# Global Information Assurance Certification Paper

# Firewalls, Perimeter Protection, and VPNs

# GCFW Practical Assignment
# Version 1.5e



**by**

**Duncan Molony**
**September 25, 2001**

**Rocky Mountain SANS**

## Section I – GIAC Security Architecture

### Background

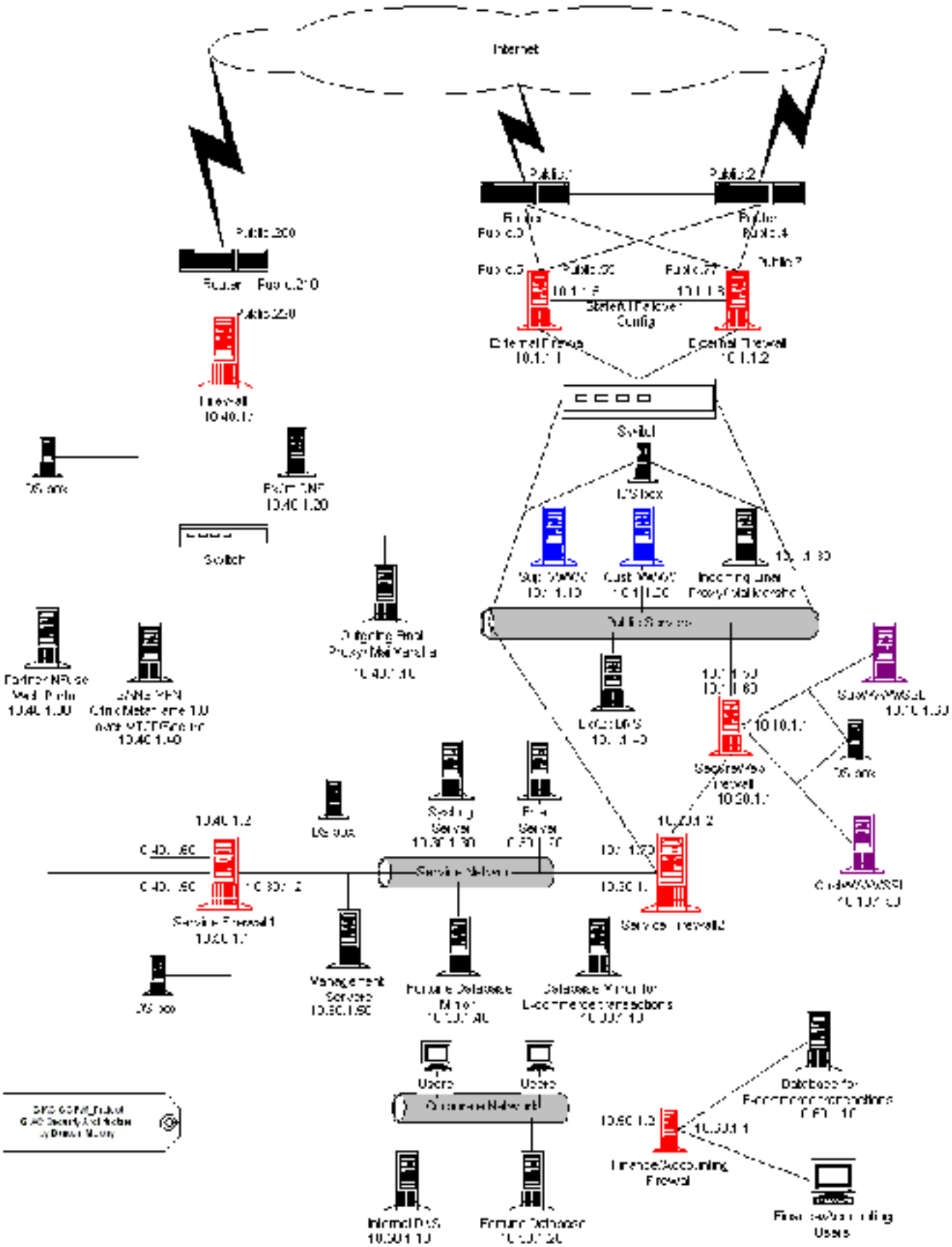
GIAC is a young, but well funded e-business specializing in the sale of fortune cookie sayings. Their customers are the manufacturers of fortune cookies; their suppliers are primarily individuals who author the sayings; and their partners are people from around the globe who translate and resell the sayings. The business model they are using relies strictly on the business-to-business sales through the Internet. Since the Internet is the ONLY sales medium GIAC is implementing, the Board of Directors realizes the importance of the technological infrastructure and technical staff and is committing a substantial percentage of the overall budget to these areas.

The company is expecting to reach their annual sales goal of $200 million in the next fiscal year. To enhance their position in the market they have recently completed the acquisition of SANS, another supplier of fortune cookie sayings that has an established customer base and a similar business model. The two companies are still operating in separate locations with the employees at the former SANS site using a VPN connection to connect to GIAC's systems.

GIAC has invested in what they consider to be a fault tolerant, user friendly and secure infrastructure. Customers and casual web surfers are provided fast access to the companies web pages; customers are provided a secure environment in which to place orders; suppliers are provided a secure environment in which to submit new sayings; partners are provided a secure VPN channel in order to perform their translations; and remote staff, travelers and SANS staff, are provided a secure VPN channel into the GIAC network. It should be noted that while partners are allowed to resell sayings this is done by way of providing the partners a web site hosted by GIAC, thus the infrastructure must have the bandwidth and address space available to host multiple web sites. This is the only way to ensure the copyright protection of GIAC's product, the fortune sayings.

### The Network

The following diagram represents the logical structure of the GIAC network. Not all detail has been included – the focus of this report is on the public and semi-public areas of the network, including the Public Servers, VPN Network, and Service Network. The Corporate network has been simplified for the demonstration purposes of this report. In addition, please note that this is not a literal, one-to-one, diagram. There are multiple boxes performing the same functions, such as Cust_WWW and Sup_WWW. The network has been divided into a Public Access side and a Private VPN side. The Public Access side is configured to allow incoming traffic to the Public Servers and allow out only very limited traffic originating from within the Public Access side. The Private VPN side is configured to allow DNS, web and email traffic out and only VPN traffic in. The basic concept is to provide one "In" door and one "Out" door and limit the exceptions to the flow of traffic. GIAC has assigned one of the IT staff to be the Security Configuration Manager. This position is responsible for ensuring that all systems are hardened and maintained with current service packs, patches, hot fixes, and firmware upgrades. The systems in this report are to be considered hardened and patched to current levels.



**Connections**:
As was stated earlier, GIAC has committed significant resources to the technological operations of its business. The first evidence of this are the data connections GIAC has committed to using. Redundant T3 lines that are supplied by different vendors service the public areas of the network, the web servers and incoming email proxy. The Board of Directors does not want a customer or potential customer waiting for web pages to load. For the VPN side of the network, multiple T1 lines are used (they are represented by one connection on the diagram in order to conserve space). GIAC has obtained a Class 'C' address space for the Network. For the purposes of this report the network address will be represented as **public.0**, where the last octet is the host id.

NOTE: The idea used to develop the network diagram is to balance a desire to minimize the occurrence of single points of failure with an absolute need for security. Security is needed to protect not only the intellectual property of GIAC, but also to protect the security of our customers and partners. If the design seems like a bit of overkill, keep in mind that GIAC is a relatively new company and expects to grow the business well beyond the short-term projections of $200 million annual sales.

**Border Routers – Public**

These routers are actually one Cisco 7576 Router Chassis that contains two independent 7500 series routers in a fault tolerant configuration running Cisco's IOS 12.2. This router will provide excellent throughput and reliability while filtering the 'noise' of the Internet. Its primary security functions will be:

1) Reduce the unwanted and possibly malicious broadcast packets;
2) Filter out packets coming from the Internet with source addresses in the private and reserved address ranges;
3) Filter spoofed packets coming from the Internet with source address within the range of addresses owned by GIAC;
4) Filter unknown protocols; and
5) Filter out packets containing questionable options such as source routing.

In addition, this Border Router will be used to perform egress filtering as a backup to the egress filtering performed by the public External Firewalls. Packets that will be blocked from exiting the network include:

1) Spoofed packets – packets that contain source addresses that are not within GIAC's address range; and
2) Broadcast packets.

**External Firewalls – Public**

Two (2) PIX 525 firewall appliances will be used as the primary line of defense between the Internet and GIAC's public network. These devices are capable of handling a significant number of concurrent connections and provide substantial data throughput. The two devices will be connected and configured to provide stateful failover. This

configuration will allow the secondary, or backup, device to assume the functions of the primary in the event of the primary device's failure while maintaining the state of existing connections. This redundancy will provide maximum availability for the visitors to the sites hosted on the GIAC network while maintaining consistent security. The security functions of these devices will include:

1) Limiting access to specific IP address and service port combinations;
2) Blocking unused ports;
3) Preventing direct access from the Internet to the internal network (Service Firewall_2);
4) Blocking packets originating from within the protected public network, with the exception of packets from the Secure Web Firewall destined for the network of the Bank which provides credit card approval services;
5) Prevent email spoofing by blocking outgoing SMTP traffic; and
6) Logging connection attempts that violate the access rules.

Since these devices are firewall appliances, no operating system hardening will be required; however, firmware updates will be applied as they become available.

**Public Servers**

All of the public Servers are running fully hardened Windows 2000. The Web servers are running IIS 5.0 with all service packs and security patches applied and kept up to date. Load balancing is used for the web servers but is not represented on the network diagram and is beyond the scope of this report.

**Cust_WWW**

This box on the diagram represents all of the servers that host GIAC's general web pages for customers and potential customers. It also represents the servers used to provide web sites for the partners who have a resale agreement with the company.

**Sup_WWW**

This server provides an entrance portal for all of GIAC's suppliers. It provides general information, news and access to the secure site where the suppliers can provide the fortunes.

**Incoming Email Proxy**

GIAC uses MailMarshall software as the email proxy. All incoming emails are inspected for suspicious content and the emails and attachments are scanned with a third party virus scanner. The Proxy is configured to only forward email destined for the GIAC domain. Once email has been inspected and scanned and deemed 'safe' it is forwarded to the GIAC Email server in the Service Network.

**External / External DNS**

This DNS server provides name resolution services for incoming Internet connections. The only entries on this server are for systems within the Public Access area of GIAC's network.

**Intrusion Detection System**

The IDS being used throughout the GIAC network is SNORT running on a hardened version of SuSE Linux 7.2. The IDS is configured to check for traffic that is denied by the rules of the External Firewall and the Border Router. All logs are sent to the Sys Log Server on the Service network.

**Secure Web Firewall**

Symantec's Enterprise Firewall (formerly Raptor) is used as application/proxy firewall to protect the e-commerce server and supplier submission server. Only SSL traffic on port 443 is allowed into the servers on the protected side of the firewall. One-to-one Network address translation (NAT) is used to further protect the servers. The only connections allowed to originate from the protected side of the firewall are connections to the GIAC Service Network for access to the database mirrors, connections to the bank that provides credit card approval, and connection from the IDS to the Syslog server in the Service Network..

**CustWWW/SSl & SupWWW/SSl**

These servers provide a secure transaction environment for customers to place orders (and in some cases, pay for orders with credit cards) and for suppliers to submit the fortune sayings. The suppliers use web forms to enter and categorize their fortune sayings.

**Service Firewall2**

Symantec's Enterprise Firewall (formerly Raptor) is used as application/proxy firewall to protect the Service Network, which contains the database mirrors, email server, syslog server, and management stations. Only traffic from the IDS's, email proxy and the e-commerce servers via the Secure Web Firewall are permitted into the Service Network. All other traffic from the Public Access is dropped. Egress filtering blocks all traffic except Management traffic from specific addresses to the servers on the Public Access Network. All unused protocols and ports are blocked.

**Service Network**

This network consists of systems that contain mirrors of the e-commerce database and fortune database, management services for email proxies, web servers, DNS, and firewalls, Syslog servers, email and Intrusion Detection. This segment of the GIAC network is segregated from both the Public Access network and the Corporate Network. Only IT staff members are allowed to directly access the systems. NAT is used to further obscure the systems on this segment.

**Email Server**

Microsoft Exchange 2000 is used for email. This server handles all internal and external email for GIAC. Email accounts have recently been added for the staff of the former SANS company. Outgoing email is forwarded to the Outgoing Email Proxy on the VPN Network, while all email coming in from the Internet is passed through the Incoming Email Proxy on the Public Access Network.

**Syslog Server**

This server collects the logs from all of the intrusion detection systems, firewalls, web servers, and routers. All logs are duplicated to an array of read only disks on an ongoing basis.

**Database Mirror for E-Commerce Transactions**

Microsoft's SQL Server 2000 is used to mirror the SQL server transaction database located in the Finance/Accounting section of the Corporate Network. Since the account policy is to maintain a complete history of customer information, the synchronization routine allows only for new entries to be passed to the official database. Any modification made to existing data will be treated as suspect and trigger an administrative notice.

**Database Mirror for Fortunes**

Microsoft's SQL Server 2000 is used to mirror the SQL server fortune database on the Corporate Network. This mirror is accessible by the SupWWW/SSl (through the Secure Web Firewall) for suppliers to add fortune sayings to the database. It is also accessible from the Partner VPN in order for the partners to be able to provide translation services for the sayings. For an extra layer of protection, the SANS staff access the mirror and not the original database when they are logged on through the SANS VPN. Employees do not need to access this mirror of the database because they have access to the original in the Corporate Network. The synchronization rules for this database are not as tight as the e-commerce mirror because edits to the records are made as partners translate and remote employees edit. The synchronization routine does check data integrity and size in an attempt to prevent corruption of the original database.

**Management Servers**

These servers are used by the IT staff to monitor and manage the systems on the Service, Public Access and VPN Networks. Only authorized IT staff are permitted to log onto these systems to perform management and monitoring.

**Service Firewall1**

Symantec's Enterprise Firewall (formerly Raptor) is used as application/proxy firewall to protect the Corporate Network. This firewall restricts access to the Service Network from both the VPN and Corporate Networks. From the VPN network, access is permitted to the Fortune database mirror for the Partners and SANS staff, and access is permitted to the email server for the SANS

staff. The Corporate Network users are allowed to access the email server on the Service Network, and surf the Internet through the VPN Network. The Database servers on the Corporate Network (Fortunes and E-Commerce) are permitted to access their respective mirrors on the Service Network. Email sent from the email server on the Service Network is allowed access to the Email Proxy on the VPN Network.

**VPN Network**

The VPN network allows partners, SANS staff, and traveling staff access to GIAC network resources, as well as providing a conduit for the outgoing email and Internet access for the GIAC staff.

**Border Router – VPN**

These routers are actually one Cisco 7576 Router Chassis that contains two independent 7500 series routers in a fault tolerant configuration running Cisco's IOS 12.2. This router will provide excellent throughput and reliability while filtering the 'noise' of the Internet. Its primary security functions will be:

1) Reduce the unwanted and possibly malicious broadcast packets;
2) Filter out packets coming from the Internet with source addresses in the private and reserved address ranges;
3) Filter spoofed packets coming from the Internet with source address within the range of addresses owned by GIAC;
4) Filter unknown protocols; and
5) Filter out packets containing questionable options such as source routing.

In addition, this Border Router will be used to perform egress filtering as a backup to the egress filtering performed by the VPN External Firewall. Packets that will be blocked from exiting the network include:

1) Spoofed packets – packets that contain source addresses that are not within GIAC's address range; and
2) Broadcast packets.

**External Firewall - VPN**

A Cisco PIX 515 firewall appliance provides the protection for this part of the network. Since the traffic on this segment is limited, partner VPN, SANS VPN and GIAC staff Internet access, this PIX model will provide adequate throughput while maintain good security. The primary security function of this device will be:

1) Block any unsolicited incoming traffic not destined for the Nfuse or VSGate servers;

2) Permit SSL connections to both the Nfuse Server and the SANS VPN (VTCP/Secure normally operates through port 11160 but can be configured to use port 443);
3) Permit the Outgoing Email Proxy to transmit SMTP packets;
4) Permit HTTP connection from the Corporate Network; and
5) Permit DNS inquiries from the External/Internal DNS Server.

This firewall will utilize Network Address Translation (NAT) to add another layer of protection. One-to-one NAT will be used for the Nfuse and VTCP/ Secure servers to provide a direct pipe through the firewall for these servers.

**Outgoing Email Proxy**

GIAC uses MailMarshall software as the email proxy. All outgoing emails are inspected for suspicious content and the emails and attachments are scanned with a third party virus scanner. The MailMarshall software is configured to look for email messages and attachments with similar formatting to the fortune sayings from GIAC's database. If a suspicious looking message is detected it is held until it can be reviewed by a supervisor. This is designed to prevent internal 'theft' of fortune sayings. Once email has been inspected and scanned and deemed 'safe' it is forwarded to its destination.

**External/ Internal DNS**

This DNS server provides name resolution services for outgoing Internet connections.

**Partner VPN – Nfuse 1.5 Web Portal**

GIAC's Partners will connect to the GIAC network through the Nfuse web portal. The single box on the diagram is representative of the web server with Nfuse as well as the servers with MetaFrame 1.8 Application Server running. The Partners connect to the Nfuse Web Site using SSL. They submit their credentials, and the MetaFrame servers, through the Nfuse Server, present the Fortune Database Partner Front End program. The MetaFrame servers are permitted to communicate through the Service Firewall1 with the Fortune Database Mirror. These machines are also permitted to access an authentication server on the Service Network (not depicted on diagram to save space).

**SANS VPN – Metaframe 1.8 / VTCP/Secure**

The SANS staff will connect through a VTCP/Secure connection to MetaFrame 1.8 on a Windows 2000 Server. The connection requires the SANS staff to use the VSClient software to connect to the VSGate Server and then they use a ISA Win32 Client to connect to the MetaFrame server. While this increases the steps required for the SANS staff to log into the GIAC network, the added security has been deemed worth the trade off. These users would have access to the Fortune Database Mirror, authentication server, and email server on the Service Network. As added security, no packets from these machines are allowed directly onto the Corporate Network.

**Corporate Network**

The Corporate network is, for the most part, beyond the scope of this report. The only specific systems that have been included in the diagram are the Internal DNS Server, original Fortune Database, Finance/Accounting Firewall and the original E-commerce Database. The database and DNS servers are represented for completeness. The Finance/Accounting Firewall is represented since it provides another layer of security.

**Finance/Accounting Firewall**

This firewall is used to segregate the Finance and Accounting department from the remainder of the GIAC Corporate Network and provide an additional layer of protection for the E-Commerce data. The F & A department, after consultation with the IT Department, has chosen a SonicWall appliance as their firewall because of its ease of configuration and management. The firewall essentially blocks all incoming communication requests. All communication to and from the F & A Department is initiated from within, even the database synchronization.

**Internal DNS**

This DNS server provides name resolution only for systems within the GIAC Corporate Network only.

## Section II – Security Policy

The philosophy used in the creation of the GIAC Network is separation of flow and separation of function. This means that in most circumstances there is only one way in to the GIAC Network and one way out. All traffic coming in will be from the Public side and all traffic leaving will do so from the VPN side. The exceptions to this are the outbound communication from the Secure Web Firewall to GIAC's banking partner. This communication will only take place for credit card authorization. The other exception is for Partner and SANS staff VPN connections. These connections will come in on the VPN side through the SSL port (443). These connections require a greater level of access to resources within the GIAC Network and therefore are separated from the other incoming connections. All outgoing traffic (HTTP, DNS and Mail) will go out through the VPN connection. The security policies implemented on the border routers and firewalls will enforce this policy.

### Border Routers – Public and VPN General Configuration

The primary security functions of these routers are to reduce network 'noise' from entering and leaving the GIAC Network and to limit the information available to the outside world about the configuration of the GIAC Network and security policies.

The first task is to secure the router(s) from unauthorized access and eliminate unnecessary communications that may reveal information about the GIAC Border router(s) or the Network.

```
service password encryption
enable secret [somesecretpassword]
no service tcp-small-servers
no service udp-small-servers
no service finger
no cdp enable
no ip http server
no ip source-route
no ip directed-broadcast
no snmp
no ip unreachables
```

These settings will accomplish the following:

1. Encrypt the router password and enable a one way hash to prevent cracking of the password;
2. Block traffic destined for services with ports lower than 20;
3. Disable the 'finger' service, which can be used to gain information about the Network;
4. Block CDP, Cisco's Discovery Protocol, which can be used to find Cisco devices on the network;
5. Disable the administration http server on the router to prevent tampering;
6. Drop packets with the Source Route bit set;
7. Prevent broadcast packet attacks (Smurf for example);
8. Disable the management protocol SNMP;

9. Disable ICMP host unreachable messages to prevent inverse mapping of the GIAC Network;

Logging has to be set up and configured to send all logs to the Syslog server on the Service Network. The Service Firewall2 is configured to allow traffic from the IP addresses on the Public Network to the Syslog Server on port 514. This will require the routers(s) and other devices to be configured to send logs to the Public Network address of Service Firewall2 – Public.70.

```
logging public.70
```

The router(s) must be configured to allow the Management Servers to Telnet in to be able to configure and manage the devices on the VTY ports. Since the only traffic that is permitted from the Service Network to the Public Network is from the Management Servers, the configuration will require allowing the Public address of the Server Firewall2 to connect to the VTY ports on the router(s). The Border Firewall – Public will provide a static NAT for this communication.

```
access-list 1 permit public.70 0.0.0.255
access-list 1 line vty 0 4
access-class 1 in
```

The following outlines the configuration of the access-list that will be applied to the inbound side of the external serial connection from the ISPs. Communications that have a source address in one of the private or experimental address ranges are assumed to be spoofed packet and are therefore dropped. The following access list will effectively block these communication attempts. Packets with a source address within the GIAC address range will also be dropped.

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny ip 0.0.0.0 255.255.255.255 any log
access-list 101 deny ip public.0 0.0.0.255 any log
```

Systems running Microsoft Windows litter the Internet with NetBIOS traffic. It is a good idea to prevent this unnecessary traffic from clogging the GIAC Network. Blocking TCP and UDP ports 135 through 139 can accomplish this. Port 445 is now used with Windows 2000 and should also be blocked.

```
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445
```

There should never be any need to connect to the router(s)'s outside ip address; therefore, connection attempts to these addresses from the Internet are blocked.

```
access-list 101 deny ip any host public.1
```
* address of corresponding router interface (public.2 and public.200 etc.)

**Border Routers - Public**

Traffic inbound for services supported by the GIAC Network should be allowed. These services include HTTP, HTTPS, DNS, and SMTP. The rules allow only traffic that has the appropriate address/service pair.

```
access-list 101 permit tcp any host public.10 eq http log
access-list 101 permit tcp any host public.20 eq http log
access-list 101 permit tcp any host public.30 eq smtp
access-list 101 permit udp any host public.40 eq domain
access-list 101 permit tcp any host public.50 eq https log
access-list 101 permit tcp any host public.60 eq https log
```

Other entries would be made for additional web servers.
To enforce egress filtering and prevent the hosts on the Public Network from being used by others to launch denial of service or other attacks, all traffic originating from within the GIAC Public Network will be blocked. The only exception will be to permit a connection from the Secure Web Firewall to an authorization server at GIAC's bank.

```
interface ethernet0
ip access-group 115 in
access-list 115 permit tcp host public.50 host bank.101 eq 443
access-list 115 deny ip any any log
```

**Border Routers – VPN**

Traffic inbound from anywhere to the Nfuse server has to be allowed through on port 443. Likewise, traffic must also be allowed from the SANS network to the VTCP/Secure server for VPN connections. However, this traffic must come from the SANS border gateway (SANS.101)

```
access-list 101 permit tcp any host public.230 eq https log
access-list 101 permit tcp host SANS.101 host public.240 eq https log
```

Finally, there is a catchall rule that disallows all other inbound traffic.

```
access-list 101 deny ip any any log
```

To apply the access-list to the inbound external interface use the following commands on all routers:

```
interface serial 0
ip access-group 101 in
```

**Border Firewalls – Public and VPN General Configuration**

These devices will provide the primary line of defense between the 'wild' and the publicly accessible areas of GIAC's Network. The general configuration of the two fault tolerant pairs, Public Network and VPN Network, will be the same, except for interface addresses and names. The configuration differences will be in the specific rule sets for each firewall. Since this report is for demonstration purposes and not a configuration manual, the PIX pair protecting the Public Network will be used for this section. When configuring a failover configuration on a PIX firewall appliance, the configuration is completed on the primary device and once completed the backup, or secondary, device is booted and the configuration is synchronized on the secondary device.

To begin the configuration, each interface is named and a security level is set for each interface. The name makes it easier to identify the interface and the security level is part of the control of traffic flow. Names can be as long as 48 characters, but shorter names are recommended since the name is how the interface will be identified in all configuration tasks and short names are easier to remember and easier to type. Security levels range from 0- 100. In general, the border interfaces should have the lowest security level, followed by the DMZ interface(s) and then by the internal interface(s). For the GIAC Border Firewall this is the interface-naming configuration:

```
nameif ethernet0 outISP1 security0
nameif ethernet1 outISP2 security0
nameif ethernet2 inside security 100
nameif ethernet3 failover security 10
```

Security on the device itself must be set. Passwords, encryption, device name, and default services are set.

```
enable password some_password encrypted
passwd some_password encrypted
hostname GIACBorder1
fixup protocol smtp 25
fixup protocol dns 53
fixup protocol http 80
fixup protocol https 443
```

IP addresses need to be set for each interface. This includes any unused interfaces. While it may seem a waste to assign an IP address to an unused interface, it is required because the failover configuration will send out 'hello' packets on all interfaces. If there are unused interfaces available in each box they should connected to one another by a crossover cable.

```
ip address outISP1 public.5 255.255.255.0
ip address outISP2 public.55 255.255.255.0
ip address inside 10.1.1.1 255.255.0.0
ip address failover 10.1.1.5 255.255.0.0
```

Failover IP addresses must also be assigned since this device is the first in a failover configuration. The first command below enables failover. The next four configure failover for each interface, and the final command specifies the name of the stateful failover interface.

```
failover
failover ip address outISP1 public.7 255.255.255.0
failover ip address outISP2 public.77 255.255.255.0
failover ip address inside 10.1.1.2 255.255.0.0
failover ip address failover 10.1.1.6 255.255.0.0
failover link failover
```

Set the logging level and the syslog server. The level of logging determines what types of messages are logged and, in a sense, the amount of information being collected. The higher the level, the more information. Level 7, or 'debugging', is the highest level and will produce the most information. Since this is a border router, the GIAC management has decided to collect all information possible in an effort to detect any possible break-ins.

```
logging host inside 10.1.1.70
logging trap debugging
```

Finally, the default route has to be set up for the outside interfaces and RIP needs to be disabled on all interfaces.

```
no rip outISP1 passive
no rip outISP1 default
no rip outISP2 passive
no rip outIPS2 default
no rip inside passive
no rip inside default
no rip failover passive
no rip failover default
route outISP1 0 0 public.3
```

**Firewall – Public specific configuration**

The policy of the Public Network firewall is to allow web connections in to the Sup_WWW and Cust_WWW servers, email in to the Incoming Mail Proxy, DNS inquiries in to the EX/EX DNS server, and HTTPS connections in to the SecureWeb Firewall for connection to CustWWW/SSL servers. The only outbound connections originating from within GIAC's Network that are allowed are https connections from the SecureWeb firewall (proxy communications from the WWW/SSL servers) to the GIAC Bank network for credit

card approval; all other outbound connections are denied. Access from the Internet to the Service Firewall2 is denied.

*NOTE: When writing access-lists for the PIX firewall, keep in mind that the list is order dependent. In other words, when a packet enters an interface the rule set of the access-list is applied from top to bottom. The first applicable rule to apply to the packet will be enforced and processing will stop. This makes it very important to pay close attention to order, especially with rules that are either sweeping permit rules or sweeping deny rules. The format for PIX firewall access-lists is:*

*access-list id action protocol source_address source_port destination_address destination_port*

*Where id is an identifying number or text for the particular access-list; action is either 'permit' or 'deny'; protocol is the specific transmission protocol being used (tcp, udp, or icmp); source_address and source_port identify the host or network address and port pair where the specific connection originated; destination_address and destination_port identify the host or network and port pair for which the communication is destined.*

**Inbound Connections**
This access-list is applied to both inbound connections, outISP1 and out ISP2.

```
static (inside,outISP1) public.10 10.1.1.10 netmask 255.255.0.0
static (inside,outISP1) public.20 10.1.1.20 netmask 255.255.0.0
static (inside,outISP1) public.30 10.1.1.30 netmask 255.255.0.0
static (inside,outISP1) public.40 10.1.1.40 netmask 255.255.0.0
static (inside,outISP1) public.50 10.1.1.50 netmask 255.255.0.0
static (inside,outISP1) public.60 10.1.1.60 netmask 255.255.0.0
static (inside,outISP1) public.70 10.1.1.70 netmask 255.255.0.0
access-list acl_isp permit tcp any public.10 eq 80
access-list acl_isp permit tcp any public.20 eq 80
access-list acl_isp permit tcp any public.30 eq 25
access-list acl_isp permit udp any public.40 eq 53
access-list acl_isp permit tcp any public.50 eq 443
access-list acl_isp permit tcp any public.60 eq 443
access-list acl_isp permit udp public.0 255.255.255.0 public.70 eq 514
access-list acl_isp deny ip any public.70
access-list acl_isp deny ip any any
access-group acl_isp in interface outISP1
```

The 16th line of the configuration is a catchall rule. Although there is an implicit deny since the interfaces for outISP1 and outISP2 have the lowest security level, this rule is included as a matter of good practice.

Note: Access-lists can be applied to either the 'in' (when packet first enters the interface) or the 'out' (when packet is leaving the interface) side of an interface. All of these access-lists will be applied to the 'in' side to reduce demand on the CPU. If the rules are applied as the

packet is leaving the interface, the firewall will have had to expend resources to process the packet through the interface.

**Outbound Connections**

This access-list will be applied to the internal interface *inside*. This access-list will allow communication from the Secure Web Firewall to the outside world on port 443 and prevent all other systems on the Public Network from initiating communications with the outside.

```
nat (inside) 1 10.1.1.50 255.255.255.255
global (outISP1) 1 public.50 netmask 255.255.255.0
nat (inside) 2 10.1.1.70 255.255.255.255
global (outISP1) 2 public.70 netmask 255.255.255.0
access-list acl_inside permit tcp host 10.1.1.50 host bank.101 eq 443
access-list acl_inside permit tcp host 10.1.1.70 public.0 255.255.255.0 eq 23
access-list acl_inside deny ip any any
access-group acl_inside in interface inside
```

**Firewall – VPN Specific Configuration**

The VPN Border firewall enforces the policies of Partner connections, SANS staff connections, outbound email and GIAC staff access to the Internet.. The firewall is configured to only allow access in to the Partner Nfuse Web Portal and the SANS VTCP/Secure server. Outbound traffic is allowed from the Outgoing Email Proxy and from the outbound connection of Service Firewall1 (10.40.1.2). The Ex/Int DNS server is also allowed to perform name resolution for the corporate network users This firewall will also provide network address translation (NAT) for all inside systems as a further level of security.

```
nat (inside) 1 10.40.1.2 255.255.255.255
nat (inside) 1 10.40.1.10 255.255.255.255
nat (inside) 1 10.40.1.20 255.255.255.255
global (outISP1) 1 public.220 – public.229 netmask 255.255.255.0
```

All communication originating from within the GIAC VPN and Corporate Networks will be translate to a public address on the outside of the firewall. Only specific types of communication will be allowed out. This will be controlled by an outbound access-list.

```
access-list acl_inside permit tcp host 10.40.1.10 any eq 25
access-list acl_inside permit udp host 10.40.1.20 any eq 53
access-list acl_inside permit tcp host 10.40.1.2 any eq 80
access-list acl_inside deny ip any any
access-group acl_inside in interface inside
```

In order to control inbound traffic, the following access-list will restrict access to the only two systems that should b receiving inbound communication on the VPN Network– Partner Nfuse and the SANS VPN.

```
static (inside, outISP1) public.230 10.40.1.30 netmask 255.255.255.255
static (inside, outISP1) public.240 10.40.1.40 netmask 255.255.255.255
access-list acl_outISP1 permit tcp any host public.230 eq 443 log
access-list acl_outISP1 permit tcp host SANS.101 host public.240 eq 443 log
access-list acl_outISP1 deny ip any any log
access-group acl_outISP1 in interface outISP1
```

**Service Firewalls and Secure Web Firewall**

The Service Firewalls are running Symantec's Enterprise Firewall 6.5. This product was formally Axent Raptor Firewall. The Symantec Raptor Management Console, a graphical interface, is used to configure and manage these firewalls. The following is a brief overview of how to configure the Firewall.

To set up the Network Interfaces of the firewall, open the Raptor Management Console and login to the Firewall you want to configure. Open the 'Base Components' group and select 'Network Interfaces' from the item listed. In the Right panel of the console you will see all interfaces which are currently configured.

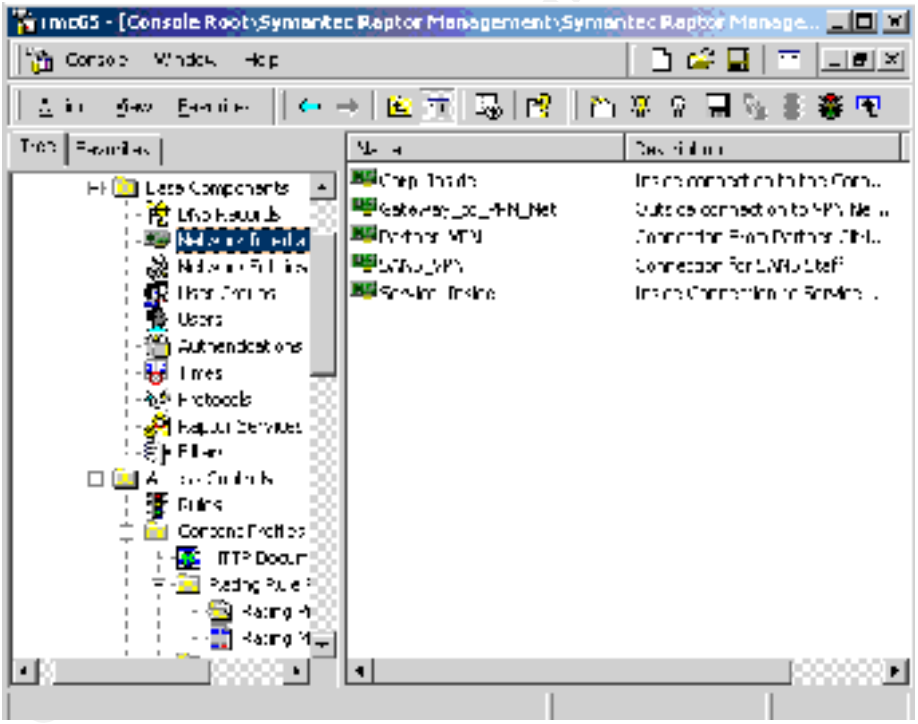


**Figure 1 - Raptor Management Console - Network Interface Configuration**

To configure a new interface, select 'Action: New: Network Interface" This will bring up the Network interface configuration screen. To edit an interface that is already configured, double click on the listing for the interface in the right panel. The "General" tab of the configuration screen is shown below.

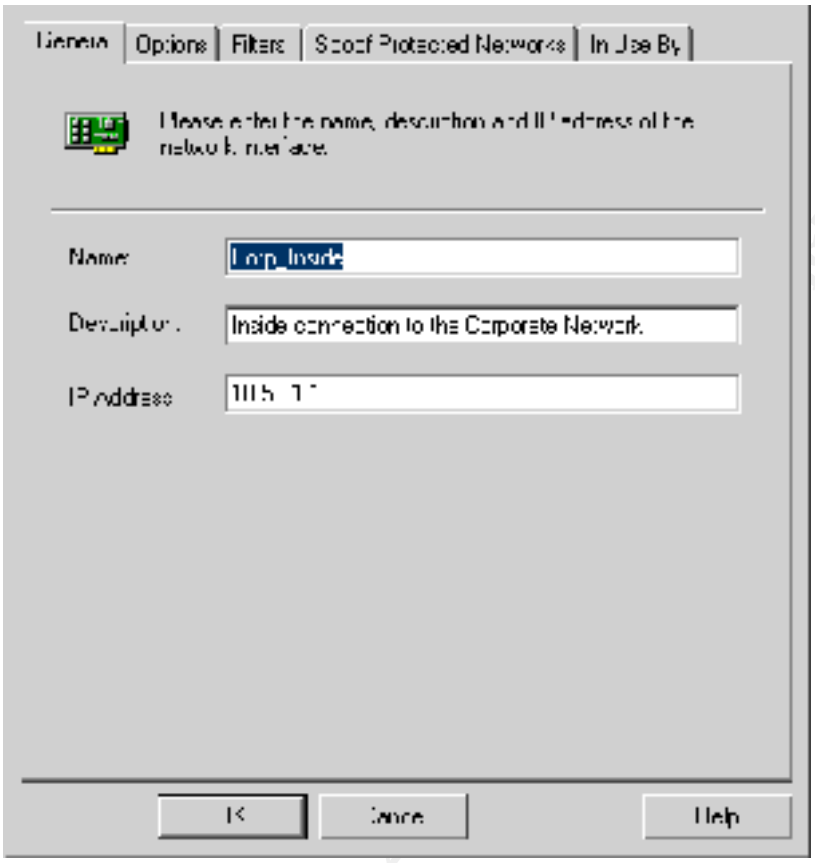



**Figure 2 - Configuration Details of Corp_Inside Interface**

As the screen shows, the "general" tab shows the Name, Description and IP Address of the Interface. The "Options" tab allows for the selection of four options pertaining to this interface. The Four Option are:

- This Address is a member of the Internal Network
- Allow Multicast (UDP-Based) Traffic
- Enable SYN Flood Protection
- Enable Port Scan Detection

To active an option, simply click the box in front of it. The Next tab, "Filter", is used to assign filters or filter groups to packets entering and leaving the interface. The filters are order dependant, so care is to be taken when creating and assigning filters. The "Spoof Protected Networks" tab is used to select networks this interface is to protect from spoofing. GIAC's Border routers perform spoof protection, however, this option can be used as a further degree of protection. The last tab, "In Use By", list the rules that use, or affect, this interface.

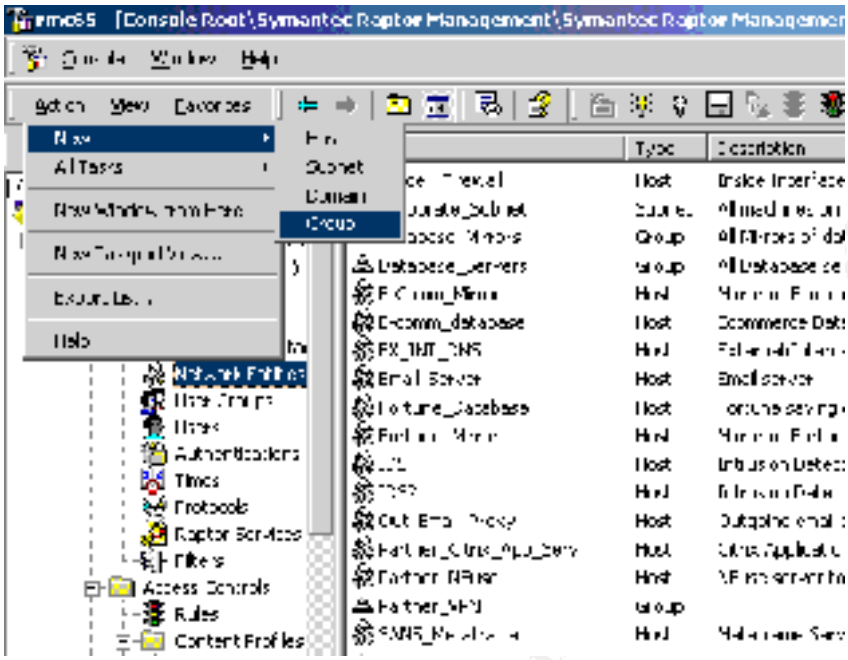



**Figure 3 - Network Entity Configuration Window**

**Figure 4 - New Host Configuration Window**

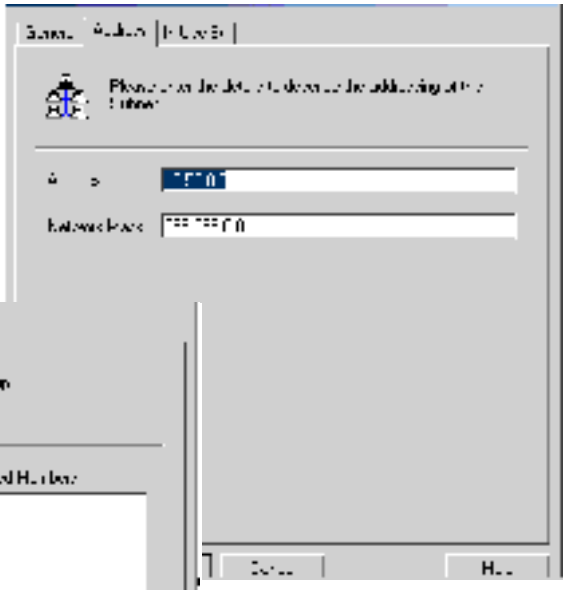


**Figure 5 - New Subnet Address Configuration**


**Figure 6 - New Group Members Configuration**

**Service Firewall1**

This firewall protects the Service Network and the Corporate Network from unauthorized traffic coming through the VPN Network. By default, the Symantec Enterprise Firewall will block all traffic unless there is a specific rule granting access. Service Firewall1 allows the following traffic through:

- From the Partner VPN to the Fortune Database Mirror on the Service Network;
- From the SANS VPN to the Email Server, Fortune Database Mirror, and Authentication Server on the Service Network;
- From the Corporate Network to the Ex/Int DNS server on the VPN Network and through the VPN Border Firewall for Internet access;
- From the Corporate Network to the Email Server on the Service Network;
- From the Email Server on the Service Network to the Outgoing Email Proxy on the VPN Network;
- From all IDS boxes in all subnets and from all servers in the VPN Network to the Syslog Server on the Service Network;
- From the Fortune and E-Commerce Servers on the Corporate Network to the Fortune Database Mirror and E-Commerce Mirror on the Service Network.

The configuration reports for this firewall follow.

**Network Entity Report**

```
          Name: AuthenticationServer
          Description: Authentication Server for the SANS VPN logon
          Type: Host
                    Address: 10.30.1.100
                    MAC Address:
==================================================
          Name: Border_Firewall
          Description: Inside Interface of VPN Border Firewall
          Type: Host
                    Address: 10.40.1.1
                    MAC Address:
==================================================
          Name: Corporate_Subnet
          Description: All machines on Corp. Network
          Type: Subnet
                    Address: 10.50.0.0
                    Network Mask: 255.255.0.0
==================================================
          Name: Database_Mirrors
          Description: All Mirrors of database servers on the Service Network
          Type: Group
          NetworkEntity Member:
                    Name: E-Comm_Mirror
                    Description: Mirror of Ecommerce database
                    Type: Host
                              Address: 10.30.1.10
                              MAC Address:
          NetworkEntity Member:
                    Name: Fortune_Mirror
                    Description: Mirror of Fortune Database
                    Type: Host
                              Address: 10.30.1.40
                              MAC Address:
==================================================
          Name: Database_Servers
          Description: All Database servers on the Corp. Network
```

```
          Type: Group
          NetworkEntity Member:
                    Name: E-comm_database
                    Description: Ecommerce Database behind finance firewall
                    Type: Host
                              Address: 10.50.1.3
                              MAC Address:
          NetworkEntity Member:
                    Name: Fortune_Database
                    Description: Fortune saying database
                    Type: Host
                              Address: 10.50.1.20
                              MAC Address:
==================================================
          Name: E-Comm_Mirror
          Description: Mirror of Ecommerce database
          Type: Host
                    Address: 10.30.1.10
                    MAC Address:
==================================================
          Name: E-comm_database
          Description: Ecommerce Database behind finance firewall
          Type: Host
                    Address: 10.50.1.3
                    MAC Address:
==================================================
          Name: EX_INT_DNS
          Description: External/Internal DNS
          Type: Host
                    Address: 10.40.1.20
                    MAC Address:
==================================================
          Name: Email_Server
          Description: Email server
          Type: Host
                    Address: 10.30.1.20
                    MAC Address:
==================================================
          Name: Fortune_Database
          Description: Fortune saying database
          Type: Host
                    Address: 10.50.1.20
                    MAC Address:
==================================================
          Name: Fortune_Mirror
          Description: Mirror of Fortune Database
          Type: Host
                    Address: 10.30.1.40
                    MAC Address:
==================================================
          Name: IDS
          Description: Intrusion Detection Server
          Type: Host
                    Address: 10.40.1.250
                    MAC Address:
==================================================
          Name: IDS2
          Description: Intrusion Detection Server
          Type: Host
                    Address: 10.50.1.250
                    MAC Address:
==================================================
          Name: Out_Email_Proxy
          Description: Outgoing email proxy
          Type: Host
                    Address: 10.40.1.10
                    MAC Address:
==================================================
          Name: Partner_Citrix_App_Serv
          Description: Citrix Application Server for Partner Access
          Type: Host
```

```
                    Address: 10.40.1.31
                    MAC Address:
==================================================
          Name: Partner_NFuse
          Description: NFuse server for Patner VPN access to Citrix Servers
          Type: Host
                    Address: 10.40.1.30
                    MAC Address:
==================================================
          Name: Partner_VPN
          Description:
          Type: Group
          NetworkEntity Member:
                    Name: Partner_Citrix_App_Serv
                    Description: Citrix Application Server for Partner Access
                    Type: Host
                              Address: 10.40.1.31
                              MAC Address:
          NetworkEntity Member:
                    Name: Partner_NFuse
                    Description: NFuse server for Patner VPN access to Citrix Servers
                    Type: Host
                              Address: 10.40.1.30
                              MAC Address:
==================================================
          Name: SANS_Metaframe
          Description: Metaframe Server for SANS Connection
          Type: Host
                    Address: 10.40.1.41
                    MAC Address:
==================================================
          Name: SANS_VPN
          Description:
          Type: Group
          NetworkEntity Member:
                    Name: SANS_Metaframe
                    Description: Metaframe Server for SANS Connection
                    Type: Host
                              Address: 10.40.1.41
                              MAC Address:
          NetworkEntity Member:
                    Name: SANS_VTCP_Secure
                    Description: VTCP/Secure server for encrypted Communication
                    Type: Host
                              Address: 10.40.1.40
                              MAC Address:
==================================================
          Name: SANS_VTCP_Secure
          Description: VTCP/Secure server for encrypted Communication
          Type: Host
                    Address: 10.40.1.40
                    MAC Address:
==================================================
          Name: SYSLOG_Contributors
          Description:
          Type: Group
          NetworkEntity Member:
                    Name: Border_Firewall
                    Description: Inside Interface of VPN Border Firewall
                    Type: Host
                              Address: 10.40.1.1
                              MAC Address:
          NetworkEntity Member:
                    Name: IDS
                    Description: Intrusion Detection Server
                    Type: Host
                              Address: 10.40.1.250
                              MAC Address:
          NetworkEntity Member:
                    Name: IDS2
                    Description: Intrusion Detection Server
```

```
                    Type: Host
                              Address: 10.50.1.250
                              MAC Address:
          NetworkEntity Member:
                    Name: Out_Email_Proxy
                    Description: Outgoing email proxy
                    Type: Host
                              Address: 10.40.1.10
                              MAC Address:
          NetworkEntity Member:
                    Name: Partner_Citrix_App_Serv
                    Description: Citrix Application Server for Partner Access
                    Type: Host
                              Address: 10.40.1.31
                              MAC Address:
          NetworkEntity Member:
                    Name: Partner_NFuse
                    Description: NFuse server for Patner VPN access to Citrix Servers
                    Type: Host
                              Address: 10.40.1.30
                              MAC Address:
          NetworkEntity Member:
                    Name: SANS_Metaframe
                    Description: Metaframe Server for SANS Connection
                    Type: Host
                              Address: 10.40.1.41
                              MAC Address:
          NetworkEntity Member:
                    Name: SANS_VTCP_Secure
                    Description: VTCP/Secure server for encrypted Communication
                    Type: Host
                              Address: 10.40.1.40
                              MAC Address:
==================================================
          Name: SYSLOG_Server
          Description: Syslog Server on Service Network
          Type: Host
                    Address: 10.30.1.30
                    MAC Address:
==================================================
          Name: Service_Net
          Description: Service Network
          Type: Subnet
                    Address: 10.30.0.0
                    Network Mask: 255.255.0.0
==================================================
          Name: Service_SANS
          Description: Servers on the Service Net accessible by SANS VPN
          Type: Group
          NetworkEntity Member:
                    Name: AuthenticationServer
                    Description: Authentication Server for the SANS VPN logon
                    Type: Host
                              Address: 10.30.1.100
                              MAC Address:
          NetworkEntity Member:
                    Name: Email_Server
                    Description: Email server
                    Type: Host
                              Address: 10.30.1.20
                              MAC Address:
          NetworkEntity Member:
                    Name: Fortune_Mirror
                    Description: Mirror of Fortune Database
                    Type: Host
                              Address: 10.30.1.40
                              MAC Address:
==================================================
          Name: Syslog_Server
          Description: Syslog Server on Service Network
          Type: Host
```

```
                    Address: 10.30.1.30
                    MAC Address:
================================================
          Name: Universe*
          Description:
          Type: Host
                    Address: 0.0.0.0
                    MAC Address:
================================================
```

## Rules Report

```
          Rule ID: 1
          Description: Syslog Entries
          Services: syslog syslog_rev
          Service Limits:  514/udp 1024-65535/udp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Gateway_to_VPN_Net
          Out Via: Any
          Source: SYSLOG_Contributors
          Destination: SYSLOG_Server
          Log Normal Activity: 1
          Application Data Scanning: 1
================================================
          Rule ID: 2
          Description: Corp_Web_Access
          Services: dns_udp http* https
          Service Limits:  http http-allurl http-allext 53/udp 443/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0  http:1 http-https:0 http-
tunnel:any http-tunnel.list: http-dcom-tunnel:0 http-ftp:0 http-gopher:0 http-finjan:0 http-
allurl:0 http-allext:0 http-proxy: http-proxy.ipaddress:
          Advanced Services:
          Application Scanning: 1
          In Via: Corp_Inside
          Out Via: Gateway_to_VPN_Net
          Source: Corporate_Subnet
          Destination: Universe*
          Log Normal Activity: 1
          Application Data Scanning: 1
================================================
          Rule ID: 3
          Description: Partner_VPN
          Services: nbdgram* netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  nbdgram 137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Partner_VPN
          Out Via: Service_Inside
          Source: Partner_VPN
          Destination: Fortune_Mirror
          Log Normal Activity: 1
          Application Data Scanning: 1
================================================
          Rule ID: 4
          Description: SANS_VPN
          Services: nbdgram* netbios_137_udp netbios_139_tcp smtp* SQL_Session
          Service Limits:  smtp nbdgram 137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0  smtp.rlimit.soft:
smtp.rlimit.hard: smtp.hide: smtp.read: smtp.check_orig_domain:0 smtp.no_srcroutes:0
smtp.no_telnet:0 smtp.loose_recip:0 smtp.loose_orig:0
          Advanced Services:
          Application Scanning: 1
          In Via: SANS_VPN
          Out Via: Service_Inside
          Source: SANS_VPN
```

```
          Destination: Service_SANS
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 5
          Description: Corp_Syslog
          Services: syslog
          Service Limits:  514/udp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Corp_Inside
          Out Via: Service_Inside
          Source: IDS2
          Destination: SYSLOG_Server
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 6
          Description: Corp_Email
          Services: smtp*
          Service Limits:  smtp smtp.no_telnet
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0  smtp.rlimit.soft:
smtp.rlimit.hard: smtp.hide: smtp.read: smtp.check_orig_domain:0 smtp.no_srcroutes:0
smtp.no_telnet:1 smtp.loose_recip:0 smtp.loose_orig:0
          Advanced Services:
          Application Scanning: 1
          In Via: Corp_Inside
          Out Via: Service_Inside
          Source: Corporate_Subnet
          Destination: Email_Server
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 7
          Description: Email_to_Proxy
          Services: smtp*
          Service Limits:  smtp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0  smtp.rlimit.soft:
smtp.rlimit.hard: smtp.hide: smtp.read: smtp.check_orig_domain:0 smtp.no_srcroutes:0
smtp.no_telnet:0 smtp.loose_recip:0 smtp.loose_orig:0
          Advanced Services:
          Application Scanning: 1
          In Via: Service_Inside
          Out Via: Gateway_to_VPN_Net
          Source: Email_Server
          Destination: Out_Email_Proxy
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 8
          Description: Fortune_DB_SYNC
          Services: nbdgram* netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  nbdgram 137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Corp_Inside
          Out Via: Service_Inside
          Source: Fortune_Database
          Destination: Fortune_Mirror
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 9
          Description: E-Comm_DB_Sync
          Services: nbdgram* netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  nbdgram 137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
```

```
          In Via: Corp_Inside
          Out Via: Service_Inside
          Source: E-comm_database
          Destination: E-Comm_Mirror
          Log Normal Activity: 1
          Application Data Scanning: 1
================================================
```

NOTE: In addition to Proxy Rules, packet filtering can also be performed on the Symantec Enterprise Firewall as a first line of defense and to block packets that cannot be blocked by the rules. While there are some basic filters applied to the interfaces, these filters only reinforce the rules and do not block additional traffic. The rules are the primary means of implementing the security policies on the Service Firewalls and Secure Web Firewall.

**Service Firewall2**

This firewall protects the Service Network from unauthorized traffic coming in through the Public Network and the Secure Web Network. The specific policies being enforced are:

- Allow communication from the CustWWW/SSL on the Secure Web Network to the E-Commerce Database Mirror on the Service Network;
- Allow communication from the SupWWW/SSL on the Secure Web Network to the Fortune Database Mirror on the Service Network;
- Allow syslog entries from the servers and firewall on the Public Network and the Secure Web Network to the Syslog Server on the Service Network;
- Allow Management communication from the Management Servers on the Service Network to the Servers, firewall and IDS boxes on the Public and Secure Web Networks;
- Allow incoming email from the Incoming Email Proxy to the Email Server on the Service Network.

Configuration reports from the Service Firewall2:

**Network Entity Report**

```
        Name: AuthenticationServer
        Description: Authentication Server for the SANS VPN logon
        Type: Host
                Address: 10.30.1.100
                MAC Address:
================================================
        Name: Border_Firewall
        Description: Inside Interface of VPN Border Firewall
        Type: Host
                Address: 10.1.1.1
                MAC Address:
================================================
        Name: Cust_WWW
        Description: Customer Public Web Server
        Type: Host
```

```
                Address: 10.1.1.20
                MAC Address:
================================================
        Name: Database_Mirrors
        Description: All Mirrors of database servers on the Service Network
        Type: Group
        NetworkEntity Member:
                Name: E-Comm_Mirror
                Description: Mirror of Ecommerce database
                Type: Host
                        Address: 10.30.1.10
                        MAC Address:
        NetworkEntity Member:
                Name: Fortune_Mirror
                Description: Mirror of Fortune Database
                Type: Host
                        Address: 10.30.1.40
                        MAC Address:
================================================
        Name: E-Comm_Mirror
        Description: Mirror of Ecommerce database
        Type: Host
                Address: 10.30.1.10
                MAC Address:
================================================
        Name: Email_Server
        Description: Email server
        Type: Host
                Address: 10.30.1.20
                MAC Address:
================================================
        Name: ExEx_DNS
        Description: External External DNS Server
        Type: Host
                Address: 10.1.1.40
                MAC Address:
================================================
        Name: Fortune_Mirror
        Description: Mirror of Fortune Database
        Type: Host
                Address: 10.30.1.40
                MAC Address:
================================================
        Name: IDS
        Description: Intrusion Detection Server
        Type: Host
                Address: 10.1.1.250
                MAC Address:
================================================
        Name: Incoming_Email_Proxy
        Description: Incoming Email Proxy and Mail Marshal Server
        Type: Host
                Address: 10.1.1.30
                MAC Address:
```

```
================================================
        Name: Management_Servers
        Description: Servers used to manage the network
        Type: Host
                Address: 10.30.1.50
                MAC Address:
================================================
        Name: Public_Syslog_Contrib
        Description: Contributors to the Syslog Server from the Public Network
        Type: Group
        NetworkEntity Member:
                Name: Border_Firewall
                Description: Inside Interface of VPN Border Firewall
                Type: Host
                        Address: 10.1.1.1
                        MAC Address:
        NetworkEntity Member:
                Name: Cust_WWW
                Description: Customer Public Web Server
                Type: Host
                        Address: 10.1.1.20
                        MAC Address:
        NetworkEntity Member:
                Name: IDS
                Description: Intrusion Detection Server
                Type: Host
                        Address: 10.1.1.250
                        MAC Address:
        NetworkEntity Member:
                Name: Incoming_Email_Proxy
                Description: Incoming Email Proxy and Mail Marshal Server
                Type: Host
                        Address: 10.1.1.30
                        MAC Address:
        NetworkEntity Member:
                Name: Sup_WWW
                Description: Suppliers Public Web Server
                Type: Host
                        Address: 10.1.1.10
                        MAC Address:
================================================
        Name: SYSLOG_Server
        Description: Syslog Server on Service Network
        Type: Host
                Address: 10.30.1.30
                MAC Address:
================================================
        Name: SecureIDS
        Description:
        Type: Host
                Address: 10.20.1.250
                MAC Address:
================================================
        Name: SecureWeb_Group
```

```
        Description: Secure Web Servers and Firewall
        Type: Group
        NetworkEntity Member:
                Name: Secure_CustWWW
                Description: Address for Secure Customer transactions from Secure Web
                Type: Host
                        Address: 10.20.1.50
                        MAC Address:
        NetworkEntity Member:
                Name: Secure_SupWWW
                Description: Address for Secure Supplier Transactions from Secure Web
                Type: Host
                        Address: 10.20.1.60
                        MAC Address:
        NetworkEntity Member:
                Name: Secure_Web_Firewall
                Description: Secure_Web_Firewall Interface
                Type: Host
                        Address: 10.20.1.1
                        MAC Address:
================================================
        Name: Secure_CustWWW
        Description: Address for Secure Customer transactions from Secure Web
        Type: Host
                Address: 10.20.1.50
                MAC Address:
================================================
        Name: Secure_SupWWW
        Description: Address for Secure Supplier Transactions from Secure Web
        Type: Host
                Address: 10.20.1.60
                MAC Address:
================================================
        Name: Secure_Web_Firewall
        Description: Secure_Web_Firewall Interface
        Type: Host
                Address: 10.20.1.1
                MAC Address:
================================================
        Name: Service_Net
        Description: Service Network
        Type: Subnet
                Address: 10.30.0.0
                Network Mask: 255.255.0.0
================================================
        Name: Sup_WWW
        Description: Suppliers Public Web Server
        Type: Host
                Address: 10.1.1.10
                MAC Address:
================================================
        Name: Syslog_Server
        Description: Syslog Server on Service Network
        Type: Host
```

```
                Address: 10.30.1.30
                MAC Address:
================================================
        Name: Universe*
        Description:
        Type: Host
                Address: 0.0.0.0
                MAC Address:
================================================


                Type: Host
                        Address: 10.1.1.250
                        MAC Address:
        NetworkEntity Member:
                Name: Incoming_Email_Proxy
                Description: Incoming Email Proxy and Mail Marshal Server
                Type: Host
                        Address: 10.1.1.30
                        MAC Address:
        NetworkEntity Member:
                Name: Sup_WWW
                Description: Suppliers Public Web Server
                Type: Host
                        Address: 10.1.1.10
                        MAC Address:
================================================
        Name: SYSLOG_Server
        Description: Syslog Server on Service Network
        Type: Host
                Address: 10.30.1.30
                MAC Address:
================================================
        Name: SecureIDS
        Description:
        Type: Host
                Address: 10.20.1.250
                MAC Address:
================================================
        Name: SecureWeb_Group
        Description: Secure Web Servers and Firewall
        Type: Group
        NetworkEntity Member:
                Name: Secure_CustWWW
                Description: Address for Secure Customer transactions from Secure Web
                Type: Host
                        Address: 10.20.1.50
                        MAC Address:
        NetworkEntity Member:
                Name: Secure_SupWWW
                Description: Address for Secure Supplier Transactions from Secure Web
                Type: Host
                        Address: 10.20.1.60
                        MAC Address:
```

```
        NetworkEntity Member:
                Name: Secure_Web_Firewall
                Description: Secure_Web_Firewall Interface
                Type: Host
                        Address: 10.20.1.1
                        MAC Address:
================================================
        Name: Secure_CustWWW
        Description: Address for Secure Customer transactions from Secure Web
        Type: Host
                Address: 10.20.1.50
                MAC Address:
================================================
        Name: Secure_SupWWW
        Description: Address for Secure Supplier Transactions from Secure Web
        Type: Host
                Address: 10.20.1.60
                MAC Address:
================================================
        Name: Secure_Web_Firewall
        Description: Secure_Web_Firewall Interface
        Type: Host
                Address: 10.20.1.1
                MAC Address:
================================================
        Name: Service_Net
        Description: Service Network
        Type: Subnet
                Address: 10.30.0.0
                Network Mask: 255.255.0.0
================================================
        Name: Sup_WWW
        Description: Suppliers Public Web Server
        Type: Host
                Address: 10.1.1.10
                MAC Address:
================================================
        Name: Syslog_Server
        Description: Syslog Server on Service Network
        Type: Host
                Address: 10.30.1.30
                MAC Address:
================================================
        Name: Universe*
        Description:
        Type: Host
                Address: 0.0.0.0
                MAC Address:
================================================
```

## Rules Report

```
          Rule ID: 1
          Description: Secure E-Comm. transactions
```

```
          Services: netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Secureweb_Interface
          Out Via: Service_Inside
          Source: Secure_CustWWW
          Destination: E-Comm_Mirror
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 2
          Description: Secure Supplier Input
          Services: netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Secureweb_Interface
          Out Via: Service_Inside
          Source: Secure_SupWWW
          Destination: Fortune_Mirror
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 3
          Description: Syslog Entries
          Services: syslog
          Service Limits:  514/udp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Gateway_to_Public
          Out Via: Service_Inside
          Source: Public_Syslog_Contrib
          Destination: SYSLOG_Server
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 4
          Description: Incoming Email
          Services: smtp*
          Service Limits:  smtp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0  smtp.rlimit.soft:
smtp.rlimit.hard: smtp.hide: smtp.read: smtp.check_orig_domain:0 smtp.no_srcroutes:0
smtp.no_telnet:0 smtp.loose_recip:0 smtp.loose_orig:0
          Advanced Services:
          Application Scanning: 1
          In Via: Gateway_to_Public
          Out Via: Service_Inside
          Source: Incoming_Email_Proxy
          Destination: Email_Server
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
          Rule ID: 5
          Description: Public_Management
          Services: telnet*
          Service Limits:  telnet
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Service_Inside
          Out Via: Gateway_to_Public
          Source: Management_Servers
          Destination: Universe*
          Log Normal Activity: 1
          Application Data Scanning: 1
==================================================
```

```
          Rule ID: 6
          Description: Secure_Web_Management
          Services: hawk telnet*
          Service Limits:  telnet 418/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Service_Inside
          Out Via: Secureweb_Interface
          Source: Management_Servers
          Destination: SecureWeb_Group
          Log Normal Activity: 1
          Application Data Scanning: 1
================================================
          Rule ID: 7
          Description: Syslog Entries
          Services: syslog
          Service Limits:  514/udp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Secureweb_Interface
          Out Via: Service_Inside
          Source: SecureWeb_Group
          Destination: SYSLOG_Server
          Log Normal Activity: 1
          Application Data Scanning: 1
================================================
```

**SecureWeb Firewall**

This firewall is included as an added layer of protection between the Public Network and the Service Network. All secure web transactions take place in this Secure Web Network. The only non-administrative traffic passing between the Secure Web Network and the Service Network are the SQL Server request from the SSL servers and the database mirrors on the Service Network. The policies being enforced are:

- Allow SQL traffic from CustWWW/SSL to the E-Commerce Database Mirror on the Service Network;
- Allow SQL traffic from SupWWW/SSL to the Fortune Database Mirror on the Service Network;
- Allow traffic on port 443 from the world to the CustWWW/SSL and to the SupWWW/SSL;
- Allow Management traffic to the servers on the Secure Web Network from the Service Network;
- Allow Syslog messages to be transferred from the Secure Web Network to the Syslog Server on the Service Network.

Below is the Rules Configuration Report for this firewall.

**Rules Report**

```
          Rule ID: 1
          Description:
          Services: https
          Service Limits:  443/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Secure_Cust_Gate
          Out Via: Inside_Secure_Net
          Source: Universe*
```

```
          Destination: Secure_CustWWW
================================================
          Rule ID: 2
          Description:
          Services: https
          Service Limits:  443/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Secure_Supplier_Gate
          Out Via: Inside_Secure_Net
          Source: Universe*
          Destination: Secure_SupWWW
================================================
          Rule ID: 3
          Description:
          Services: netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Inside_Secure_Net
          Out Via: Secure_CustWWW
          Source: CustWWW_SSL
          Destination: E-Comm_Mirror
================================================
          Rule ID: 4
          Description:
          Services: netbios_137_udp netbios_139_tcp SQL_Session
          Service Limits:  137/udp 139/tcp 1433/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Inside_Secure_Net
          Out Via: Secure_SupWWW
          Source: SupWWW_SSL
          Destination: Fortune_Mirror
================================================
          Rule ID: 5
          Description:
          Services: syslog
          Service Limits:  514/udp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Inside_Secure_Net
          Out Via: Secure_Web_Firewall
          Source: IDS
          Destination: Syslog_Server
================================================
          Rule ID: 6
          Description:
          Services: hawk
          Service Limits:  418/tcp
          Proxy Limits: ftp-disallow-gets:0 ftp-disallow-puts:0
          Advanced Services:
          Application Scanning: 1
          In Via: Secure_Web_Firewall
          Out Via: Inside_Secure_Net
          Source: Service_Firewall
          Destination: Secure_Manage
```

**Finance/Accounting Firewall**

Even though the internal firewalls are beyond the specific scope of this report, this description is being included for completeness. This device is a SonicWall firewall appliance. This device is a relatively simple firewall in that it has only three interfaces

(WAN, LAN and DMZ). The device is configured by using a web interface built into the appliance. The policies enforced by this firewall are:

- Allow web, email and DNS traffic out of the Finance/Accounting Network to the Universe;
- Allow the E-Commerce Database to synchronize with the E-Commerce Database Mirror in the Service Network;
- Block traffic from the Corporate Network

**VPN Connections**

GIAC has chosen to utilize Citrix MetaFrame for both the Partner and SANS Staff VPNs. The difference is the way in which each VPN channel will authenticate. Since GIAC's Partners change frequently and are located around the world, a solution had to be implemented that would allow good security for their connections while not requiring a client side software that may be difficult to implement and possibly illegal to deport to some contries. To meet these requirements, GIAC chose to implement an Nfuse Web Portal as the VPN front end for the partners (Figure 7). The Nfuse portal will provide an encrypted communication channel over SSL. This makes Partner connections much easier since all that is required is an Internet connection and a web browser capable of SSL. Once authenticated through the Nfuse server, the Partners will have access to the Partner MetaFrame Servers to access the front-end application for the Fortune Database.

The SANS VPN connection has additional security requirements since these users will typically be connected for a longer period of time and will have greater access to the Service Network. The SANS staff will connect to a VTCP/Secure VSGate server by using the VSClient software from their workstations. This provides a triple-DES encrypted tunnel for the SANS staff. Once this tunnel is established, the next step is to connect to the SANS VPN MetaFrame servers using a Citrix ICA Client. Once authenticated to the MetaFrame Server, the SANS staff will have access to the email server and fortune database mirror on the Service Network.

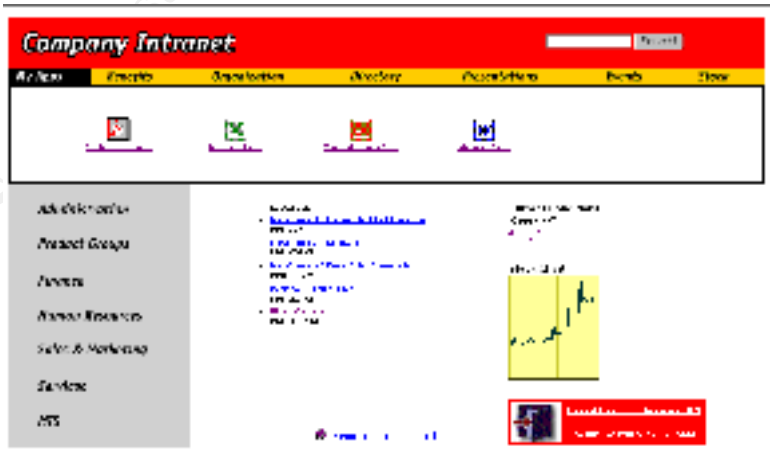



**Figure 7 - Sample Citrix NFuse HTML Interface**

**Section III – Audit of Border Firewalls**

In order to ensure the protection of the GIAC Networks, an internal audit will be performed every quarter and a full audit carried out under the direction of an outside Security Consultant will be performed annually. The quarterly audits are checks performed by GIAC staff under the direction and authority of the GIAC CIO. Primarily GIAC staff will also perform the annual audit; however, an external consultant will direct this audit. The consultant will perform the initial review, planning, some of the actual testing, and the reporting. The GIAC Board of Directors, being acutely aware of the importance of security for an Internet business and understanding the risks involved in the testing, have singed off on the audit. This gives the GIAC staff and the consultant the authority to perform the test without fear of reprisals, assuming the tests are performed according to the plan submitted by the consultant.

**Audit Plan and Scope**

The audit plan submitted calls for testing to be performed over three days in the early morning hours, from 2AM to 6AM. This time frame is the time of lowest network usage from customers, suppliers and partners. Even though the scope of the audit was to be limited to the border firewall, the consultant suggested, and the board agreed, that the audit should include the publicly accessible systems. Therefore the audit will include the following:

- Scanning for open ports and protocols on the border;
- Spoofed address testing;
- Information scanning to find out what information about GIAC and its Network is readily available for users on the Internet;
- Vulnerability scanning on all publicly accessible systems;
- Egress filter scanning from the Public Network out to the Internet;
- TCPDump logs from both outside and inside the Border Firewalls
- Review of information on the Syslog Server.

The testing and scanning will be performed from three location – inside GIAC's Network, the consultant's network and the SANS network. The resources needed will be:

- Two scanning systems, one located at GIAC and one located at SANS. These systems are existing within the GIAC and SANS inventory;
- Two host to serve as TCPDump hosts – one between the Border Router and the Border Firewall and one behind the Border Firewall;
- Three IT staff members – one at SANS to perform testing from there, one at GIAC to perform testing and another at GIAC to monitor the testing and guard against real attacks.

**Cost of Audit**

The direct cost of the audit will be the consultant fees and the time of three GIAC staff members.The indirect costs will include lost income from the very few clients using the Network at the time of the tests. All clients will be warned well in advance; however it is anticipated that there will still be some customers trying to use the Network. A few of these will become aggravated, which will require the time and efforts of the sales and marketing staff to appease

them. The consultant's time for review of policies and development of testing plan is 3 days (24 hours). The testing time is 12 hours, and the time needed for evaluation of results and report generation is 16 hours. The GIAC staff will be needed for 12 hours each (12x3=36 hours), and their salaries average to an hourly cost of $37.50/hour. They will be paid overtime, so the actual amount is $56.25/hour. Total direct costs for this audit will be:

| | | |
|---|---|---|
| Consultant | 52 hours X $200 | $10,400 |
| GIAC Staff | 3 X (12 Hours X 56.25) | $ 2,025 |
| | Total Direct Costs | $12,425 |

**Audit Tools**

There are several tools to be used in the Audit of the GIAC border firewalls and public systems. These include:

**nmap** – a tool for scanning networks to determine which hosts are running and 'visible' and what ports are open on the hosts that are running. nmap will be used to scan the border firewall to ensure that only authorized ports are available. Further scanning will be done on the hosts beyond the firewall to make sure only designated address/port combinations are passing through the firewalls.

**Nessus** – a vulnerability-scanning tool. This tool checks for known vulnerabilities on systems and will be used to ensure that all systems are sufficiently patched and hardened.

**TCPDump** – a packet capturing tool. TCPDump will be used to capture for analysis all of the packets traveling between the border routers and border firewalls and behind the firewalls. The information will be examined to check for any unexpected penetration by the security tools.

**Sam Spade** – a multifunction scanning tool. This tool will be used to do general reconnaissance to find out how much information is publicly available about GIAC's Network. The specific tools to be used are DNS, WHOIS, finger, zone transfer check and SMTP relay check.

**Implementation**

**TCPDump**: In order to record the traffic entering the GIAC Border Network to analyze whether or not certain tests, or attacks, are successful. This will be done by installing a listening host on the network segment between the Border Firewall and the Border Router. Another listening host will be placed behind the Border Firewall to capture any packets which get through the firewall. These listening hosts will be hardened versions of SuSE Linux 7.2 running TCPDump. TCPDump will be set to capture all traffic on the network segment and write it to a file which can later be analyzed using a third party tool. The command for this action is:

*tcpdump –v –w **filename***

There are two options set for the captures. The 'v' option, or verbose, outputs more information about the packets. The 'w' option writes the output to a file for later analysis, keeping the data as raw packets. The '***filename'*** tag is the name of the output file from the tcpdump scan.

*Note: TcpDump is being used to detect any penetrations during the audit instead of relying on the IDS running SNORT. There are two reasons for this: 1) The audit is testing GIAC's security policy and that security policy was used when writing the SNORT rules. If there are any misconfigurations, or worse, if there are any bad policies the SNORT rules will not detect the intrusion.*

**Sam Spade:** The first check performed is the general reconnaissance to see what information about the GIAC Network is readily available from the Internet. This will be done by using Sam Spade from the SANS site as well as the consultant's office. Sam Spade is an easy to use graphical interface scanning tool. The initial screen of Sam Spade is shown in Figure 8. The basic scanning tools can be seen on the left side of the window. The more advanced tools, such as DNS Zone Transfer check and SMTP relay check are located in the 'Tools' menu. To use Sam Spade, enter an address or domain name in the box on the top left of the window, then select the tool you want to use. Some tools require the address of a DNS server be known as well, but using the IPBlock tool can usually discover this.

**Figure 8 - Initial Screen of Sam Spade**

The audit calls for the following Sam Spade tools be run:

- Whois – to find out what information is available from the registration record of the domain name "giac.com". This information can be used for social engineering and general information such as email address format, names, physical address, and geographical location. Only a minimal amount of information should be available from this scan. No names of individuals should be included in the record and email address should be something like webadmin@giac.com.
- IPBlock - to find the owner of the block of IP addresses and the DNS servers for the site.
- DIG (advanced DNS) – to find all DNS entries for the domain
- DNS Zone Transfer – to test if the GIAC EX/EX DNS server will respond to requests for a zone transfer. Zone transfers are dangerous because they

can give away a great deal of information, and can leave the DNS server open to corruption.

- SMTP Relay Check – to see if the GIAC Incoming Email Proxy can be used to relay or send spoofed emails. This is a trick used primarily by 'spammers' to send out bulk emails using someone else's resources and address.

**Nessus**: This is a free open source network security scanner. It tests the devices on the network, including hosts, servers, routes sand firewalls, for known vulnerabilities. Nessus has two components, a server and a client. The server component is responsible for performing the actual attack, or tests, on the targeted devices and is run on a Linux system. The client (Figure 9) is the 'front end' of the tool. It is used to set the options, which test will be performed, any special rules to be applied to the test and the address range of the targets.
The GIAC audit calls for this tool to be run from the Public, VPN and Secure Web Network segments to test all publicly accessible servers and firewalls. There will also be a test performed on the outside of the Border Firewalls. All devices will be thoroughly tested using all available test provided with Nessus. The Denial of Service test will be performed separately, and only against the exterior of the Border Firewalls to test the failover configuration of the PIX firewalls.

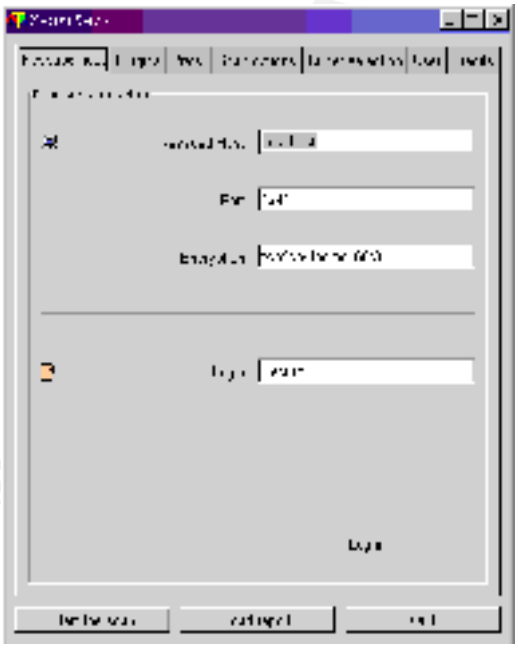


**Figure 9 - Nessus Client**

**nmap**: This network scanning tool is used to scan a range of addresses and service ports. There are many different types of scans that can be performed, such as several TCP scans, ping scans, UDP scans and more. The information gathered from the scans can be used to map out a target network and/or plan attack strategies. In addition, nmap can fingerprint, or identify, what operating system the target system is running; it can determine predictability of IP and TCP sequence numbers the target system is generating, and can be used to determine how much time has passed since a target system was rebooted. The tool even has an option to spoof the source address of the attacking machine.

For the GIAC audit, this tool will be run from the SANS Network and from the consultants site. There are several options that will be utilized for the GIAC audit that include:

-sS This option will send a 'SYN' packet to a range of service ports on the target address(es), if a response comes back ('SYN/ACK') that is evidence of an open port. If a reset, or 'RST' comes back that is evidence of a closed port.

-sU This will perform a UDP scan of the target. Since UDP is a connectionless protocol (it does not require a response for packets sent), there will be no response unless a port is closed. If a port is closed then a ICMP 'port unreachable' message will be sent back. This information can be used to create an inverse map of the listening ports.

-v Verbose mode will output more information about the results of the scans.

-O With this option set, nmap will attempt to identify the operating system of the target system. Other valuable information can be gathered through this option as well, including uptime and sequence number prediction.

-S This option allows the source address of the attacking system to be spoofed. This can allow the attacker to send packets that appear to come from non-routable addresses or even from within the target network.

-p This will allow the attacker to specify a range of ports to scan out of the more that 65,000 ports.

-oX This will output the result into an XML file, which can then be imported into a third party analysis tool for review.

Note that the option flags are case sensitive. There are many other options available, but the options listed above will provide a sufficient audit of the GIAC border network. Scans will be run against the full range of GIAC's class C address space, Public.0 /24, however the address space will be broken up into ranges and these ranges will be scanned separately. This is done to focus the scans on particular network segments. The VPN Network will be test separately from the Public Network, and the Border Routers and Firewalls will be tested separately as well.

**Results**

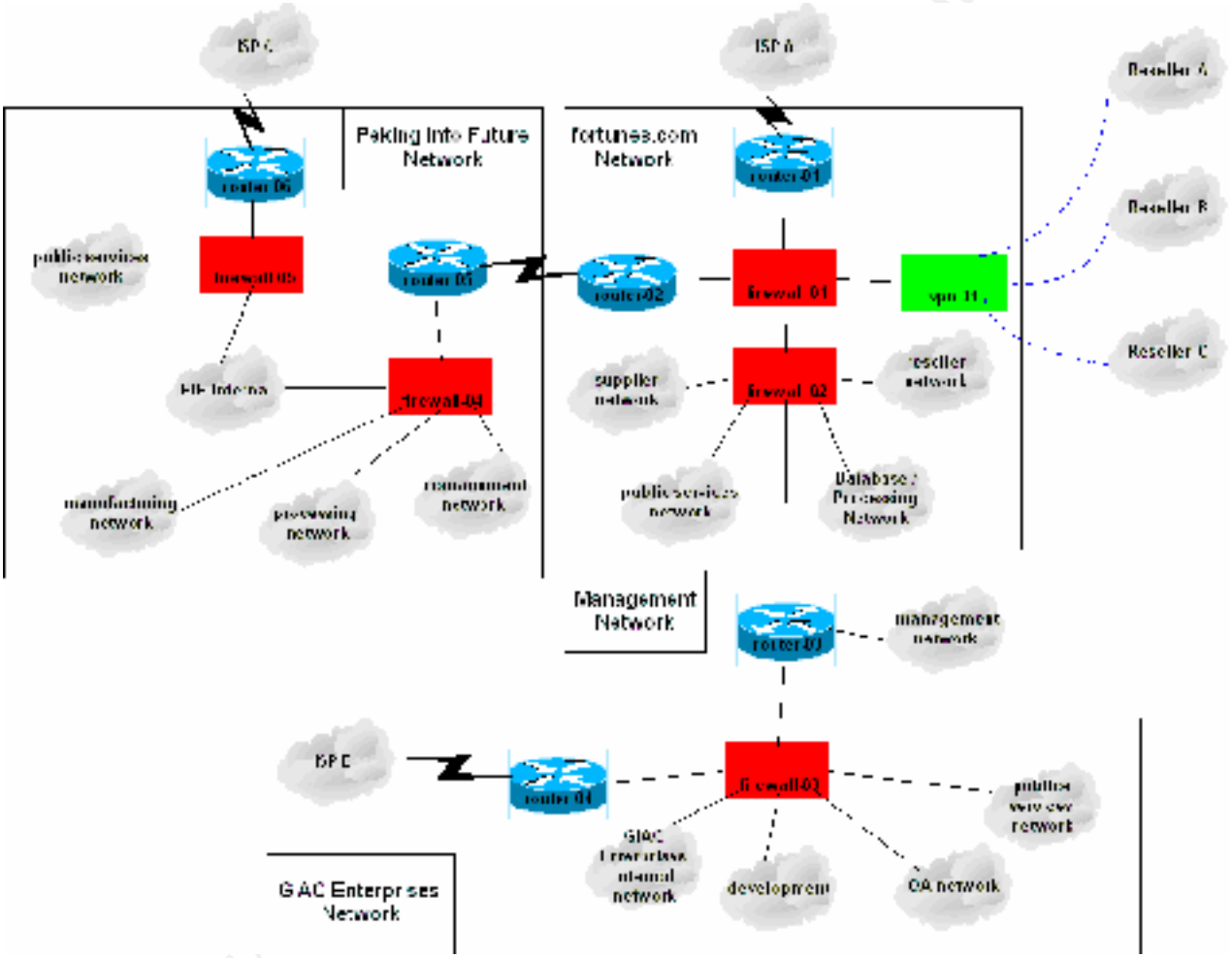
The GIAC staff and the security consultant are reasonably happy with the results of the audit. More importantly, the GIAC Board of Directors is happy with the audit.

## Section IV - Design Under Fire

A review of a previous design of the GIAC Network demonstrates some potential weaknesses with the previous design. Eric Wadell provided the design and his design documents can be located on the Internet at the following address:

http://www.sans.org/y2k/practical/Eric_Waddell_GCFW.doc

Below is the Network Diagram:




The potential weakness to attack will be demonstrated by three different attacks:

1) An attack against the Border Firewalls, which are all Nokia Appliances running Checkpoint's Firewall-1 version 4.1;
2) A Denial of Service attack against the fortunes.com network (this attack could be used against all three border firewalls since the are all running the same firewall version); and
3) An attack against an internal host through a border router.

**Attack on the Firewalls**

Check Point has acknowledged a vulnerability that will allow packets to pass through the firewall, bypassing the default rules. This vulnerability uses a proprietary Check Point protocol RDP, which is used for internal communications within Firewall-1. This proprietary protocol uses UDP port 259. Below is the summary from the Check Point web site.

> **Summary:**
> Check Point uses a proprietary protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/FireWall-1 allows RDP packets to traverse firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/FireWall-1 gateway without being explicitly allowed by the rule base.

In order to take advantage of this vulnerability custom packets have to be crafted to include the RDP headers. With this done, it is possible to target any system being protected by the firewall or inside interface of the firewall itself. With constructed packets, it would be possible to attack any or all of Firewall-01, Firewall-02 and Firewall-03 as designed in the above diagram. After a bit of reconnaissance it is discovered that this configuration is not using network address translation (NAT). With this we can use Sam Spade to discover what address range is being used by GIAC and attempt to exploit the systems at each address in the range.
There is currently a patch available for this vulnerability; however if the patch is not accessible for any reason there is a workaround. The workaround requires editing a configuration file for Firewall-1. Check Point's description of the workaround is below.

> **RDP Bypass workaround for VPN-1/FireWall 4.1 SPx**
>
> RDP communication may be blocked in VPN-1/FireWall-1 versions 4.1 and 4.1 without applying the security hotfix by the applying the INSPECT changes below to the management station. No changes need to be applied to the modules themselves. The files referenced below may be found in $FWDIR/lib/. Please make sure all management GUIs are closed before editing the files. After editing the files, install a policy to push the changes to the modules.
>
> **Known Limitations:**
> Please note these changes will disable FWZ encryption, MEP resolution and automatic interface resolving (automatically determining closest interface for remote VPN connections to gateways with multiple interfaces). Blocking RDP on edge routers will achieve the same results, with the same limitations.
>
> The files referenced below may be found in $FWDIR/lib/. Please make sure all management GUIs are closed before editing the files. After editing the files, install a policy to push the changes to the modules.
>
> **For 4.1:**
> Comment (or remove) the following line in base.def; *comments begin with the symbol "/*" (omitting quotes) and conclude with the symbol "*/" (omitting quotes).*

```
/*accept_fw1_rdp;*/
```

**Denial of Service**

There are many options for launching a denial of service attack, but for this report Tribal Flood Network 2000 (TFN2K) will be used. TFN2K is comprised of two components – a server and a client. The server component is responsible for the actual attacks, while the client is what is used to control the servers. In order to be effective against a commercial target the server will have to be installed on many compromised systems on the Internet. The client can also be installed on a compromised system, however the compromise has to be complete so that the attacker has access to root.

For this attack, there have been around 200 servers installed throughout the Internet on home user systems with DSL connections. The client is installed on a compromised host on the network of a University. The servers have been split up into 4 groups and each group is listed in a separate attack file that will be used to attack different hosts within the GIAC Network. The servers will attack using random protocols and random spoofed addresses and a mix of attacks will be used depending on the target. The attack will be performed at a peak time, such as 11:00 am on a Monday. This will ensure there are many legitimate connections adding to the demand on resources. To implement the attack once the servers and client are ready use the following commands:

```
./tfn -f attck1.giac -c8 -i firewall-01.fortunes.com
./tfn -f attck2.giac -c5 -i public.fortunes.com -p 80
./tfn -f attck3.giac -c5 -i supplier.fortunes.com p- 80
./tfn -f attck4.giac -c5 -i partner.fortunes.com -p 443
```

The first line issues an attack on the firewall itself. The attack being used is the MIX flood attack that uses UDP, TCP and ICMP interchanged. The other three attacks are against the web servers - public (or customer), supplier, and partner - an uses the TCP/SYN flood attack. The first two web servers are attacked through port 80 since this port is allowed. The third web server, partner, is attacked through port 443. Even if the border router is blocking miscellaneous ports and protocols, it will have to permit the traffic destined for the web servers. This should be sufficient to bring down the network. The attacks could be staggered to prolong the pain of the GIAC staff giving the staff enough time to recover from one attack and launching another one.

There is no known way to protect against this kind of attack. One possible workaround would be to have redundant connections provided by different ISPs, and have fault tolerant configuration on the border routers and border firewalls. This may be an expensive solution, but is may be cost effective in the long run since GIAC depends solely on the Internet for its entire business.

**Attack on a Internal Host**

Rather than going through the front door of the fortunes.com network with its two firewalls, it would be easier, and potentially more valuable, to go through the back door this design has left. The GIAC Enterprises network is only guarded by one firewall and has a public services network attached to an internal router. Although the configuration of this firewall is not included in the design documents, it will be assumed that similar rules exist blocking all

unapproved ports and protocols. This leaves the http and DNS services on the public services network open to attack. To find out what web server and version of DNS is being used and what possible entry points are available any of a number of tools can be utilized for reconnaissance. Among the tools are:

- nmap to list open ports and to attempt to discover the operating system of the servers,
- Sam Spade to try and discover the web and email servers, and
- nessus to examine for possible vulnerabilities on the publicly accessible servers.

Once the O/S's, software and versions are discovered, a search on the Internet should yield a number of available exploits. One scenario would require placing a Trojan or backdoor on one or more of the publicly accessible servers and using those systems as a launching pad to attempt to compromise the management server, which are only two routers away and not protected by another firewall.

A possible line of attack is any DNS server in the GIAC Enterprises Network running Bind versions 8.2 through 8.2.3 beta. Once the DNS server is located and identified through the scanning techniques listed above, the "tsig bug" can be used to take over the system. This bug allows a buffer overflow handling the tsig queries. A further search of the Internet produces some exploit code available for download. Once some modifications are made to the exploit code and the overflow occurs, the attacking connection can place needed files onto the compromised system and proceed to move on to bigger and better targets within the network. A password sniffer can be placed on the compromised DNS server to collect passwords for further exploits.

Assuming that the Web Server is running IIS 4.0, with a stolen password from the sniffer on the DNS server, a compromise of the Remote Date Service could provide access to the various databases accessible from the web server. The compromise can be found at http://www.microsoft.com/security/bulletins/ms98-004.htm

If the above don't work, and time is not a factor, one could patiently go through the ever-growing list of vulnerabilities available on Internet until an exploit is found to work.

## References

http://www.checkpoint.com/techsupport/alerts/rdp.html
- Firewall-1 Vulnerabilities

http://www.securiteam.com/securitynews/5YP0G000FS.html
- Tribal Flood Network 2000

http://www.isc.org/products/BIND/bind-security.html
- Bind Vulnerabilities

http://www.zdnet.com/pcweek/news/0713/17miis.html
- IIS Vulnerabilities

http://www.microsoft.com/security/bulletins/ms98-004.htm
- IIS Vulnerabilites

http://www.tbtf.com/archive/1998-07-20.html#s05
- Remote Data Services Vulnerability

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/config.pdf
- PIX Configuration Guide

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/advanced.pdf
- PIX Advanced Configuration Guide

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/commands.pdf
- PIX Commands Reference

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/
- Cisco IOS 12.2 Reference Material

ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/nt_2000/6.5/manuals/configguidew2k65.pdf
- Symantec Enterprise Firewall 6.5 Configuration Guide

http://www.sans.org/y2k/practical/Michael_Vars_GCFW.zip
- Michael Vars' Practical Assignment

http://www.sans.org/y2k/practical/Edward_Luck_GCFW.zip
- Edward Luck's Practical Assignment

http://www.sans.org/y2k/practical/Eric_Waddell_GCFW.doc
- Eric Waddell's Practical Assignment (Design Under Fire)

Eric Cole, "Denial of Service Attacks." *Hackers Beware*, First Edition, USA: New Riders August 2001