Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 1.7

Robert Wildt
May 13, 2002

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Certified Firewall Analyst (GCFW) 1
Practical Assignment 1
Version 1.7 1
Assignment 1 – Security Architecture: 3
Business Background: 3
Business Process: 3
Proposed network architecture: 5
Required connections: 6
Network Architecture: 7
Assignment 2 – Security Policy and Tutorial: 9
Basic Security Policy: ..... **Error! Bookmark not defined.**
Cisco 2514 Border Router: 9
Cyberguard Firewall (non VPN components): 13
Cyberguard firewall (VPN) tutorial: 19
Assignment 3 – Verify the firewall policy: 25
Assignment 4 – Design Under Fire: 34
Firewall Attack: 36
Nov, 1999, newsgroup comp.security.firewalls 37
Denial of Service Attack: 37
Compromising an Internal host: 38
The Social Engineering Aspect. 39
References: 40
Appendix A - Project Requirements: 41
Basic Requirements: 41
Assignment 1 – Security Architecture (15 points): 41
Assignment 2 – Security Policy and Tutorial (35 points): 42
Assignment 3 – Verify the Firewall Policy (25 points): 43
Assignment 4 – Design Under Fire (25 points): 43

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 – Security Architecture:

Business Background:
GIAC Enterprises (GE) is a business whose product is selling fortune cookie sayings (fortunes). GE is a model of enterpreneurship and is an example of a "virtual" company. There are only a few true company employees. Some business processes are outsourced to external contractors. This includes duties such as fortune creation, sales and accounting. GE's product is perfect for this type of business as it deals strictly with information. There are no physical production and distribution facilities. Distribution of product is through the Internet. Therefore the protection of its information is of paramount importance. Because of the technology dependence (and because GE's principal owner is very interested in information technology), GE has chosen to build its own IT infrastructure, rather than outsourcing it to an external hosting company. However, when spending money for IT infrastructure, one must still keep in mind that GE is a small company with limited monetary and staffing resources.

Business Process:
GE obtains its fortunes by contracting with telephone psychic companies, whose employees are mostly housewives and college students who write fortunes in the slack time between phone sessions. Being as they are both in the fortune-telling business, these psychic solicitors would love to have access to GE's customer database. Not wishing to have their customer list stolen, GE wishes to give its suppliers only minimal access to the GE network.

The supply contractors upload text files containing new fortunes to GE using FTP over SSH to GE's publicly accessible FTP server. GE staff members download the files from the FTP server to their workstation and review the fortunes. Those fortunes accepted are imported into an SQL-Server database on GE's internal network. Two text files are returned back to the supplier's FTP directory. The first is a list of accepted fortunes. The suppliers use this list to generate their invoices to GE. The second file contains fortunes that were rejected. The suppliers add both files to a database that is used to filter out previously used/rejected fortunes before sending new fortunes to GE. Suppliers generally download the previous transfer's accept/reject files as they upload a new fortune file to GE. GE will only allow SSH connections from known supplier IP addresses.

GE's has two types of customers: casual and regular. Casual customers may purchase and download fortunes using the GE website. The transactions use encrypted SSL sessions in order to protect both data and customer credit card information. Regular customers who subscribe to GE's bulk service have the option to pick up their fortunes via the same FTP-over-SSH mechanism that GE's suppliers use. These customers are invoiced through the normal GE accounting system. GE will only allow SSH connections from known customer IP addresses.

GE also has business partners in foreign countries. These partners have access to the entire GE fortune database via a VPN connection into GE's fortune database server. Partners pull fortunes from the GE database, translate them into their local language and resell them through their own distribution channels.

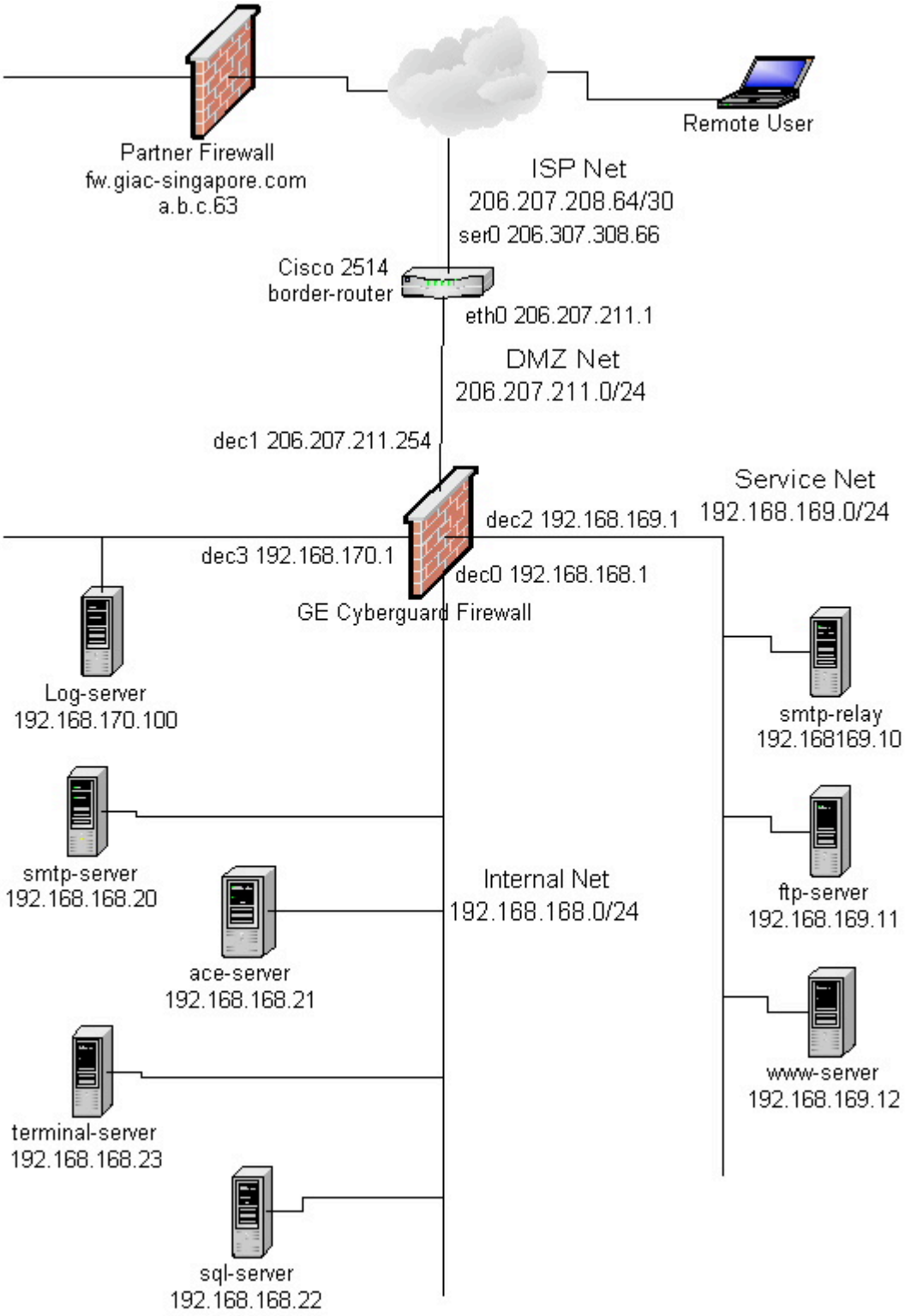
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GE also has a requirement for access to their internal network by telecommuters. these telecomuters include a mobile sales force, the outsourced accounting staff, general telecommuters and the IT support staff. Access is via client VPN. Depending on the needs of the remote user, two methods of access are provided. Sales, accounting and most other telecommuters only require access to an internal server offering Microsoft Terminal Server. Remote workers log into the Terminal Server and run the applications they need. IT staffers require access to the entire network in order for them to perform their system administration duties. All client VPN connections will be authenticated by the use of one-time passwords provided by SecurID tokens (URL: http://www.rsasecurity.com/products/securid/).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Proposed network architecture:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Required connections:

Public:

- DNS lookups (53/udp, 53/tcp) to firewall external interface.
- Web access (80/tcp) to service net public webserver.

Suppliers:

- Same connections as Public.
- SSH access (22/tcp) to service net ftp server.

General Customers:

- Same connections as Public.
- Web SSL access (443/tcp) to service net public webserver.

Regular Customers:

- Same connections as General Customers.
- SSH access (22/tcp) to service net ftp server.

Partners:

- Same connections as Public.
- IPSec VPN access (500/udp, 50/ip) to firewall. Firewall then allows SQL-Server access (1433/tcp) to internal SQL-Server. Database access is read-only to the fortune database..

Internal Employees:

- Web access (80/tcp) to service net webserver.
- SSH access (22/tcp) to service network and logging network.
- Web proxy access (8080/tcp) to firewall internal interface.
- DNS lookups (53/udp, 53/tcp) to firewall internal interface.

General remote employee VPN:

- Terminal Server access (3389/tcp) to internal MS Terminal Server.

IT admin remote employee VPN:

- Access to all networks.

Inter-host processing:

- TFTP (69/tcp) from border router to logging server.
- Syslog (514/udp) from border router to logging server.
- Syslog (514/udp) from firewall to logging server.
- Syslog (514/udp) from service net to logging server.
- SecurID (5500/udp) from firewall to ace server (SecurID)

These are the connections required for basic business processes. In reality, other ports may need to be opened for additional business reasons. An example would be allowing non-browser FTP for software updates. These requests should be evaluated against need and company security policy. If the connection is approved, firewall rules should make the port, source IP and destination IP as narrow and specific as possible.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Architecture:
Where possible, "defense-in-depth" mechanisms will be used. Simply put, this means that similar security measures will exist on multiple devices or in multiple areas of the network. Like all companies both small and large, GE's IT security strategy is a triangular balance between ideal security, acceptable business risk and cost. Being a small company, GE is always mindful of its IT expenses.

Border router:
The border router is the first security-enabling device seen by inbound Internet traffic and it is the last security-enabling device seen by traffic bound for the Internet. Static packet filtering can be implemented on this device to both protect the Internet firewall from unwanted network traffic and protect the Internet from possible malicious or misconfigured traffic outbound from GE's internal network.

The router to be used is an existing Cisco 2514 router belonging to GE. Although this router is no longer available from Cisco (URL: http://www.cisco.com/warp/public/cc/pd/rt/2500/index.shtml), it will fit the needs of GE. This router is large enough to route and filter GE's T1 Internet connection. It also has an additional serial port and Ethernet port to allow for possible expansion such as an additional T1 line. The router is running IOS 12.0

Firewall:
The firewall chosen is a Cyberguard appliance firewall, Firestar model (URL: http://www.cyberguard.com/SOLUTIONS/Solutions_Product_eal4.html). The Firestar offers 850mhz CPU, 128mb of ram, 5 network interfaces and 200-mbps throughput in a 1u rackable form factor. The hardware is Intel based. The software version is 5.0, psu2. This model offers an optional high-availability capability by pairing it with another Firestar.

The choice to use a Cyberguard appliance is based on the following criteria:

- Cyberguard's security reputation. Cyberguard firewalls have Common Criteria Evaluation Assurance Level 4 (EAL4) certification (URL: http://www.commoncriteria.org/epl/AssuranceLevel/index.html).
- The need for vendor support and software maintenance. The GE IT staff is small and wishes to leverage the knowledge and support provided by a commercial firewall vendor.
- The appliance models run on a hardened OS based on SCO UnixWare. This lessens the burden of hardening a commercial OS for firewall use.
- Cyberguard firewall features include stateful packet filtering, application proxying, VPN capability and split-DNS service. Integrating all these services on one platform may not always be the optimum configuration. However, in consideration of GE's small budget and IT staffing, it is felt that this is an acceptable risk.
- Cyberguard appliances are available in 5 sizes. Some with high-availability options. Upgrading to a larger firewall in the future should cause minimal problems.
- IT Staff familiarity and previous experience with Cyberguard products.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Switches/hubs:
It is recommended that network switches be used in place of hubs, especially in the service and logging networks. In addition to enhancing network performance by reducing collision domains, switches have the additional benefit of removing traffic not bound for a host on a particular port. The additional cost to implement this is small.

DNS:
DNS will be split-dns, in which internal and external hosts will access separate DNS databases. The internal database contains all host entries for the internal giace.com network. The external database contains only hosts for giace.com that GE wishes the public Internet to know about. The Cyberguard firewall provides a hardened split-DNS service.

The external DNS master server will run on the firewall external interface. GE's Internet service provider will host the secondary external DNS server. The external DNS configuration file will allow zone transfers only to its secondary nameserver.

The internal DNS master server will housed on an internal server. A secondary internal DNS server will run on the firewall internal interface. This will reduce DNS lookup traffic between the firewall internal interface and the internal DNS server. All internal DNS servers (including the secondary on the firewall internal interface) forward unknown lookups to the DNS server running on the firewall external interface. No DNS queries or zone transfers will pass directly through the firewall.

Logging:
A logging server will be placed in a service network connected to a separate firewall network interface. The border router, firewall and service net hosts will send Syslog entries to the log server. The log server will not be allowed access beyond its local network. Access to the log server for administration and log review will be via SSH (version 2) from the internal network only.

Optional considerations:
Additional systems could be implemented to provide additional security, but are not part of the scope of this project. Such additional systems might include:

- Intrusion Detection Systems (IDS) (network-based and host-based). These would provide additional alerting of possible intrusion attempts.
- Host-based firewalls. Pass only protocols/ports specifically required for a particular host's processes.
- Anti-virus scanning of web and email traffic in addition to host-based antiviral scanning. The recommendation would be to place a TrendMicro Interscan host in the logging network. All http and smtp executable files passing through the firewall application proxies would be sent to the Interscan host via Content Vectoring Protocol (CVP) for virus scanning, then returned to the firewall for forwarding to its destination.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2 – Security Policy and Tutorial:

All network devices will, if possible, be configured in the following manner:

- Log to internal Syslog server.
- Display the following banner when presented with a login:

```
Unauthorized access prohibited.
All communications may be monitored.
Illegal use will result in prosecution.
```

- Display the following banner after successful login:

```
Consistent with GIAC Enterprises, Inc.'s Electronic Communications
Acceptable Usage Policy, this computer system, which includes, but
is not limited to all related software, hardware, communication
networks, e-mail, internet access and any supporting infrastructure
is the property of GIAC Enterprises, Inc. and is provided only for
users with express prior authorization from GIAC Enterprises, Inc.

GIAC Enterprises, Inc. monitors its computer systems and all data or
information placed on, stored on, received by, or sent by such
systems. Data or information that is monitored by GIAC Enterprises,
Inc. may be examined, recorded, copied, deleted, purged and used for
by GIAC Enterprises, Inc. for any purpose.

Unauthorized access or use of GIAC Enterprises, Inc.'s computer
systems or any information or data placed on, stored on, received by
or sent by such systems is prohibited.
```

Cisco 2514 Border Router:

The border router has three jobs:

1. Route packets between the Internet and GE's public IP addresses.
2. Provide access control lists (ACLs) to block packets inbound from the Internet that GE shouldn't or doesn't want to receive. The objective is to protect the firewall from having to handle useless traffic that it would be blocking anyway. This is a good example of defense in depth. Examples would be:
   - Packets with source addresses from private (rfc 1918) IP networks that do not route across the Internet. Examples: 10.0.0.0/8, 127.0.0.0/8 (localhost). No valid network connections would ever come from these addresses.
   - Packets from IP hosts or networks that GE does not wish to receive connections from. Example: known email spammers.
   - Protocols that are security risks. Example: finger.
   - Protocols that GE does not wish to receive. Example: netbios.
3. Provide ACL's to block packets outbound to the Internet that shouldn't be there or are possibly the result of internal network misconfiguration. Again, this is an example of defense in depth, as the firewall should also be blocking this traffic. Such egress filtering makes GE a good Internet citizen by keeping unwanted traffic from leaving the GE network and getting dumped onto the Internet. Examples would be:
   - Packets from private (rfc 1918) IP networks that do not route across the Internet. Examples: 10.0.0.0/8, 127.0.0.0/8. No valid network connections would ever go to these addresses.
   - Packets with source addresses of GE internal networks. In our case, these addresses

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

are rfc 1918 private addresses and should never be seen on the Internet.
- Protocols that GE does not use on the Internet. Example: netbios.
- Application ports that are used by malicious software to "phone home". Virii, worms, adware and spyware applications often attempt to make connections back to a home server. GE doesn't want company information to possibly leak out of its network.

The filtering capability of most routers is somewhat coarse, so it is generally used only to block major undesirable traffic. ACL lists can become large, convoluted and confusing, making configuration difficult and error-prone. Also, it may take a powerful router to handle many ACLs. Although many organizations protect their network from the Internet with only router ACLs, convention is to only sweat the big stuff here and fine-tune access controls with a firewall.

The following listing is a configuration file that can be imported to the border router via a tftp service running on the logging server. This file is self-documenting. Note that as the router processes the configuration file, comments will be stripped out. If the configuration is tftp'd back to the tftp server, the file will no longer contain comments.

This file was initially created with Cisco's Configmaker software (downloadable from URL: http://www.cisco.com/warp/public/cc/pd/hemnsw/cm/index.shtml). Further modifications were made in accordance with guidelines found on the Cisco website (www.cisco.com) and in SANS Institute (URL: http://www.sans.org) "Firewall, Perimeter Protection and VPNs" courseware.

```
! ****************************************************************
! giace.com
! Hostname: border-router
! last update 5/1/02 bw
! ****************************************************************
!
hostname border-router
!
! Timestamping
service timestamps debug uptime
service timestamps log uptime
!
! Encrypt passwords
service password-encryption
enable secret mOre$1ls
!
! Disable unneeded services
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http server
no ip bootp server
no snmp-server
no cpd run
!
! Log critical messages to console
logging buffered 10000 informational
logging console critical
!
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
! Log to syslog
! Syslog server IP is a static NAT on the firewall.
logging trap informational
logging facility local2
logging 206.207.211 253
!
! Disable DNS lookups
no ip domain-lookup
!
! Routing
no ip source-route
no ip classless
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0
ip route 192.168.168.0 255.255.255.0 206.207.211.254 1 permanent
ip route 192.168.169.0 255.255.255.0 206.207.211.254 1 permanent
ip route 192.168.170.0 255.255.255.0 206.207.211.254 1 permanent
!
! Interface configurations
! eth1 and ser1 are unused
! Internal - allowing redirects and unreachables for firewall messages
interface Ethernet 0
 no shutdown
 description connected to EthernetLAN
 ip address 206.207.211.1 255.255.255.0
 ip access-list internet_outbound
 keepalive 10
!
interface Ethernet 1
 no description
 no ip address
 shutdown
!
! External
! Kill ICMP redirects and unreachables on this interface
interface Serial 0
 no shutdown
 description connected to Internet
 ip address 206.207.208.66 255.255.255.252
 encapsulation hdlc
 ip access-list internet_inbound
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
!
interface Serial 1
 no description
 no ip address
 shutdown
!
! Set banners
! Motd banner.  Seen after successful login
banner motd #Consistent with GIAC Enterprises, Inc.'s Electronic
Communications
Acceptable Usage Policy, this computer system which includes,
but is not limited to all related software, hardware, communication
networks, e-mail,  internet access and any supporting infrastructure
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
is the property of GIAC Enterprises, Inc. and is provided only for
users with express prior authorization from GIAC Entgerprises, Inc.

GIAC Enterprises, Inc. monitors its computer systems and all data or
information placed on, stored on, received by, or sent by such systems.
Data or information tht is monitored by GIAC Enterprises, Inc. may be
examinied, recorded, copied, deleted, purged and used for by GIAC
Enterprises, Inc. for any purpose.

Unauthorized access or use of GIAC Enterprises, Inc.'s computer
systems or any information or data placed on, stored on, received
by or sent by such systems is prohibited.#
!
! Login banner.  Seen with login prompt.  Don't tell who you are
banner login #Unauthorized access prohibited.
All communications may be monitored.
Illegal use will result in prosecution.#
!
! Allow login from console
line console 0
 exec-timeout 0 0
 password gTr&bS2g
 login
!
! Allow telnet login from firewall and by extension any hosts behind it
line vty 0 4
 access-class admin in
 password gTr&bS2g
 login
!
!
! Access lists
!
! Admin to internal vty port
ip access-list extended admin
 remark allow from firewall external address & NATed addresses beyond
 permit tcp host 206.207.211.254 any eq telnet log-input
 deny ip any any log-input
!
! Inbound from Internet
ip access-list extended internet_inbound
 remark Don't allow spoofs of our internal addresses
 deny ip 206.207.211.0 0.0.0.255 any log-input
 remark Deny MS networking ports
 deny udp any 206.207.211.0 0.0.0.255 range 135 139 log-input
 deny udp any 206.207.211.0 0.0.0.255 range 135 139 log-input
 deny udp any 206.207.211.0 0.0.0.255 eq 445 log-input
 deny tcp any 206.207.211.0 0.0.0.255 eq 445 log-input
 remark Deny snmp
 deny udp any 206.207.211.0 0.0.0.255 eq snmp log-input
 remark Deny private addresses
 deny ip 10.0.0.0 0.255.255.255 any log-input
 deny ip 172.16.0.0 0.15.255.255 any log-input
 deny ip 192.168.0.0 0.0.255.255 any log-input
 remark Deny localhost
 deny ip 127.0.0.0 0.255.255.255 any log-input
 remark Deny hosts with no ip address
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
 deny ip host 0.0.0.0 any log-input
 remark Allow return tcp connections
 permit tcp any any established log
 remark Allow all remaining traffic to our DMZ subnet.  The subnet
 remark is included because we may have other static NAT addresses
 remark on the firewall.
 permit ip any 206.207.211.0 0.0.0.255 log
 remark Deny all other traffic
 deny ip any any log-input
!
! Outbound to Internet. Belt and suspenders for firewall
ip access-list extended internet_outbound
 remark Allow return tcp connections
 permit tcp any any established log
 remark Deny MS networking ports
 deny udp any any range 135 139 log-input
 deny udp any any range 135 139 log-input
 deny udp any any eq 445 log-input
 deny tcp any any eq 445 log-input
 remark Deny snmp
 deny udp any any eq snmp log-input
 remark Allow anything else out from our subnet
 permit ip 206.207.211.0 0.0.0.255 any log-input
 remark Deny all other traffic - includes private addresses
 deny ip any any log-input!
!
end
```

The access lists above contain mostly just the basics. An argument could be made that the inbound ACL should allow only the ports required to reach the public servers:

- 22/tcp to the ftp server.
- 80/tcp and 443/tcp to the web server.
- 25/tcp to the mail relay server
- 500/udp and 50/ip to the firewall.

However, this would require changes to the ACL as new services are offered by GE. Since there is a firewall behind this router, it was decided to keep the ACLs simple. The router logs will be monitored and if there is evidence of needing additional ACL entries, they will be created as needed.

Cyberguard Firewall (non VPN components):

The Cyberguard firewall will route and manage traffic between four networks:

- Interface dec0 192.168.168.1/24 – Internal network. This network is not directly reachable by Internet hosts (except in the case of VPNs).
- Interface dec1 206.207.211.254/24 – Buffer zone (DMZ) between the firewall and the border router. All packets outbound from this interface will be NATed (PAT) to this IP address, except for any internal addresses that use a static NAT to a specific external address. Connections via the application proxies will connect to this IP address. There are also two static NATs configured to allow non-proxied inbound connections.
  1. 206.207.211.253 NATs to 192.168.170.100 for the border router to connect to the Syslog server via Syslog and TFTP.
  2. 206.207.211.252 NATs to 192.168.169.11 for the Internet public to connect to the ftp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

server via SSH.
- Interface dec2 192.168.169.1/24 – Service network housing publicly accessible web server, ftp server and smtp mail relay server.
- Interface dec3 192.168.170.1/24 – Logging network containing Syslog server.

Below is listed the basic filter rules formatted as they would be in the Cyberguard packet filter configuration file /etc/security/firewall/ng_inet/netguard.conf. Comments are added for clarity and for documenting how they relate to the *Required Connections* section in Assignment 1.

Sections of the netguard.conf file are placed in specific areas by the management GUI. The administrator is free to place additional rules where he wishes. These hand edits are usually done from the management GUI. Rules are evaluated in router fashion (top-down, first matching rule is executed).

Cyberguard allows the following keywords:
- # - comments
- DENY – deny packets that match the rule.
- PERMIT – packets that match the rule are allowed via packet filtering. TCP port rules are automatically stateful. UDP port rules are normally not stateful, but can be flagged to allow return connections within the TTL of the rule.
- PROXY – packets that match the rule are allowed via one of the application proxies. At first glance, some of the proxy rules appear to be very generic and possibly even lax. However, some of the proxies contain additional rules within them. These additional rules will be documented in separate sections following the basic packet filter rules. Also note that one proxy rule usually requires two packet-filter rules if the firewall is being used as an explicit proxy. One is for the actual source to destination, the second is either source to firewall or firewall to destination depending on whether the rule is inbound or outbound. This second rule allows the firewall to make the proxied connection.

There are advantages to using the application proxies when available. The first is that the proxy can perform application level checks against the content of packets. Here are a couple of examples: The SMTP proxy only allows the following commands: HELO, MAIL FROM, RCPT TO, DATA and QUIT. You cannot run the DEBUG command. The FTP proxy can allow or disallow commands. It may allow you to GET a file, but not DELETE one. Secondly, the application proxies provide much more logging information, which is helpful in monitoring and troubleshooting.

The Cyberguard ruleset allows source, destination and protocol to be defined as groups in another section of the configuration GUI. The ruleset below keeps the use of groups to a minimum. The result is more rules, but better clarity without having to refer to what is contained in specific groups. In real life, creating a group for common sources, destinations and protocols could combine some of these rules.

The Cyberguard firewall is paranoid about DNS. Domain names cannot be used as source or destination entities. Any host or network named in a rule must be defined in the firewall /etc/hosts or /etc/networks file. Host names in this example have obvious names (i.e. www-

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

server). In, in real life, you might want to make host names more ambiguous, especially names contained in the external DNS.

```
##############################################################################
#
#
#     Internet Protocol Packet Filter Rules Configuration File
#
##############################################################################
#
#
##############################################################################
#
#
# Select any alternative from each column.
#
# Action service/protocol Frm host/subnetmask To host/subnetmask  Options
# ====== ==============  ================== ==================  ===========
#
# PERMIT service/protocol INTERNAL_NETWORK    INTERNAL_NETWORK
ENABLE_REPLY
# DENY   service          EXTERNAL_NETWORK    EXTERNAL_NETWORK    DONT_AUDIT
# PROXY  ALL              LOCAL_HOST          LOCAL_HOST
TIME_OUT=nnn
#        ALL/protocol     EVERYONE            EVERYONE            NO_IF_CHECK
#                         if_NETWORK          if_NETWORK          TCPSYNFLD
#                      nnn.nnn.nnn.nnn   nnn.nnn.nnn.nnn
TCPSYNFLD_TIMEOUT=nnn
#                         nnn.nnn.nnn.nnn/subnet nnn.nnn.nnn.nnn/subnet
#
##############################################################################
#
# Setup Script Definitions (Leave this line here!)
#
##############################################################################
##############################################################################
# The following line is used to locate the end of the header comments.
# DO NOT DELETE OR MODIFY THIS LINE.
# Place site-specific rules here, above the rules that are generated
# automatically by the firewall administrative interface.
#
#BLOCK AND DON'T LOG - Keeps this stuff from filling up logs.
#Microsoft netbios
deny  137/tcp     EVERYONE    EVERYONE    DONT_AUDIT time_out=60 NO_IF_CHECK
deny  137/udp     EVERYONE    EVERYONE    DONT_AUDIT time_out=60 NO_IF_CHECK
deny  138/tcp     EVERYONE    EVERYONE    DONT_AUDIT time_out=60 NO_IF_CHECK
deny  138/udp     EVERYONE    EVERYONE    DONT_AUDIT time_out=60 NO_IF_CHECK
#
#Global outbound blocks.  These hosts don't need to reach the Internet.
deny  ALL   sql-server  ALL_EXTERNAL
deny  ALL   dns-internal-server     ALL_EXTERNAL
deny  ALL   log-server  ALL_EXTERNAL
#
#OUTBOUND APPLICATION PORTS (except proxied HTTP/S/FTP and SMTP).
#SSH for admin in service and logging nets, file transfer to fpt-server.
permit      22/tcp      192.168.168.0/24  192.168.169.0/24
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
permit      22/tcp      192.168.168.0/24  192.168.170.0/24
#
#INBOUND TO SERVICE NETS (except proxied HTTP/S and SMTP).
#SSH used for supplier/customer ftp file transfer.
#Connections to ftp-server require a static NAT from 206.207.211.252 to
#192.168.169.11.
#Note that this group of rules is an ideal candidate for combining
#individual hosts into a group.
permit      22/tcp      supplier-1  ftp-server
permit      22/tcp      supplier-2  ftp-server
permit      22/tcp      customer-1  ftp-server
permit      22/tcp      cusonter-2  ftp-server
#TFTP from border router.
#Connections to log-server require a static NAT from 206.207.211.253 to
#192.168.170.100 (log-server).
permit      69/tcp      border-router     log-server
#SYSLOG from border router and service net servers.
#Border-router connects to a static NAT 206.207.211.253 which redirects to
#192.168.170.100 (log-server).
permit      syslog/udp  border-router     log-server
permit      syslog/udp  www-server  log-server
permit      syslog/udp  ftp-server  log-server
permit      syslog/udp  smtp-server log-server
#
#INBOUND FROM SERVICE NET.
#SQL Server from webserver
permit      1433/tcp    www-server  sql-server
#
#VPN
#Gateway to gateway VPN rules.
#Security associations are contained within the VPN config.
#Remote user VPN rules are in the Passport One profiles.
#(See Assignment 2 VPN tutorial).
#SQL-server from partner VPN.
permit      1433/tcp    172.16.16.0/24    sql-server  ipsec=GIAC_standard:sa-
per-net:0x2:auto:auto
#
#FIREWALL ACCESS TO SECURID ACE SERVER. (Passport One logins)
permit      5500/udp    FIREWALL    ace-server  ENABLE_REPLY
#FIREWALL DIAGNOSTICS. Let the firewall do some stuff.
#Let the firewall ping and answer pings, but don't allow the outside
#interface to answer pings.
permit      echo/icmp   FIREWALL    EVERYONE
deny        echo/icmp   DEC1_NETWORK      FIREWALL
permit      echo/icmp   EVERYONE    FIREWALL
#Used for general connectivity testing.
permit      ftp/tcp     FIREWALL    EVERYONE
permit      telnet/tcp  FIREWALL    EVERYONE
permit      ssh/tcp           FIREWALL    EVERYONE
#
#FIREWALL MANAGEMENT FROM INTERNAL WORKSTATION.
#Note: the above echo/icmp rules supercede the rules below.
#Since they are automatically added, leave them there anyway.
# DO NOT DELETE OR MODIFY THE FOLLOWING LINE.
# DO NOT DELETE: The following rules are added during initial boot.
permit      8080/tcp    192.168.168.15    FIREWALL
permit      8443/tcp    192.168.168.15    FIREWALL
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
permit      3144/tcp    192.168.168.15    FIREWALL
permit      3144/tcp    FIREWALL    192.168.168.15
permit      5307/tcp    192.168.168.15    FIREWALL
permit      5307/tcp    FIREWALL    192.168.168.15
permit      echo/icmp   192.168.168.15    FIREWALL     ENABLE_REPLY
permit      echo/icmp   FIREWALL    192.168.168.15     ENABLE_REPLY
# DO NOT DELETE: The above rules are added during initial boot.
# Automatically-generated rules added here.
#Passport One is used for VPN user authentication
# Passport One rules (added automatically)
permit      3443/tcp    ALL_INTERNAL      FIREWALL
# End of Passport One rules
# Auditlogd Syslog rules (added automatically)
permit      syslog/udp  FIREWALL    log-server
# End of Auditlogd Syslog rules
#FIREWALL MANAGEMENT FROM INTERNAL WORKSTATION.
#Command line and X over SSH.
# Secure Shell rules (added automatically)
permit      22/tcp      192.168.168.15    dec0_IPADDRESS
# End of Secure Shell rules
# Portguard proxy rules (added automatically)
# End of Portguard proxy rules
#NOTE: SSL rules look lax here.
#NOTE: Further refined within SSL proxy config.
#NOTE: outbound SSL is handled by the HTTP proxy.
# SSL proxy rules (added automatically)
# Proxy paramters (ssl): inToFirewall
proxy 443/tcp     ALL_EXTENRAL      www-server
proxy 443/tcp     ALL_EXTERNAL      FIREWALL
# End of SSL proxy rules
#NOTE: HTTP rules look lax here.
#NOTE: Further refined within HTTP proxy config.
#NOTE: Also handles proxied SSL and FTP.
# HTTP proxy rules (added automatically)
# Proxy parameters (http): inToFirewall outToFirewall
proxy https/tcp   ALL_INTERNAL      ALL_EXTERNAL
proxy ftp/tcp     ALL_INTERNAL      ALL_EXTERNAL
proxy 80/tcp      ALL_EXTERNAL      www-server
proxy 80/tcp      ALL_EXTERNAL      FIREWALL
proxy 80/tcp      ALL_INTERNAL      ALL_EXTERNAL
proxy 80/tcp      ALL_INTERNAL      FIREWALL
# End of HTTP proxy rules
# SMTP proxy rules (added manually)
# Let smtp-relay connect out.
proxy smtp/tcp    smtp-relay  ALL_EXTERNAL
proxy smtp/tcp    FIREWALL    ALL_EXTERNAL
# Let smtp-relay and smtp-server talk.
proxy smtp/tcp    smtp-server smtp-relay
proxy smtp/tcp    FIREWALL    smtp-relay
proxy smtp/tcp    smtp-relay  smtp-server
proxy smtp/tcp    FIREWALL    smtp-server
# End of manual SMTP proxy rules.
# SMTP proxy rules (added automatically)
# Proxy parameters (smtp): inToFirewall
proxy smtp/tcp    ALL_EXTERNAL      smtp-relay
proxy smtp/tcp    ALL_EXTERNAL      FIREWALL
# End of SMTP proxy rules
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# telnet proxy rules (added automatically)
# End of telnet proxy rules
# Gopher proxy rules (added automatically)
# End of Gopher proxy rules
# FTP proxy rules (added automatically)
# End of FTP proxy rules
# Split DNS rules (added automatically)
permit      domain/tcp  ALL_EXTERNAL      EXTERNAL_INTERFACES
permit      domain/tcp  EXTERNAL_INTERFACES     ALL_EXTERNAL
permit      domain/udp  ALL_EXTERNAL      EXTERNAL_INTERFACES
permit      domain/udp  EXTERNAL_INTERFACES     ALL_EXTERNAL
permit      domain/tcp  ALL_INTERNAL      INTERNAL_INTERFACES
permit      domain/tcp  INTERNAL_INTERFACES     ALL_INTERNAL
permit      domain/udp  ALL_INTERNAL      INTERNAL_INTERFACES
permit      domain/udp  INTERNAL_INTERFACES     ALL_INTERNAL
deny  domain/tcp  EVERYONE    EVERYONE
deny  domain/udp  EVERYONE    EVERYONE
# End of Split DNS rules
# End of automatically generated rules.
#
# This deny rule should always be the last rule.
#
deny  ALL   EVERYONE    EVERYONE     ENABLE_REPLY
```

FTP proxy configuration:
The FTP proxy is not currently used because all FTP traffic is tunneled within SSH.

HTTP proxy configuration:
Below are listed the basic HTTP proxy configuration commands as would be found in the configuration file /etc/security/firewall/proxies/httpd-proxy.conf. When the firewall is configured as an explicit proxy in a client browser, the HTTP proxy also handles HTTPS (SSL) and browser-based FTP connections. Comments are added for clarity and to documentation.

```
#
# HTTP proxy configuration file.
#
# Connection requests received at the external interface are fowarded
# to a webserver, not the default firewall HTTP handler.
WebServiceHandler independent
# User authentication is not required.
Authenticate     none
# Additional rules applied to the basic ALL_INTERNAL to ALL_EXTERNAL
# HTTP proxy rules.  NOTE: these rules are evaluated from bottom up
# in 2 passes. 1=entries with no wildcards, 2=entries with wildcards.
# Final rule is an implicit deny any any.
#
# Service net and logging net are considered inside interfaces, but
# we won't give them access.  Just allow the office network out.
Client      192.168.168.* -permit *
#
# Forward requests received at the external interface to this server.
# Allow post, put, delete.
WebServer    www-server post put delete
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SMTP proxy configuration:
The firewall external IP address (206.207.211.254) is the mail exchanger (MX) for giace.com.

Below are listed the basic SMTP proxy configuration commands as would be found in the configuration file /etc/security/firewall/proxies/smtpd-proxy.conf. Comments are added for clarity and to documentation.

```
#
# SMTP proxy configuration file.
#
# Allow 5 packet errors before aborting connection.
MaximumErrorCount 5
# Mail received at the firewall external interface will be forwarded
# to mailserver smtp-server.  Only accept mail addressed to domain
# giace.com.
MailServer   smtp-server aliases yes giace.com
```

Cyberguard firewall (VPN) tutorial:
The Cyberguard manual "Configuring the Cyberguard Firewall Release 5.0" was used as a reference for this tutorial section. (URL: ftp://ftp.cyberguard.com/Unix/5.0/Doc/Manual/cg50cfg.pdf)

The Cyberguard VPN will be used for these VPNs

1. Gateway to gateway VPN tunnels with business partners. These tunnels will only allow access to the internal SQL-Server server.
2. Host to gateway VPN tunnels for remote general users. These users will only be allowed access to the internal Microsoft Terminal Server server.
3. Host to gateway VPN tunnels for remote IT users. These users will be allowed complete access to the internal network.

All tunnels will employ a shared secret for key exchange.

User authentication for remote users will use SecurID tokens (RSA Security Inc, URL: http://www.rsasecurity.com).This method will provide two-factor authentication (what you know, what you have). For access, remote users must know a PIN number, and must have a SecurID token, which issues a changing password. This method of authentication was chosen over client certificates because a remote user may not always be using a specific PC for remote access.

Remote users will first authenticate to the firewall via the Passport One feature of the Cyberguard firewall. Users make an HTTPS connection to the firewall using a web browser. Once authenticated, the firewall creates specific access rules linked to the IP address of the remote user. These rules are in effect as long as the user keeps the authenticating HTTPS session open. Once the connection is closed, the firewall removes the session-specific rules. The advantage to the Passport One method is that ports 500/udp (IPSEC IKE) and protocol 50 (IPSEC ESP) are not available on the firewall until a valid Passport One login is performed.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Gateway to Gateway VPN configuration:
A gateway to gateway VPN is used to allow business partners to access GE's SQL-server server via the Internet.

Cyberguard VPN has IPSec and IKE "Protection Strategies", which can contain a list of encryption and authentication algorithms used to negotiate a match on the remote gateway/host. Since we know what algorithms are being used at the far end, we will create our own Protection Strategies that contain only one entry.

Create an IPSec Protection Strategy:
1. From the Cyberguard management GUI, select **Configuration->IPSec Protection Strategies**
2. Click on the **Protection Strategy** tab
3. Click on **Show Editor**, then **Insert**
   - Protection Strategy = GIAC_standard
4. Click on the **Cryptographic Properties** tab
5. Highlight "GIAC_standard" in the **Protection Strategy** frame
6 Click on **Insert**
   - Encryption Algorithm = 3des-cbc
   - Authentication Algorithm = hmac-sha1-96
   - SA Lifetime Seconds = 7200 (renegotiate keys every 2 hrs)
   - SA Lifetime kbytes = Unspecified (we don't expect a lot of data transfer, but will depend on the SA Lifetime timeout.

7.Click on **Save**, then **Use** to implement the changes

Create an IKE Protection Strategy:
1 From the Cyberguard management GUI, select **Configuration->IKE Protection Strategies**
2 Click on the **Protection Strategy** tab
3 Click on **Show Editor**, then **Insert**
   - Protection Strategy = GIAC_standard
4 Click on the **Cryptographic Properties** tab
5 Highlight "GIAC_standard" in the **Protection Strategy** frame
6 Click on **Insert**
   - Encryption Algorithm = 3des-cbc
   - Hash Algorithm = sha1
   - Diffe-Hellman Group = 2
   - SA Lifetime Seconds = 10800 (Cyberguard default)
   - SA Lifetime kbytes = Unspecified
7 Click on **Save**, then **Use** to implement the changes

Create the tunnel:
1 From the Cyberguard management GUI, select **Configuration->VPN Secure Channels**
2 Click on the **Channel Information** tab
3 Click on **Show Editor**, then **Insert**.
   - Channel Name = GIAC-Singapore

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Peer Type = Gateway
- Host Name = fw.giac-singapore.com (partner firewall)
- Establish Keys Using = IKE
- Preshared Secret = <string>

4 Click on the **Peer Protected Networks** tab
5 Highlight "GIAC_Singapore" entry in the **VPN Secure Channels** frame
6 Click on **Show Editor**, then **Insert**
- Network Address = 172.16.16.0/24

7. Click on **Save**, then **Use** to implement the changes

Create Packet Filter: (Allowing only access to internal SQL-server server)
1 From the Cyberguard management GUI, select **Configuration->Packet-Filtering Rules**
2 Click on **Show Editor**, then the **Basic** tab.
3 In the rule window, determine where in the rule order you wish to insert your rules. Click on the rule just above the insert to highlight it.
4 Click on **Insert**
- Type = Permit
- Port or Service = 1433/tcp
- Packet Origin = 172.16.16.0/24
- Packet Destination = sql-server
- Protect using IPSec = checked
- Take defaults on remaining fields

5. Click on the **IPSec** tab
- IPSec Protection Strategy = GIAC_standard
- SA Granularity = Network (choices are Port, Protocol, Host, Network. Use largest granularity possible unless there are security considerations to create a specific SA
- Take defaults on remaining fields

6. Click on **Save**, then **Use** to implement the changes

Host to Gateway VPN configuration:
Host to gateway VPNs are used to allow remote users access to resources on the GE internal network. There is no need to create new IPSec and IKE Protection Strategies as we can use the GIAC_standard strategies created for the gateway to gateway VPN. We will create Secure Channel, two new user accounts and two different Passport One profiles/rulesets (one for general remote users and one for IT remote users.

Create the tunnel:
1. From the Cyberguard management GUI, select **Configuration->VPN Secure Channels**
2. Click on the **Channel Information** tab
3. Click on **Show Editor**, then **Insert**.
- Channel Name = remote_users
- Peer Type = host
- Interface Name = dec1 (allow connection to outside interface)
- Establish Keys Using = IKE
- Preshared Secret = <string> NOTE: this is a common secret for all remote users. A more secure solution would be certificates. Since we are authenticating with SecureID, a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

tunnel could be built, but no packet filter rules are created for the connection until Passport One authenticates the connection.

NOTE: Since we do not know the IP address of the incoming remote client, there are no settings on the Peer Protected Networks tab.

4 Click on **Save**, then **Use** to implement the changes

Create Passport One profile and packet filters for general remote users: (Allowing only access to internal Terminal Server)

1 From the Cyberguard management GUI, select **Configuration->Passport One**
2 Click on the **Setup** tab.
3 Click the **Enable** checkbox
4 Click on the interfaces you wish to allow Passport One access. In our case it will be the external interface fw.giace.com 206.207.211.254.
5 In the **Authentication Ports** group, check **HTTPS**, port 3443 and uncheck **HTTP** and **Telnet**
6 Take defaults on the remaining fields
7 Click on the **Profiles** tab, Click **Insert**, and enter the name **remote_general**
8 Click on the **Rules** tab, choose **Profile Name** = remote_general
9 Click on **Editor**, **Insert**, and choose the **Basic** tab
- Type = Permit
- Port or Service = 3389/tcp (MS Terminal Server)
- Packet Origin = %USER (this is the IP address of the client authenticating with Passport One
- Packet Destination = terminal-server
- Protect using IPSec = checked
- Take defaults on remaining fields

10 Click on the **IPSec** tab
- IPSec Protection Strategy = GIAC_standard
- SA Granularity = Network (choices are Port, Protocol, Host, Network. Use largest granularity possible unless there are security considerations to create a specific SA
- Check the **To Packet Origin** box and select Secure Channel "remote_users" from the drop box
- Check the **To Packet Destination** box and select Secure Channel "remote_users" from the drop box (NOTE: these last two steps are done because there is not a know IP address on the peer. The Cyberguard cannot determine which Secure Channel to use for this rule. Usually the Cyberguard compares IP addresses/subnets in the Secure Channel list to the **Packet Origin** field in the packet filter **Basic** tab.

11 Click on **Save**, then **Use** to implement the changes

Create Passport One profile and packet filters for IT remote users: (Allowing access to all networks)

1 Return to the Passport One **Profiles** tab, Click **Insert**, and enter the name **remote_it**
2 Click on the **Rules** tab, choose **Profile Name** = remote_it
3 Click on **Editor**, **Insert**, and choose the **Basic** tab
- Type = Permit
- Port or Service = ALL

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Packet Origin = %USER (this is the IP address of the client authenticating with Passport One
- Packet Destination = Grp-GE-internal-nets. NOTE: this is a group defined as subnets 192.168.168.0, 192.168.169.0, 192.168.170.0)
- Enable Replies = checked
- Protect using IPSec = checked
- Take defaults on remaining fields

4 Click on the **IPSec** tab
- IPSec Protection Strategy = GIAC_standard
- SA Granularity = Network (choices are Port, Protocol, Host, Network. Use largest granularity possible unless there are security considerations to create a specific SA
- Check the **To Packet Origin** box and select Secure Channel "remote_users" from the drop box
- Check the **To Packet Destination** box and select Secure Channel "remote_users" from the drop box (NOTE: these last two steps are done because there is not a know IP address on the peer. The Cyberguard cannot determine which Secure Channel to use for this rule. Usually the Cyberguard compares IP addresses/subnets in the Secure Channel list to the **Packet Origin** field in the packet filter **Basic** tab.

5. Repeat steps 3 and 4 to create a rule for traffic in the opposite direction. In this new rule Packet Origin = Grp-GE-internal-nets and Packet Destination = %USER
6. Click on **Save**, then **Use** to implement the changes

Create account for remote user associate with a Passport One profile. We will create two user accounts. One is a general remote user, the other an IT remote user. In practice, a user account will need to be set up for each remote user.

1 From the Cyberguard management GUI, select **Configuration->Passport One**
2 Click on **Show Editor** then **Insert** then **User Information** tab
- User Type = Proxy
- Enter **Login ID** and **Full Name**

3. Click on the **Authentication** tab
- External Method =SecurID

4. Click on the **Passport One** tab, then **Show Editor** and **Insert**
- Pick "remote_general" from the Profile drop list
- Source Address = ***** (we don't know what the remote user's address will be)

5. Repeat steps 2 through 4 for the next user. If the user is an IT remote user, pick "remote_it" in the Passport One Profile drop list.

This next section shows the packet filters rules activated when a remote user logs in with Passport One"

```
# For general remote users
# /etc/security/firewall/clas/profiles/local/remote_users):
permit      3389/tcp    %USER terminal-server   ipsec-GIAC_standart:sa-per-
net:0x2:remote_users:remote users

# For it remote users
# /etc/security/firewall/clas/profiles/local/remote_it):
permit ALL  %USER Grp-GE-internal-nets    ENABLE_REPLY
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
      ipsec=GIAC_standard:sa-per-net:0x2:remote_users:remote_users
permit ALL  Grp-GE-internal-nets     %USER ENABLE_REPLY
      ipsec=GIAC_standard:sa-per-net:0x2:remote_users:remote_users
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 3 – Verify the firewall policy:

(AUTHOR NOTE): Not being able to actually build the GE infrastructure, I have not been able to fully test the complete configuration. For the verification process I have configured a Cyberguard firewall and small lab network to duplicate the functionality of the GE networks as best I can. The results of this section reflect testing against this lab configuration. The tests were conducted from the DMZ zone, not the Internet proper. Therefore, border router ACLs were not involved in the test. Some ports seen in scans would have been blocked by the border router. See comments below. IP addresses shown in the reports have been changed to protect the innocent. (END NOTE)

GE management wishes to have an independent audit performed against the external side of their Internet firewall. GE IT staff argued for an audit of the complete network, but the request was declined. Further testing and auditing of the remaining internal network will be performed by GE IT staff members at a later date.

During the 3rd-party audit, GE IT staff will be working in cooperation with the auditor. The auditor will be teamed with a member of the GE staff throughout the audit. This should offer two benefits: 1) GE staff will get to see an audit "close up" and hopefully learn more about the process and tools. 2) During the audit process, questions continually spring up. By having a staffer immediately available to the auditor, it is hoped that questions can be answered quickly, thereby minimizing consultant hours. The consultant to be used charges $150/hr for his services.

IT tools to be employed are Nessus (URL: http://www.nessus.org – a security scanner), nmap (URL: http://www.insecure.org – a port scanner) and simple connections to various ports via a telnet client. Firewall logs will also be reviewed and correlated to scans performed.

Before the auditors arrive, the GE IT staff is expected to have documentation in order. The base documents are those provided for Assignment 1 (GE Security Architecture) and Assignment 2 (Security Policy) earlier in this project. Also included in the documentation will be other non-technical security policy documents, such as GE's Electronic Usage Policy, which governs employee use of GE networks and of the Internet.

When performing an active audit, such as the one proposed, there is always the possibility that the network or host scans could cause service outages. These outages could range from a simple denial of service because of a busy network/host to a crashed host in need rebuilding. The GE staff must be prepared for the possibility of these problems.

Therefore, the GE staff is also required to ensure that the firewall and all related devices and servers including in the testing are fully backed up, and that there are procedures in place (and previously tested) to restore or rebuild all systems.

The audit will proceed in three phases. The first is information gathering and staging of any test hosts. Auditors will review the provided network maps, connection requirements and rule lists. This is expected to require 8 consultant hours of onsite work, which can be performed during normal office hours.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The second phase is the actual employment of the scanning tools. Because of the possibility of service outage, these tests will take place on a Saturday morning, allowing time to recover or rebuild any hosts or services damaged by the scans before resumption of business on the following Monday. This phase is expected to require 4 consultant hours.

The third phase is the review of results, correlation to logs, report generation and presentation to GE management and staff. This phase is expected to require 12 consultant hours.

In all the project is expected to require 24 consultant hours, resulting in a fee of $3600.

Test Results (nmap):
Output from nmap –sT –O 206.207.211.254 (tcp scan using connect):

```
* * * * * * * *
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Interesting ports on dec1.giace.com (206.207.211.254):
(The 1536 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
137/tcp    filtered    netbios-ns
443/tcp    open        https

Remote operating system guess: SCO UnixWare 2.1.2
* * * * * * * *
```

Evaluation from nmap –sT –O 206.207.211.254:
The open ports for 25(smtp), 53(domain), 80(http) and 443(https) are expected, since these ports must be available to the Internet public.

Port 137(netbios) is similar in that it is explicitly denied and not logged. This is to minimize netbios connections attempts in firewall logfiles. Security vulnerability is minimal, but there is a suggestion in "suggestions" section below. Note that the border router has a ACL to block port 137/tcp from reaching the firewall, but this test was performed from inside the border-router.

The operating system guess is correct. Cyberguard appliances are based on SCO UnixWare. However Cyberguard has hardened the OS and while the entry lists the OS, it does not reveal that it is a Cyberguard firewall.

Output from nmap –sU –O –P0 206.207.211.254 (udp scan, don't ping):

```
* * * * * * *
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Host dec1.giace.com (206.207.211.254) appears to be up ... good.
Initiating UDP Scan against dec1.giace.com (206.207.211.254)
The UDP Scan took 184 seconds to scan 1453 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting ports on dec1.giace.com (206.207.211.254):
(The 1448 ports scanned but not shown below are in state: closed)
Port       State       Service
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
53/udp     open         domain
137/udp    filtered     netbios-ns
138/udp    filtered     netbios-dgm
161/udp    filtered     snmp
162/udp    filtered     snmptrap

Remote OS guesses: AIX v4.2, Axis 200+ Web Camera running OS v1.42, IBM MVS
TCP/IP stack V. 3.2 or AIX 4.3.2, Lexmark Optra S Printer, AXIS or Meridian
Data Network CD-ROM server, Meridian Data Network CD-ROM Server (V4.20 Nov 26
1997)
* * * * * * *
```

Evaluation from nmap –sU –O 206.207.211.254:
The open port for 53(domain) is expected, since this port must be available to the Internet public.

Ports 137 & 138 (netbios) are reported because of explicit deny/nolog rules for these ports. These are to minimize netbios connection attempts in firewall logfiles. Security vulnerability is minimal, but it has led to a suggestion in "suggestions" section below. Note that the border router has a ACL to block port these ports from reaching the firewall, but this test was performed from inside the border-router.

Ports 161 & 162 (snmp) must be a function of internal Cyberguard processes or hardening. No snmp agent runs on the firewall. There are no snmp rules in the manageable rulebase. However, there are additional rules in a Cyberguard configuration that at not available to normal management. Cyberguard's support database (URL: http://www.cyberguard.com/SUPPORT/Support_onlinesupport.html) did not address the issue.

The operating system guess is inconclusive.

I was expecting to see more ports exposed in the nmap scans. There are some firewall management ports open (supposedly only on the internal interface) that use some higher ports (8080/tcp, 8443/tcp, 3144/tcp, 5307/tcp). Also Passport One is supposed to be listening on the external interface using port 3443/tcp. Being curious, I ran another nmap tcp scan, this time scanning ports up to 9000. The results were the same as the scan above.

I decided to run a scan against the internal interface just for comparison.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sT -p 1-9000 -T Polite -oN
ictfwt1_scan.txt 192.168.168.1
Interesting ports on ictfwt1.kochind.com (192.168.168.1):
(The 8995 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
137/tcp    filtered    netbios-ns

# Nmap run completed at Thu May  9 13:40:58 2002 -- 1 IP address (1 host up)
scanned in 3699 seconds
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There is no mention of the Cyberguard management ports. These ports are only available from a single internal IP address. It appears that for nmap to consider a port open or filtered there must be a proxy running on the port or there must be an explicit permit or deny rule that permits or denies all IP addresses hitting an interface. Rules allowing connection from a specific IP addresse(s) don't show up in the nmap scans.

Test results (nessus). Comments are within the report:

```
Nessus Scan Report
------------------
SUMMARY
 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 1
 - Number of security notes found : 9

TESTED HOSTS
 206.207.211.254 (Security holes found)

DETAILS
+ 206.207.211.254 :
 . List of open ports :
   o general/tcp (Security notes found)
   o smtp (25/tcp) (Security hole found)
   o domain (53/tcp) (Security warnings found)
   o http (80/tcp) (Security notes found)
   o https (443/tcp)
   o general/udp (Security notes found)

 . Information found on port general/tcp
    "Default scan" set. nmap will ignore the user specified port range and
scan
     only the 1024 first ports and those declared in
     nmap-services

 . Information found on port general/tcp
    Nmap found that this host is running SCO UnixWare 2.1.2

 . Information found on port general/tcp
    QueSO has found out that the remote host OS is
    * BSDi or IRIX

    CVE : CAN-1999-0454

 . Vulnerability found on port smtp (25/tcp) :
    The remote SMTP server did not complain when issued the
    command :
      MAIL FROM: |testing

    This probably means that it is possible to send mail
    that will be bounced to a program, which is
    a serious threat, since this allows anyone to execute
    arbitrary commands on this host.

    *** This security hole might be a false positive, since
    *** some MTAs will not complain to this test, but instead
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
    *** just drop the message silently

    Solution : upgrade your MTA or change it.

    Risk factor : High
    CVE : CVE-1999-0203
```

* * * * * * * *

Author comment: The firewall did quietly drop this message. See SMTP proxy log analysis below.

* * * * * * * *

```
 . Information found on port smtp (25/tcp)
    a SMTP server is running on this port
    Here is its banner :
    220 dec0 SMTP Proxy Service Ready (Version: Tue Feb 19 00:21:39 EST
     2002)

 . Information found on port smtp (25/tcp)
    Remote SMTP server banner :
    dec0 SMTP Proxy Service Ready (Version: Tue Feb 19 00:21:39 EST 2002)
    502 HELP is
     unimplemented
```

* * * * * * * *

Author comment: The SMTP proxy does reveal the hostname of the firewall.

* * * * * * * *

```
 . Warning found on port domain (53/tcp)
    The remote name server allows recursive queries to be performed
    by the host running nessusd.

    If this is your internal nameserver, then forget this warning.

    If you are probing a remote nameserver, then it allows anyone
    to use it to resolve third parties names (such as www.nessus.org).
    This allows hackers to do cache poisoning attacks against this
    nameserver.


    Solution : Restrict recursive queries to the hosts that should
    use this nameserver (such as those of the LAN connected to it).
    If you are using bind 8, you can do this by using the instruction
    'allow-recursion' in the 'options' section of your named.conf

    If you are using another name server, consult its documentation.

    Risk factor :
     Serious
```

* * * * * * * *

Author comment: Cyberguard runs a custom and hardened version of bind 4.9.7. It is unknown whether recursion can be restricted to specific resolvers. This issue should be taken to Cyberguard Technical Support.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
* * * * * * * *

 . Information found on port http (80/tcp)
    a web server is running on this
     port

 . Information found on port http (80/tcp)
    The remote web server type is :

    Apache/1.3.9 (Unix)  (Red Hat/Linux)

    We recommend that you configure your web server to return
    bogus versions in order to not leak information

 . Information found on port http (80/tcp)
    An information leak occurs on Apache based web servers
    whenever the UserDir module is enabled. The vulnerability allows an
external

    attacker to enumerate existing accounts by requesting access to their
home
    directory and monitoring the response.

    Solution:
    1) Disable this feature by changing 'UserDir public_html' (or whatever)
to
    'UserDir  disabled'.

    Or

    2) Use a RedirectMatch rewrite rule under Apache -- this works even if
    there is no such  entry in the password file, e.g.:
    RedirectMatch ^/~(.*)$ http://my-target-webserver.somewhere.org/$1

    Or

    3) Add into httpd.conf:
    ErrorDocument 404 http://localhost/sample.html
    ErrorDocument 403 http://localhost/sample.html
    (NOTE: You need to use a FQDN inside the URL for it to work properly).

    Additional Information:
    http://www.securiteam.com/unixfocus/5WP0C1F5FI.html


    Risk factor : Low
    CVE : CAN-2001-1013

* * * * * * * *
```

Author comment: These are Apache web server issues and they will be forwarded to the GE IT staff member supporting web servers.

```
* * * * * * * *

 . Information found on port general/udp
    For your information, here is the traceroute to 206.207.211.254 :
    206.207.211.254
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

General Findings:
Not many open ports were found on the firewall. Other than ports requiring public access (DNS, HTTP, HTTPS, and SMTP), little else is accessible. There are a couple of reasons for the lack of open ports. 1) Where possible, efforts have been made to only allow specific source IP addresses to make connections through the firewall (Example: access to the "public" ftp server is allowed only from known supplier and customer IP addresses). 2) Some inbound rules (mostly VPN-based) are not even in the standard ruleset until a remote connection is made via Cyberguard's Passport One feature. After an authenticated Passport One connection is made, additional rules are dynamically added, with the source IP address being the IP address of the remote user.

Additional Suggestions:
The auditor noted that by using FTP over SSH for file transfers, the firewall FTP proxy was not being used. Logging for SSH connections is limited to simple connection reporting, while FTP proxy logging includes all commands issued during a session and filenames of files transferred. Further discussion determined that the need for encryption overrode the need for logging. It was recommended to provide as much logging as possible on the FTP server.

Addendum: An argument for proxying firewalls.
Reviewing firewall log entries revealed an interesting point. It was mentioned earlier in this document that the Cyberguard SMTP proxy only allowed the commands HELO, MAIL FROM, RCPT TO, DATA and QUIT. Below are Nessus scan attempts that were dropped by the Cyberguard SMTP proxy, thus sparing the smtp-relay server from having to deal with them. Normal connection and termination records have been omitted:

```
2002/05/08 14:01:26: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "□
2002/05/08 14:01:26: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "_.□
2002/05/08 14:01:26: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "□
2002/05/08 14:01:26: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "□
2002/05/08 14:01:27: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "GET"
2002/05/08 14:01:27: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command ""
2002/05/08 14:03:22: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "EXPN"
2002/05/08 14:03:23: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "VRFY"
2002/05/08 14:03:40: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:03:40: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "HELP"
2002/05/08 14:03:40: smtp: 146.209.128.120 --> 206.207.211.254 MAIL FROM:
<test_1@nessus.org>
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2002/05/08 14:03:40: smtp: 146.209.128.120 --> 206.207.211.254 RCPT TO:
<test_2@nessus.org>
2002/05/08 14:03:40: smtp: 146.209.128.120 --- 206.207.211.254 mail not
addressed to a recognized domain (test_2@nessus.org) - Dropped
2002/05/08 14:09:29: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:09:29: smtp: 146.209.128.120 --> 206.207.211.254 MAIL FROM:<>
2002/05/08 14:09:29: smtp: 146.209.128.120 --> 206.207.211.254 RCPT TO:
nobody@nessus.org
2002/05/08 14:09:29: smtp: 146.209.128.120 --- 206.207.211.254 mail not
addressed to a recognized domain (nobody@nessus.org) - Dropped
2002/05/08 14:09:42: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "`"
2002/05/08 14:09:45: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "`/bin/id`"
2002/05/08 14:09:47: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "`/usr/bin/id`"
2002/05/08 14:09:55: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "debug"
2002/05/08 14:09:56: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:09:57: smtp: 146.209.128.120 --> 206.207.211.254 MAIL FROM:
root@206.207.211.254
2002/05/08 14:09:58: smtp: 146.209.128.120 --> 206.207.211.254 RCPT TO:
root@host1@206.207.211.254
2002/05/08 14:09:58: smtp: 146.209.128.120 --- 206.207.211.254 mail not
addressed to a recognized domain (root@host1@206.207.211.254) - Dropped
2002/05/08 14:10:06: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:10:06: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "HELP"
2002/05/08 14:10:06: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:10:06: smtp: 146.209.128.120 --> 206.207.211.254 MAIL FROM:
root@206.207.211.254
2002/05/08 14:10:06: smtp: 146.209.128.120 --> 206.207.211.254 RCPT TO:
/tmp/nessus_test
2002/05/08 14:10:06: smtp: 146.209.128.120 --- 206.207.211.254 mail not
addressed to a recognized domain (/tmp/nessus_test@) - Dropped
2002/05/08 14:10:07: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:10:07: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "AUTH"
2002/05/08 14:10:07: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
2002/05/08 14:10:07: smtp: 146.209.128.120 --> 206.207.211.254 MAIL FROM:
root@206.207.211.254
2002/05/08 14:10:07: smtp: 146.209.128.120 --> 206.207.211.254 RCPT TO:
|testing
2002/05/08 14:10:07: smtp: 146.209.128.120 --- 206.207.211.254 mail not
addressed to a recognized domain (|testing@) - Dropped
2002/05/08 14:10:08: smtp: 146.209.128.120 --> 206.207.211.254 QUIT
2002/05/08 14:10:08: smtp: 146.209.128.120 <-- 206.207.211.254 221 dec0
closing connection
2002/05/08 14:11:21: smtp: 146.209.128.120 --> 206.207.211.254 HELO
nessus.org
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2002/05/08 14:11:21: smtp: 146.209.128.120 --> 206.207.211.254 MAIL
FROM:nessus@nessus.org
2002/05/08 14:11:21: smtp: 146.209.128.120 --> 206.207.211.254 RCPT TO:
Administrator
2002/05/08 14:11:21: smtp: 146.209.128.120 --- 206.207.211.254 mail not
addressed to a recognized domain (Administrator@) - Dropped
2002/05/08 14:11:21: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "BDAT"
2002/05/08 14:11:21: smtp: 146.209.128.120 --- 206.207.211.254 WARNING:
attempt to use unimplemented command "b00mAUTH"
2002/05/08 14:11:21: smtp: 146.209.128.120 --> 206.207.211.254 QUIT
2002/05/08 14:11:21: smtp: 146.209.128.120 <-- 206.207.211.254 221 dec0
closing connection
```

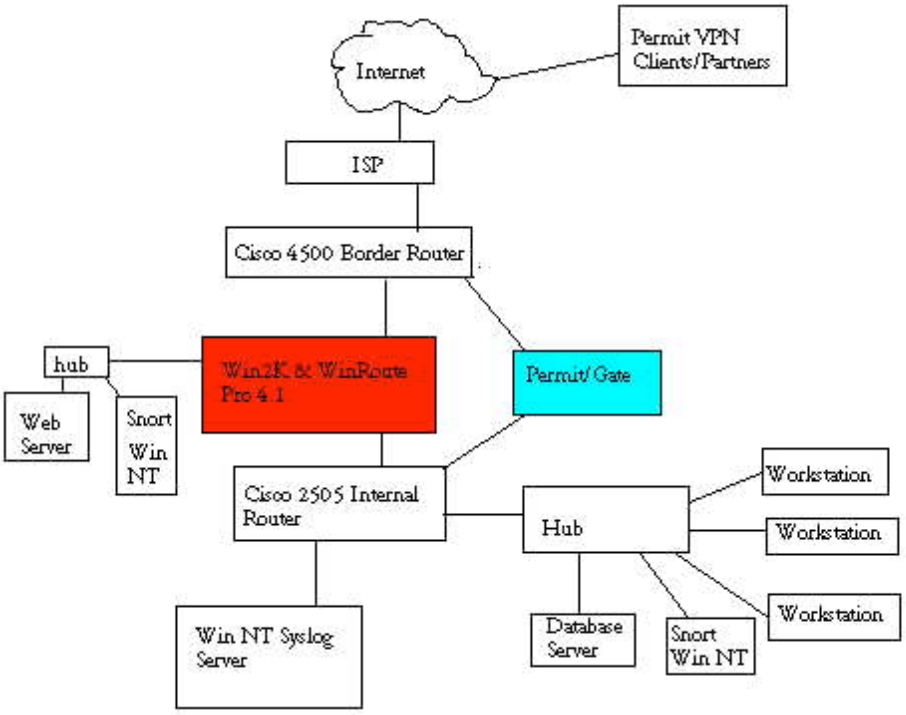
Of course, an application proxy is only as good as its implementation.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 4 – Design Under Fire:

I have chosen to test the practical by William Rybczynski. Mr. Rybcznski's practical can be found at URL: http://www.giac.org/practical/William_Rybczynski_GCFW.zip.



Mr. Rybczynski is employing a WinRoute Pro firewall (URL: http://www.kerio.com). This firewall is generally marketed toward small to medium companies, and finding that GIAC Enterprises is using this firewall solution may give potential hackers a hint as to the size of the company. Also, researching vulnerabilities in WinRoute Pro should be a welcome diversion from all the other Checkpoint, PIX and Netfilter firewalls.

Before proceeding further, we need to gather information about our target network. I was fortunate to obtain a copy the diagram above from an undisclosed source. The diagram outlines some devices, some operating systems and some application software that is in the network.

Running a port scan against the Internet-facing network would be the first order of business. A tool such as nmap (URL: http://ww.insecure.org) would work nicely. This would give me a list of possible attack ports and possible types of operating systems. The network diagram indicates an IDS system (snort) on the service network and internal network, but does not indicate one on the external network. Even so, I may want to scan slowly (nmap –T Paranoid) in an attempt to fly in under the IDS radar.

AUTHOR NOTE: Unfortunately, this network isn't really available to scan against, and I didn't have access to a Winroute Pro firewall and network to test it on. Although general an attacker would not have access to Mr. Rybczynski's practical (but it could happen), I am going to use it to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

make some assumptions about what might be seen with an nmap scan. END NOTE.

Below are the results of the fictitious scan. There appears to be either not much answering to a scan. Either the router/firewall rules are very tight or offered services are only available to specific source IP addresses (according to the practical, both cases are true). The only IP address answering to the public Internet was 199.158.28.94. Here are the results of the fictitious scan:

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sT -p 1-9000 -T Polite
199.158.28.94
Interesting ports on (199.158.28.94:
(The 8995 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
80/tcp     open        http
443/tcp    open        https
```

With this few ports, nmap may have trouble identifying the operating system.

There aren't many ports open, not even DNS. GIAC Enterprises' ISP must host their external DNS. Running nslookup against my usual DNS server verifies this:

```
c:\>nslookup
Default Server:  ns1.hacksrus.net
Address:  a.b.c.d

> set query=ns
> fortunesun.com
Server:  ns1.hacksrus.net
Address:  a.b.c.d

Non-authoritative answer:
fortunesun.com          nameserver = ns1.bigisp.net
fortunesun.com          nameserver = ns2.bigisp.net

ns1.bigisp.net          internet address = e.f.g.h
ns2.bigisp.net          internet address = e.f.i.j
>
```

I also know there should be a VPN server on the GIAC Enterprises DMZ, but it must only allow connections from specific IP addresses to connect to it.

My ill-gotten network diagram lists the firewall as a WinRoute Pro. I check out http://www.winroute.com, which takes us to http://www.kerio.com. Here's a lot of interesting information. A 30-day evaluation copy of WinRoute Pro is available at URL: http://www.kerio.com/parser/mainpage.php?id=79&lg=1. Someone making a serious attempt at breaking into this network should obtain a trial copy and spend some time trying to break it.

Kerio was also very kind in having their WinRoute Pro manual online at URL: http://www.kerio.com/dwn/wrp/wrp42en.pdf. This is another good way to get some background on the product. WinRoute Pro runs on a Windows 2000 platform, so there is the possibility of finding vulnerabilities in both the application and the operating system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Firewall Attack:
WinRoute Pro appears to be your basic packet-filtering firewall. It is "stateful" to the extent that it is aware of the syn/syn-ack/ack handshake. An http proxy is mentioned, plus a smtp/pop3 mail server. However, documentation did not mention that the proxies/servers actually do any application or rfc-compliant checking. Also, I could not find information on what OS hardening is done, other than their claim that they insert their application very low into the TCP/IP stack so that their application gets first chance to look at network packets. Some of the

In researching vulnerabilities, the following Internet sites were used:
http://cve.mitre.org
http://www.packetstorm.com
http://www.securityfocus.com
http://www.incidents.org
http://www.cert.org
http://groups.google.com (newsgroup search)

A search for WinRoute Pro vulnerabilities was not very fruitful. I did unearth a couple of issues. Some of these statements come from newsgroup discussions and verification may be suspect.

http://online.securityfocus.com/archive/1/153953
"Message Type: Informational Risk: Low Software: WinRoute Pro v4.1 all current builds. Other versions of WinRoute may also be affected but I have not confirmed this. Platform: Windows 2000 Description: I have discovered that the WinRoute installer disables memory write protection under Windows 2000. WinRoute refuses to run if memory write protection is enable. Memory write protection enabled is the default for Windows 2000. The registry key affected is: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\EnforceWriteProtection Disabling. Memory write protection can indirectly affect the stability and security of the machine. Malicious software such as viruses may find it easier to corrupt the system or hijack system processes. Buggy software will crash the system more easily. A hacker may be able to use this information to more easily penetrate a WinRoute firewalled system. Tiny Software initially denied that they were disabling memory write protection. After many email messages and sending them a sample capture taken using regmon they have changed their tune. The current story is that WinRoute needs to shim the operating system to be able to intercept networking functionality at a low enough level to ensure security."

An interesting fact to remember: WinRoute Pro may lessen Windows internal memory management protection? Maybe the Win2000 under the firewall app may be weaker then usual.

Jan, 2002, newsgroup comp.os.ms-windows.nt.admin.security
"WinRoute is an adequate firewall for very small networks, even if Tiny Software fudges the truth a bit when they say that it is stateful. What they mean by stateful is simple packet filtering based on ACK and SYN flags--which is not stateful filtering at all. I chewed them out about this once and their reaction was "Oh well." Also, the product claims to operate "below" the Windows NT protocol stack, which they say allows it to start up before any of the other communications

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

services, making the system more secure. This, too, is not true. Simply do a contiuous ping to a WinRoute machine during the boot process and you will observe replies for a short period before the WinRoute service starts. This demonstrates that a WinRoute machine is at least partially vulnerable for a period during boot. This leads to the biggest problem with WinRoute. It does not "fail closed," which is to say that if something goes wrong with the WinRoute service and it fails to start, then it can leave the host wide open. Ugh."

Some of this sounds good. This guy claims that WinRoute Pro doesn't behave as its documentation states. This is an unsubstantiated claim, but worth testing against.

Mar, 2000, newsgroup comp.security.firewalls
"...Winroute does have one security flaw of that I'm aware. The administration account defaults to Username=admin, Password=<blank>. I think the install should force a password choice."

Surely the GIAC Enterprises admin wouldn't leave the default !! Unfortunately it would be hard to test, since the nmap scan of the firewall didn't show any admin ports open to public IP addresses.

Nov, 1999, newsgroup comp.security.firewalls
"...The only caveat with its use of which I'm aware probably applies to most software firewall and NAT products...don't run internet services on an unattended Winroute machine. Sometimes, after rebooting after a change to the network setup (eg., change of NIC or driver), the Winroute service may fail to start. Without Winroute running, there is no firewall, and any services running on the Winroute machine are open on the Internet..."

Based on the above comments (especially the comments on failing open and failure of the WinRoute service to start, I would suggest a firewall attack that would overpower the firewall via a denial of service, causing a failure of the gateway software or a reboot. The denial of service scenario below might be able to kill the WinRoute Pro application or cause the entire system to crash and be rebooted. Once the firewall was no longer responding to the denial of service attack, begin scanning for open ports that may now be exposed.

Denial of Service Attack:
Using the 50 broadband zombie systems at my command, I am going to mount a SYN flood attack against the firewall.

The attack method:
A SYN packet is the first packet of the three-packet "handshake" sent at the beginning of a TCP connection. The target system replies with a SYN/ACK packet, indicating that is will accept the connection, but needs final confirmation of the connection from the source system (the final ACK packet). In a SYN flood attack, the target receives a SYN packet from an attacking system. Often the source IP address is spoofed, which provides the attacking host both anonymity and protection from the answering SYN/ACK packets. The targeted system responds with its SYN/ACK packet and patiently waits for the final ACK packet to arrive back. Unfortunately, the final ACK never arrives because the attacking system never sends it. While waiting for this

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

never-to-come final ACK, the target system expends system resources to hold open this half-opened connection (the SYN_RECV state) until the connection attempt times out. At that point the target system does finally close the connection and release the system resources used for that connection.

These system resources are finite. The idea of a SYN flood is to open more connections on the target than the target has resources for. The target can now no longer accept any new connections. At the least, access to this target prohibited. It is too busy to service legitimate business connections. At most, there is the possibility that the target system cannot handle this exhaustion of resources and become unstable, causing the target to crash individual processes or even the operating system.

At this point the system may be vulnerable to attack because protective services may no longer be running. Remember the newsgroup message about WinRoute Pro listed above? If someone were to crash the firewall process on this firewall, and if when crashed, the firewall fails in an "open" configuration, nothing may be blocked. There is now the possibility to make a connection to the firewall or a system behind it and compromise it by changing its configuration or installing a root kit/trojan/virus/remote control program.

The attack tool will be Tribal Flood Network 2000 (TFN2K). The source code for this tool can be found at URL: ftp://ftp.ntua.gr/pub/security/technotronic/denial/. TFN2K is capable of a number of different attacks: Smurf attack, SYN floods, UDP floods and ICMP floods.

SYN Attack countermeasures:

- Allocate more system resources to the connection queue. This allows the attacked system to handle more connections and half-open connections at a time. Of course, there are memory and other system constraints that limit how many resources can be allocated.
- Decrease the time-to-live for half-open connections. There is a limit to how small you can set this time-out. You don't want to time-out legitimate connections because of latency across the Internet.
- Some firewalls have SYN-flood protection that can be enabled. This feature keeps track of how long SYN/ACKS have gone unanswered and kills the unanswered ones. Extra system resources are required to perform this. Most firewall vendors recommend that this feature not be turned on except when the firewall is actually under a SYN flood attack.

Compromising an Internal host:

The GIAC Enterprises web server and the smtp server on the WinRoute Pro firewall itself appear to be the only hosts to mount an attack against. Not having much information about the WinRoute smtp service, the webserver may be an easier target.

idserve.exe from Gibson Research Corp. URL: http://www.grc.com) is a program that will easily report header and greeting messages from http servers. It can also extract banners and such from other servers (i.e. ftp and smtp servers). Using this tool against the fictitious www.fortunesun.com server reveals `Microsoft IIS/5.0`. It is a Windows platform running Microsoft Internet Information Server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Microsoft IIS has a history of vulnerabilities. Microsoft issues patches to these vulnerabilities, but not all webservers are up-to-date on their patch levels.

The "NIMDA" worm mounts an attack against a list of vulnerabilities and would be a good test for an attempted compromise of the GIAC Enterprises web server. Details on NIMDA can be found at URL: http://www.incidents.org/react/nimda.pdf. The NIMDA worm is still very prevalent on the Internet. If the GIAC Enterprises web server is susceptible to NIMDA, it may already become compromised before you can mount your attack against it :-). Unpatched Internet webservers can become infected with NIMDA only hours after the are put online.

The Social Engineering Aspect.

Often the easiest way to break into a network is with social engineering—using deception to gain information from people. This may be the best way to gain access to GIAC Enterprises. As resistance to social engineering goes, GIAC Enterprises has one thing going for it—it is a small company. It also has something against it—it is a small company. Let me explain:

Being a small company, GIAC Enterprises employees probably know everyone else in their office. An attempt to gain information by calling on the telephone and posing as an employee who "lost" his password probably wouldn't work, because everyone could notice that the imposter isn't really Barney the salesguy.

However, in most small companies, internal security is lax because everyone is trusted. Accounts get shared. Passwords are weak. Notes and documentation are scattered all around. Computers logged in without locking screensavers. If a potential hacker were to gain physical access to the office, he would probably find a wealth of usable information just lying around. In addition, he may find that the company's servers are sitting out in the open—to access machine consoles only requires that one pull up a chair to the keyboard.

If I were intent on gaining access to GIAC computers, I would strongly consider making a visit to its office—either as a business-hours visitor or as a "non-business-hours" visitor. Sometimes the best solution is not the high-tech one :-)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References:

Cisco Corp. Configmaker software.
URL: http://www.cisco.com/warp/public/cc/pd/hemnsw/cm/index.shtml

Cisco Corp. 2514 Router information.
URL: http://www.cisco.com/warp/public/cc/pd/rt/2500/index.shtml

Cisco Corp. Website search.
URL: www.cisco.com

Cyberguard Corp. Cyberguard online manuals.
URL: ftp://ftp.cyberguard.com/Unix/5.0/Doc/Manual/

Gibson Research Corp. IDServe software.
URL: http://www.grc.com

Google Groups. Internet newsgroups search.
URL: http://groups.google.com

Kerio Technologies Inc. WinRoute Pro online manual.
URL: http://www.kerio.com/dwn/wrp/wrp42en.pdf

McClure, Stuart; Scambray, Joel; Kurtz, George. "Hacking Exposed: Network Security Secrets & Solutions". Osborne/McGraw-Hill, 1999.

RSA Security. SecurID product.
URL: http://www.rsasecurity.com/products/securid/

SANS Institute. "Firewall, Perimeter Protection and VPNs" courseware.
URL: www.sans.org

SANS Institute. "Nimda Worm/Virus Report – Final"
URL: http://www.incidents.org/react/nimda.pdf.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A - Project Requirements:

Basic Requirements:
This assignment consists of four related parts. Please check your spelling and read through your wording! This is how the world will see you; you will not be allowed to "clean up" your paper once it has been submitted. You will be graded primarily on the accuracy and educational value of your submission, but appearance also counts.

Your completed submission (all four assignments) should be a minimum of 20 pages long, and should also meet all of the other requirements listed in the Administrivia under "Formatting and Minimum Length". Your work should include diagrams, screen shots, code examples, references, and/or appendices as appropriate.

Note that many students get bogged down with putting a lot of extraneous information into the assignment. In their efforts to write a comprehensive paper, they leave out the specific items that are asked for in the assignments below. Focus on the required items listed in the assignment, and then work on any additional information you want to include.

Assignment 1 – Security Architecture (15 points):
Define a network security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.

Your architecture must consider access requirements (and restrictions) for:

- Customers (Companies or individuals that purchase bulk online fortunes)
- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)
- Partners (International companies that translate and resell fortunes)
- GIAC Enterprises employees located on GIAC Enterprise's internal network
- GIAC Enterprises mobile sales force and teleworkers

You must explicitly define how the business operations of GIAC Enterprises will take place. How will each of the groups listed above connect to or communicate with GIAC Enterprises? How will GIAC Enterprises employees access the outside world? What services, protocols, or applications will be used?

Defining access requirements and the reasoning for those requirements is **critical** to this assignment. If you have not thought through how this access will take place, you will not be able to adequately define your security policy and ACLs/rulesets later in the paper.

In designing your architecture, you **must** include the following components:

- Filtering Router(s)
- Firewall(s)
- VPN(s)

Your architecture may also include the following **optional** components if they are appropriate to your design:

- Internal firewalls (Are internal firewalls appropriate for additional layered protection; to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

segment internal networks…?)
- Additional secure remote access (Is additional remote access – other than the VPN – required by administrators, salespeople, telecommuters…?).
- Intrusion detection systems

You must include a diagram or set of diagrams that shows the layout of GIAC Enterprise's network and the location of each component listed above. You must provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

The network can be as complex or as simple as you like as long as it meets the functional requirements that you define according to the guidelines given above. The important thing is not how elaborate your network is, but that your design actually works.

You must justify the appropriateness of your design. Is it both technically reasonable and financially feasible? Are you building a $1000 fence to contain a $100 horse? You may provide a cost or bill of materials if you wish.

Assignment 2 – Security Policy and Tutorial (35 points):

Based on the security architecture that you defined in Assignment 1, provide a security policy for the following three components:
- Border Router(s)
- Primary Firewall(s)
- VPN(s)

You may optionally include policy for other devices (i.e., - internal firewalls).

By "policy" we mean the specific set of ACLs, ruleset, or IPSec policy for that device – **not** corporate or organizational policy (though note that organizational policy may dictate the specific ACLs or ruleset in effect).

For each component, be sure to consider the access requirements for customers, suppliers, partners, remote users, and internal users that you defined in Assignment 1. The policies you define must accurately reflect those business needs as well as appropriate security considerations.

You must include the complete policy (meaning explicit ACLs, Ruleset, IPSec policy, etc.) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" The policies may be included in an Appendix if doing so will help the "flow" of the paper (clearly state if this is the case).

For each rule in all policies, you must include the general purpose of the rule and why it is important.

You must also include a discussion of the order of the rules, and why order is (or is not)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

important.

For **one** of the three security policies defined above, you must incorporate a tutorial on how to implement the policy. Clearly separate and label your tutorial. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information to clarify your instructions. Be certain to include a general explanation of the syntax or format of the ACL, filter, or rule for your device, as well as a general explanation of how to apply a given ACL, filter, or rule.

Be certain to point out any tips, tricks, or potential problems.

Assignment 3 – Verify the Firewall Policy (25 points):

You have been asked to conduct a technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced as described in Assignments 1 and 2. To conduct the audit, you will need to:

- Plan the audit.
- Describe the technical approach you will use to assess the firewall.
- Be certain to include considerations such as what shift or day you would do the assessment.
- Estimate costs and level of effort.
- Identify risks and considerations and how they are addressed.

Using the approach you described conduct the audit.

- Demonstrate how you validated that the primary firewall is actually implementing GIAC Enterprise's security policy.
- Be certain to include the tools and commands used. Include screen shots in your report if possible.

Evaluate the audit. Based on your assessment (and referring to data from your assessment):

- Provide an analysis of the audit results.
- Make recommendations for improvements or alternate architectures.
- **Supportive diagrams are strongly recommended for this part of the assignment.**

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but you must annotate/explain the output.

Assignment 4 – Design Under Fire (25 points):

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any GCFW practical posted in the previous **6 months** and paste the graphic into your submission. Be certain to list the URL of the practical you are using.

Research and design the following three types of attacks against the architecture:

1. An attack against the firewall itself.
   - Research and describe a vulnerability that has been found for the type of firewall chosen for the design.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- •Design an attack based on the vulnerability.
- •Explain the results of running that attack against the firewall.

2.A denial of service attack.

- •Subject the design to an attack from 50 compromised cable modem/DSL systems.
- •Describe the countermeasures that can be put into place to mitigate the attack that you chose.

3.An attack plan to compromise an internal system through the perimeter system.

- •Select a target and explain your reasons for choosing that target.
- •Describe the process to compromise the target.

Your attack information should be detailed – include the specifics of how the attack would be carried out. Do not simply say "I would exploit the vulnerability described in Vendor Security Bulletin XXX". What commands would you use to carry out the attack? Are exploit tools or scripts available on the Internet? What additional steps would you need to take prior to conducting the attack (reconnaissance, determining internal network layout, determining valid account name…)? Would any of your methods be noticed (log files, IDS…)? What "stealth" techniques could you employ to avoid detection? What countermeasures would help prevent your attack from succeeding?

If it is possible to carry out the attack on a test system, include screen shots, log files, etc. as appropriate to illustrate your methods.

In designing your attacks, keep the following in mind:

- •The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.
- •The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should **not** assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)
- •You must supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

The attack does not necessarily have to succeed. If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.