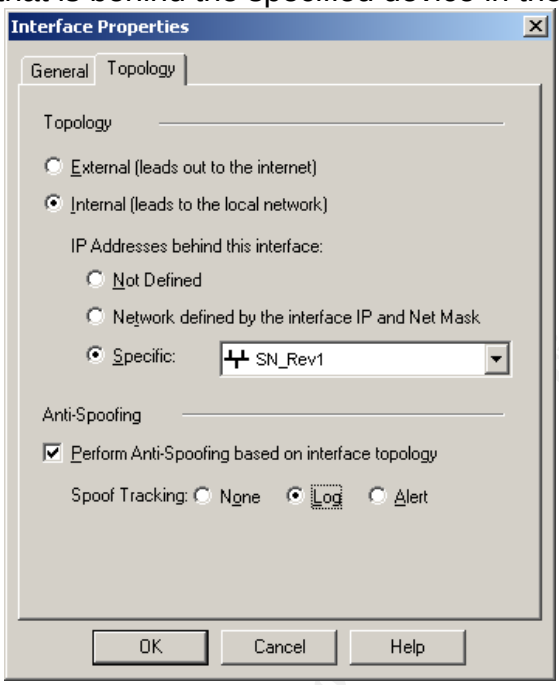


Figure 29

Click on “OK”. Click the “Manually defined” radio button and select the associated subnet entity for the home network of the device that is being configured.

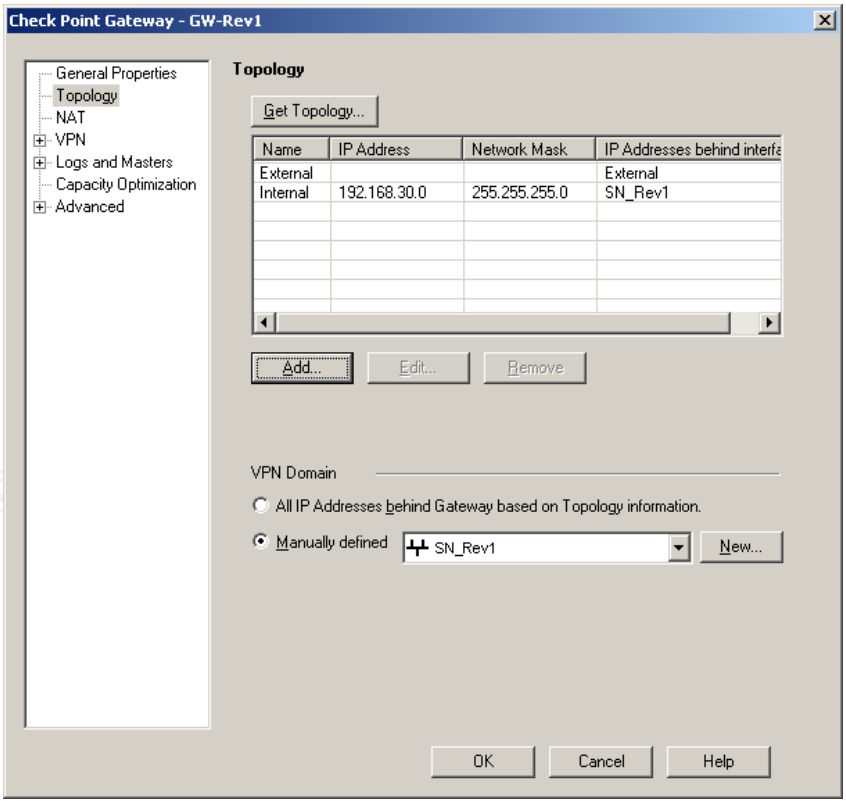


Figure 30

Select “OK”. A window will appear to notify you that IKE properties for the configured device will be set and a certificate will be created. Select “OK”.

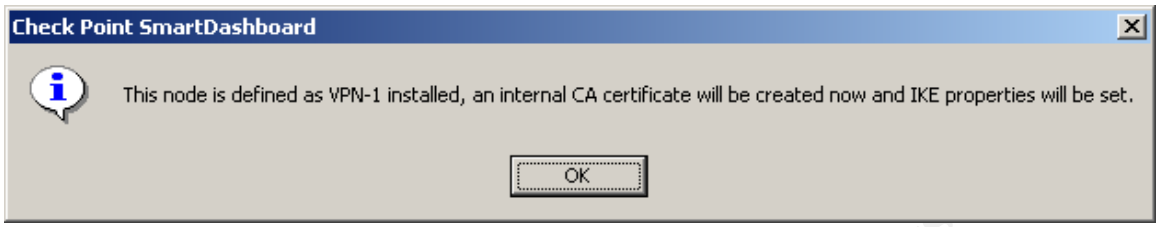


Figure 31

Click on “OK” on the subsequent box that notifies you the certificate has been created. Repeat this process for each IP30 gateway device listed in the table above.

Next we need to go the “VPN Manager” tab from the top of the screen displayed in figure 4. We will need two VPN communities according to the following table:

Community Name	Members	Comment
Comm-Dev	GW-Dev1, GW-SnrDev1	Developer's VPN Community
Comm-Rev	GW-Rev1, GW-Rev2, GW-Rev3	Reviewer's VPN Community

Right click in the top pane next to “Remote Access”, but not on it, and select “New Community -> Star”. Fill in the name and comment from the table above.

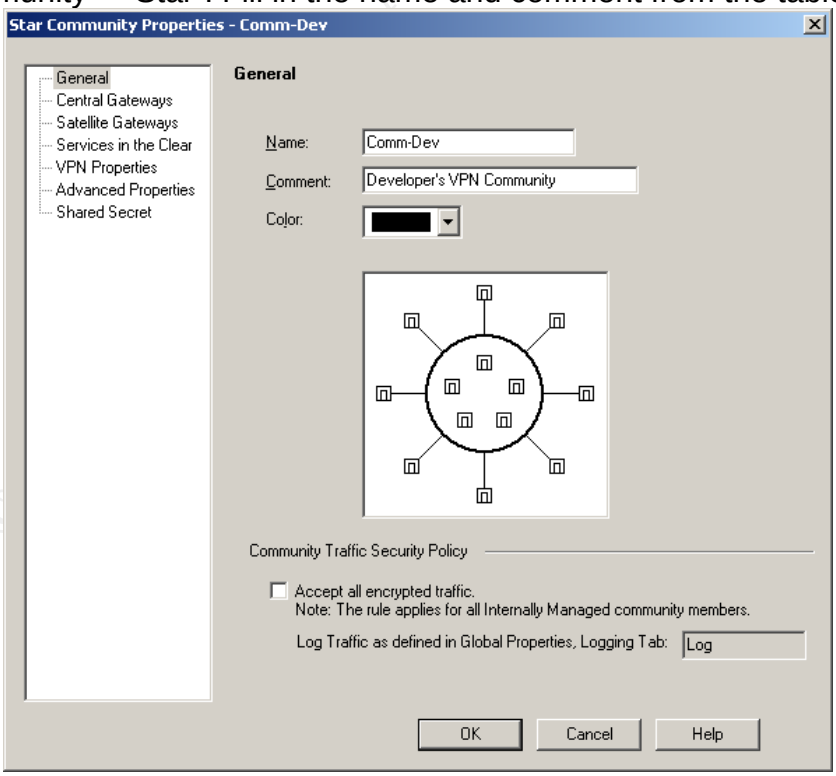


Figure 32

Click on “Central Gateways” in the left pane and click on “Add” to select your “firewall” network object.

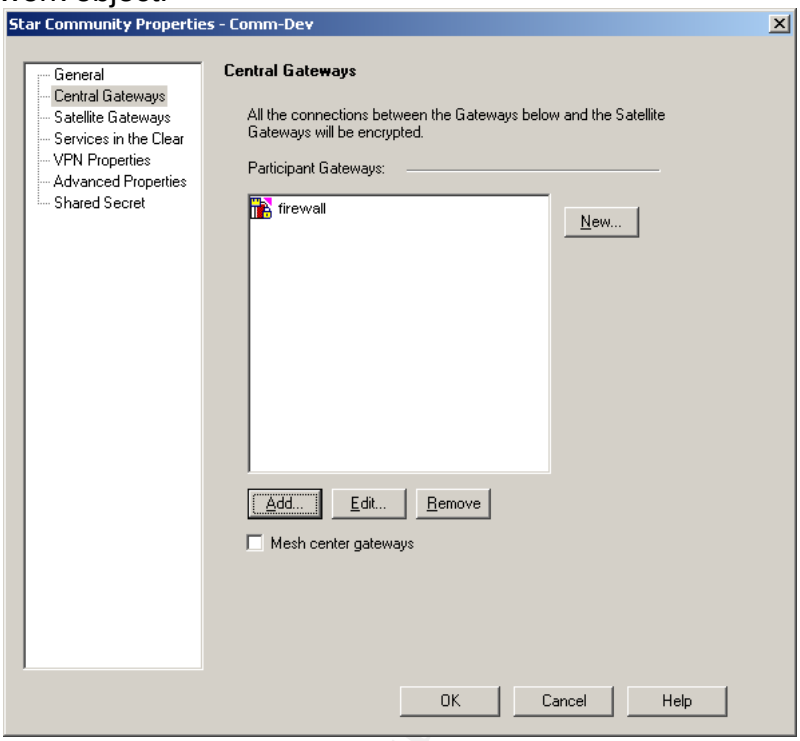


Figure 33

Next, click on “Satellite gateways” and select the associated gateways for the community from the table above.

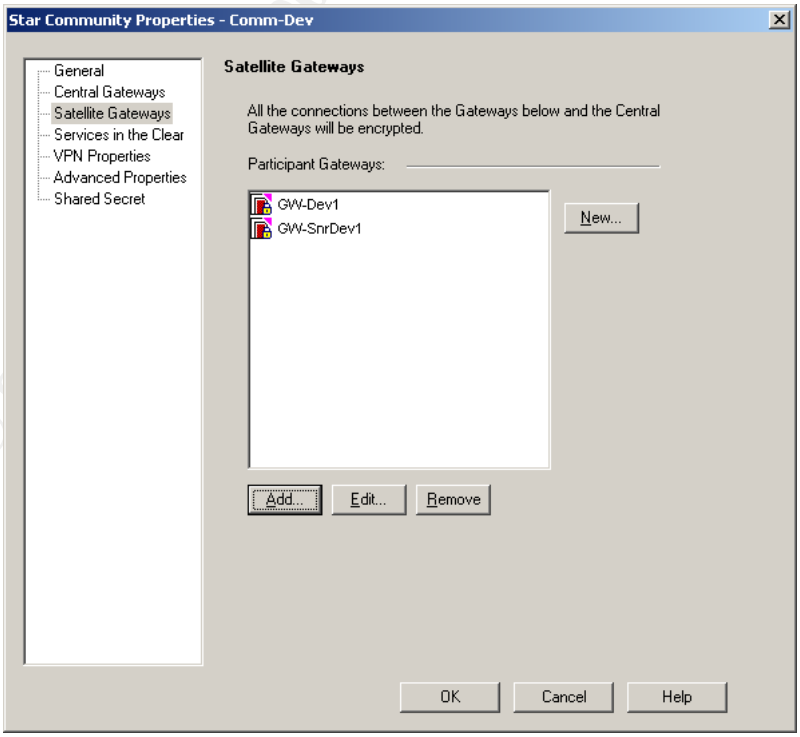


Figure 34

The remaining default values should be appropriate. More complete instructions for this configuration can be found at http://support.checkpoint.com/kb/docs/public/sofaware/pdf/DAIP_Support.pdf.

Now that users and user groups are defined, we need to revisit the firewall object and configure it as the Policy Server for SecureClient users. Edit the "firewall object". On the first screen, select the check box next to "SecureClient Policy Server". Next, click on "Authentication" in the left pane and in the "Policy Server" section, select the "VPN_All" group.

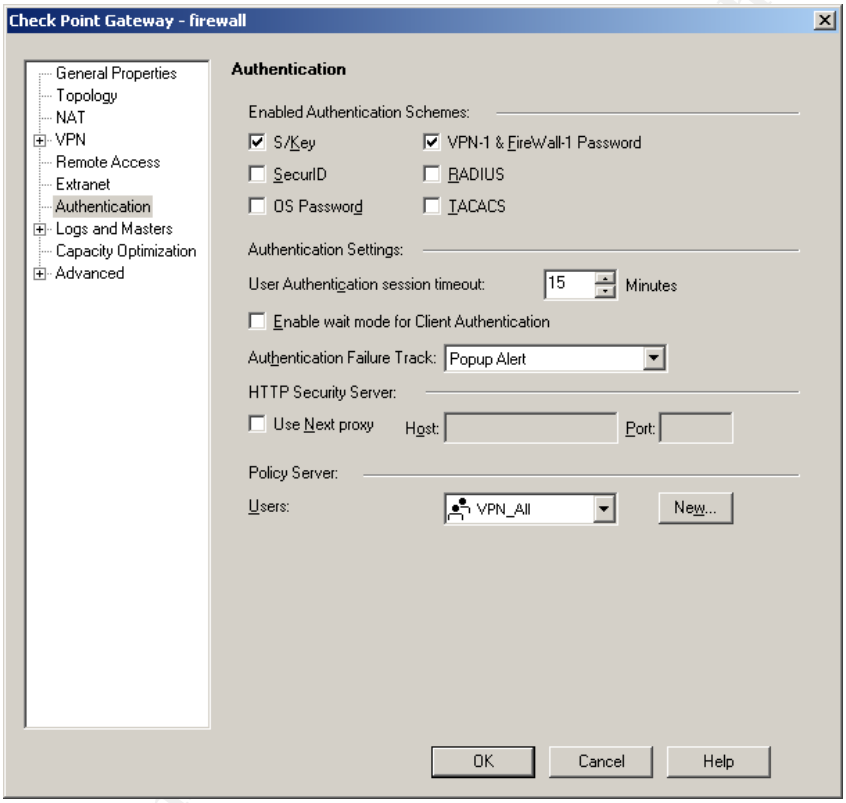


Figure 35

Click on "OK". Now, go back to the "VPN Manager" tab and double click on "Remote Access". Select "Participating Gateways" in the left hand pane. Click on "Add" and add your "firewall" object. If the Management Server were on a separate host as originally designed, this configuration would be done on the Management Server object instead.

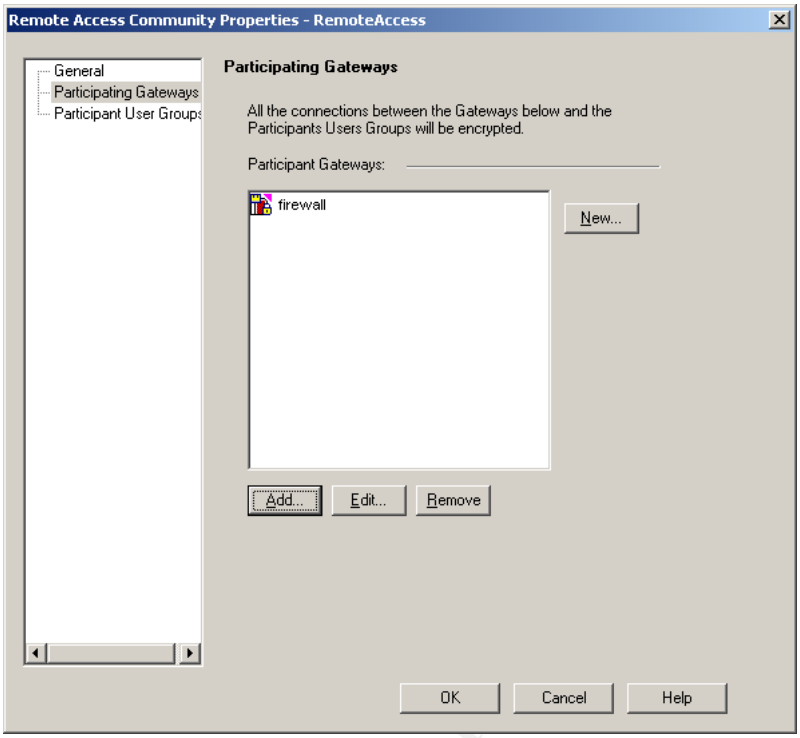


Figure 36

Click on “OK” and you’re done. More detailed information on SecureClient configuration can be found at http://support.checkpoint.com/kb/docs/public/securemote/ng/pdf/scngfp3_config.pdf.

We’ve now completed the VPN community preparation and are ready to begin configuring the rule base.

2.6.6 Firewall Rule Base Configuration

I’ll provide a quick tutorial on how to add rules and then provide the table for the required rules. It’s up to you to fill in all the information.

Section Titles

Section titles help to divide sections of the rule base. To add a section title, right click on the rule above which you want the title to be place in the “No” column. Select “Add Section Title -> Above” and fill in the appropriate information. Section titles are specified in the table for the rules with a row that says “Header: <Information to be put in section title>”. Simply copy the text from the table and use it in the section title configuration.

Rule creation fundamentals

To create a new rule at the top of the rule base, select the  icon. To add a new rule at the bottom of the rule base, select the  icon. To add a rule above

the currently highlighted rule, select the  icon. To add a rule below the currently highlighted rule, select the  icon.

To populate each field of the specified rule, you should right click in the specified field and either select add to select the appropriate item from a drop down box or select the appropriate item from the drop down box that comes up. One exception is in the case where rules specify in the source field something similar to “User_Group@Any”. In this case, you right click on the appropriate field and select “Add Users Access”.

The table that contains the rules does not have “Track”, “Install On” or “Time” field. The “Track” field should say “Log” in all cases. The “Install On” field is left at default except where specified in the section title for the VPN section. The “Time” field should be left at its default value.

The first rule should look as follows:

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	
1	* Any	firewall	* Any	IPSEC	accept	Log	* Policy Targets	* Any	Rec

Figure 37

Note that we could not display the entire line due to space limitations on the screen.

If the network object specifies “Negate”, then after you have added the object to the appropriate column, right click on it and select “Negate Cell”.

The following three pages contain the rules in table format.

No	Source	Destination	Service	If VIA	Action	Comment
Header: Firewall Access rules						
1	Any	Firewall	IPSEC, FW1_pslogon_NG, FW1_scv_keep_alive		Accept	Required for VPN access to the firewall
2	SN_Screened, SN_Monitor, SN_Data	Firewall	FW1_clntauth_http, FW1_clntauth_telnet		Accept	User authentication for temporary access
3	FW_Mgmt_Client	Firewall	CPMI		Accept	Firewall control connections
Header: Client Auth rules						
4	Auth_Admin@SN_Screened	Any	HTTP, HTTPS, FTP		Client Auth	Admin special access from DMZ Network
5	Auth_Admin@SN_Monitor	Any	HTTP, HTTPS, FTP		Client Auth	Admin special access from Monitor Network
6	Auth_Admin@SN_Data	Any	HTTP, HTTPS, FTP		Client Auth	Admin special access from Data Network
Header: Stealth Rule						
7	Any	Firewall	Any		Drop	Stealth Rule
Header: VPN Connections ("firewall" should be selected in the "Install on" column)						
8	VPN_All@Any	GIAC-DC1, GIAC-DC2, GIAC-Exchange	Any	Remote-Access	Accept	General VPN traffic for all VPN users
9	VPN_All@Any	GIAC-Intranet_Parser	HTTP	Remote-Access	Accept	General VPN traffic for all VPN users
10	VPN_Admin@Any	SN_Screened, SN_Data, SN_Monitor	TCP3389	Remote-Access	Accept	Special VPN access for IT admins for Terminal Services
11	Any	GIAC-DC1, GIAC-DC2, GIAC-Exchange	Any	Comm-Rev, Comm-Dev	Accept	Access permitted for all IP30 users
12	Any	GIAC-Intranet_Parser, GIAC-Web	FTP	Comm-Dev	Accept	Access permitted only for developers for IP30 access
Header: Internet Inbound						
13	Any	GIAC-DNS1, GIAC-DNS2	domain-udp		Accept	Access to the DNS server
14	Any	GIAC-Dropchute	TCP2030		Accept	Custom port for DropChute delivery
15	Any	GIAC-Imail	SMTP		Accept	Ability to send mail to GIAC Enterprises
16	Any	GIAC-WEB	HTTP, HTTPS		Accept	Access to the public web server

No	Source	Destination	Service	If VIA	Action	Comment
17	Border_Router	SnortCenter_Console	NTP, FTP, SYSLOG			Provide for the border router to send logs and keep accurate time
18	G_InternalNets (Negate)	G_InternalNets	Any		Drop	Any traffic not explicitly permitted is ignored from the Internet to internal hosts
Header: Internet Outbound						
19	SN_Screened, SN_Monitor, SN_Data, GIAC-DC1, GIAC-DC2	G_InternalNets(Negate)	NTP		Accept	Time synchronization
20	FW_Mgmt_Client	G_InternalNets(Negate)	TCP981		Accept	SSL over TCP 981 for IP30 management
21	GIAC-DC2	G_InternalNets(Negate)	TCP2847		Accept	Norton virus definitions updates
22	GIAC-DNS1, GIAC-DNS2	G_InternalNets(Negate)	DNS		Accept	DNS Queries
23	GIAC-DropChute	G_InternalNets(Negate)	TCP2030		Accept	Custom port used by GIAC for DropChute
24	GIAC-Imail	G_InternalNets(Negate)	DNS, SMTP		Accept	Send outbound emails
25	GIAC-Imail	Ext_Fprot	HTTP, HTTPS, FTP		Accept	F-Prot antivirus updates
26	GIAC-Intranet_Parser	Ext_CCAuth	HTTPS		Accept	Credit Card Authorization
27	SN_Corporate	Border_Router	SSH		Accept	Permit management of border router
28	SN_Corporate	G_InternalNets(Negate)	HTTP, HTTPS		Accept	Permit general web browsing from corporate LAN
29	Whatsup_Gold	Any	SNMP, icmp-proto		Accept	General monitoring access
30	G_InternalNets	G_InternalNets(Negate)	Any		Reject	Drop all other traffic not explicitly allowed for outbound access
Header: Pre-block/Management Rules						
31	SN_Corporate	SN_Data, SN_Screened, SN, Monitor	TCP3389		Accept	Terminal Server for server management
Header: Internal traffic to Data network						
32	GIAC-WEB	GIAC-Database	MS-SQL-Server		Accept	Database queries
33	GIAC-DropChute, GIAC-WEB	GIAC-Intranet_Parser	FTP		Accept	Transferring files
34	SN_Corporate	GIAC-Fin_Payroll	Any		Accept	Access to the accounting server

No	Source	Destination	Service	If VIA	Action	Comment
35	SN_Corporate	GIAC-Intranet_Parser	HTTP, FTP		Accept	Access to the Intranet server
36	Any	SN_Data	Any		Reject	Block any non explicitly permitted access
Header: Internal traffic from Data network						
37	GIAC-Intranet_Parser	GIAC-DropChute, GIAC-WEB	FTP		Accept	Transferring files
38	SN_Corporate, SN_Screened, SN_Monitor, SN_Data	GIAC-DNS1,GIAC-DNS2	domain-tcp		Accept	DNS Queries
39	SN_Data	Any	Any		Reject	Rejects any non explicitly permitted traffic
Header: Remaining rules, ranked in order of priority						
40	GIAC-Imail	GIAC-Exchange	SMTP		Accept	Sending mail
41	SN_Corporate	GIAC-WEB	FTP		Accept	To upload new web sites
42	SN_Corporate	GIAC-DNS1, GIAC-DNS2	HTTPS		Accept	Management of DNS Servers
43	SN_Corporate	SnortCenter Console	HTTP, SSH		Accept	Snort Management
44	SN_Corporate	Whatsup Gold	HTTP		Accept	Viewing Whatsup Gold site
Header: Cleanup Rule						
45	Any	Any	Any		Drop	If it wasn't allowed before, it should be dropped here

When you're done, the first page should look similar to the following:

Figure 38

2.6.7 SecureClient Policies

Finally, we configure the SecureClient policies by clicking on the "Desktop Security" tab from figure 4 and filling in the information as shown below. The method for configuration is the same as with the security policy rule base.

Security - Standard | Address Translation - Standard | VPN Manager | Desktop Security - Standard

Inbound Rules

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
1	GIAC-DC1 GIAC-DC2 GIAC-Exchang GIAC-Intranet_	VPN_All@Any	* Any	Encrypt	Log	Domain access
2	* Any	VPN_All@Any	* Any	Block	Log	Block everything else

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
3	VPN_All@Any	GIAC-Exchange GIAC-DC1 GIAC-DC2	* Any	Encrypt	Log	General VPN Access
4	VPN_All@Any	GIAC-Intranet_Parse	TCP http	Encrypt	Log	General VPN Access
5	VPN_Admin@Any	SN_Data SN_Screened SN_Monitor	TCP TCP3389	Encrypt	Log	Sysadmin specific rules
6	VPN_All@Any	G_InternalNets	TCP http TCP https ?? icmp-proto dns	Accept	Log	General Internet Access
7	VPN_All@Any	* Any	* Any	Block	Log	Block all other access

Figure 39

2.6.8 Installing the policy

All that's left at this point is to install the policy. Click on the  icon at the top of the screen from figure 4. Deselect all check boxes except for those next to the "firewall" object and then click on "OK".

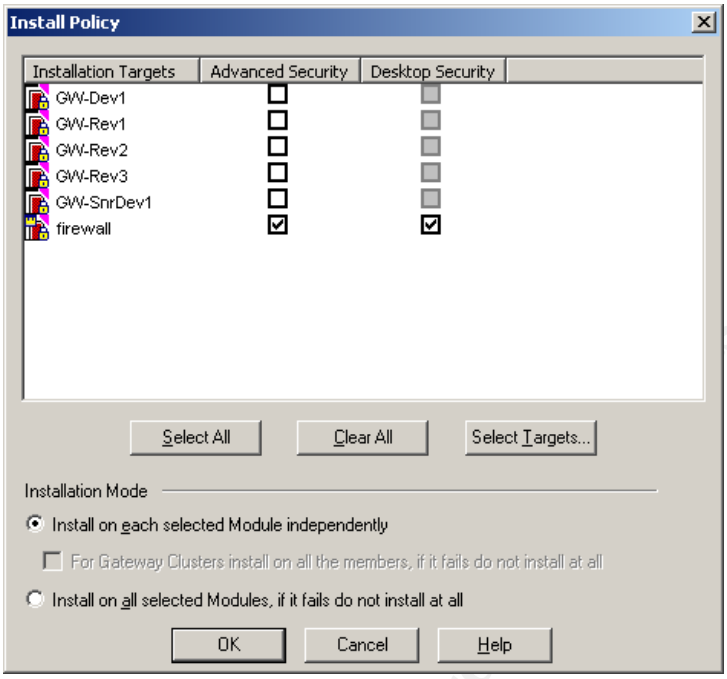


Figure 40

If everything goes well, you'll see the installation completed as follows:

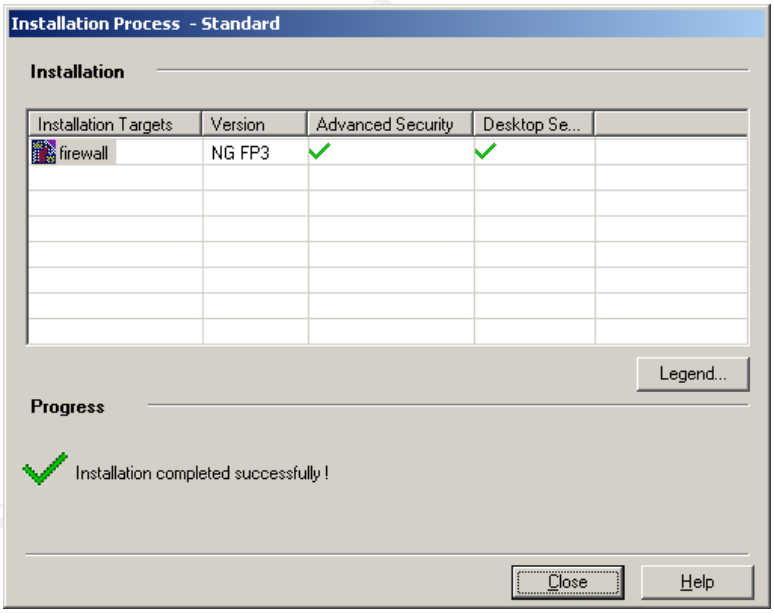


Figure 41

Assignment 3 – Verify the firewall Policy

In order to verify that the implemented policy meets the intended goals, it is essential to validate the firewalls rule base. This section presents the plan, execution and evaluation of the firewall policy audit.

3.1 Validation plan

Planning is essential when performing a policy audit. It will set the expectation for potential risk, cost and time involved as well as ensure that the time is well spent and organized to achieve the desired goal. This section discusses the plan for performing the validation on GIAC Enterprises implemented firewall policy.

3.1.1 Method of validation

The firewall policy will be validated by performing TCP, UDP and IP protocol scans from each network to each of the other networks. In addition, these same scans will be performed against the firewall itself. Five systems will be deployed to run the scans simultaneously. nmap will be used to run the scans. To identify what traffic got through the firewall, the firewall logs will be used and double checked with the IDS systems that will be listening for the scan traffic with tcpdump. In order to streamline the scanning process, scripts will be created to minimize the amount of time needed to actually perform the scans. There will be one script file for each network and one batch file for each interface of the firewall. When scanning the "Internet" a single IP will be used and the scan process will ensure that none of this scan traffic actually leaves the border router. The audit will be done in such a way to minimize risk and downtime. The scanning hosts and scan scripts they will run is as follows:

Scanning Host	**corporate**	**data**	**screened**	**external**	**monitor**	**internet**	**fwall**
Inet (12.13.14.1)				y			external
Data (192.168.210.1)	y		y		y	y	data
Screened (192.168.200.1)	y	y			y	y	screened
Corporate (192.168.150.1)		y	y		y	y	internal
Monitor (192.168.100.1)	y	y	y			y	internal

3.1.2 Timeline of events

With the 4th of July holiday coming up in the near future, it was determined that GIAC Enterprises could take advantage of the timing in order to reduce impact to their business. Therefore, the entire validation process is timed around July 4th. The timeline of events is as follows:

Notifications:
June 30th – July 1st: Vendor and Partner relationship consultants will notify vendors and partners.
June 30th: A memo will be sent out to all employees requesting that they enjoy their 4th of July holiday and that their VPN connectivity will not be available beginning 8pm CDT on Friday until midnight.

June 30th-July 5th: The public web site will include a notification that there is a possibly for downtime beginning 8pm CDT until midnight as a result of system maintenance.

Preparation:
June 30th-July 1st: A new system will be brought online and loaded with Checkpoint. It will have the rule-base of the production firewall installed.
July 2nd: Usability testing will be performed to ensure that the second system will permit the desired business critical access.
July 3rd: Any potential problems will be addressed and resolved. The test bed will be prepared for July 4th's activities. Scan scripts will be created.

The main event: Friday, July 4th
8:00pm – 8:30pm: The DropChute and Web servers will be taken offline after verifying that there are no active connections.
8:30pm-9:00pm: The production firewall will be disconnected from the network and the temporary firewall configured in the preparation stage will be put into its place. The DropChute and Web services will be restarted and usability testing will be performed. If all is well, then the firewall will be deployed into the prepared test bed for firewall rule verification. SmartDefender configurations will be changed to remove the additional protection it provides. All "Block" rules will be changed to "Reject" to increase the speed of the scans. tcpdump commands will be started on the IDS systems. Note: the "Internal" network will not be attached to the temporary firewall. It will remain attached to the production firewall.
9:00pm-9:30pm: All scanning systems will run their scans against the firewall.
9:30pm-10:00pm: The scanning system outside the firewall will run its scan against the public IP space. The scanning host on the monitor network will scan the Internet. The other hosts will scan the monitor network.
10:00pm-10:30pm: The corporate network scanning host will scan the Internet. The other internal scanning hosts will scan the Corporate LAN.
10:30pm-11:00pm: The data network scanning host will scan the Internet. The other internal scanning hosts will scan the Data LAN.
11:00pm-11:30pm: The screened network scanning host will scan the Internet. The other internal scanning hosts will scan the Screened LAN.
11:30pm-11:35pm: The firewall logs pertaining to the scans will be exported to text file. SmartDefender options will be put back to the original configuration. The original rule base will be restored to put "Drop" rules back to "Drop", instead of the temporary "Reject".
11:35pm-12:00pm: The Web server and DropChute server will be stopped according to the same process at 8pm. The temporary firewall will be disconnected and the primary firewall will be put back into production. The Web server and DropChute servers will be reinitiated. Usability testing will be performed to ensure everything is working correctly.

3.1.3 Estimate of costs and level of effort

Internal Staff: (Indirect cost)

Vendor/Partner Relationship Consultants – 8 hrs total notifying vendors/partners
Net/Security Admin – 16 hrs building temporary firewall and assisting consultant
Sysadmins – 4 hours assisting Net/Security Admin
Senior Developer – 1.5 hours assisting in usability testing during audit and other small tasks

Total cost: 29.5 hrs

Consultant Staff: (Direct cost @ $200/hour)
1 hr – Preparing scan scripts
1 hr – Assist Net/Security admin in building and verifying temporary firewall
4 hr – Perform audit
2 hr – Create and present report

Total cost: 8 hrs @ $1600

3.1.4 Potential risks

Although great care will be taken to prevent risk, there is always the potential for problems. It is not expected that any email will be lost due to the short period of time the mail server will be off the Internet and the inherent fault tolerance of mail servers in case of temporary failure. It is not expected that any DropChute files may be lost due to the inherent protection that it provides. It is not expected that any orders will be lost since the Web server will be brought offline after verifying no one is connecting to it for purpose of moving the firewall connections. The greatest risk in this plan is the ability to perform all the tasks necessary in a limited timeline.

3.2 Conducting the validation

3.2.1 Scripts

Ten separate script files were generated to perform the scripts. One was created for each interface of the firewall and one for each of the networks identified in section 3.1.1. To increase the speed of the scanning and to reduce the time needed to re-run specific scans that fail, the 65,535 ports were broken up into 44 subscripts that each contained 15 nmap commands to be run sequentially. The IP Protocol scan consisted of three lines only since there are only 256 IP protocols. Here is a subset of the script generated to scanning the external interface of the firewall:

```
echo nmap -sS -p 1-100 -P0 -T 5 -n -vv -oN tcp1.log 206.45.67.10 >> tcp1.bat
echo nmap -sS -p 101-200 -P0 -T 5 -n -vv -oN tcp2.log 206.45.67.10 >> tcp1.bat
echo nmap -sS -p 201-300 -P0 -T 5 -n -vv -oN tcp3.log 206.45.67.10 >> tcp1.bat
…
echo nmap -sS -p 1501-1600 -P0 -T 5 -n -vv -oN tcp16.log 206.45.67.10 >> tcp1.bat
echo nmap -sS -p 1601-1700 -P0 -T 5 -n -vv -oN tcp17.log 206.45.67.10 >> tcp2.bat
…
echo nmap -sS -p 65401-65535 -P0 -T 5 -n -vv -oN tcp655.log 206.45.67.10 >> tcp44.bat
echo nmap -sU -p 1-100 -P0 -T 5 -n -vv -oN udp1.log 206.45.67.10 >> udp1.bat
```

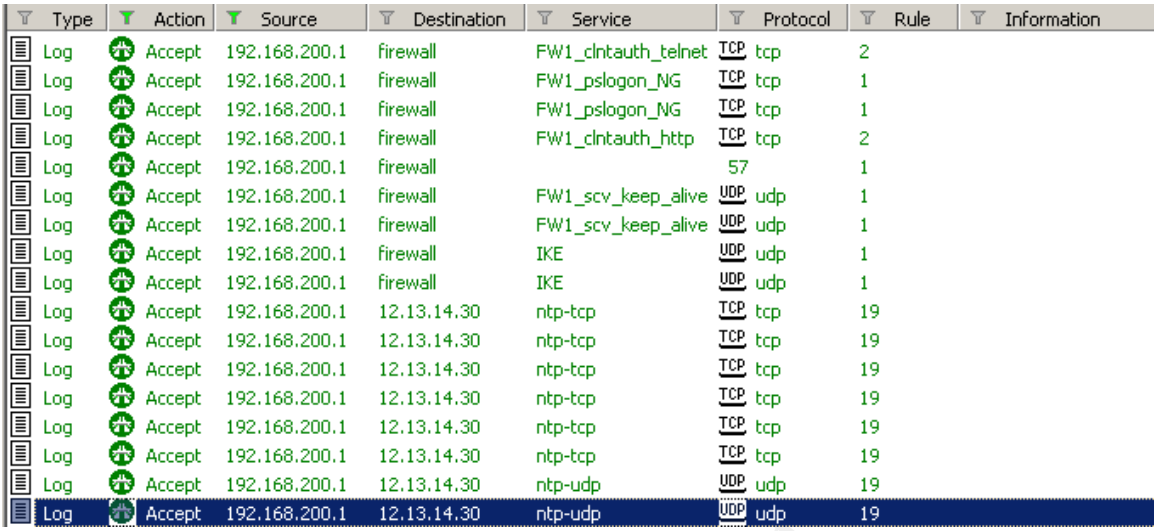
```
echo nmap -sU -p 101-200 -P0 -T 5 -n -vv -oN udp2.log 206.45.67.10 >> udp1.bat
…
echo nmap -sU -p 65401-65535 -P0 -T 5 -n -vv -oN udp655.log 206.45.67.10 >>
udp44.bat
echo nmap -sO -p 1-100 -P0 -T 5 -n -vv -oN ip1.log 206.45.67.10 >> ip1.bat
echo nmap -sO -p 101-200 -P0 -T 5 -n -vv -oN ip2.log 206.45.67.10 >> ip1.bat
echo nmap -sO -p 201-255 -P0 -T 5 -n -vv -oN ip3.log 206.45.67.10 >> ip1.bat
./tcp1.bat &
./tcp2.bat &
…
./tcp44.bat &
./udp1.bat &
./udp2.bat &
…
./udp44.bat &
./ip1.bat &
```

Each network, as defined in section 3.1.1 were scanned only for the hosts that are known to be live on that network. To create the other scan scripts, the IP of 206.45.67.10 was replaced with the appropriate IP(s). The chart of scanned IPs for each script is as follows:

Script	**IP(s) scanned**
fwallexternal	206.45.67.10
fwallinternal	192.168.20.10
fwalldata	192.168.210.10
fwallscreened	192.168.200.10
Monitor	192.168.100.100 192.168.100.110 192.168.100.120 192.168.100.200 192.168.100.210 192.168.100.220
Data	192.168.210.20 192.168.210.25 192.168.210.30
Screened	192.168.200.12 192.168.200.13 192.168.200.14 192.168.200.15 192.168.200.16
Corporate	192.168.150.30 192.168.150.40 192.168.150.50 192.168.150.60 192.168.150.129
Internet	12.13.14.30
External	206.45.67.12 206.45.67.13 206.45.67.14 206.45.67.15 206.45.67.16 204.45.67.101 204.45.67.120 204.45.67.100 204.45.67.150 204.45.67.210

3.2.2 Results

The tcpdump captures were cross-checked against the firewall logs and found to be correct. The following image shows the scan performed from the Screened network:



Type	Action	Source	Destination	Service	Protocol	Rule	Information
Log	Accept	192.168.200.1	firewall	FW1_clntauth_telnet	tcp	2	
Log	Accept	192.168.200.1	firewall	FW1_pslogon_NG	tcp	1	
Log	Accept	192.168.200.1	firewall	FW1_pslogon_NG	tcp	1	
Log	Accept	192.168.200.1	firewall	FW1_clntauth_http	tcp	2	
Log	Accept	192.168.200.1	firewall		57	1	
Log	Accept	192.168.200.1	firewall	FW1_scv_keep_alive	udp	1	
Log	Accept	192.168.200.1	firewall	FW1_scv_keep_alive	udp	1	
Log	Accept	192.168.200.1	firewall	IKE	udp	1	
Log	Accept	192.168.200.1	firewall	IKE	udp	1	
Log	Accept	192.168.200.1	12.13.14.30	ntp-tcp	tcp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-tcp	tcp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-tcp	tcp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-tcp	tcp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-tcp	tcp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-tcp	tcp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-udp	udp	19	
Log	Accept	192.168.200.1	12.13.14.30	ntp-udp	udp	19	

Figure 42

For ease of presentation, I have compiled these tables to identify the access that was granted by the firewall from each of the scanning hosts:

External Scanner:

Source	Destination	Port	Protocol
12.13.14.1	206.45.67.12	domain-udp	udp
12.13.14.1	206.45.67.13	domain-udp	udp
12.13.14.1	206.45.67.14	http	tcp
12.13.14.1	206.45.67.14	https	tcp
12.13.14.1	206.45.67.15	smtp	tcp
12.13.14.1	206.45.67.16	TCP2030	tcp
12.13.14.1	firewall	IKE	udp
12.13.14.1	firewall	FW1_pslogon_NG	tcp
12.13.14.1	firewall	FW1_scv_keep_alive	udp
12.13.14.1	firewall		57

Monitor Scanner:

Source	Destination	Service	Protocol
192.168.100.1	12.13.14.30	ntp	tcp,udp
192.168.100.1	firewall	FW1_clntauth_telnet	tcp
192.168.100.1	firewall	IKE	udp
192.168.100.1	firewall	FW1_clntauth_http	tcp
192.168.100.1	firewall	FW1_pslogon_NG	tcp
192.168.100.1	firewall	FW1_scv_keep_alive	udp
192.168.100.1	firewall		57
192.168.100.1	GIAC-DNS1	domain	tcp, udp
192.168.100.1	GIAC-DNS2	domain	tcp, udp
192.168.100.1	GIAC-Dropchute	TCP2030	tcp
192.168.100.1	GIAC-Imail	smtp	tcp
192.168.100.1	GIAC-WEB	http	tcp
192.168.100.1	GIAC-WEB	https	tcp

Corporate Scanner:

Source	Destination	Service	Protocol
192.168.150.1	12.13.14.30	http	tcp
192.168.150.1	12.13.14.30	https	tcp
192.168.150.1	Data Network	TCP3389	tcp
192.168.150.1	Screened Network	TCP3389	tcp
192.168.150.1	firewall	FW1_pslogon_NG	tcp
192.168.150.1	firewall	FW1_scv_keep_alive	udp
192.168.150.1	firewall	IKE	udp
192.168.150.1	firewall		57
192.168.150.1	GIAC-DNS1	domain-tcp	tcp
192.168.150.1	GIAC-DNS1	domain-udp	udp
192.168.150.1	GIAC-DNS1	https	tcp
192.168.150.1	GIAC-DNS2	domain-tcp	tcp
192.168.150.1	GIAC-DNS2	domain-udp	udp
192.168.150.1	GIAC-DNS2	https	tcp
192.168.150.1	GIAC-Dropchute	TCP2030	tcp
192.168.150.1	GIAC-Fin-Payroll	ALL*	ALL*
192.168.150.1	GIAC-Imail	smtp	tcp
192.168.150.1	GIAC-Intranet_Parser	ftp,http	tcp
192.168.150.1	GIAC-WEB	ftp, http, https	tcp
192.168.150.1	Monitor Network	TCP3389	tcp
192.168.150.1	SnortCenter_Console	http, ssh	tcp
192.168.150.1	Whatsup_Gold	http	tcp

* note that “All” doesn’t really mean all. This is explained in the analysis section.

Screened Scanner:

Source	Destination	Service	Protocol
192.168.200.1	12.13.14.30	ntp	tcp
192.168.200.1	12.13.14.30	ntp	udp
192.168.200.1	firewall	FW1_clntauth_telnet	tcp
192.168.200.1	firewall	FW1_clntauth_http	tcp
192.168.200.1	firewall	FW1_pslogon_NG	tcp
192.168.200.1	firewall	FW1_scv_keep_alive	udp
192.168.200.1	firewall	IKE	udp
192.168.200.1	firewall		57

Data Scanner:

Source	Destination	Service	Protocol
192.168.210.1	12.13.14.30	ntp	tcp
192.168.210.1	12.13.14.30	ntp	udp
192.168.210.1	12.13.14.30	ntp	udp
192.168.210.1	192.168.200.12	domain	tcp
192.168.210.1	192.168.200.12	domain	udp
192.168.210.1	192.168.200.13	domain	tcp

192.168.210.1	192.168.200.13	domain	udp
192.168.210.1	192.168.200.14	http	tcp
192.168.210.1	192.168.200.14	https	tcp
192.168.210.1	192.168.200.15	smtp	tcp
192.168.210.1	192.168.200.16	TCP2030	tcp
192.168.210.1	firewall	FW1_clntauth_telnet	tcp
192.168.210.1	firewall	FW1_clntauth_http	tcp
192.168.210.1	firewall	FW1_pslogon_NG	tcp
192.168.210.1	firewall	FW1_scv_keep_alive	udp
192.168.210.1	firewall	IKE	udp
192.168.210.1	firewall		57

3.3 Evaluate the results

3.3.1 Result analysis

The firewall responded almost exactly as expected. The only exception to this rule is in the connection to the Finance server from the Corporate LAN. Although the firewall rule-base is configured with “Any” as the allowed services, the firewall did not actually allow “any” traffic. The reason for this is that CheckPoint will only permit traffic to pass on “any” if there is a configured service for the access in question and the “Match for any” option is selected as part of the service configuration.

3.3.2 Recommendations for change

Although the audit was nearly a complete success in terms of verifying the rule-base, a few issues were made clear that should be addressed for possible change. First of all, IP protocol 57 was allowed to the firewall. This is a member of the CheckPoint preconfigured IPSEC group. Since this is not required for the VPN traffic that is being used, rule 1 in the firewall rule base should be changed to remove the IPSEC group and include udp IKE. Additionally, it’s not necessary for internal hosts to talk to the firewall for the purpose of establishing a VPN tunnel. Therefore, it would seem prudent to change the source column in this same rule to be G_InternalNets (negate).

In regards to the Corporate networks connection to the Finance Server, it is of particular interest that “any” is used in the service column for this rule. Access to the finance server should be investigated for what is actually required and rule 34 should be adjusted accordingly. If GIAC Enterprises is unable to do so, then it would be well advised to move the Finance server to the Corporate network instead of leaving it on the Data network. Better yet, it may have been more prudent to isolate the finance server onto an additional network by making use of the VLAN infrastructure deployed with the Cisco 2621 router and route-map filter in order to not have performed the original designed network layout. This change would put the people who access the finance server on their own network with the finance server and would require some additional changes to the firewall. It would be much better to do this than to use “any” in the firewall rule.

The final issue that became clear as a result of the firewall rule integrity check is the unrestricted access to the Internet for time synchronization. If many internal hosts are all seeking their time synchronization from external sources, then there is potential for time synchronization issues to occur in the local network without a more controlled time synchronization infrastructure. Since the SnortCenter Console is being made an NTP server for the border router, I would recommend that some external means of time synchronization be provided for this system (such as a serially connected device that obtains its correct Naval Observatory time from the radio waves). The other hosts should then be configured to obtain their time synchronization from the SnortCenter Console and rule 19 should be changed to have the SnortCenter Console in the destination column.

Another point of issue that should be considered is the lack of fault tolerance in GIAC Enterprises infrastructure. With a single link to the Internet, a single border router, a single firewall, a single internal switch that servers connect to and single servers that provide the core function of GIAC Enterprises, there are many devices that could fail that would take GIAC Enterprises offline. Decisions were made in the design phase for this network that were focused on budgetary concerns. Now that GIAC Enterprises is in full production with the E-business effort, it is expected that there is now an increase in revenue. As budget allows, I would recommend eliminating as many of these single points of failure as possible.

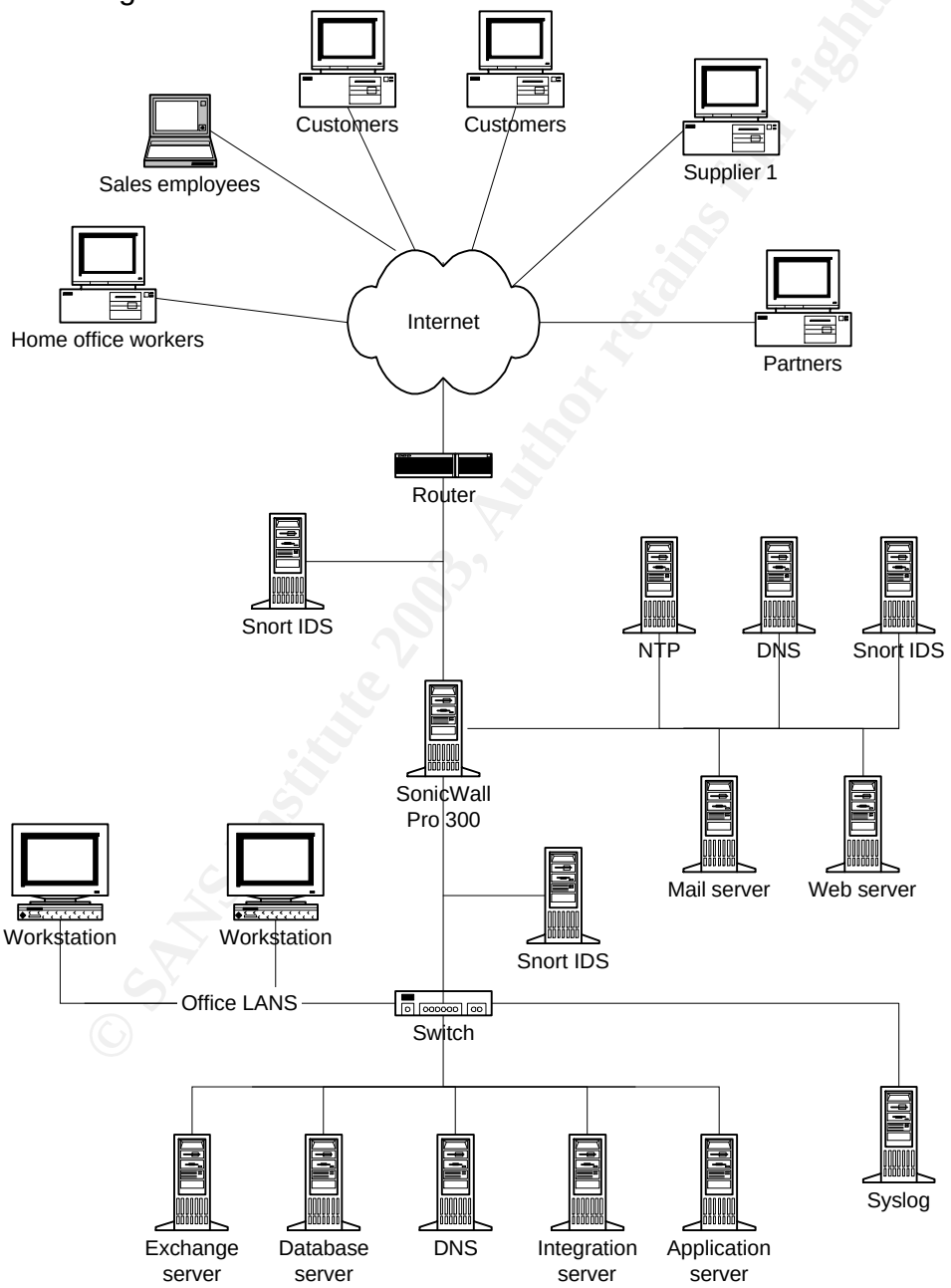
As a point of good network design, the security restrictions should be reviewed with regards to ICMP messages. While ICMP messages were initially blocked as a means to hinder potential reconnaissance scans, as implemented this design also hinders normal network flow controls and troubleshooting that are handled by the ICMP protocol. The border router and firewall configuration should be reviewed to consider permitting ICMP messages related to flow control such as “fragmentation needed and DF set” or “source quench” messages.

There were some implementation features that could have been deployed in the border router that were not due to a comfort level with the ability for GIAC Enterprises to continue to support the configuration. GIAC Enterprises should consider becoming familiar with rate-limitting and reflexive access lists as they can provide a means for a more secure environment. Rate-limiting would give the ability for GIAC Enterprises to deploy a configuration that would assist in hindering the capability of DOS attacks by limiting the amount of bandwidth that can be consumed by a defined traffic condition (such as SYN packets or http traffic). Reflexive access lists could change the focus of the ingress filter from “block what we don’t want” to “allow what we do want”. This significant change could go a long way to providing additional defense in depth, but at the cost of addition CPU utilization on the border router and a more complicated implementation that must be maintained.

Assignment 4 – Design under fire

This section seeks to perform a targetted penetration test against a design done by another individual in order to identify potential weaknesses that need to be addressed. For purposes of this assignment, I have selected the GCFW practical located at: http://www.giac.org/practical/GCFW/Brad_Tauer.pdf.

Network diagram:



4.1 An attack against the firewall itself

The implemented infrastructure is using a SonicWall. Although the diagram provided shows it is a SonicWall Pro 300, the firewall configuration discusses a SonicWall Pro 200. However, for the purposes of this exploit, either of these two versions are appropriate.

The attack we will use is described at http://www.securityfocus.com/archive/1/319712 with a bugtraq notice posted at http://www.securityfocus.com/bid/7435.

This bug notice describes a situation where a large HTTP POST is sent to a Sonicwall Pro 100/200/300 firewall. The effect is that the system will reboot.

Although the original designer discusses the fact the firewall provides stateful inspection firewall, it is also important to point out that it implements application proxy services. This is important to note since the vulnerability that will be used is one that indicates a buffer overflow problem with the http daemon that is running on the firewall. Since the firewall is providing an application proxy service for the protocol that will be used, we do not need to direct the attack at the firewall directly. Being an http buffer overflow attack, we'll target the attack at the web server instead, with expectation that the firewall will be affected.

4.1.1 The Attack

To prepare for this attack, I first would obtain the IP address associated with www.giac.com for the described implementation. In this case it would be 172.135.192.22. In order to perform this attack, either one of the following commands must be run from a system with nessus installed:

```
nasl -t 172.135.192.22 www_too_long_post.nasl
```

or

```
nasl -t 172.135.192.22 alibaba_overflow.nasl
```

4.1.2 The Results

Without testing the actual implementation, it's difficult to know the success of this attack. Since no mention is made of patch maintenance, it is assumed that this DoS attack against the firewall would succeed. If successful, the effect would be that the firewall would reboot. A prolonged small traffic attack could be performed by setting up a routine that would perform the commands listed above every minute.

4.1.3 Countermeasures

If the patches are properly maintained on the firewall at the time the vulnerability exploit is performed, it is expected that the attack will fail. This should stress the importance for patch maintenance.

4.2 A distributed denial of service attack

Although I was unable to find anything in the posted practical to suggest the size of the Internet connection, I will assume a T1.

4.2.1 Setting the Stage

I do not wish to provide an excruciatingly simple step by step how to for this section. Therefore, I will refer to the tools required and, later, steps to help protect against them.

For purposes of this DDoS attack, I will be using TFN2K. Since this tool does not provide the means to compromise the hosts that will be used for the DDoS, we must first find a way to deploy the TFN2K daemon onto at least 50 compromised hosts. This can be done with many different methods, but the most common of which is the deployment of a Trojan of some kind. An attacker can take advantage of Trojans that have already been deployed or to distribute some type of application through social engineering in order to obtain a list of infected hosts. For purposes of reducing the amount of time for preparation, I will choose to search for systems that have already been infected. To this end, I will scan ranges of IP address known to belong to Cable/DSL users for the existence of BackOrifice. Nmap will be used to scan the hosts quickly. In order to prevent administrators from being able to determine the true source of the widespread scan that must be performed, I will make utilization of netstumbler to find a wireless network with access to the Internet. I will also ensure that the network being used is at least 30 miles from my home and work and in a heavily populated area.

After the initial scans have been performed and a possible list of BackOrifice hosts has been found, I would then need to deploy a TFN2K daemon onto the BackOrifice infected systems. This could take quite some time and will be done again from a rogue wireless network, but from a different location than the first stage. In order to ensure that at least 50 hosts would be available, I would setup 75 hosts with TFN2K and list them all in my agent list for the TFN master. With the control that BackOrifice provides, I'll ensure the systems are rebooted in order to complete the installation of TFN2K daemon.

4.2.2 The Main Event

Now that the ground work has been laid down, it's time for the attack. Again, a rogue wireless network would be found and the DDoS would be launched. The TFN2K hosts would be instructed to target GIAC Enterprises with spoofed source addresses to perform SYN attacks against the web server on port 80 and the email server on port 25.

4.2.3 The Results

With 50 or more hosts working hard sending traffic at an average of 200 kb/s or more to GIAC Enterprises, it is expected that the T1 to the Internet would be filled quickly. Since the border router configuration has nothing in its access-list that would prevent this traffic, it is unlikely that the connection would stay up for long. The SonicWall firewall does provide some protection against SYN floods, but with spoofed source addresses, any action that would be taken to block any and all SYN attacks to these servers on these ports would effectively shut down the web and email servers from outside interaction; thus achieving the desired goal anyways. If the firewall successfully handled all SYN packets, it could be expected that either the internal hosts would be depleted of resources through half open connections or that the firewall would be depleted of resources due to its utilization of application proxy services. If the firewall increases the rate at which it closes half-open connections in reaction to this event, then it would likely close half-open sessions to real customers as well, since they would be having trouble completing the three way hand shake due to the saturation of the T1 link. The end result would be a successful DDoS against GIAC Enterprises through multiple layers of an over-utilization of resources.

4.2.4 Countermeasures

Several issues are at play in this attack, all of which can be addressed to assist in protecting against this DDoS scenario. I will outline them and discuss each one at a time.

4.2.4.1 802.11b networks

802.11b networks are inherently insecure. It is very easy to find a wireless network that provides a potential intruder anonymous access to the Internet. While GIAC Enterprises can do nothing to protect against an intruder from using one of these networks, the rest of the world can take actions that over time will make this less and less of a likelihood. Any time an 802.11b network is deployed, in the very least WEP should be turned on with the 128 bit encryption keys. Even though this encryption can usually be broken within 24 hours, it can serve as a valuable deterrence against people making use of your network. If you feel compelled to deploy a wireless network, you should look into some of the new 802.11 technologies coming out that provide a more secure environment. Corporate users should invest money in technologies such as Cisco's LEAP devices that make the unauthorized use of wireless networks even more difficult. In your corporate environment, it would be a good idea to use netstumbler on a regular basis to identify potential rogue access points that users may have deployed on your corporate network without official permission.

4.2.4.2 BackOrifice

Again, there is very little that GIAC Enterprises can directly do to prevent users from being infected by BackOrifice. ISPs with a large always on user base could block access to port 31337 to help reduce, but ISPs who provide this service

generally refuse to do so. Alternatively, they could drastically reduce DHCP lease times in order to shorten the amount of time a known BackOrifice IP address is still valid. The real fix for the problem is for home users to deploy strong anti-virus protection and host based firewalls in order to protect their home systems from these types of compromises.

4.2.4.3 TFN2K

The usage of virus protection and host based firewalls on home user systems would also provide good protection against becoming a TFN2K daemon host. Router administrators should also ensure they have appropriate ingress and egress filtering to help reduce the amount of spoofed traffic that leaves their network.

For the remainder of this section, we'll focus on what GIAC Enterprises can do. Unfortunately, the answer is not much. One of the most difficult things about TFN2K is actions that could be taken to limit its impact against GIAC Enterprises is really just a mitigation. If any TCP services are allowed through, as they must be, then with enough hosts, GIAC Enterprises connection to the Internet can be saturated. However, all is not without hope. The following are a list of items that could be implemented to reduce the impact that this attack would have against GIAC's network:

- Deploy rate limiting devices that can specify a limit to the amount of bandwidth that can be consumed by the particularly defined traffic. In this example, traffic to the web server and mail server might have been limited to 400kbps. While this would not have prevented the DDoS against the web and email server, it would have made for any other traffic to be able to pass.
- Establish a good relationship with the upstream provider in order to provide quick assistance when these types of attacks occur. The upstream provider can make changes to the router you interface with to help alleviate the problem while it is occurring. They could also be instrumental in helping to track down the true source of the traffic for the purpose of shutting it down. Unfortunately, for this attack, this would be very time consuming.
- By adding more bandwidth, GIAC Enterprises can mitigate the problem by increasing the number of hosts it takes to perform a successful DDoS. Due to its limited success, this is not a very cost effective solution. A better alternative might be to host your public facing applications with a service provider who has a larger connection to the Internet. This usually comes coupled with a more knowledgeable staff capable of identifying and assisting in protecting against these types of attacks.
- GIAC Enterprises could deploy a better ingress filter in this case. Many unassigned addresses are permitted in and very little traffic is actually stopped from entering the network. Review the Secure IOS template

found at http://www.cymru.com/Documents/secure-ios-template.html for more information.

4.3 An attack plan to compromise an internal system

The attack plan is one based primarily around social engineering. Many companies provide a means for sales staff to connect to the corporate office with a VPN for purposes of demos and checking their email and other functions. This is taken as an assumption. With this assumption in hand, the following outline of events has been prepared to stage the compromise of an internal system at GIAC Enterprises.

Targetted host: For this attack, my eventual target is the internal database server. This server is likely to contain all the fortunate cookie sayings for the company as well as a list of customers and potentially even credit card numbers.

Step 1: Make a sales call request to GIAC Enterprises. Use a fictitious company and fictitious name. Preferably, I'll meet the sales person in a city other than my own with the guise that I am a traveling business man and am working on a deal with a well known Chinese Food chain in a given tri-state area to take over management. I select a hotel room to meet the sales engineer at that has a high speed Internet connection and I'm sure to select one that will accept cash and not require proper identity.

Step 2: When the sales person meets with me in the hotel, I'll be sure to meet near dinner or lunch time. After talking with the sales person for at least 30 minutes, I'll ask if he's received my email (that was sent 5 minutes prior to your scheduled meeting) detailing the number and location of stores and the expected volume of purchases, among other things, and if he had any thoughts on price breaks he might be able to cut you. When he says "no", I request that he take a look at the spreadsheet I sent him. As he's connecting to the high speed connection in the hotel room, I suggest that I'm quite hungry and that as soon as he's done checking the email, the two of us should go grab a bite to eat. As he pulls up the email, he'll discover its several pages long with some complicated charts, business growth plan and other details. At this time, I'll pull out my portable printer and suggest that he really needs to print it out. I'll have him hook up the printer and start the job. I'll suggest that the printer takes a long time and you should just leave it to print while the two of you go grab a bite to eat. Insist on a Chinese restaurant.

Step 3: In comes an accomplice who enters the hotel room just after he sees the two of us leave for dinner/lunch. He'll install a keylogger and Trojan software with "phone home" capability over port 80 to post critical information (such as user name and passwords) to a publicly available site known to the both of us that has been compromised through some other means (BackOrifice for example). He'll ensure that the keylogger and Trojan will automatically remove itself and all traces after 2 weeks. The accomplice should also get a look at network settings, host files, DNS server settings, Exchange server settings and IP address, etc… to try to ascertain the identity of any critical internal resources. Also, he'll look for

any files on the laptop that look like they might be certificates used for VPNs. He'll take a look at his calendar to determine when the sales person will be in and out of the office.

Step 4: This stage is dependant upon the success of step 3. It is possible that I may have obtained all the information necessary to establish a VPN connection as the sales personnel. It's also possible that we may have the ability to remotely control the sales persons' laptop while he's on the Internet and take advantage of the VPN session he initiated without his knowledge. At any rate, depending upon the success of stage 3, it's now time to perform an unhindered attack against GIAC Enterprises internal systems. It should not be long before I've been able to determine the internal addressing scheme and critical hosts based upon identifying the internal Exchange server, determining its IP address and then taking a look at other hosts on the Internal network. I expect to stumble upon the Database server. I could attempt to use the sales persons system to try and extract information from the database server, but I'll assume that limited capability exists based upon his login credentials.

Step 5: To gain better access rights, I wait for a time when the sales person schedule has him in his home office and I remove the sales person from his local Windows domain. When the system administrator comes to take a look at the system, it is expected he'll login as an administrator or use the administrator account in order to add the system back to the domain. Since I've still got the keylogger running, I should be able to obtain the administrator user name and password.

Step 6: Now for the crown jewels. The internal database server has been identified and the administrator username and password is known. A series of ODBC queries will be performed to take a dump of the database and then to ftp the results out. At this point in time the objective has been achieved and time will be spent cleaning up any evidence that may exist.

4.3.1 Likelihood for success

Under most circumstances, I would expect this plan to fail miserably. However, the infrastructure that is being reviewed for this assignment lacks the detail of information that would suggest that this procedure would be impossible. The majority of the success of this attack depends upon the success of step 3. Without knowing the human nature of the sales person that would be targeted in this attack, it's difficult to assess the ability of me and my accomplice to perform these tasks. There is no mention of virus protection that would likely work against my ability to install a keylogger and Trojan on the sales person computer. Additionally, many systems are deployed where the employee who uses them has administrative rights to their own system, making the installation of these applications easy to obtain. Although the infrastructure described provides for a host based firewall for home users, no such provision is made for the mobile sales staff. Additionally, the VPN makes it possible for the sales person to connect to any resource on the internal LAN on any port. This includes the Database server, which is potentially the most valuable system to GIAC Enterprises. If done carefully, this attack would avoid detection entirely since it is

using permitted protocols in expected manners. The only possible exception to this is the Trojan that was installed. However, since this was a custom piece of code created for this purpose, it's unlikely that the Snort IDS will have an appropriate signature. It is important to note that in order for the Trojan application to work over port 80, it must conform to standards for that protocol, since the implementation in question is using an application gateway and traffic that does not conform to the content standards for the protocol is likely to be dropped.

4.3.2 Countermeasures

There are many issues that can be addressed to aid against this type of attack. Some of them are as follows:

- User training: All staff should be trained in appropriate security practices. This is especially true for mobile users who will often find themselves and their laptops in potentially hostile environments. They should know how to protect this asset against possible theft and misuse. In this case, the sales person might have found it reasonable to lock the workstation when he left. He also could have disconnected from the VPN while he was out to lunch. Better yet, he could have taken his laptop with him and decided to print it later.
- Virus protection: Virus protection is a crucial part of a secure network. In this scenario, it might have made the job of my accomplice a lot more difficult.
- Administrative control: Users should not in general be granted administrative rights on the machine they use. By denying users the ability to install applications on their system, you can help prevent things like this from occurring.
- Separation of networks: When possible, critical systems should be separated from the network used by general users. That is to say workstations should be on a different network from the Database Server, et al. and across the firewall to assist in further tightening the access to these systems. This would also provide for making it more difficult for a potential intruder to guess the whereabouts of your key systems if they should obtain access to an internal host via a Trojan of some kind.
- Deny what is not required: Avoid outbound access permitted from internal systems that don't need it. In this example, there's no clear practical reason why ftp is permitted outbound. However, since it is, this was a convenient means to send the retrieved database out.
- Avoid permitting "All" in a VPN to any network. It might be easier to do, but it's not necessarily the most secure.
- Host based firewall: Many host based firewalls can detect applications attempting to connect to the Internet. In this scenario, this could potentially defeat the Trojan.

References

[1] "Basic System Management Commands"
URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt3/frf012.htm#1019552 (July 2003)

[2] "Configuring Site-to-Site VPN between Safe@Office with DAIP and VPN-1 NG"
URL:http://support.checkpoint.com/kb/docs/public/sofaware/pdf/DAIP_Support.pdf (July 2003)

[3] "Declude Virus server anti-virus for your IMail mail server"
URL: http://www.declude.com/Virus/index.html (July 2003)

[4] Degner, Mark. "Securing Your Network With AN Internet Access Router"
URL: http://www.sans.org/rr/papers/38/242.pdf (July 2003)

[5] Dietrich, Dave et al… "The Bogon Reference Page"
URL: http://www.cymru.com/Bogons/index.html (July 2003)

[6] "DShield - Distributed Intrusion Detection System"
URL: http://www.dshield.org (July 2003)

[7] "F-Prot Antivirus for Windows, Linux, BSD, Exchange, AIX and DOS | F-Prot AVES - anti-spam and anti-virus e-mail filtering service"
URL: http://www.f-prot.com/products/home_use/dos/ (July 2003)

[8] Graesser, Dave. "Cisco Router Hardenning Step-by-Step"
URL: http://www.sans.org/rr/paper.php?id=794 (July 2003)

[9] Green, Joe. "How to configure SecureClient, Office Mode, Certificates, and Remote Access Communities in NG FP-3."
URL:http://support.checkpoint.com/kb/docs/public/securemote/ng/pdf/scngfp3_config.pdf (July 2003).

[10] "Hilgraeve: DropChute Products: Using DropChute Behind a Firewall"
URL: http://www.hilgraeve.com/dcplus/dcfirewall.html (July 2003)

[11] "Hilgraeve: Products: DropChute Enterprise"
URL: http://www.hilgraeve.com/dropchute/enterprise/index.html (July 2003)

[12] "IMail Server by Ipswitch - The 20 Minute E-Mail Solution."
URL: http://www.ipswitch.com/products/imail_server/index.html (July 2003)

[13] “Infoblox - DNS, DHCP, LDAP, and RADIUS Server Appliances and Network Identity Management Solutions”
URL: http://www.infoblox.com/ (July 2003)

[14] “Millennium Bankcard - The Free e-Solution”
URL: http://www.mbankcard.com/ (July 2003)

[15] Scott, Steven. “Snort Enterprise Implementation”
URL: http://www.superhac.com/docs/snort_enterprise.pdf (July 2003)

[16] “Secured by Check Point Appliances”
URL: http://www.checkpoint.com/products/choice/platforms/nokiaip30.html (July 2003)

[17] “SecurityFocus BUGTRAQ Vulns Info: SonicWALL Pro Large HTTP POST Denial of Service Vulnerability”
URL: http://www.securityfocus.com/bid/7435 (July 2003)

[18] Smith, Greg. “SecurityFocus BUGTRAQ Mailing List: BugTraq”
URL: http://www.securityfocus.com/archive/1/319712 (July 2003)

[19] Tauer, Brad. “GIAC Certified Firewall Analyst, Practical Assignment”
URL: http://www.giac.org/practical/GCFW/Brad_Tauer.pdf (July 2003)

[20] Thomas, Rob. “Secure IOS Template v3.0 08 APR 2003 Rob Thomas robt@cymru.com”
URL: http://www.cymru.com/Documents/secure-ios-template.html (July 2003)

[21] “WhatsUp Gold by Ipswitch - Easy to Use Network Monitoring Software”
URL: http://www.ipswitch.com/Products/WhatsUp/index.html (July 2003)

Appendix A – Internal Router configuration

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service dhcp
!
hostname GIAC_Internal
!
boot system flash c2600-is-mz.120-7.T2.bin
logging buffered 4096 debugging
enable secret 5 $1$RZQw$B4c5aKJGQpUUBnvfcBSxQ0
!
clock timezone CDT -6
ip subnet-zero
no ip source-route
no ip finger
!
no ip bootp server
!
interface FastEthernet0/0
 no ip address
 no ip directed-broadcast
 speed 100
 full-duplex
 no cdp enable
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 192.168.100.20 255.255.255.0
 no ip directed-broadcast
 ip policy route-map filter
!
interface FastEthernet0/0.2
 encapsulation dot1Q 150
 ip address 192.168.150.20 255.255.255.0
 no ip directed-broadcast
 ip policy route-map filter
!
interface FastEthernet0/1
 ip address 192.168.20.20 255.255.255.0
 no ip directed-broadcast
 speed 100
```

```
 full-duplex
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 Null0
no ip http server
!
access-list 50 permit 192.168.100.0 0.0.0.255
access-list 50 permit 192.168.150.0 0.0.0.255
no cdp run
route-map filter permit 10
 match ip address 50
 set ip next-hop 192.168.20.10
!
banner motd ^C
*** NOTICE ***** NOTICE ***** NOTICE ***
*                               *
* Unauthorized access is prohibited!   *
* All access is subject to logging and *
* unauthorized access to this device   *
* is subject to criminal prosecution.  *
* If you do not have authorized access *
* to this device, then you must        *
* disconnect now.                      *
****************************************


^C
!
line con 0
 exec-timeout 0 0
 password 7 1040581E0D031E5A0B0C3E
 login
 transport input none
line aux 0
 password 7 130B46150318087B2C2C3C
 login
line vty 0 4
 password 7 09421F0E11111B430C0410
 login
!
end
```

Appendix B – Border Router configuration

```
Current configuration
!
version 12.3
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
no service dhcp
!
hostname GE-Border
!
boot system flash:c3725-ik9s-mz.123-1a.bin
logging buffered 16384 debugging
no logging console
enable secret 5 $1$EAje$2gZvU3p7P9n579eVQCYH0.
!
username giacsa password 7 13151601181B0B382F
clock timezone CDT -6
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
aaa session-id common
ip subnet-zero
no ip source-route
!
!
ip cef
ip ftp username rooter
ip ftp password 7 12090404011C03162E
no ip domain lookup
ip domain name giac.net
!
no ip bootp server
ip ssh source-interface FastEthernet0/0
!
!
!
```

```
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
interface Null0
 no ip unreachables
!
interface FastEthernet0/0
 description Internal ethernet interface
 ip address 206.45.67.20 255.255.255.0
 ip access-group 110 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 duplex auto
 speed auto
!
interface Serial0/0
 description T1 interface to Internet
 ip address 12.13.14.13 255.255.255.0
 ip access-group 120 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 12.13.14.14
ip route 0.0.0.0 254.0.0.0 Null0
ip route 2.0.0.0 255.0.0.0 Null0
ip route 5.0.0.0 255.0.0.0 Null0
ip route 7.0.0.0 255.0.0.0 Null0
ip route 10.0.0.0 255.0.0.0 Null0
ip route 23.0.0.0 255.0.0.0 Null0
```

```
ip route 27.0.0.0 255.0.0.0 Null0
ip route 31.0.0.0 255.0.0.0 Null0
ip route 36.0.0.0 254.0.0.0 Null0
ip route 39.0.0.0 255.0.0.0 Null0
ip route 41.0.0.0 255.0.0.0 Null0
ip route 42.0.0.0 255.0.0.0 Null0
ip route 49.0.0.0 255.0.0.0 Null0
ip route 50.0.0.0 255.0.0.0 Null0
ip route 58.0.0.0 254.0.0.0 Null0
ip route 70.0.0.0 254.0.0.0 Null0
ip route 72.0.0.0 248.0.0.0 Null0
ip route 83.0.0.0 255.0.0.0 Null0
ip route 84.0.0.0 252.0.0.0 Null0
ip route 88.0.0.0 248.0.0.0 Null0
ip route 96.0.0.0 224.0.0.0 Null0
ip route 169.254.0.0 255.255.0.0 Null0
ip route 172.16.0.0 255.240.0.0 Null0
ip route 173.0.0.0 255.0.0.0 Null0
ip route 174.0.0.0 254.0.0.0 Null0
ip route 176.0.0.0 248.0.0.0 Null0
ip route 184.0.0.0 252.0.0.0 Null0
ip route 189.0.0.0 255.0.0.0 Null0
ip route 190.0.0.0 255.0.0.0 Null0
ip route 192.0.2.0 255.255.255.0 Null0
ip route 192.168.0.0 255.255.0.0 Null0
ip route 197.0.0.0 255.0.0.0 Null0
ip route 198.18.0.0 255.254.0.0 Null0
ip route 223.0.0.0 255.0.0.0 Null0
!
!
logging trap debugging
logging facility local5
logging 206.45.67.101
access-list 20 remark SNMP ACL
access-list 20 permit 206.45.67.100
access-list 20 deny   any log-input
access-list 90 permit 206.45.67.150 log
access-list 90 deny   any log-input
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq smtp
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq www
access-list 110 permit udp 206.45.67.0 0.0.0.255 any eq domain
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq domain
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 443
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 2030
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 123
access-list 110 permit udp 206.45.67.0 0.0.0.255 any eq ntp
```

```
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 981
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq 2847
access-list 110 permit tcp 206.45.67.0 0.0.0.255 any eq ftp
access-list 110 permit udp 206.45.67.10 0.0.0.0 any eq 500
access-list 110 deny   ip any any log-input
access-list 120 deny   ip 0.0.0.0 1.255.255.255 any log-input
access-list 120 deny   ip 2.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 5.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 7.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 10.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 23.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 27.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 31.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 36.0.0.0 1.255.255.255 any log-input
access-list 120 deny   ip 39.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 41.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 42.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 49.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 50.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 58.0.0.0 1.255.255.255 any log-input
access-list 120 deny   ip 70.0.0.0 1.255.255.255 any log-input
access-list 120 deny   ip 72.0.0.0 7.255.255.255 any log-input
access-list 120 deny   ip 83.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 84.0.0.0 3.255.255.255 any log-input
access-list 120 deny   ip 88.0.0.0 7.255.255.255 any log-input
access-list 120 deny   ip 96.0.0.0 31.255.255.255 any log-input
access-list 120 deny   ip 169.254.0.0 0.0.255.255 any log-input
access-list 120 deny   ip 172.16.0.0 0.15.255.255 any log-input
access-list 120 deny   ip 173.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 174.0.0.0 1.255.255.255 any log-input
access-list 120 deny   ip 176.0.0.0 7.255.255.255 any log-input
access-list 120 deny   ip 184.0.0.0 3.255.255.255 any log-input
access-list 120 deny   ip 189.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 190.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 192.0.2.0 0.0.0.255 any log-input
access-list 120 deny   ip 192.168.0.0 0.0.255.255 any log-input
access-list 120 deny   ip 197.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 198.18.0.0 0.1.255.255 any log-input
access-list 120 deny   ip 223.0.0.0 0.255.255.255 any log-input
access-list 120 deny   ip 224.0.0.0 31.255.255.255 any log-input
access-list 120 deny   ip 206.45.67.0 0.0.0.255 any log-input
access-list 120 permit tcp any host 206.45.67.14 eq www
access-list 120 permit tcp any host 206.45.67.14 eq 443
access-list 120 deny   tcp any any eq www
access-list 120 deny   tcp any any eq 443
access-list 120 deny   tcp any any eq 1433
```

```
access-list 120 deny   tcp any any eq 1434
access-list 120 deny   tcp any any eq 445
access-list 120 deny   udp any any eq netbios-ns
access-list 120 deny   udp any any eq netbios-dgm
access-list 120 deny   tcp any any eq 139
access-list 120 permit ip any 206.45.67.0 0.0.0.255
access-list 120 deny   ip any any log-input
no cdp run
!
snmp-server community makeithardtoguess RO 20
snmp-server enable traps tty
!
radius-server authorization permit missing Service-Type
!
!
!
!
line con 0
 exec-timeout 15 0
line aux 0
 exec-timeout 0 10
 no exec
line vty 0 4
 access-class 90 in
 exec-timeout 15 0
 transport input ssh
!
exception core-file GE-Border
exception protocol ftp
exception dump 206.45.67.101
ntp authentication-key 6767 md5 0058202327692E3224047510 7
ntp authenticate
ntp trusted-key 6767
ntp server 206.45.67.101 key 6767
!
end
```