



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 permitted without express written permission.

Firewalls, Perimeter Protection and VPNs
Practical Assignment (v 1.6a)
GIAC Enterprises
Fortunesun.com
William H. Rybczynski
SANS Aloha IV

© SANS Institute 2000 - 2005, Author retains full rights.

Assignment #1 – Security Architecture:

Define security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.

Consider access requirements and restrictions for:

Customers (companies that purchase bulk online fortunes)

Suppliers (authors of fortune cookie sayings that connect to supply fortunes)

Partners (international partners that translate and resell fortunes)

GIAC Enterprises (employees located on internal network)

GIAC Enterprises is a small startup company that has begun operations with 10 employees. As a Security Consultant for NetSec Consulting we have been brought in to assist with securing the company's network perimeter and infrastructure. The original IT personnel had purchased the following items from other startup companies that had since gone out of business. (1) Cisco 2505, (1) Cisco 4500-M, (1) Windows 2000 SP2 Server, (3) NT 4.0 SP6a Servers and (1) Permit/Gate 7520 VPN device. We have been tasked with securing the networking using these devices.

GIAC Management has a limited budget of \$1000.00 to be used for security purchases. Once GIAC begins to make a profit, funds will become available upon request for upgrades.

GIAC Enterprises runs an internal network made up of Windows NT 4.0 SP6a Workstations and Servers. Due to the fact that GIAC Enterprises is still a start-up company, they do not plan to retain an on-site Security Staff. This is important to note upfront when planning how to administer the different devices on the network that we are configuring. Special attention must be placed on the ability to remotely connect to these devices from the consulting home office. With these guidelines in place, WinRoute Pro has been selected as the Firewall platform that will run on the Windows 2000 Server. WinRoute Pro is an ICSA-certified Firewall that scales well for small to medium size businesses. Tiny Personal Firewall was selected as the workstation firewall solution. Tiny Software is fielding a Centrally Managed Desktop Security solution that incorporates the Tiny Firewall. Although not available during the initial installation of GIAC Enterprises security, this is seen as a viable future purchase for securing the GIAC network, as well as, their partners and employees. The CMDS will offer a central management solution for distributed desktop firewall management. WinRoute Pro was selected because of its ease of use and low cost. WinRoute starts all rulesets before any network traffic comes in contact with the computer running the firewall software. WinRoute Pro also has a fail-safe mechanism that prevents all network traffic from traversing the firewall computer if the WinRoute Pro engine fails. This effectively stops all traffic from being routed across the firewall. (Reference: WinRoute Pro Reference Guide for Version 4.1 build 22 and later) Although this could create a self-imposed denial of service if the box were compromised, this is a more desirable situation than to have the engine fail and not be alerted. Remote administration of the firewall will be permitted from NetSec Consulting as GIAC Enterprises has selected a remote management option due to the fact that they do not desire an onsite staff. WinRoute Pro uses Blowfish for encryption of all administration

traffic. The Permit Gate 7520 will be used as the VPN for GIAC Enterprises Partners. Additionally, GIAC Enterprises has purchased the domain name www.fortunesun.com for their web presence.

Although there are better devices available for configuring a network, we have to work with the gear on hand. It has been decided that these devices will be used in the following manner.

Cisco 4500-M – Border Router

Permit/Gate 7520 - VPN

Cisco 2505 – Internal Router

Windows 200 Server – Firewall running WinRoute Pro v4.2

(1) NT Server –IDS running Snort for Windows on the Internal Network

(1) NT Server – Syslog Server

(1) NT Server – IDS running Snort for Windows on the DMZ

Connectivity to the Internet will be provided through the local RoadRunner ISP.

GIAC Enterprises has (1) web server for e-commerce use. This server will be connected on the service network to keep it isolated from the internal network. The web server will also provide general company related information. GIAC Management has stated that they want to implement VISA's "Ten Commandments for Securing Your Web Assets." Customers and partners will be able to place orders online for fortunes. GIAC employees will confirm and fill all order requests.

Business Operations:

Customers. GIAC Enterprises focus is on the purchase of bulk fortunes from its web site (<http://www.fortunesun.com/>). These customers connect to the GIAC site and review an online database of fortune themes. Once a particular theme is selected, the customer is able to submit his order in 50 fortune blocks. Purchases can only be made from the web and at this time GIAC accepts most major credit cards from an HTTPS/SSL connection.

Suppliers. GIAC Enterprises maintains a database of the top 10 fortune writers in the world segregated by themes. These suppliers are notified via email when their next batch of fortunes is due for submittal. All fortunes must be submitted via the web to Fortunes2002@fortunesun.com. Once approved the supplier is sent a check for his service. GIAC Enterprises pays \$50.00 for every 75 fortunes submitted and accepted.

Partners. GIAC Enterprise partners are notified via email when updated fortunes have been submitted. These emerging partners are able to access the internal fortunes database via VPN to determine which "new fortunes" they would like to request for translation to their customer base. Currently the business partners of GIAC Enterprises are made up of several start-up businesses around the world trying to break into the fortune cookie market. Partners will receive shared secret passwords and usernames via the postal service for accessing the VPN. (Although this is not the most secure method for authentication, it is an accepted security practice from GIAC Management.) Partners will then be given

usernames and passwords for read-only access to the Database Server.

GIAC Enterprises Employees. GIAC's 10 employees must have web, email and internal access to the fortunes database server. Access to the Web Server for uploading fortunes will be granted using SSH from the internal network. Employees will be able to access resources on the database server on the internal network after authenticating with the PDC.

Security Guidelines:

Using the same general security principles presented by Kofi Arthiabah and the Visa Ten Commandments for Securing Your Web Assets, the following guidelines have been established.

1. Err on the side of security.
2. Keep the network as secure as possible with available resources.
3. GIAC will use the Cisco 4500-M as the border router.
4. The Windows 2000 machine will act as a Firewall utilizing WinRoute Pro 4.2.
5. The Cisco 2505 will serve as the internal router.
6. One NT Server will serve as the IDS running Snort for Windows on the Service Network and one NT Server running Snort will serve as the IDS on the Internal Network.
7. One NT Server will serve as the Syslog Server.
8. Everything is explicitly denied unless explicitly required/allowed.
9. Create a defense-in-depth environment.
10. ACLs will be used to establish this from the Border Router through the Internal Router.
11. Outside access to internal resources will be accomplished via encrypted VPN using IPSec and shared secret passwords.
12. Personal Firewalls will be installed on all internal user computers.
13. All systems will use Norton Anti-Virus Corporate Edition.
14. Purchase items that can be incorporated into the existing network components.
 - a. WinRoute Pro
 - b. Tiny Software Personal Firewall
 - c. Norton Anti-Virus
15. Whenever possible, use web-browser based applications with SSL-based security.
16. All access to resources will require a username and password combination. This will allow GIAC to track access to data by unique ID.
17. Each user with computer access will have a unique ID.
18. Regularly test security systems and processes.
19. All systems will be scanned before being connected to the network to ensure a secure baseline has been established.
20. The GIAC internal network will be scanned once a month to identify vulnerabilities.
 - a. The perimeter will be scanned once a month to identify vulnerabilities.
 - b. All systems will be scanned daily for viruses.

Device Configurations:

Border Router: The border router will be used as a screening router to drop any traffic that meets specific guidelines. Traffic will be segmented to either the Permit Gate VPN or Firewall depending on destination. We will screen all internal addresses that could be spoofed as well as all unassigned public IP addresses. We will screen ICMP traffic and NetBIOS traffic here. Ingress filtering will be applied for loopback, private addresses, and unallocated IPs. Any firewall subverting services like AOL IM (205.188.7.0/23) and www.gotomypc.com will be blocked. Logging will be implemented when feasible. These logs will be reviewed and compared against the SANS Top 10 “bad guys” at www.incidents.org and if necessary rules will be implemented to block them as well.

Firewall: The firewall will permit incoming traffic on port 80 and port 433 only to the web server. All incoming traffic for port 25 from the ISP mail server will be allowed due to the fact the WinRoute Pro can also be used as a mail server. Although this is not the best security practice, cost restraints prevent GIAC from purchasing an independent mail server at this time. Critical Services will be blocked here. The Windows 2000 Operating System will be hardened using recommendations from NIST Special Publication 800-43 System Administration Guidance for Securing Microsoft Windows 2000 Professional System. Outbound traffic will be allowed using NAT. The use of NAT will also allow for stateful inspection of all traffic traversing the firewall. Outbound web traffic will be permitted to include HTTP/HTTPS and FTP. All established connections from the web server will be permitted. Access to the firewall engine will only be granted by user name and password using strong authentication. Traffic traversing the firewall will be logged and time stamped. The firewall will act as a NAT device for all traffic. Ant-spoofing rules will be established to prevent invalid source addresses from originating from the GIAC local network. The DNS Forwarder will be used to forward DNS queries to the ISP DNS and queries will be stored in the internal cache on the WinRoute Pro Firewall. (Although it is desirable to use a separate device for DNS, GIAC Enterprises is restricted due to current costs and the low number of local users. If it is determined that the added DNS overhead is too much for the firewall, a case will be presented to management to purchase a separate system for running DNS.) The email server will also be enabled for receiving and distributing email messages to GIAC Enterprises employees.

Virtual Private Networks: The Permit Gate will be used for the GIAC VPN IPSec solution. The Permit Gate will be placed in parallel to the Firewall. This will reduce the traffic load on the Firewall. Shared Secret passwords will be used for authentication when accessing the network resources via the VPN. Although certificates are considered a more secure authentication method, partners will confirm receipt of their passwords via a phone call to the GIAC offices. All shared secret passwords will be sent via registered mail. Once receipt of the password has been confirmed by both the phone call and registered mail, partners will receive the Permit Client software via email. Although not 100% secure, these separate layers of confirmation help to ensure the integrity of the shared secret password.

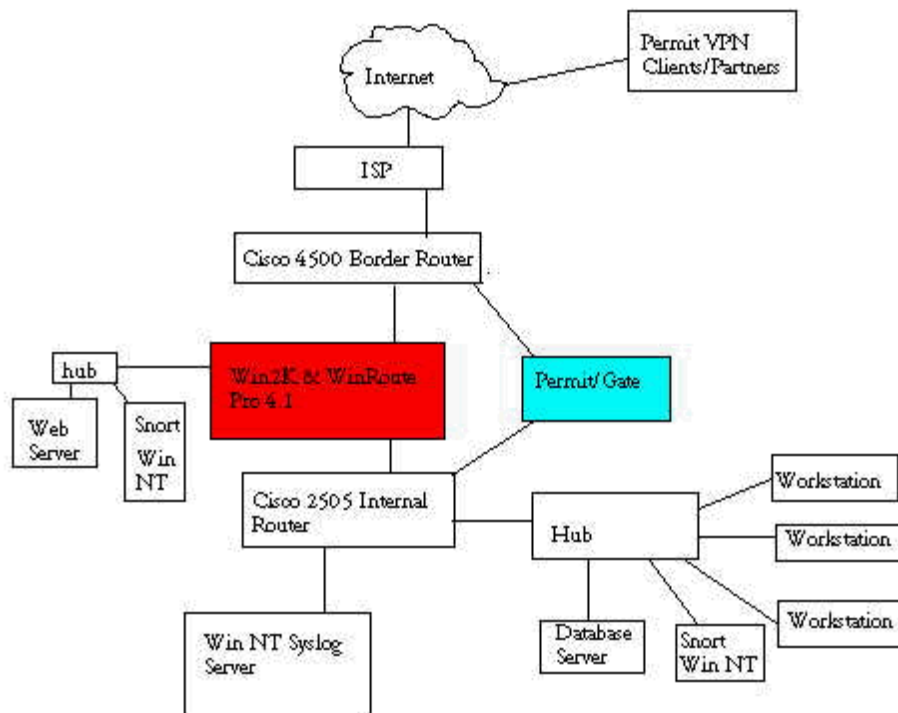
Internal Router: The internal router will be used to segment the internal network and to route traffic correctly between the VPN and Firewall. The Syslog Server will reside on it's

own subnet off of the internal router. GIAC employee computers will also establish connectivity here. Egress filtering will be applied here.

The SNORT IDS systems will run with their network cards in promiscuous mode to monitor web server traffic and internal network traffic. All logs will be sent to the Syslog Server and will be reviewed weekly per the established security contract with NetSec.

Internal Machines: All internal systems will be assigned private IP addresses. All employee computers will have Tiny Personal Firewall installed. Norton Anti-Virus Corporate Edition will be used for virus protection on the user workstations.

A diagram of the GIAC network is provided.



Assignment #2 – Security Policy

Important IP Addresses for GIAC Architecture.

Border Router to Firewall Interface: 199.158.28.65

Border Router to VPN Interface: 199.158.28.66

Firewall Outside Interface: 199.158.28.94

Firewall to GIAC Internal Network: 192.168.2.1

Firewall to Service Network Interface: 192.168.1.3

Web Server: 192.168.1.1

VPN Outside Interface: 199.158.28.93

VPN Inside Interface: 192.168.7.1

Border Router Ruleset:

Below is an example of the GIAC Border Router configuration. Explanations and references are provided, where appropriate.

Current configuration:

```
!  
version 11.3  
>>CONFIGURED FROM GLOBAL CONFIGURATION MODE  
>>GIAC_Border#conf t  
>>GIAC_Border(config)#  
!TIMESTAMP LOGS FOR EVENT CORRELATION IF NEEDED  
service timestamps debug datetime  
service timestamps log uptime  
!PREVENTS PASSWORDS FROM BEING STORED IN THE CLEAR  
service password-encryption  
!  
hostname GIAC_Border  
!  
>>CONFIGURED FROM GLOBAL CONFIGURATION MODE  
>>GIAC_Border#conf t  
>>GIAC_Border(config)# enable secret ALOHA  
>>GIAC_Border(config)# no enable password  
!CREATES PASSWORD FOR PRIVILEGED ACCESS TO ROUTER  
enable secret 5 $1$QNd/$t36jrEr95GYp8yj8Xs5ac1  
!  
>>CONFIGURED IN GLOBAL CONFIGURATION MODE  
>>GIAC_Border#conf t  
>>GIAC_Border(config)#  
!IMPROVING SECURITY ON CISCO ROUTERS  
!http://www.cisco.com/warp/public/707/21.html#redirect  
!PREVENTS DENIAL OF SERVICE ATTACKS THROUGH ABUSE OF THESE  
SELDOM USED SERVICES. DISABLED BY DEFAULT IN IOS 12.0 AND HIGHER  
no service tcp-small-servers  
no service udp-small-servers  
!PREVENTS FORWARDING OF ANY PACKETS WITH THE SOURCE ROUTING  
OPTION SET  
no ip source-route  
!PREVENTS ABUSE OF THIS SERVICE TO DETERMINE LOGGED IN USER  
no ip finger  
!PREVENTS BOOTP RESPONSES  
no ip bootp server  
!PREVENTS ROUTER FROM RESOLVING ADDRESSES TO HOST NAMES  
no ip domain-lookup
```


!PREVENTS ROUTER FROM ACCEPTING INCOMING OR OUTGOING PACKET
ASSEMBLER/DISASSEMBLER CONNECTIONS

no service pad

!RAPIDLY DROPS PACKETS WITH INVALID DESTINATION ADDRESSES

ip route 0.0.0.0 0.0.0.0 null 0 255

!DISABLES PACKET FORWARDING FOR UNRECOGNIZED SUBNETS

no ip classless

!DISABLES MAINTENANCE OPERATION PROTOCOL

no mop enabled

!DISABLES IOS DHCP SERVICE

no service dhcp

!DISABLES HTTP SERVER

no ip http server

!

!

!INCREASE LOCAL BUFFER SIZE

>>CONFIGURED FROM GLOBAL CONFIGURATION MODE

>>GIAC_Border#conf t

>>GIAC_Border(config)#

!REFERENCE IMPROVING SECURITY ON CISCO ROUTERS

!http://www.cisco.com/warp/public/707/21.html#redirect

!INCREASES LOGGING BUFFER SIZE IN LOCAL ROUTER RAM

logging buffered 10000

logging console emergencies

logging trap debugging

!LOCATION OF LOGGING SERVER

logging 192.168.3.2

!DISABLED TO PREVENT ABUSE OF CDP INFORMATION

no cdp run

!

!WARNING BANNER TO BE DISPLAYED DURING LOGIN ATTEMPTS

banner motd ^C WARNING: AUTHORIZED ACCESS ONLY! VIOLATORS WILL BE
PROSECUTED! ^C

!

!CONFIGURES CONSOLE PORT TO REQUIRE PASSWORD FOR LOGIN.

MITIGATES INSIDER THREAT BUT ALLOWS ACCESS TO AUTHORIZED
PERSONNEL

line con 0

>>GIAC_Border(config-line)#

password 7 121A0C041104

login

!CONFIGURES AUXILIARY PORT TO REQUIRE PASSWORD FOR LOGIN.

MITIGATES INSIDER THREAT BUT ALLOWS ACCESS TO AUTHORIZED
PERSONNEL

line aux 0

```

password 7 060506324F41
login
!ALLOWS ACCESS TO ROUTER VIA TELNET SESSIONS BUT ESTABLISHES
PASSWORD REQUIREMENT
line vty 0 4
!PREVENTS IDLE VTY SESSIONS FROM TYING UP ROUTER
exec-timeout 8
password 7 13061E010803
login
!ALLOWS ACCESS TO TWO SEPARATE TELNET SESSIONS FOR AUTHORIZED
PERSONNEL ONLY
line vty 5
password 7 122A091A1E4A
login
line vty 6
password 7 05380A022D0D
login
!
!
>>CONFIGURED IN GLOBAL CONFIGURATION MODE/INTERFACE
CONFIGURATION MODE
>>GIAC_Border#conf t
>>GIAC_Border(config)#interface Ethernet0
>>GIAC_Border(config-if)#
!ASSIGNS DESCRIPTION TO INTERFACE
description BORDER TO ISP
!ASSIGNS IP ADDRESS TO INTERFACE E0
ip address 199.158.28.253 255.255.255.252
!ASSIGNS INBOUND ACCESS-LIST TO INTERFACE COMING INTO ROUTER
FROM ISP
ip access-group Inbound in
!PREVENTS ICMP REDIRECTS
no ip redirects
!PREVENTS ROUTER FROM BEING USED AS AN AMPLIFIER FOR "SMURF
ATTACKS"
no ip directed-broadcast
!PREVENTS ROUTER FROM RESPONDING TO ARP REQUESTS FOR HOSTS
THAT ARE NOT ON THE SAME NETWORK AS THE SENDING MACHINE WHICH
COULD BE USED TO MAP NETWORK
no ip proxy-arp
!SERVICE DISABLED BECAUSE IT'S NOT NEEDED
ntp disable
!SERVICE DISABLED BECAUSE IT CAN BE ABUSED AND USED TO LEARN
TYPE OF CISCO DEVICE, MODEL NUMBER AND IOS VERSION, ALL OF WHICH
COULD BE USED TO ATTEMPT DIRECTED ATTACKS

```

```

no cdp enable
!PREVENT ROUTER FROM SENDING IP UNREACHABLE MESSAGES WHICH
CAN BE USED TO MAP NETWORK RESOURCES
no ip unreachable
!
!SAME AS ABOVE FOR INTERFACE ETHERNET 0
interface Ethernet1
ip address 199.158.28.65 255.255.255.224
!ASSIGNS INBOUND ACCESS-LIST TO INTERFACE GOING TO GIAC FIREWALL
ip access-group Inbound out
no ip redirects
no ip directed-broadcast
no ip proxy-arp
ntp disable
no cdp enable
!ASSIGN ADDRESS TO INTERFACE TO VPN
interface Ethernet 3
ip address 199.158.28.93 255.255.255.224
!ASSIGN VPN ACCESS-LIST TO INTERFACE
ip access-group vpn out
!
!ALLOWS ROUTER TO COMMUNICATE WITH ISP ROUTER
router rip
version 2
network 199.158.28.0
neighbor 199.158.28.254
!
!CREATING NAMED ACCESS LIST FOR FILTERING UNWANTED INBOUND
TRAFFIC
!USING A NAMED LIST ALLOWS YOU TO ENTER INFORMATION DIRECTLY TO
LIST
>>CONFIGURED FROM GLOBAL CONFIGURATION MODE
>>GIAC_Border#conf t
>>GIAC_Border(config)#ip access-list extended Inbound
>>GIAC_Border(config-ext-nacl)#
!PERMITS TRAFFIC TO THE FIREWALL INTERFACE
!KEYWORD established CREATES STATEFUL FILTER
permit tcp any host 199.158.28.94 gt 1023 established
!
!PERMITS INTERNET TRAFFIC TO THE WEB SERVER VIA BOTH HTTP AND
HTTPS THRU THE NAT FIREWALL
permit tcp any host 199.158.28.94 eq 80
permit tcp any host 199.158.28.94 eq 443
!PERMITS MAIL TO THE MAIL SERVERS
permit tcp any host 199.158.28.94 eq smtp

```

!PERMITS VPN CONNECTIONS

permit udp any host 199.158.28.93 eq 500

permit ip any host 199.158.28.93 eq 50

!

!AN EXAMPLE OF SANS TOP 10 OFFENDERS

!NOTE: THIS LIST WILL BE MONITORED AND COMPARED TO THE LOG FILES
!OF THE BORDER ROUTER

!ALL EXAMPLES ARE PRECEDED BY AN EXCLAMATION MARK

!http://www.dshield.org/top10.html

! deny ip host 62.163.117.199 any

! deny ip host 217.227.109.182 any

! deny ip host 193.170.238.247 any

!DENY GOTOMYPC.COM

deny ip host 63.251.224.169 any

!PRIVATE NETWORK ADDRESSES

!RFC 1918

deny ip 10.0.0.0 0.255.255.255 any log

deny ip 172.16.0.0 0.15.255.255 any log

deny ip 192.168.0.0 0.0.255.255 any log

!SANS TOP 20 LIST

!http://www.sans.org/top20.htm

deny ip host 0.0.0.0 any log

deny ip 169.254.0.0 0.0.255.255 any log

deny ip 192.0.2.0 0.0.253.255 any log

deny ip 224.0.0.0 31.255.255.255 any log

deny ip 240.0.0.0 15.255.255.255 any log

!LOOPBACK ADDRESS

deny ip 127.0.0.0 0.255.255.255 any log

!RESERVED IANA IP ADDRESSES

!http://www.iana.org/assignments/ipv4-address-space

deny ip 1.0.0.0 0.255.255.255 any log

deny ip 2.0.0.0 0.255.255.255 any log

deny ip 5.0.0.0 0.255.255.255 any log

deny ip 7.0.0.0 0.255.255.255 any log

deny ip 23.0.0.0 0.255.255.255 any log

deny ip 27.0.0.0 0.255.255.255 any log

deny ip 31.0.0.0 0.255.255.255 any log

deny ip 37.0.0.0 0.255.255.255 any log

deny ip 39.0.0.0 0.255.255.255 any log

deny ip 41.0.0.0 0.255.255.255 any log

deny ip 42.0.0.0 0.255.255.255 any log

deny ip 58.0.0.0 1.255.255.255 any log

deny ip 60.0.0.0 0.255.255.255 any log

deny ip 69.0.0.0 0.255.255.255 any log

deny ip 70.0.0.0 0.255.255.255 any log

deny ip 71.0.0.0 0.255.255.255 any log
deny ip 72.0.0.0 7.255.255.255 any log
deny ip 82.0.0.0 1.255.255.255 any log
deny ip 84.0.0.0 3.255.255.255 any log
deny ip 88.0.0.0 7.255.255.255 any log
deny ip 96.0.0.0 31.255.255.255 any log
!UNNECESSARY/VULNERABLE PORTS FROM THE INTERNET
!http://www.sans.org/top20.htm
deny tcp any any eq 23 log
deny tcp any any range 512 514 log
deny tcp any any range 135 139 log
deny udp any any range 135 139 log
deny tcp any any range 161 162 log
deny udp any any range 161 162 log
deny tcp any any eq 445 log
deny udp any any eq 445 log
deny tcp any any eq 515 log
deny udp any any eq 515 log
deny udp any any range snmp snmptrap log
deny udp any any eq tftp log
deny tcp any any eq NNTP log
deny tcp any any eq BGP log
deny tcp any any eq 1080 log
deny udp any any eq syslog log
deny tcp any any range 6000 6255 log
deny udp any any range 6000 6255 log
deny tcp any any eq 111 log
deny udp any any eq 111 log
deny tcp any any eq 2049 log
deny udp any any eq 2049 log
deny tcp any any eq 4045 log
deny udp any any eq 4045 log
deny tcp any any eq 389 log
deny udp any any eq 389 log
deny tcp any any range 32770 32789 log
deny udp any any range 32770 32789 log
deny icmp any any redirect
!STOP AOL INSTANT MESSENGER TRAFFIC
deny ip host 205.188.7.0 any log
!
!CREATING NAMED ACCESS LIST FOR FILTERING PERMITTED OUTBOUND
TRAFFIC
!USING A NAMED LIST ALLOWS YOU TO ENTER INFORMATION DIRECTLY TO
LIST
!PERMIT OUTBOUND TRAFFIC FROM NAT ADDRESS ONLY

```
>>CONFIGURED FROM GLOBAL CONFIGURATION MODE
>>GIAC_Border#conf t
>>GIAC_Border(config)#ip access-list extended Outbound
!PERMIT OUTBOUND TRAFFIC FROM INTERNAL NETWORK ONLY
permit ip host 199.158.28.0 any
deny ip any any log
!
!PERMITS INTERNET TRAFFIC TO THE WEB SERVER VIA BOTH HTTP AND
HTTPS THRU THE NAT FIREWALL
permit tcp any host 199.158.28.94 eq 80
permit tcp any host 199.158.28.94 eq 443
!
!PERMIT ACCESS TO VPN
>>CONFIGURED FROM GLOBAL CONFIGURATION MODE
>>GIAC_Border#conf t
>>GIAC_Border(config)#ip access-list extended VPN
>>GIAC_Border(config-ext-nacl)#
!PERMITS TRAFFIC ON THE VPN INTERFACE
permit udp any host 199.158.28.93 eq 500
permit ip any host 199.158.28.93 eq 50
permit ip any host 199.158.29.93 eq 51
!
end
```

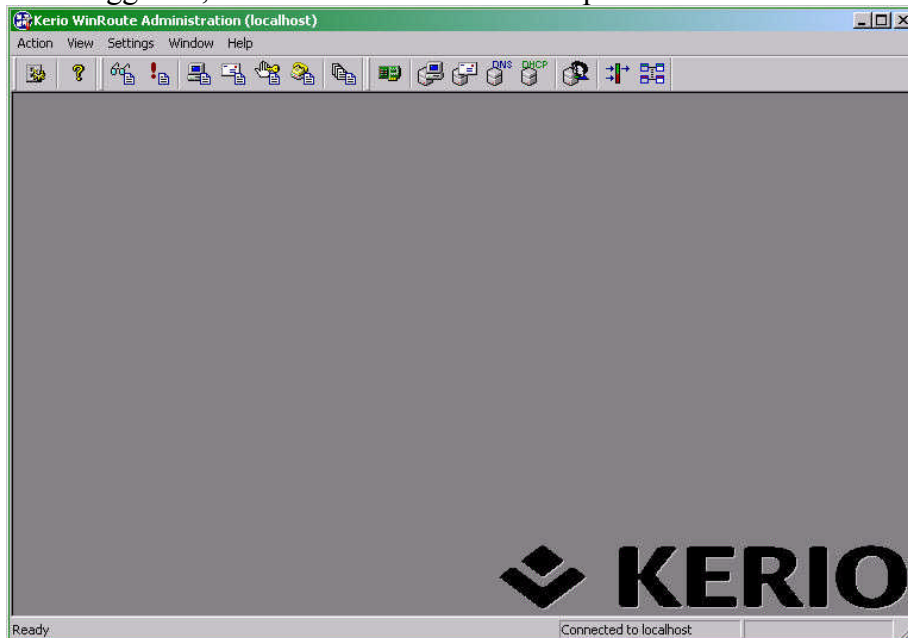
Firewall Ruleset

The following information details the configuration of the GIAC Firewall to reflect the Security Policy for the network.

When first logging into WinRoute Pro firewall, the login screen is presented. With no accounts created on the firewall simply press <ENTER> to continue.

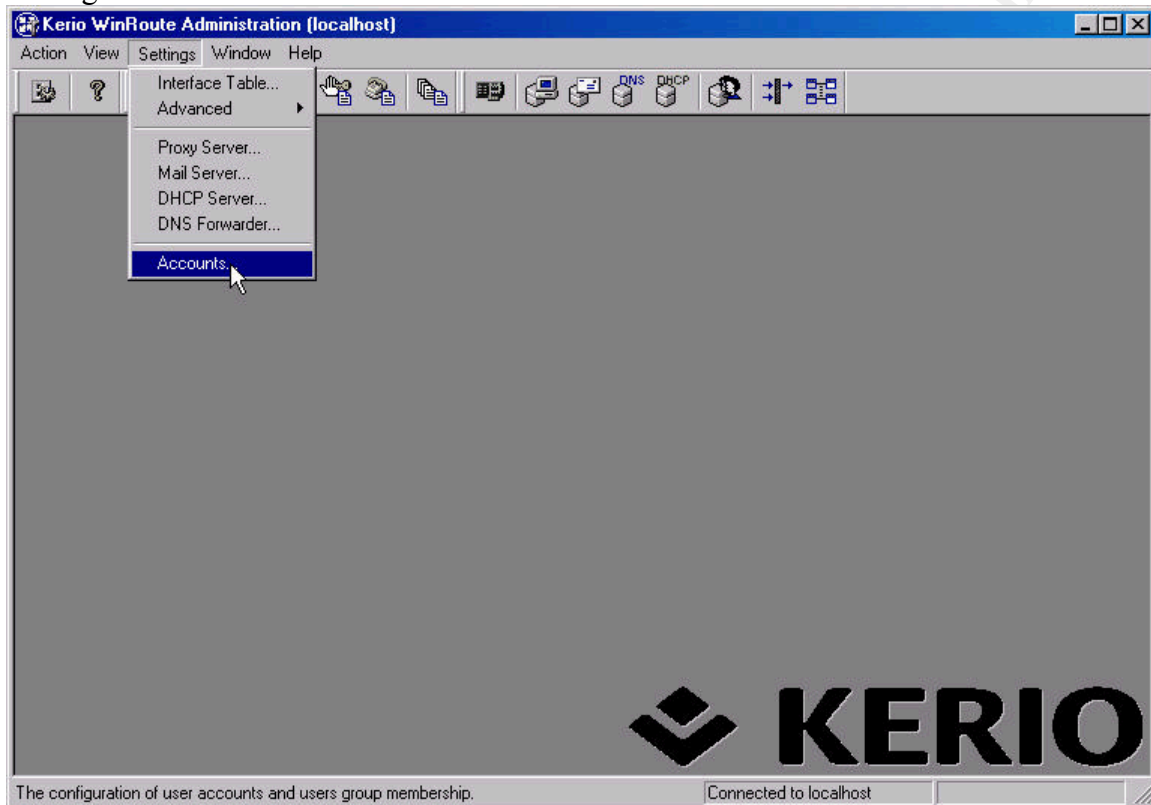


Once logged in, the Administration screen is presented.

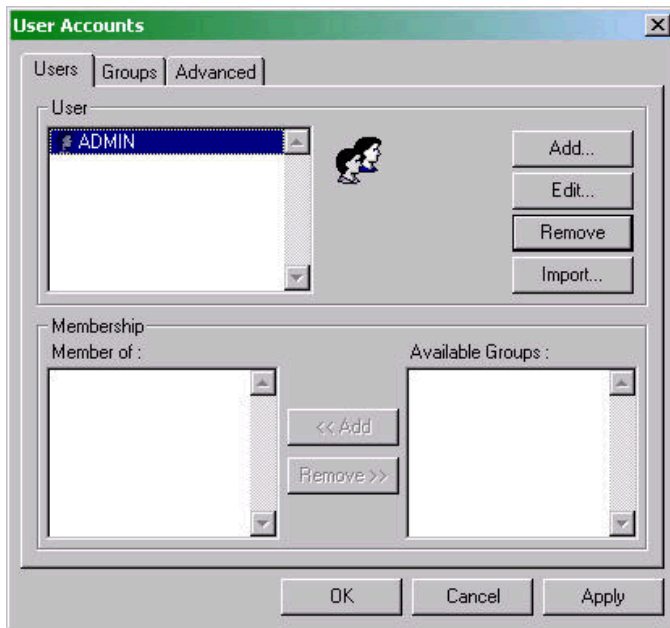


User Accounts

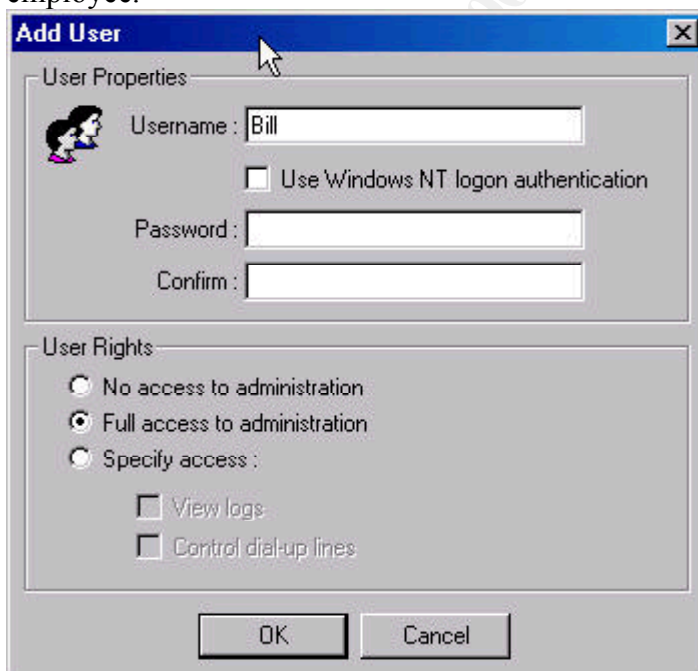
The first step is to remove the default ADMIN account for firewall administration. Attempts to login to the firewall using this account will be logged in the event that an attempt is made to compromise the firewall. This is accessed by selecting Settings>Accounts.



The User Account screen will appear.



The Bill Account has been added and given Full Access to Administration. A second account, Arnold has also been added and given Full Access to Administration. Two NetSec Consulting employees will be responsible for firewall administration. Although a shared account with a generic name could have been created, this would diminish NetSec's ability to audit employee activity and is not recommended. Two users with full administration rights also prevents a single point of failure if something happens to one employee.

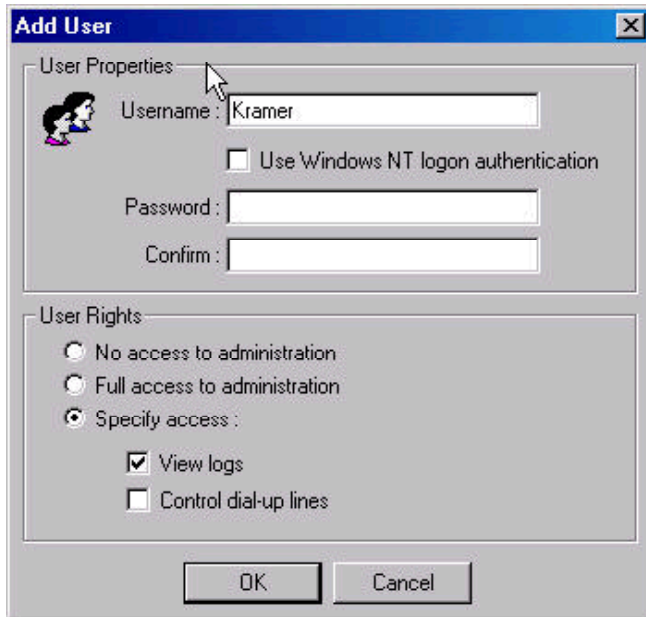


Note: There are several levels of access or user rights that can be granted to users. The first, "No access to administration" creates a user account that allows no administration

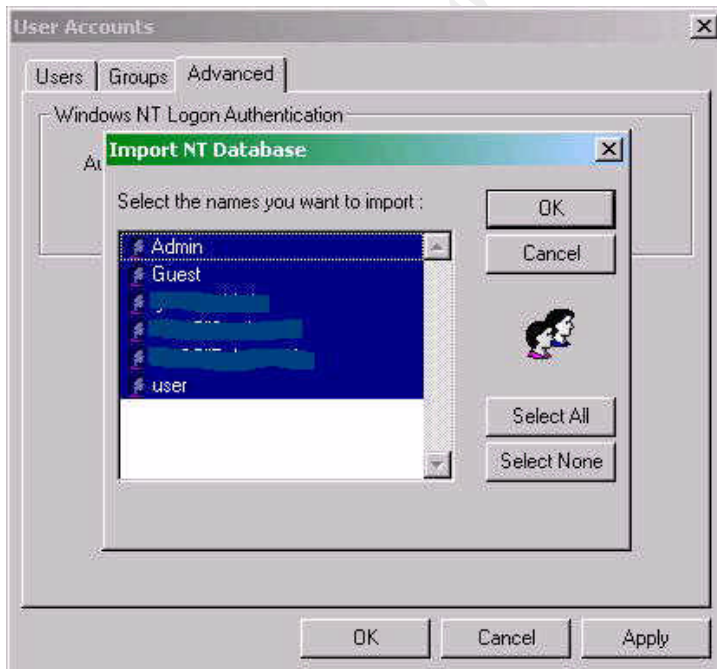
access to occur. The second, “Full access to administration” allows a user to administer all aspects of the WinRoute Pro Firewall. The use of these rights must be tightly controlled. The third “Specify access” allows a user to “view logs only” and/or “Control dial-up lines.” A user with “view logs only” rights can access the WinRoute Administrator console, but can only view the log windows and cannot make any other changes. A user with “control dial-up lines” can login to the Administrator console and can establish or disconnect the Internet connection, but cannot make any other changes.

© SANS Institute 2000 - 2005, Author retains full rights.

The Kramer account has been added to allow review of the log files only. This user will be allowed to log into the firewall remotely and view the log files for analysis if necessary. This is necessary due to NetSec's contracted Security Services that are not provided by an on-site 24x7 staff.



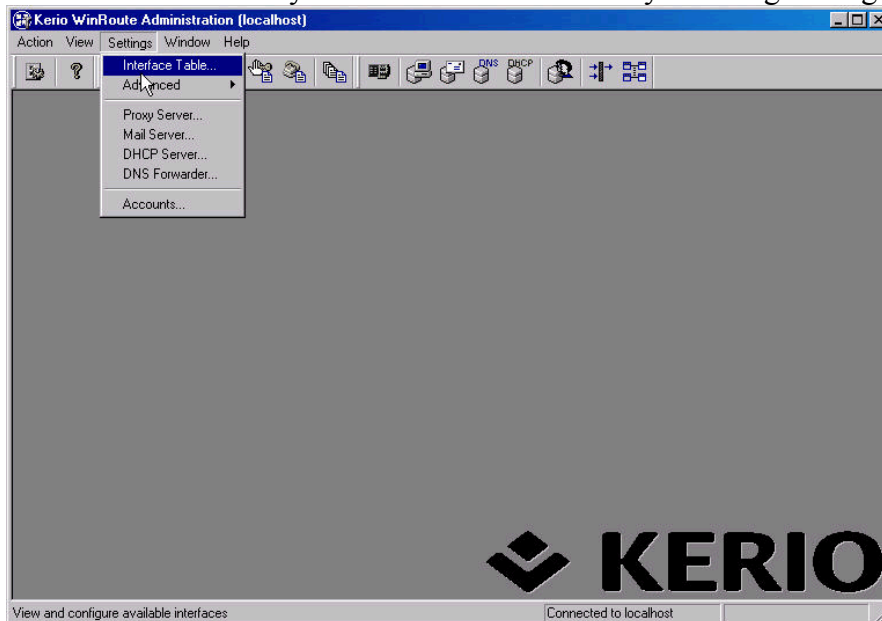
Although user accounts can be imported from either the local computer or the domain, this feature will not be used. The additional login and password on the firewall adds an additional layer if an internal user's account is compromised. (The configuration box is shown below in the event that someone would want to do this.)



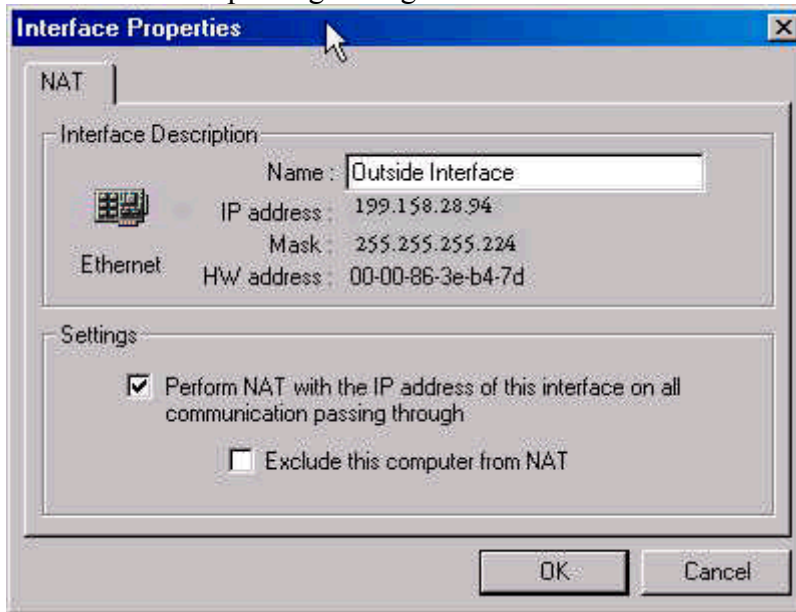
NAT

We decided to use NAT for the GIAC Enterprises network for a number of reasons. Event correlation will be easier with one device logging traffic. NAT also allows for stateful packet inspection because the firewall maintains a table of all packets that originated from within the GIAC network traversing it. If a packet with an internal address were received on the external interface of the firewall the packet would be dropped because there is no entry in the NAT table that corresponds to that traffic.

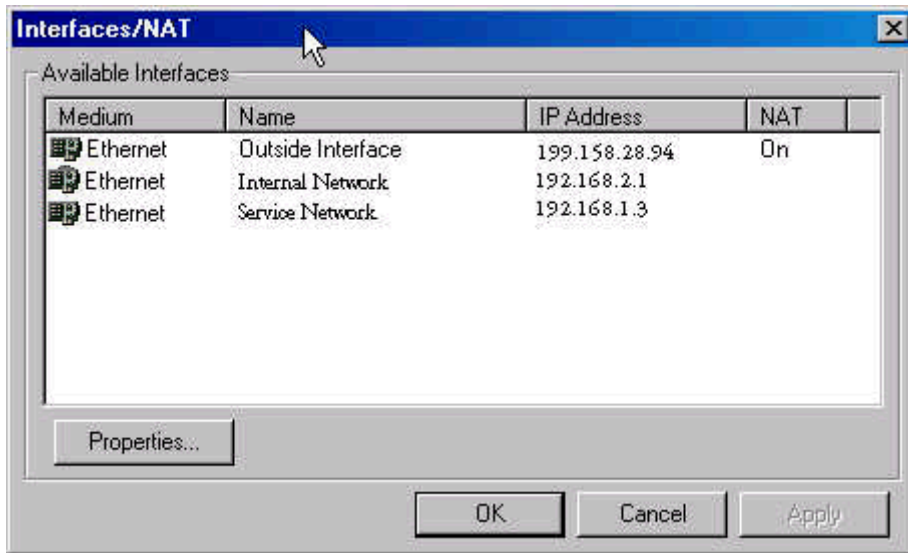
NAT is first enabled by from the Interface Table by selecting Settings > Interface Table



Next we have to select the Properties of the interface that we want to enable NAT on. We changed the name of the interface to Outside Interface to make it easy to identify in the logs. By selecting the “Perform NAT with the IP address of this interface on all communications passing through” NAT is now enabled.



Note: You must ensure that there is no Gateway set for any of the other interfaces on your WinRoute Pro Firewall. Failure to do this will result in no traffic passing to the NAT interface and out to the Internet. When configuring the clients on your network ensure that you do set the appropriate interface as the Gateway for you subnet. This Gateway address will be either an interface on the firewall or an internal router interface depending on the network configuration. GIAC Enterprises Service Net must use the Firewall interface 199.168.1.3 and the internal network must use the internal router interface 199.168.4.1. The internal router would use 199.168.2.1 (internal firewall interface) as it's default gateway. The complete interface table is shown below.



Note: If public addresses are used on an internal network, you can use the Advanced Nat option. Because we have chosen to NAT all internal addresses due to our private IP addresses use, this option is not being utilized.

NAT Security

WinRoute Pro offers several configurations for security. These NAT security options allow the firewall to perform stateful inspection of all incoming packets. The NAT interface maintains a table of all outbound traffic and automatically compares that header information with the header information maintained in its NAT table. If the inbound packet matches information found in the table, the firewall will change the header to the correct destination IP and forward the packet. If no match is found the firewall will either deny or drop the traffic based on the ruleset configuration. With NAT enabled on “Outside” interface all inbound ports are closed by default.

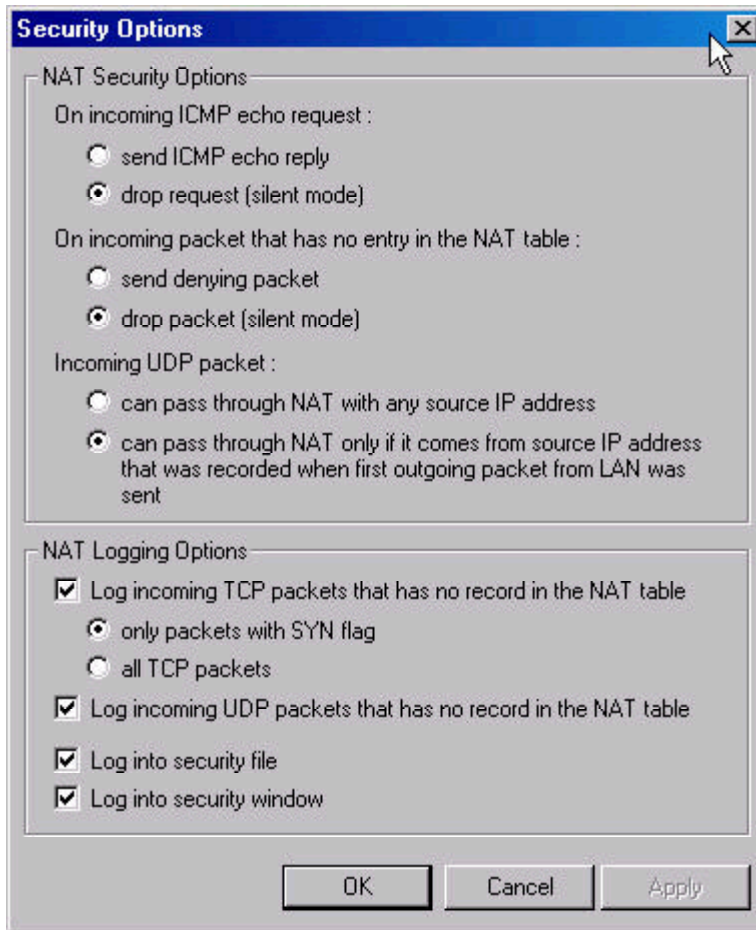
In order to make the most of WinRoute Pro’s ability to filter traffic, a user may decide to use the Basic Security Options that WinRoute provides. These filters are located in the <Settings+Advanced+Security Options> field. The first configuration possible will drop any incoming ICMP echo requests. This will prevent any network scans from identifying that a listen computer is present at that IP address. The firewall will respond with a “request timed out.”

The second rule will drop any incoming packets that are not present in the NAT table. This enables our stateful packet filtering and prevents a hacker from receiving responses to incoming SYN ACK packets. The firewall will drop the packet and the network will appear non-existent because no packet was sent back.

The third rule also only allows incoming UDP packets if they match a corresponding entry in the NAT table from a packet was first sent.

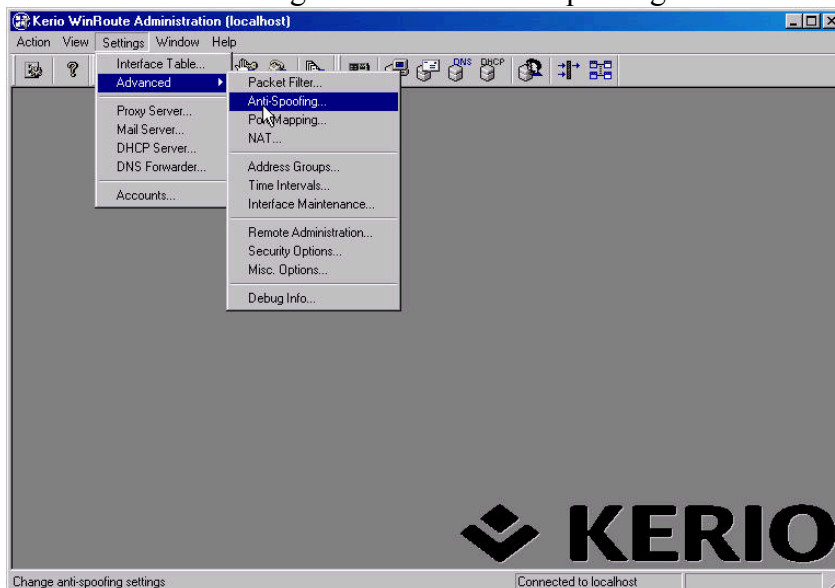
The fourth rule will log any incoming TCP packets that do not have an entry in the NAT table to allow for later analysis. Only incoming packets with the SYN flag set will be recorded. If necessary, the administrator can log all incoming packets, but this is not recommended unless malicious activity is suspected, as the log files will be quite large.

The final rule defines how the administrator can view the logs. We have chosen to log to both a security file and the security window. Logging to the security file allows use to view and export the information that is recorded in the logs. Normally this is stored in c:/Program Files/WinRoute Pro/Logs. Logging into the security window allows a user with appropriate access to view the logs from the WinRoute Pro Administrator Console. We had to ensure that all logging that we wanted to be able to view was designated to be saved to both a log file and the security window.

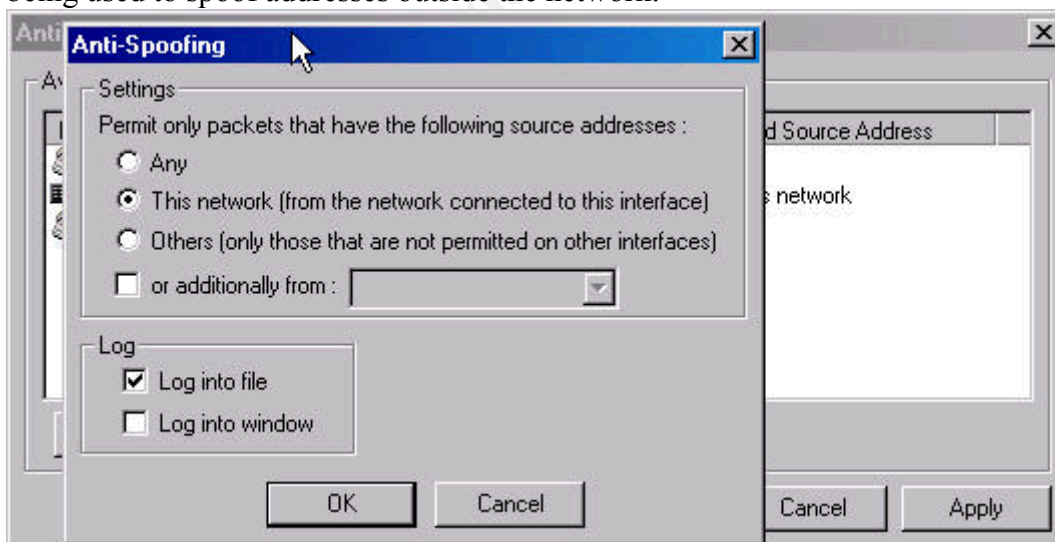


Anti-Spoofing

To prevent spoofing on our network we will configure the NAT interface so that only internal addresses are allowed to pass through the interface. To access the Anti-Spoofing window select <Settings+Advanced+Anti Spoofing>



Now we must configure the interface to only allow internal addresses to pass through it to the Internet. If an internal machine were compromised, this will prevent the machine from being used to spoof addresses outside the network.



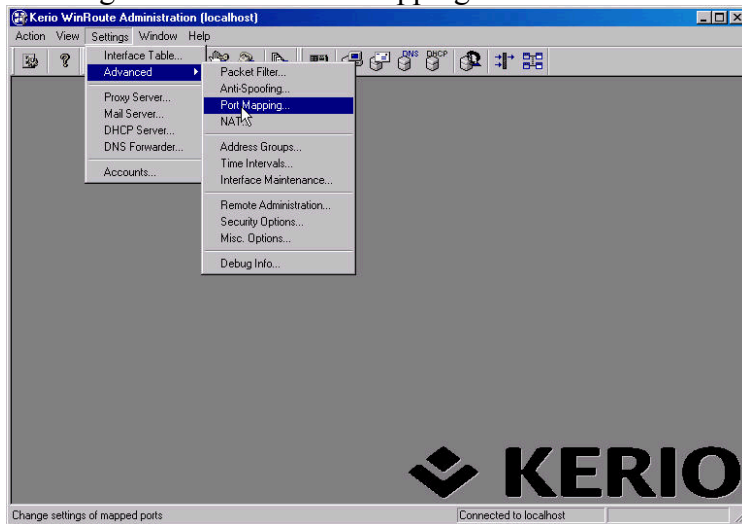
Note that we are logging any attempts to send packets that do not have our internal network address as their source. This will be important during the weekly log reviews to help in determining if an internal GIAC computer has been compromised by a remote control Trojan or other malicious program.

Note: Although the screen shot does not show it, logging is enabled to both file and

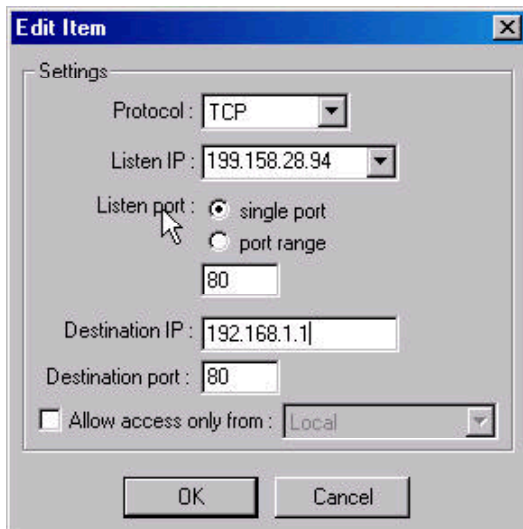
window.

Port Mapping

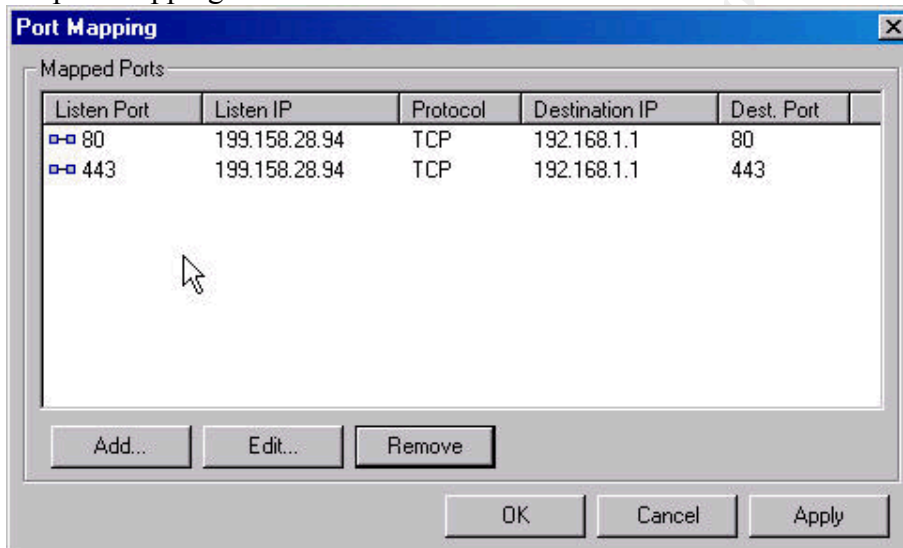
Because we are running NAT, our internal systems are not available via IP address from the Internet. With WinRoute Pro we do have the option of using their port-mapping feature. We will setup port mapping so that traffic destined for the web server, which has a private IP address, can reach its destination. Port mapping is only needed and effective for inbound connections. First we open the port-mapping window by selecting <Settings+Advanced+Port Mapping>



We next need to define the port-mapping configuration so that once a packet is received from the Internet it will reach the web server after it has been checked against the port-mapping table. Because we are using NAT, the DNS entry for www.fortunesun.com will be for our external interface. GIAC has also registered the external interface as the IP address for their web site. We would now create a port mapping rule that routes all traffic with that destination IP address and port 80 or 443 to our internal web server at 192.168.1.1 Below is an example of configuring port mapping for port 80 to the web server.



Once all rules have been applied to allow access via HTTP (port 80) and HTTPS (port 443) the port mapping rules would look like:



There are several different options for port mapping.

Protocol: The protocol that is used by the application or service. For example HTTP uses TCP.

Listen IP: This is the IP Address that incoming IP packets will arrive at. If using DHCP to acquire IP addresses you can leave this unspecified. If you have a legal IP address assigned enter it here.

Listen Port: The port that inbound requests will come to. For example HTTP requests come to port 80 by default.

Destination IP: The IP address that incoming requests will need to access. For instance,

the web server for GIAC Enterprises is at 192.168.1.1 so all inbound HTTP requests need to be mapped to this IP address.

Destination Port: The port that the destination application, HTTP in this case, is listening on. Normally this is the same as the listen port.

Allow access only from: You can pre-define address groups by name to restrict access to certain port. For web traffic we would not want to do this, however when we define Remote Administration on the Firewall this option will be used.

Note: Again, port mapping only applies to inbound traffic. WinRoute allows all outbound traffic by default. In order to provide the appropriate level of protection and auditing through log analysis for GIAC Enterprises, we have to utilize packet-filtering rules. All GIAC Enterprises packet-filtering rules will be presented later in this document after further port-mappings have been explained.

Testing of Rules: First test

To test the functionality of this rule I would try to access the GIAC web page, www.fortunesun.com from a computer outside the local GIAC network. If successful, the web page will be seen in the browser window. If the test fails, no web page will appear and an HTTP-404 – File not found error will appear. This could indicate that the port mapping is incorrect or it may indicate that the web site's IP address is not registered correctly.

DNS

Due to GIAC's limited resources and small user base, the firewall will also act as the DNS server for the local network. The DNS settings window is access from Settings>DNS Forwarder. We have enabled DNS forwarding from our internal network to our ISP's primary and secondary DNS at 66.12.10.23 and 66.12.10.24. We enabled cache as well to allow local caching of commonly requested domain names. This will increase the response time for sites that are often requested by GIAC Enterprises employees. We also decided to use the HOSTS file for simple DNS resolution to speed up common queries. For instance, each local computer has a "computer name" assigned of GIAC1, GIAC2, etc. This information is contained in the HOSTS file that resides on the firewall. By also entering the DNS domain for "fortunesun.com" we are required to only enter the computer name and the domain name is automatically appended.

DNS Forwarder [X]

☒ Enable DNS forwarding

☐ Forward DNS queries to the server automatically selected from DNS servers known to the operating system

☒ Forward DNS queries to the specified DNS server(s)

DNS Server(s) :

Use semicolon (;) to separate entries

☒ Enable cache for faster response of repeated queries

Simple DNS resolution

Before forwarding query, try to find name in :

☒ HOSTS file

☒ DHCP lease table

When resolving name from HOSTS file or lease table combine it with DNS domain below :

To allow our local GIAC Enterprise users to surf to the GIAC Web Server at www.fortunesun.com I have included the following information in the HOSTS file.

This is the HOSTS file for GIAC Enterprises.

#

#

This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.

#

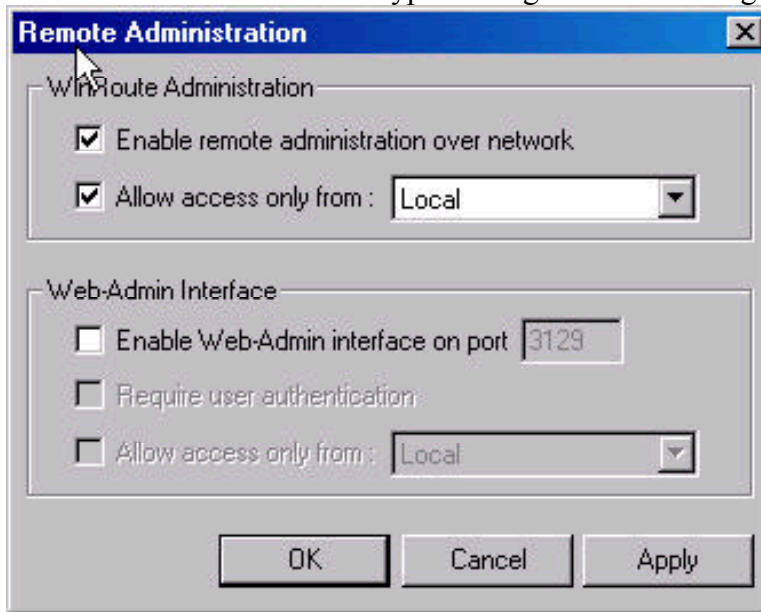
#

192.168.4.2	GIAC2	#Workstation
192.168.4.3	GIAC3	#Workstation
192.168.4.4	GIAC4	#Workstation
192.168.4.5	GIAC5	#Workstation
192.168.4.6	DBServ	#Database Server
192.168.1.1	www.fortunesun.com	#GIAC Web Server

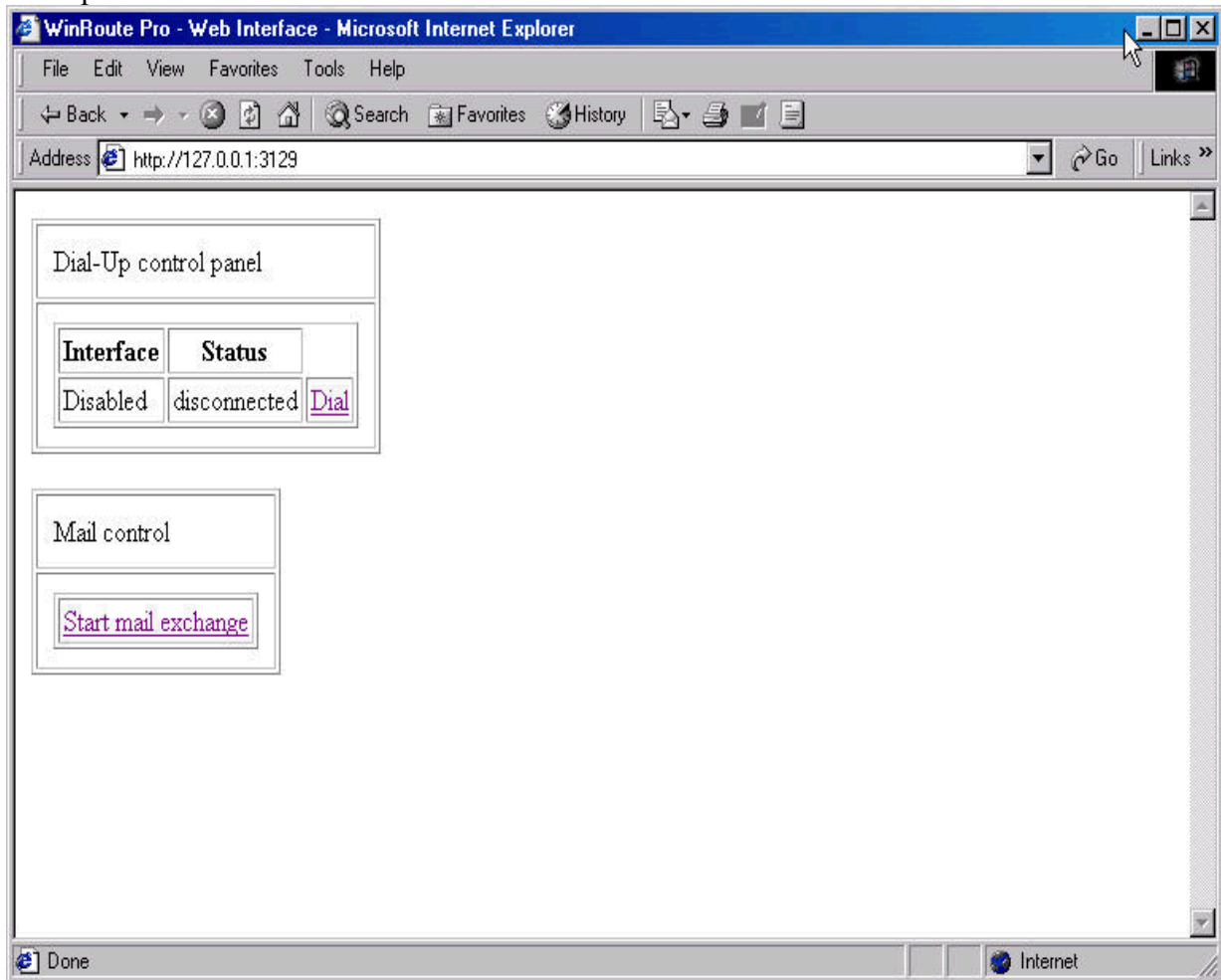
Note: You must configure the IP address for the ISP DNS in order for the DNS forwarder to function correctly. Also, internal client computers must be configured to use the Firewall for their DNS. The internal network would point to interface 192.168.2.1 and the Service Network would point to 192.168.1.3. We could have also chosen to point the client DNS queries to the ISP DNS.

Remote Administration

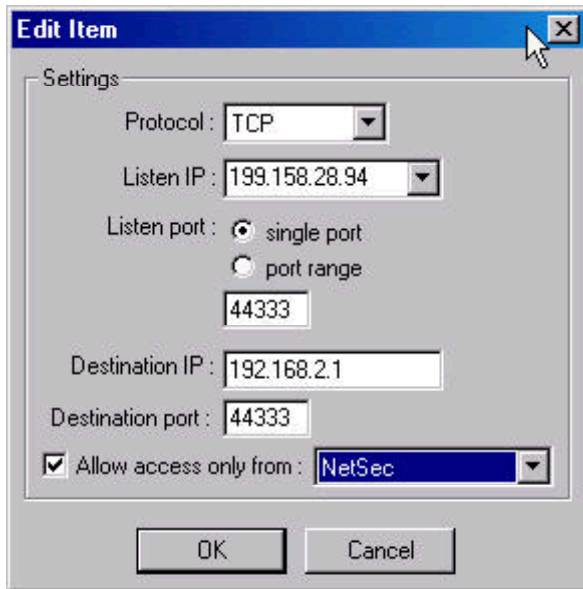
Remote local administration of the firewall is restricted to only the internal Security Workstation at IP 192.168.4.2. This Security Workstation must have the WinRoute Pro Administration software (wradmin.exe) installed to allow for remote administration. Local admin can be conducted using the accounts (username and password pairs) that were created earlier. Local Administration is configured from Settings>Advanced>Remote Administration. You must select the checkbox “Enable remote administration over network.” Because we only want to allow access from our internal Security Workstation, we have selected the Address Group Local. (Creating Address Groups is outlined below.) We have not enabled the Web-Admin interface because we did not see the need for it at this time and due to it’s limited functionality. Remote administration is encrypted using the Blowfish algorithm.



Example of Web Interface:



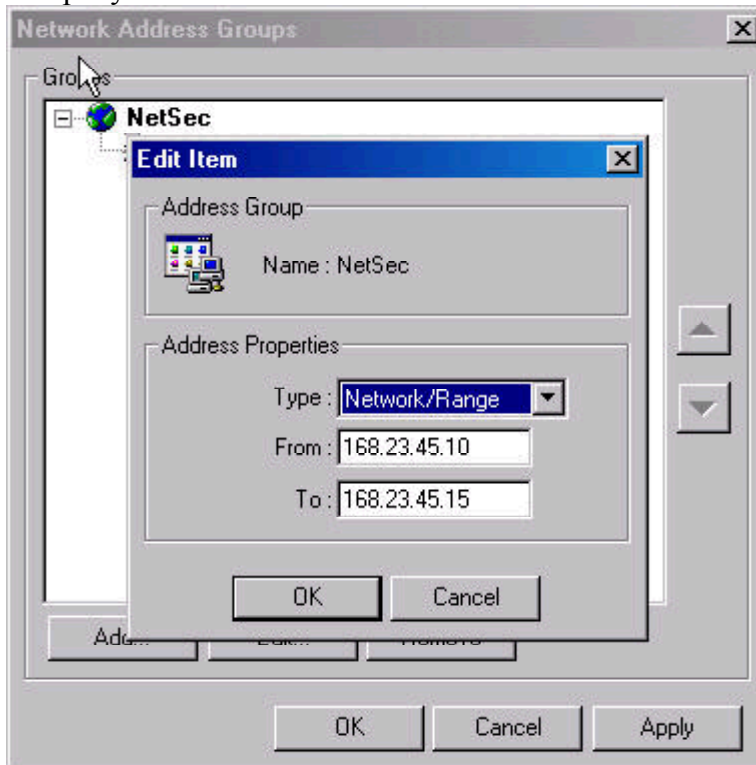
Additionally, we are allowing web administration to the GIAC WinRoute Pro Firewall from outside the GIAC network. This access is only granted to the NetSec Consulting network. The same administration can be conducted remotely using the accounts created earlier. This remote admin rule is configured in the port mapping Settings>Advanced>Port Mapping. The protocol setting is UDP/TCP and the listening IP is the set to the outside interface 199.158.28.94. The checkbox at the bottom labeled “Allow access only from:” is set to the Address Group NetSec, which includes all addresses on the NetSec Consulting network. This allows for multiple machines to be used for remote administration if necessary. (An example of configuring the Address Group is shown below.) The remote administration port is 44333. Destination IP is set to the internal interface of the firewall at 192.168.2.1 and the destination port is 44333.



We have reinforced this port mapping with a packet-filtering rule that will allow logging of this traffic.

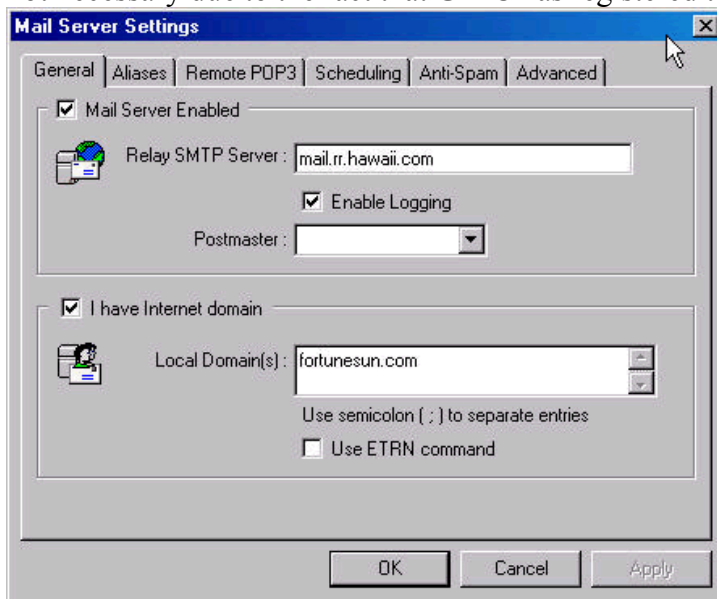
Creating Address Groups

Address Group. The Address Group is configured from Settings>Advanced>Address Group. Click ADD and select a name for the address group. Then you must select Type, which is Host, Network/Mask (which allows and entire network access) or Network/Range (which allows a range of IP address access). We chose Network/Range because there are several computers on the NetSec Consulting network that are used for remote access to the GIAC network and several other networks managed by the company.

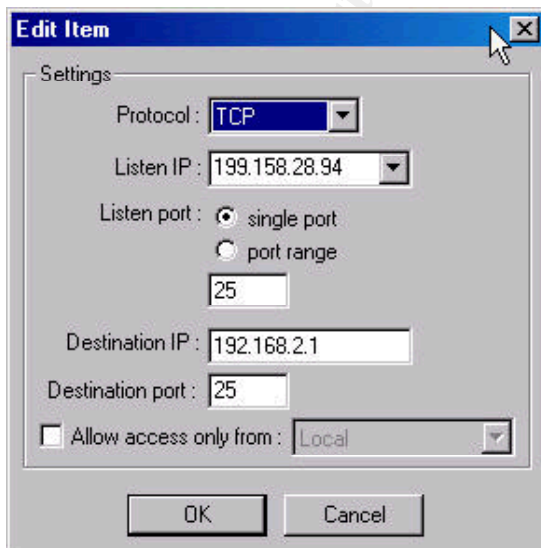


Mail Server

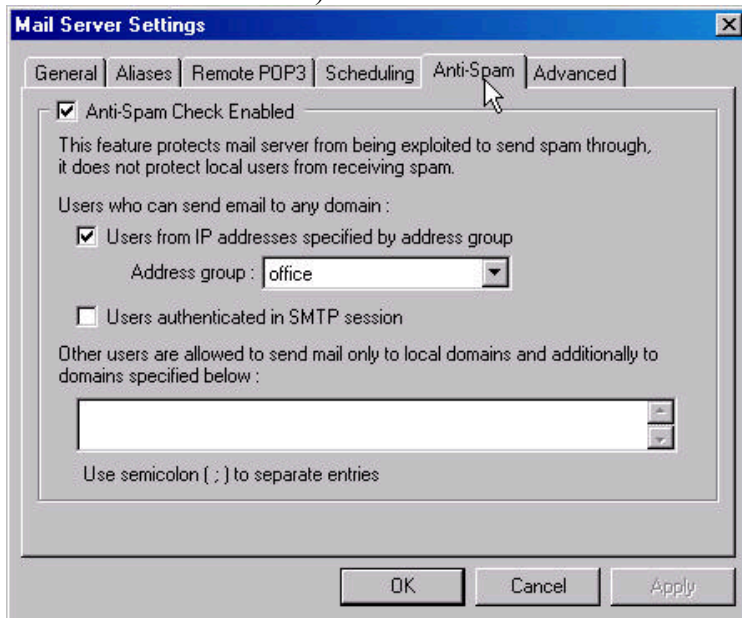
Due to the limited size of GIAC Enterprises, it was decided to use the Mail Server functionality of WinRoute Pro. GIAC has registered the domain fortunesun.com to the external or public IP address of the firewall. The MX Record for GIAC's upstream ISP points to the external interface IP address. To begin configuring the Mail Server go to Settings>Mail Server and select the Mail Server Enable checkbox and the "I have Internet domain" checkbox. Here we have entered the GIAC Enterprises domain fortunesun.com. We also had to enter the name of the relay SMTP Server where we will send all of GIAC's outgoing email. This is the mail server of our ISP. (mail.rr.hawaii.com) POP3 is not necessary due to the fact that GIAC has registered their domain.



Because we are using NAT, we must also map SMTP (port 25) to the internal interface of the firewall. Failure to do this will result in no mail being delivered.

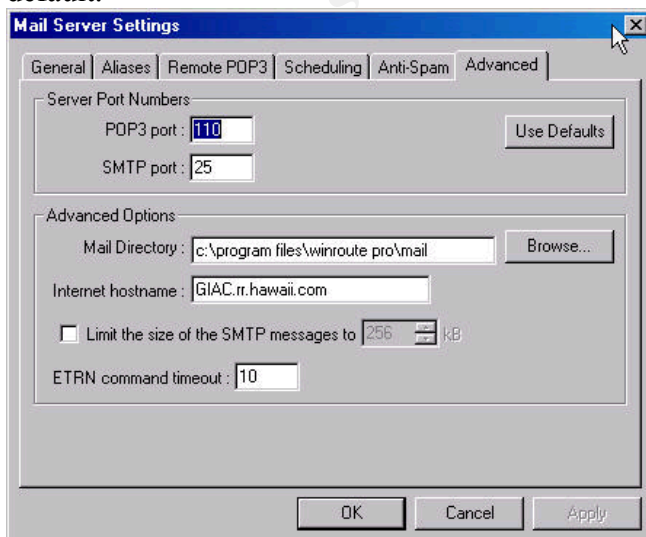


To prevent the firewall from being used for Spam mail, the Anti-Spam tab must be selected. Check the Anti-Spam Check Enable checkbox and allow only users from the Address Group “Office” to send email. By enabling this by Address Group we have restricted the local mail server on the firewall to only allow email from the local network. (The Address Group Office is configured the same as the past address groups as outlined earlier in this document.)

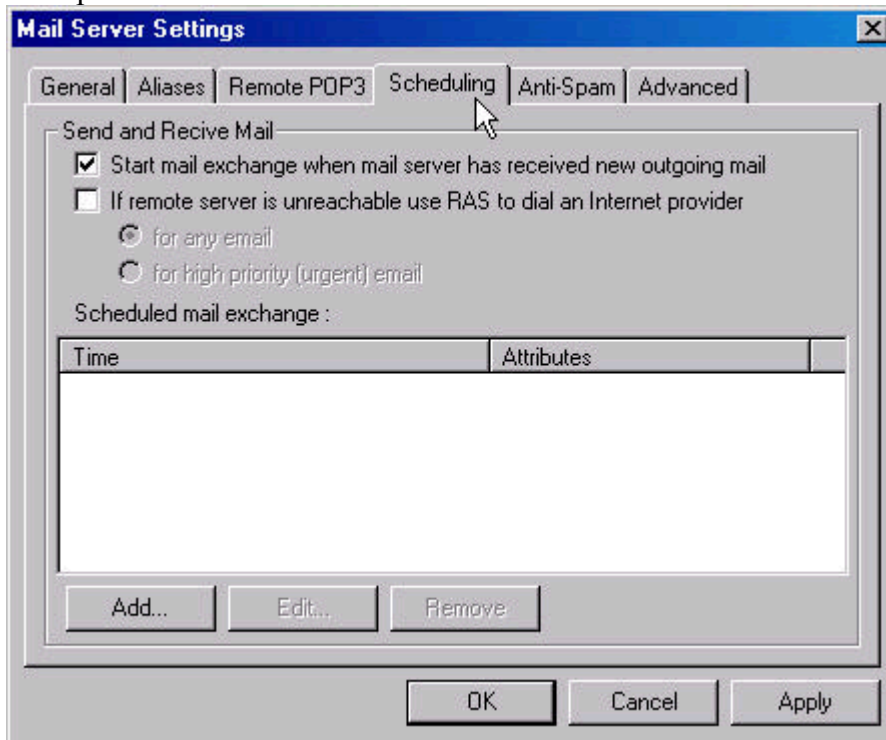


Note: When configuring the email clients on the user workstations, you must assign the WinRoute Pro Firewall as the outgoing SMTP email server.

Our ISP also requires authentication of email being sent from our local mail server. This is to help prevent spamming. GIAC must provide the hostname of the WinRoute Pro mail server. This is configured under the Advanced Tab. The Server Port numbers are set to the default.



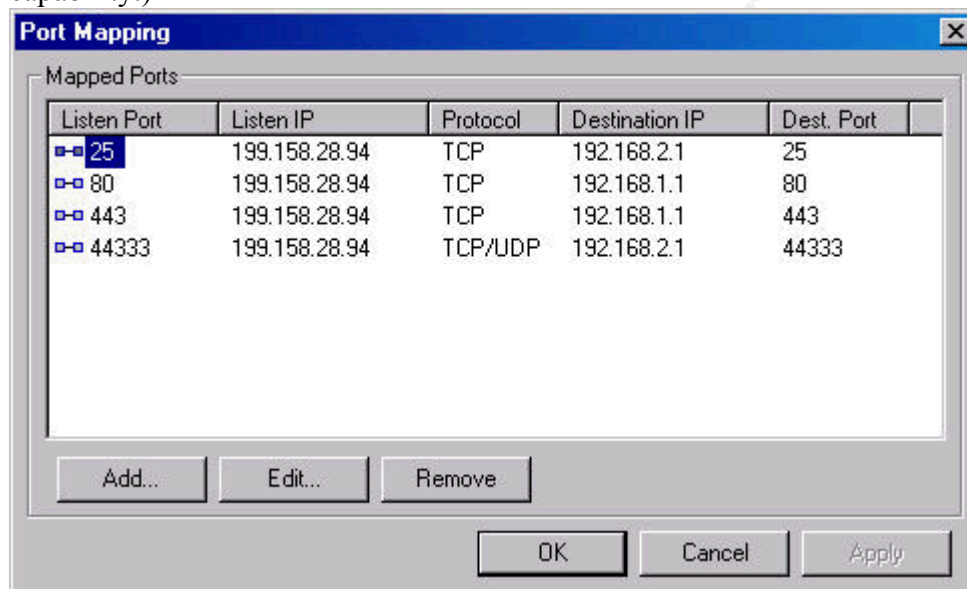
The ability to send and receive email is vital to GIAC Enterprises. The mail server will always be activated. All SMTP email will automatically be delivered to the mail server when routed. The mail server will send email when the outgoing message queue contains email. By selecting the Scheduling tab, we are able to configure the mail server. Check the box “Start mail exchange when mail server has received new outgoing mail.” We also have the option to schedule when mail is sent and to dial out to an alternate ISP. GIAC does not have an alternate ISP and maintains an always-on connection to the Internet so this option is not in use.



Detailed Port Mapping

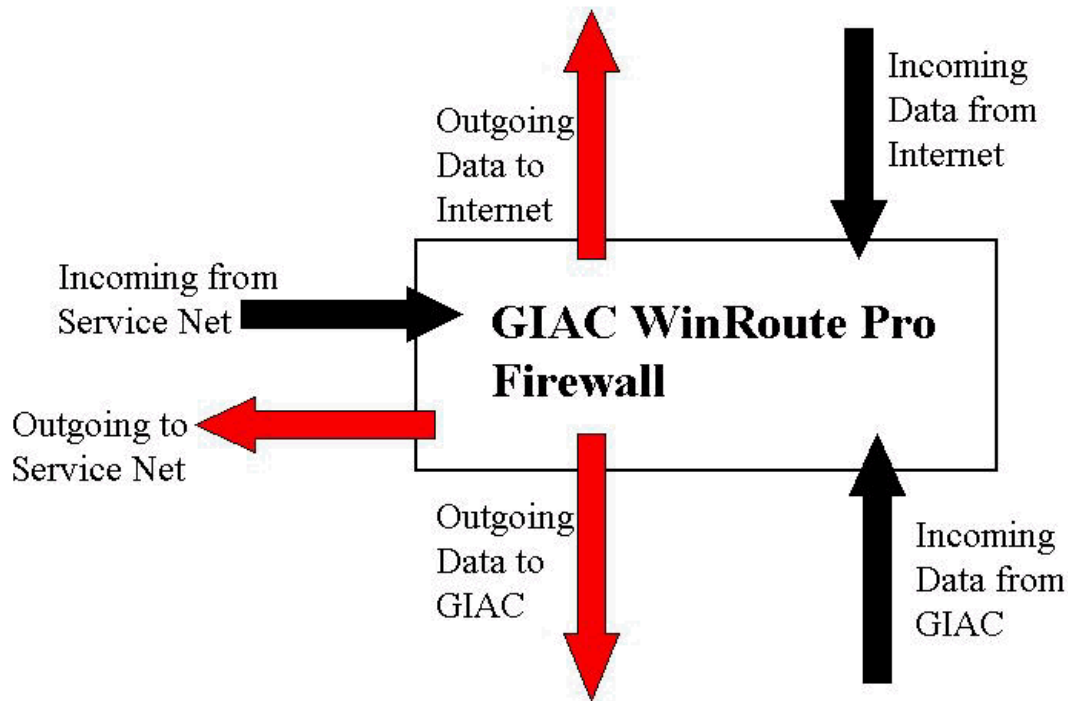
The following are the port mapping configurations that we put in place on the GIAC Enterprise network.

- The external firewall interface (199.158.28.94) is the public IP address for www.fortunesun.com. So that all incoming HTTP and HTTPS traffic destined for the internal web server (192.168.1.1) reaches its destination the rules for ports 80, and 443 were put in place.
- The rule for Listen Port 25 allows SMTP traffic to and from the mail server running on the WinRoute Pro firewall. The destination IP must be the internal interface of the firewall. (Packet Filtering of Port 25 traffic will be created to enable logging in the event that we suspect the GIAC Mail Server is being used as a SPAM relay.)
- The rule for Listen Port 44333 allows remote administration from the external network defined in Address Group NetSec. (Packet Filtering rules will be created to reinforce this capability.)



Packet Filtering

WinRoute Pro allows for packet filtering on both incoming and outgoing packets. WinRoute considers all packets that are leaving the WinRoute Pro Firewall as outgoing packets regardless of their destination. Any packets that are coming into the WinRoute Pro Firewall, from any port are considered incoming packets.



All rules are read from top to bottom and packets will be affected by the first rule they match. The firewall views SYN and ACK flags in the following manner. All SYN flags are referred to as “establishing” in the Ruleset. All ACK flags are referred to as “established” in the Ruleset. When configuring the rules in WinRoute Pro, it is important to note that the “establishing” flag for a SYN is shown as just the word **SYN** in the ruleset. When a rule is created using the “established” or ACK flag an exclamation mark precedes the word SYN (i.e. **!SYN**).

When a packet finds the first match in a rule set, the rule is applied and the no further rules are processed. This is significant in that we want to ensure that all rules that apply to large volumes of traffic are placed at the “top” to speed processing. The firewall’s stateful inspection ability also means that we do not have to create inbound and outbound rules at each interface for traffic that has been permitted on one interface. As long as subsequent packets passing through the firewall have a match in the NAT table the traffic will be permitted. This simplifies writing rules in WinRoute Pro. With WinRoute Pro, we can apply rules in a number of ways to include rules for single hosts, ranges of addresses, an entire subnet or network and a user-defined address group. We can also apply rules by

time of day, but see no need for this currently. Although the NAT interface closes all ports inbound by default we have still created several rules to enable logging of suspicious or unwanted traffic. We also want to ensure that the border router and firewall are operating as advertised and need to have logs to check that! While we could simply deny inbound traffic we have chosen to drop the majority of this traffic. This will help to keep the firewall in stealth mode and hidden from the Internet.

An example of adding a packet-filtering rule for SMTP is shown below. This window is accessed by selecting Settings>Advanced>Packet Filter. Next you select the interface you are creating the rule for. In this case, the Outside (NAT) Interface and click the Add button.

Edit Item

Packet Description

Protocol : TCP

Source

Type : Address Group

Name : Mail Server

Port : Equal to (=) 25

Destination

Type : Host

IP Address : 199.158.28.94

Port : Equal to (=) 25

TCP Flags

☒ Only established TCP connections

☒ Only establishing TCP connections

Action

☒ Permit

☐ Drop

☐ Deny

Log Packet

☒ Log into file

☒ Log into window

Valid at

Time interval : (Always)

OK Cancel

In the Packet Description field select the protocol type of packet the filter rule will apply to. In this case we selected TCP. The Source Type is the Address Group Mail Server that is the IP address of the ISP mail server. The port is equal to ANY. (Example should show source port of any.) The Destination is the interface IP address and the destination port is SMTP port 25. Both establishing and established connections are permitted by the Action allow button and all packets will be logged into both a file and the mail log window for remote viewing. The rule is Valid at all times. (Logging will probably not be necessary once the configuration of the Mail Server and firewall are confirmed, but has been enabled at this point to aid in troubleshooting.)

Next we will configure a packet-filtering rule that drops any other SMTP connection attempts to the mail server. These connection attempts, regardless of flags set, will also be logged but only into a file to aid in troubleshooting and auditing.

The 'Add Item' dialog box is used to configure a packet-filtering rule. It contains the following sections:

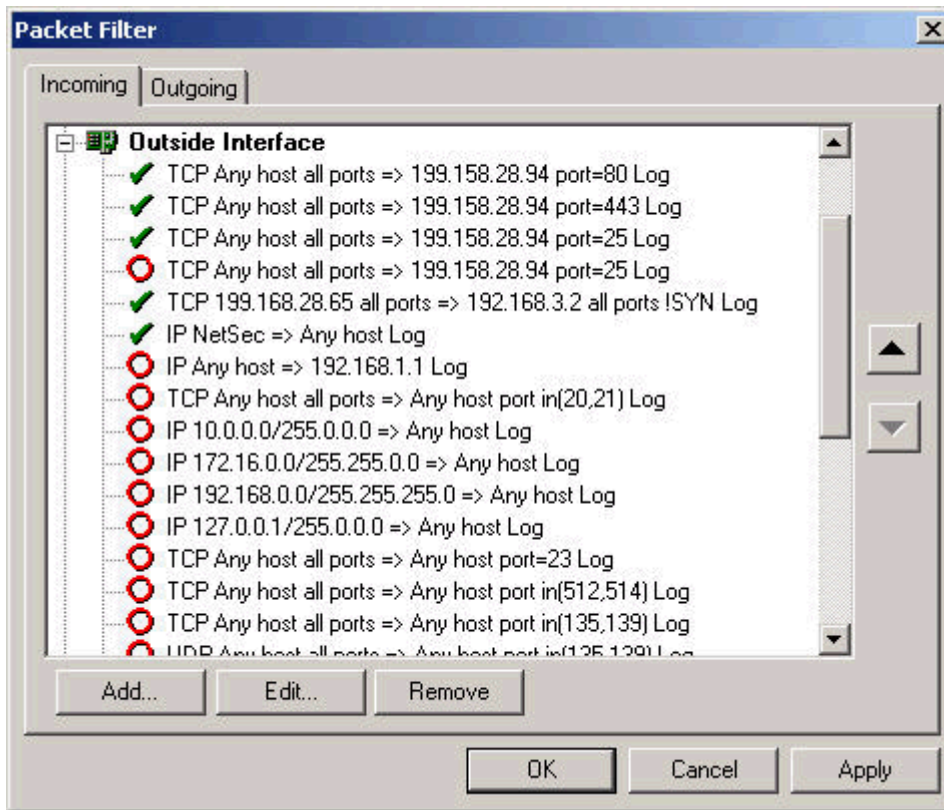
- Packet Description:** Protocol is set to TCP.
- Source:** Type is 'Any address', Port is 'Equal to (=)' 25.
- Destination:** Type is 'Host', IP Address is '199.158.28.94', Port is 'Equal to (=)' 25.
- TCP Flags:** Two checkboxes are present: 'Only established TCP connections' and 'Only establishing TCP connections', both of which are unchecked.
- Action:** Three radio buttons are present: 'Permit' (unchecked), 'Drop' (selected), and 'Deny' (unchecked).
- Log Packet:** Two checkboxes are present: 'Log into file' (checked) and 'Log into window' (unchecked).
- Valid at:** Time interval is set to '(Always)'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Note: The Source Port has been changed to “any” for attempts to connect on port 25.

Next is an example of the Incoming packet filtering ruleset created for GIAC Enterprises. Note that the Outside Interface is the NAT interface that has a public IP address assigned. The interface assigned to the internal network is labeled Internal Network and the interface assigned to the service network is label Service Network.

When reading the rules, a green checkmark indicates that the rule is permitting an action to occur. A red X indicates that the rule is denying an action and the red circle indicates that the action is being dropped at the interface. Actions that are dropped will not send any response back to sender. Also, rules can be moved up or down the ruleset by clicking on the appropriate arrow on the right side of the window.



Incoming Ruleset Explained:

- ✓ TCP Any host all ports => 199.158.28.94 port=80 Log
- ✓ TCP Any host all ports => 199.158.28.94 port=443 Log

These two rules permit TCP traffic inbound on the NAT interface from any host on either port 80 or 443 to the NAT IP with the SYN or establishing flag set. This compliments the port-mapping rule created earlier. These rules are first due to the high volume of traffic expected to the web server.

- ✓ TCP Mail Server all ports => 199.158.28.94 port=25 Log
- TCP Any host all ports => 199.158.28.94 port=25 Log

SMTP traffic will be GIAC's next biggest traffic. The first rule permits SMTP traffic from the Mail Server to the NAT interface where it will then be port-mapped to the internal address for the mail server. All of these establishing and established connections will be logged in the beginning for event correlation and troubleshooting. The second rule drops any other attempts to connect to the mail server and logs those attempts.



- ✓ TCP 199.168.28.65 all ports => 192.168.3.2 all ports !SYN Log

The rule permits the Border Router to send data to the internal syslog server and logs all establishing and established connections.





- ✓ ICMP NetSec => Any host Log

The rule allows the Address Group NetSec, which consists of the NetSec Consulting IP



address range, to use ICMP echo requests (PING) to test connectivity to the firewall. All of these connections are also logged to allow correlation with NetSec Consulting logs. If the logs do not match this could indicate that NetSec Consulting addresses are being spoofed!

-  IP Any host => 192.168.1.1 Log
-  TCP Any host all ports => Any host port in(20,21) Log



The first rule here drops any IP traffic from any host to the private IP address of the web server and logs such attempts. The second rule drops any FTP connection attempts to any GIAC host and logs the attempts.

-  IP 10.0.0.0/255.0.0.0 => Any host Log
-  IP 172.16.0.0/255.255.0.0 => Any host Log
-  IP 192.168.0.0/255.255.255.0 => Any host Log
-  IP 127.0.0.1/255.0.0.0 => Any host Log






These rules compliment the ruleset placed on the Border Router and drop and log any connection attempts from any private IP address or from the loopback address. GIAC should never see this traffic on the firewall, but if it does show up in the logs this will indicate that there is a problem with the Border Router rules.

-  TCP Any host all ports => Any host port=23 Log
-  TCP Any host all ports => Any host port in(512,514) Log

Drops and logs any attempts to telnet (port 23) or Rlogin (ports 512 and 514) to any GIAC host. If these connection attempts appear in the firewall logs this will also indicate a problem with the Border Router. These are popular port attempts automated scanning tools and could indicate a reconnaissance.

-  TCP Any host all ports => Any host port in(135,139) Log
-  UDP Any host all ports => Any host port in(135,139) Log

Drops any Windows NT NetBIOS attempts and logs these attempts. GIAC should not see this type of traffic due to the Border Router Ruleset, but these rules are in place as an extra layer of protection to allow the Border Router and Firewall to compliment each other's rules.

-  TCP Any host all ports => Any host port in(161,162) Log
-  UDP Any host all ports => Any host port in(161,162) Log
-  TCP Any host all ports => Any host port=445 Log
-  UDP Any host all ports => Any host port=445 Log
-  ICMP Any host => Any host Log

The first two rules above drop any SNMP connection attempts and log them. This is important due to the recent vulnerabilities reported in SNMP by CERT in Advisory CA-

2002-03. The following two rules drop and Windows 2000 NetBIOS traffic on port 445. Finally ICMP traffic is dropped from any host to any host. This will assist in maintaining the stealth mode of the firewall for all ICMP traffic except for what was permitted from NetSec. Note that all of these connection attempts are logged for analysis and correlation.

Internal Network

- ✓ ICMP Office => 192.168.1.1 Log
- ✓ TCP Office all ports => 192.168.1.1 port=22 Log
- ✓ TCP Office all ports => Any host port=80 Log
- ✓ TCP Office all ports => Any host port=443 Log
- ✓ TCP Office all ports => Any host port in(20,21) Log

From the Internal Network the first rule permits ICMP traffic from the Address Group Office to the web server and all connections are logged. SSH (port 22) traffic from the Address Group Office to the web server is also permitted and logged. Port 80, 443 and FTP traffic is permitted and only logged for the initial audit.

Testing of Rules: Second test

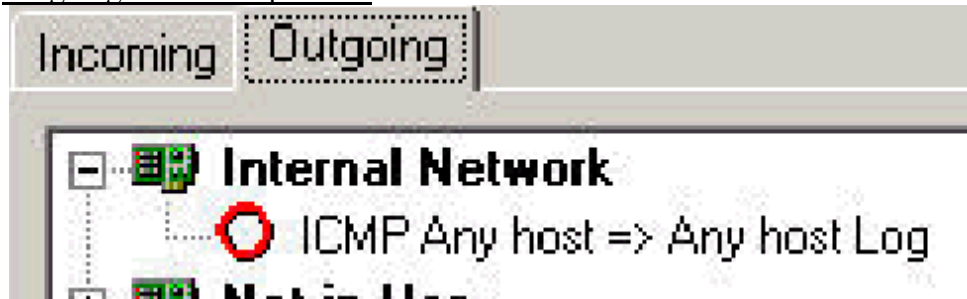
We can test the second rule here for SSH by attempting to connect from an internal computer in the Address Group Office to the Web Server at 192.168.1.1. If the connection is successful then the rule is correct and SSH has been correctly configured on the web server and on the Office computer. If the connection failed, we will need to check the WinRoute Pro logs to determine if the connection attempt was successfully established or if it was blocked. It is critical that this rule and SSH are configured correctly in order for GIAC employees to be able to update the fortunes file on the web server.

Service Network

- ✓ TCP 192.168.1.1 port=80 => 199.158.28.94 port=80
- ✓ TCP 192.168.1.1 port=443 => 199.158.28.94 port=443
- ✓ TCP 192.168.1.1 port=22 => Office port=22 !SYN Log

On the Service Network Interface, HTTP and SSL traffic on ports 80 and 443 is permitted to the NAT interface. SSH traffic is permitted inbound to the Address Group Office and logged.

Outgoing Ruleset Explained:



This rule drops ICMP traffic to prevent a compromised inside host from creating bogus ICMP traffic. The ICMP rule will drop ICMP redirects, ICMP unreachable, time exceeded, source quench and parameter problem messages as shown below.

The 'Edit Item' dialog box is shown, which is used to configure the details of an ICMP rule. The dialog has a title bar 'Edit Item' with a close button. It contains several sections:

- Packet Description:** A dropdown menu for 'Protocol' is set to 'ICMP'.
- Source:** A dropdown menu for 'Type' is set to 'Any address'.
- Destination:** A dropdown menu for 'Type' is set to 'Any address'.
- ICMP Types:** A section with checkboxes for various ICMP types. The checked options are: Redirect, Time Exceeded, Param. Problem, Unreachable, and Source Quench. The unchecked options are: All, Echo Reply, Echo Request, and Time Exceeded.
- Action:** A section with radio buttons for 'Permit', 'Drop', and 'Deny'. The 'Drop' option is selected.
- Log Packet:** A section with checkboxes for 'Log into file' (checked) and 'Log into window' (unchecked).
- Valid at:** A section with a dropdown menu for 'Time interval' set to '(Always)'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons. A faint watermark '© SANS' is visible across the bottom of the dialog.

Outside Interface

- ✓ TCP Office all ports => Any host port=80 SYN
- ✓ TCP Office all ports => Any host port=443 SYN
- ✓ TCP Office all ports => Any host port in(20,21)
- ✓ UDP Office all ports => Any host port in(20,21)
- ✓ TCP Office all ports => 192.168.2.1 port=25

On the Outside (NAT) Interface, the Address Group Office is permitted to access the Internet on port 80 and port 443. These rules allow GIAC employees to surf the web. Once a connection is established no further rules are required. The next two rules allow GIAC Employees to establish FTP connections. The last rule allows the Address Group Office to connect to the Mail Server on SMTP port 25. This rule is required for the email clients to retrieve mail from WinRoute Pro.

Testing of Rules: Third test

We will conduct our third test by attempting to access a web page via HTTP and HTTPS from a GIAC Office computer. This rule states that computers in the Address Group Office are permitted to access the Internet. If the connection attempt is successful then the rules are correct. If the connection fails we will need to begin troubleshooting. Our first step will be to attempt to access several other external web sites via ports 80 and 443. If these subsequent connection attempts are successful then the problem was with the first web site we tried to access. If no connections are made, we will check the WinRoute Pro logs to determine if the connection attempts were permitted through the firewall. Successful connection attempts here will validate the firewall ruleset and may indicate a problem with the ACL on the Border Router or a DNS resolution problem. We can test the firewall rule by changing the outbound rule to allow connections from any host or from a specific IP address. If these connection attempts are successful, the problem is with the range of addresses defined for the Address Group Office.

Service Network

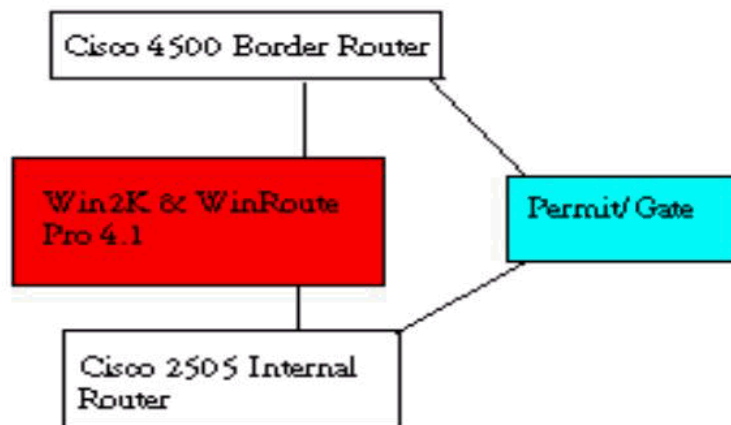
- ✓ TCP Office all ports => 192.168.1.1 port=22 !SYN Log

On the Service Network Interface, the Address Group Office will be permitted SSH (port 22) connections to the web server for secure file transfer over established connections only and all connections will be logged for event correlation.

VPN Configuration:

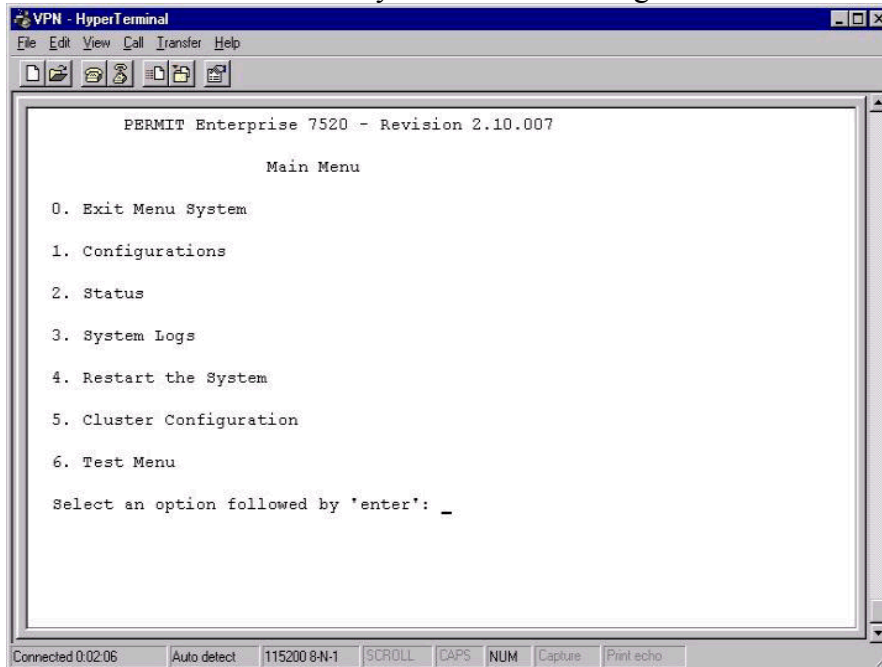
The Permit/Gate 7520 is an IPSec compliant VPN appliance. (Note: The Permit/Gate 7520 is now marketed as the Alcatel Permit/Gate 7137.) We have chosen to use shared secrets for authentication of Business Partners who will connect using the Permit Client. Shared secrets will be stored in the Permit Authentication Table on the Permit Gate. All users have been directed to not enable the “save shared secret” capability in the Permit Client. This is to mitigate the possibility of the node being compromised and allowing unauthorized, but authenticated access to the database server. All shared secrets will be assigned by NetSec and will contain random sequences of numbers and upper and lower case alphanumeric characters. This will not prevent a shared secret from being guessed, but is a good security practice. GIAC Enterprises plans to migrate all partners to public key certificates in the future.

Perimeter diagram:

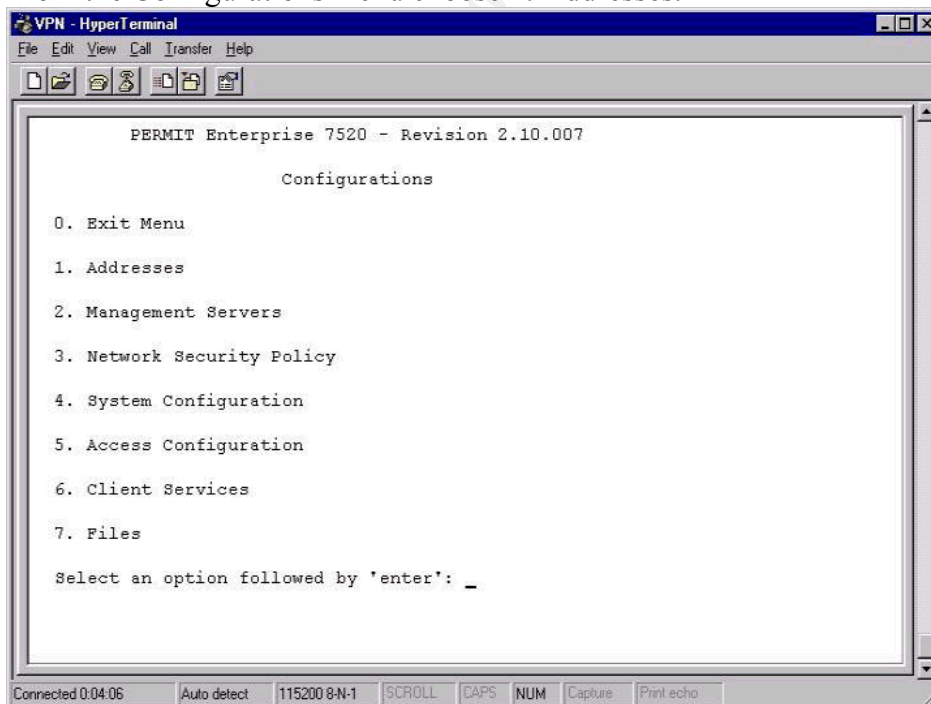


Basic Permit Gate Configuration:

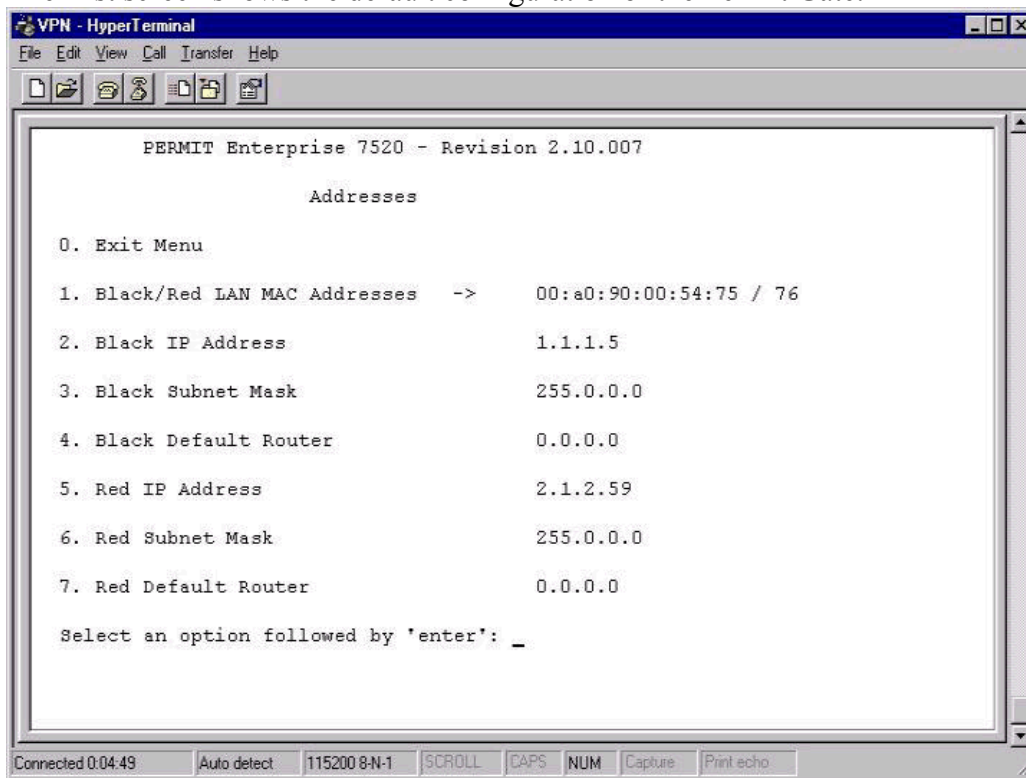
The Permit Gate must be configured to allow access to the Public and Private (GIAC) Networks. Configuration will be accomplished via the console port using HyperTerminal. From the Main Menu below you choose 1. Configurations



From the Configurations menu choose 1. Addresses.



The first screen shows the default configuration of the Permit Gate.



We had to assign the correct addresses for our network configuration as follows:

Note: MAC addresses cannot be changed.

Black (Public) IP Address: 199.158.28.93 (Outside interface of VPN)

Black Subnet Mask: 255.255.255.192

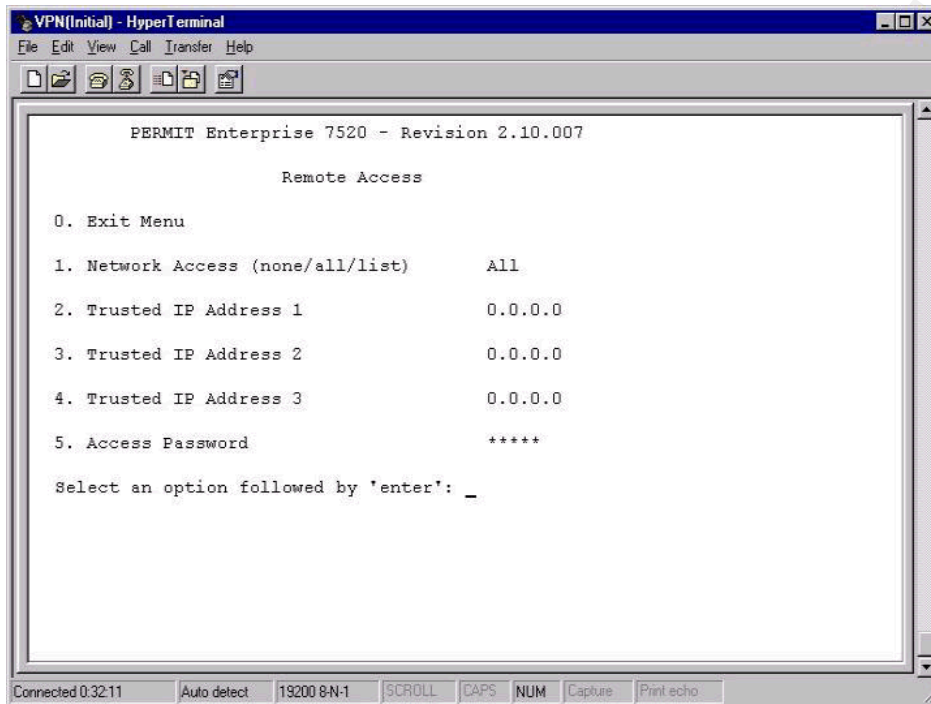
Black Default Router: 199.158.28.66 (Connection between Permit Gate and Border Router)

Red (Private) IP Address: 192.168.7.1 (Inside Interface to GIAC)

Red Subnet Mask: 255.255.255.0

Red Default Router: 192.168.7.2 (Internal Router)

To permit NetSec to remotely administer the VPN, remote access using Permit/Config must be enabled. From the Remote Access Window we have changed the setting to List and have entered the maximum of 3 addresses from the NetSec Consulting Office. (168.23.45.10) (168.23.45.12) (168.23.45.15) We have also changed to remote password. All communications between the Gate and Permit/Config workstations will be across a secure tunnel. *The Permit Gate authenticates each configuration packet with an MD5 HMAC (using the remote access password as a shared secret), sensitive data is encrypted (also using MD5), and a counter variable is used to thwart replay attacks.*¹



To allow secure communications between the Permit Gate and GIAC Business Partners using Permit Client, the Red Security Policy must be configured. From the Main Menu we would choose 1. Configurations, then 3. Network Security Policy and 1. Red Security Policy.

This policy defines the host (Database Server) that users will be granted access to. A separate Security Association must be created for each subnet listed. The Permit Gate does not support broadcast messages so we had to define the subnet between the Gate and the internal router and the destination IP address of the database server. We did not include the subnet address between the internal router and the firewall here because that would allow traffic to be routed to the firewall. Information on the 2 policies created is listed below:

Policy 1

Red IP Address/Range: 192.168.7.0 255.255.255.0 (defines the subnet between to VPN

¹PERMIT/Config version 2.1 Installation Guide

and Internal Router)

Enter Mode: ISAKMP-Shared (defines that shared secrets are used for authentication)

Enter Allowed Clear: no (tells the Gate not to allow the node in this security policy, the internal router itself, from initiating an unencrypted connection to the public network)

Enter Secure Map: no (tells the Gate to not include this subnet in it's secure map between the Gate and Client)

Enter Red Router: 0.0.0.0 (default red-side router)

Policy ID: left blank because no certificates are being used.

Policy 2

Red IP Address/Range: 192.168.4.6 255.255.255.0 (IP address of Database Server. This could have been left as the 192.168.4.0 subnet, but would allow access to the entire subnet)

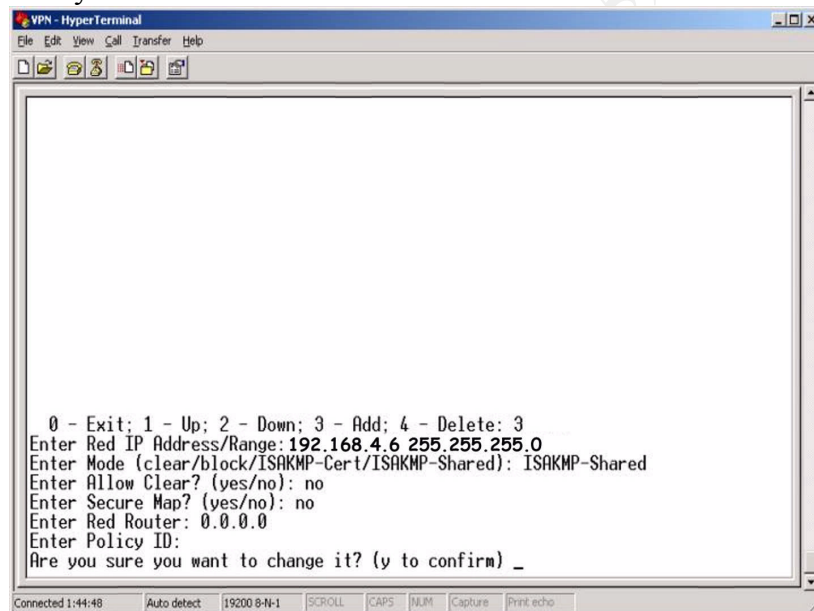
Enter Mode: ISAKMP-Shared

Enter Allowed Clear: no (prevents Database Server from initiating unencrypted connections)

Enter Secure Map: yes (tells Gate to include this IP address in the secure map)

Enter Red Router: 0.0.0.0 (left the same because the 192.168.4.0 subnet uses the same default router)

Policy ID: blank



The final Red Security Policy will look like this:

Item	Red IP Address/Range	Mode	Clear	Map	Red Router	Policy ID
1	192.168.7.0	Isakmp-Shared	n	n	0.0.0.0	
2	192.168.4.6	Isakmp-Shared	n	y	0.0.0.0	

IPSec Policy:

We will configure the Permit Gate to allow “mobile clients with shared secret” for

authentication. This is configured in the tssecdes.cfg file that defines the security level on between devices on the VPN tunnel. This is a text file that is stored in flash memory on the Permit Gate. An example of the shared secret configuration for GIAC is shown below.

```
#
begin security-descriptor
    Name "Moblie Client w/Shared Secret"
    IPsec "ESP DES Minute 300
          or ESP DES HMAC MD5 MINUTES 300
          or ESP 3DES HMAC MD5 MINUTES 300"
    ISAKMP "IDENTIFY PFS DES MD5 MINUTES 1440"
end
#
```

During the first-level of establishing the Security Association between the Permit Gate and Permit Client, the key exchange is defined in the line ISAKMP, with DES used as the cipher algorithm and MD5 as the hashing algorithm. In this example the IDENTIFY specifier is shown. This must be removed to allow the Permit Client to identify itself in order for the Permit Gate to lookup the appropriate shared secret in it's shared secret authentication table. The line should read ISAKMP "PFS DES MD5 MINUTES 1440" The PFS statement sets the Permit Gate to use the Perfect Forward Secret method for key negotiation which ensures that old keys are not used to generate new keys.

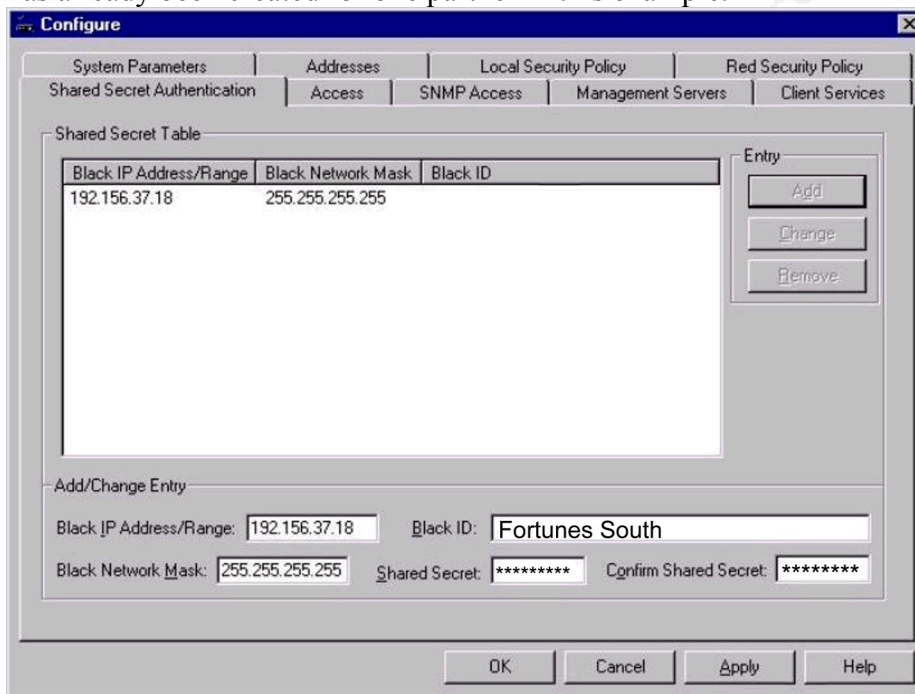
During the second level of Security Association establishment between the Permit Gate and Permit Client the IPsec line defines which protocol and algorithms can be negotiated to secure the data in the VPN tunnel. We have chosen ESP because both authentication and encryption of the data will occur. If we had chosen AH, the Permit Gate would have only performed authentication. The two nodes will now negotiate down the list to determine which cipher algorithm, integrity algorithm (optional for ESP), and the lifetime of the SA before it expires and must be renegotiated.

A Security map, the tssecmap.cfg file, is also created on the Permit Gate that only allows access to the Database server at 192.168.10.1. An example is shown below.

```
Begin static-map
    Name "Database Server"
    Target "192.168.10.1"
    Tunnel "199.158.28.93"
    Mode "ISAKMP-Shared"
End
```

The mapping will direct all traffic that arrives on the outside interface of the Permit Gate to the Database Server only. This effectively prevents GIAC Business Partners from accessing the rest of the internal network.

Finally we have to define the shared secret associations for GIAC Business Partners. Because we have chosen “mobile clients with shared secret” the shared secret will use the partner’s business name or a static IP address as their Unique Identifier. Using Permit/Config we selected the Shared Secret Authentication tab after connecting to the Permit Gate. We then entered the partner’s ID, Fortunes South in this example, in the Black ID space. Next we entered the predetermined shared secret in the both the Shared Secret and Confirm Shared Secret fields. (Remember that first this shared secret will be sent to the Partner via registered mail to confirm receipt. Once receipt has been confirmed, the appropriate entry will be made in Permit Gate.) If we were establishing gate-to-gate or static IP VPNs we would enter the partner’s far side address in the Black IP Address/Range field and 255.255.255.255 in the Black Network Mask field to only allow that IP address to connect. If a static IP address is not entered Permit/Config will display the address field with an all addresses specifier (*. *.*.*) A static IP address association has already been created for one partner in this example.



The Permit Gate is now capable of accepting connections from the Permit Client. GIAC Partners are provided with step-by-step installation instructions for the Client software.

Assignment 3: Audit Your Security Architecture

GIAC Enterprises has requested that we audit the configuration of the firewall as soon as possible. GIAC Management has asked that the audit be conducted during weekend hours when they normally experience a significant drop in business and normally only have 1 person in the office. We will perform the audit on Saturday beginning at 7 AM. We will use 1 NetSec systems engineer, at the cost of \$25.00 per hour, and 1 senior engineer, at the cost of \$35.00 per hour, to conduct the audit. We expect the firewall audit to take 8 hours, but have budgeted for 12 in the event that there are problems. We expect the audit to conclude on Saturday no later than 7 PM. We will monitor the log files on the WinRoute Pro firewall and run our attacks using a number of free tools available from Foundstone to include SuperScan and UDP Flooder. Although it is possible that our audit may have adverse affects on the network, we have created backups of all critical information on the network. We will also ensure that the fortunes database is backed up and will test the backup be restoring it before beginning the audit. The scanning system will be placed between the Border Router and the Firewall and all scans will be run against the outside interface of the firewall. This will allow us to truly trust the ruleset on the firewall itself without relying on the Border Router for screening. A second audit will be conducted against the Border Router to ensure it's rulesets are valid.

A quick reference to WinRoute's logs is included here for clarity and information purposes. WinRoute Pro offers six logs. As detailed in the WinRoute Pro 4.2 Reference Guide the logs are shown below:

HTTP Log	Displays only HTTP data passing through the WinRoute Proxy server; includes source IP address and username, time stamp, and HTTP queries and responses
Mail Log	Records all operations of the WinRoute's built-in mail server; records SMTP an POP3 send/receive activities
Security Log	Shows all activities defined as "Log to window/file" in packet filter rules (see below for detailed description of items recorded)
Dial Log	Records usage information for dial-up interfaces monitored by WinRoute
Debug Log	A la carte settings to record all ARP , ICMP , UDP , TCP, and/or DNS packets that physically cross any interface of the WinRoute router; granular configuration available under Settings Advanced Debug Info, Debug tab.
Error Log	Displays all unsuccessful operations occurring in any running WinRoute module

The logs that we would use for GIAC's implementation of the firewall are the Mail Log, Security Log, Debug Log and Error Log. The log information recorded include

- Date
- Time
- Packet Filter rule impacted
- Interface
- Action (Permit, Drop, Deny)
- Source IP address and TCP port
- Destination IP address and TCP port

To read the Debug Log, which we used for the audit, the following information is provided from the reference material.

How to read the log?

From the left you may see following:

Time stamp - the date and time displaying exactly when the event happened or packet crossed the interface.

The protocol - the type of protocol of the packet

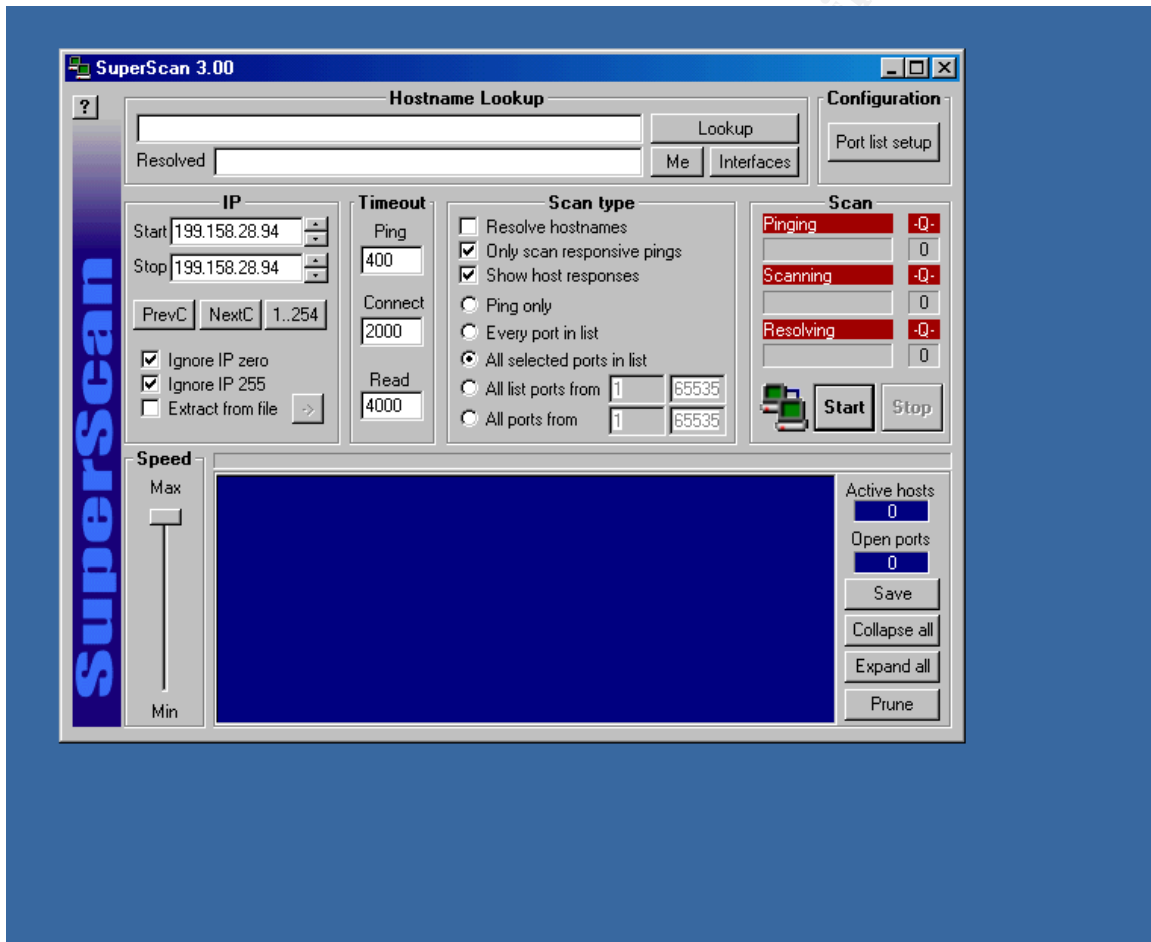
From/To Interface name - the name of the interface and whether the packet went **To** or came **From** the interface (imagine that WinRoute is running on the PC and interfaces are meant to be the "gates" between the computer and the network).

Source IP -> Destination IP address - the source and destination IP addresses present in the packet.

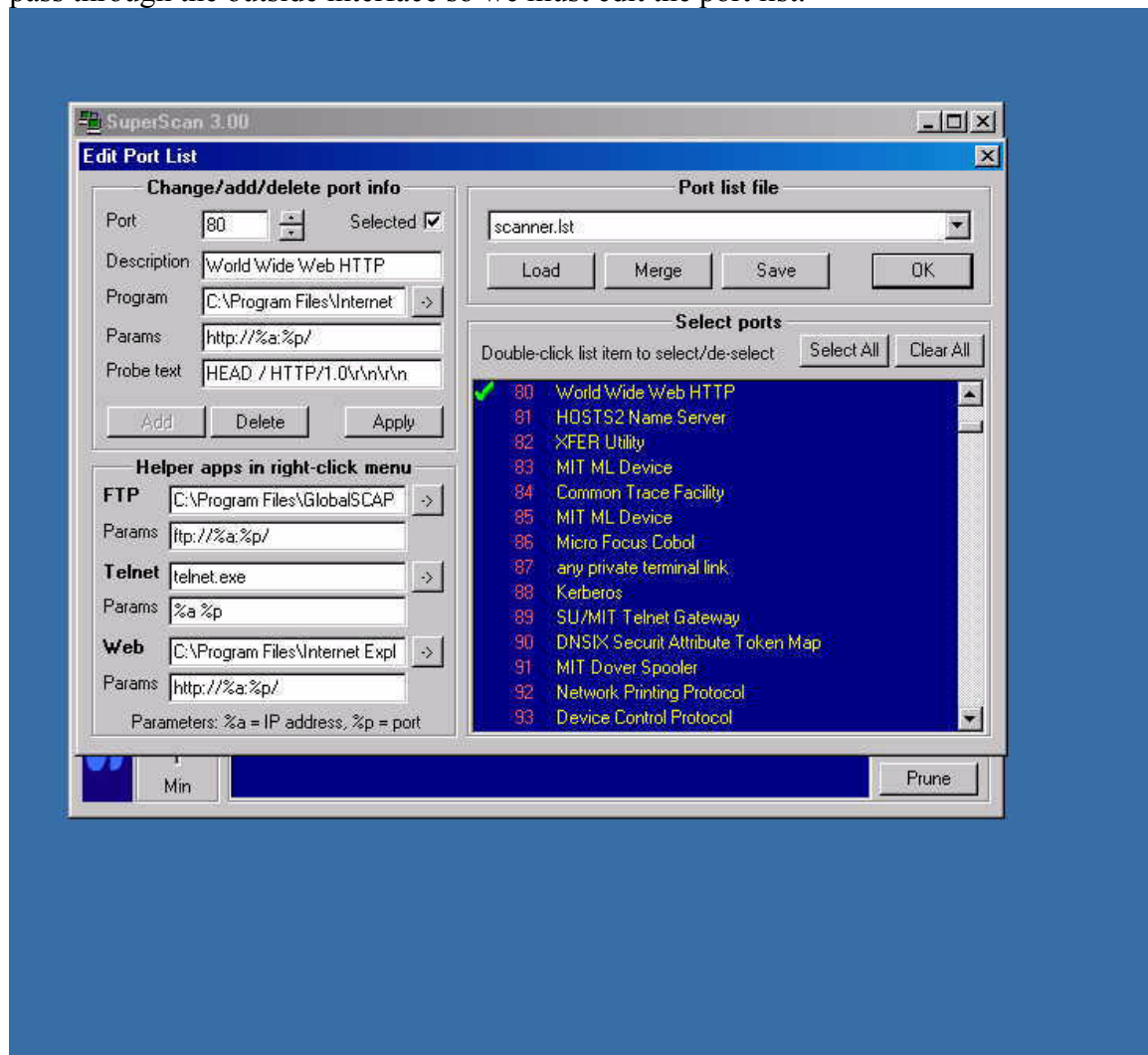
The flags - further identification about the action.

Foundstone's SuperScan 3.00 will be the first tool used for the audit. As described in the help file "SuperScan is a TCP port scanner, pinger and hostname resolver" and several of the functions that we will use for the audit include:

- perform simple ping tests to tell whether a remote computer is alive
- attempt to connect to other computers on a TCP network to see what services they are running
- read responses from connected hosts
- scan from a range of addresses and ports
- scan from a list of ports
- scan from selected ports from a list



Before running our scan, we need to configure SuperScan for all of the information gathering we want to attempt. We must configure the ports that will attempt connections using SuperScan. We first want to validate that port 80, 443 and 25 traffic is allowed to pass through the outside interface so we must edit the port list.



(Note: Security log output has been changed to Courier New for easier viewing.)

We now run the first scan against the firewall and the security log show that.

```
[29/Mar/2002 18:58:39] Packet filter: ACL 4:5 Outside Interface:
drop packet in: ICMP 199.158.28.65 -> 199.158.28.94 type 8 code
0
```

The outside interface ACL 4.5 dropped the inbound ICMP packet from 199.158.28.65

```
[29/Mar/2002 18:58:40] Packet filter: ACL 4:2 Outside Interface:
permit packet in: TCP 199.158.28.65:3665 -> 199.158.28.94:25
```

Outside interface ACL 4.2 permitted inbound traffic from our test laptop on port 25.

```
[29/Mar/2002 18:58:40] Packet filter: ACL 4:0 Outside Interface:
permit packet in: TCP 199.158.28.65:3666 -> 199.158.28.94:80
[29/Mar/2002 18:58:40] Packet filter: ACL 4:1 Outside Interface:
permit packet in: TCP 199.158.28.65:3667 -> 199.158.28.94:443
Outside Interface ACL 4.0 permitted inbound port 80 and 443 traffic
```

So that we are not relying on only the results of one program we also used Foundstone's FScan a command line port scanner. (Note: FScan is not as reliable for testing UDP ports, as noted in the readme file, so it was only used for testing TCP ports.) To check the outside interface using this tool we ran the command:

```
C:> FScan -p 80, 443, 25 199.158.28.94 -o result1.txt
```

(This command scans TCP ports 80, 443, and 25 on the IP address specified and sends the output results to the file results1.txt) Note: After several attempts to use the FScan tool as "advertised" it was discovered that each port must be preceded by a "-p". Without the -p the program selects ip addresses from the 0.0.0.# network and appends the other number to the last octet. We also found that the results.txt file provides nothing useful and stopped using it.

When we ran FScan -q -v -p 25 -p 80 -p 443 199.158.28.94 (no ping, display verbose information and scan the listed ports) the FScan output displayed was

```
Adding TCP port 25
Adding TCP port 80
Adding TCP port 443
Adding IP 199.158.28.94
Using 64 threads.
Connect timeout set to 600 ms.
Ping timeout set to 500 ms.
Scan delay set to 0 ms.
Quiet mode selected. No pings.

Scan started at Fri Mar 29 18:50:28 2002

Scanning TCP ports on 199.158.28.94

Scan finished at Fri Mar 29 18:50:29 2002
Time taken: 3 ports in 0.611 secs (4.91 ports/sec)
```

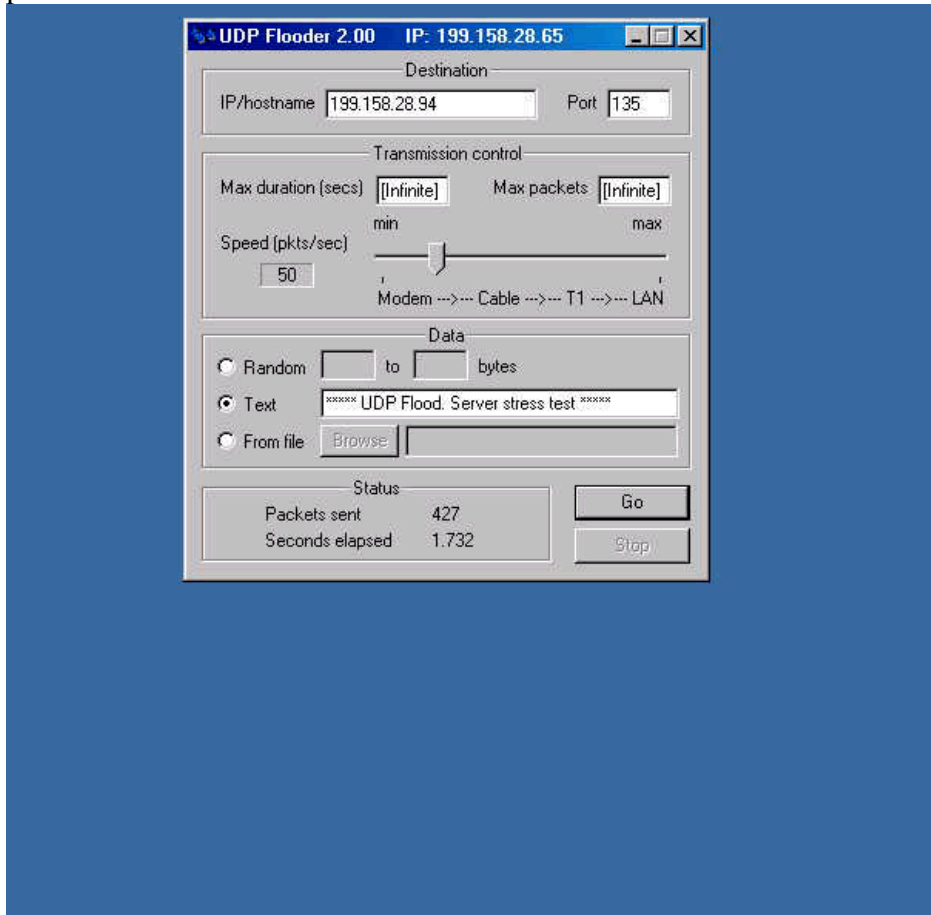
the results on the firewall showed that the inbound traffic was permitted as noted above and FScan did not attempt to ping the target.

We now create a port list to test all rules that we set to deny or drop traffic and compare them to the results of both the debug log and the security log. This will tell us if the firewall is actually logging the traffic we wanted logged.

```
[29/Mar/2002 20:11:38] Packet filter: ACL 4:7 Outside Interface:
drop packet in: TCP 199.158.28.65:3801 -> 199.158.28.94:20
[29/Mar/2002 20:11:38] Packet filter: ACL 4:7 Outside Interface:
drop packet in: TCP 199.158.28.65:3802 -> 199.158.28.94:21
[29/Mar/2002 20:11:38] Packet filter: ACL 4:12 Outside
Interface: drop packet in: TCP 199.158.28.65:3803 ->
199.158.28.94:23
[29/Mar/2002 20:11:38] Packet filter: ACL 4:2 Outside Interface:
permit packet in: TCP 199.158.28.65:3804 -> 199.158.28.94:25
[29/Mar/2002 20:11:38] Packet filter: ACL 4:16 Outside
Interface: drop packet in: TCP 199.158.28.65:3805 ->
199.158.28.94:161
[29/Mar/2002 20:11:38] Packet filter: ACL 4:16 Outside
Interface: drop packet in: TCP 199.158.28.65:3806 ->
199.158.28.94:162
[29/Mar/2002 20:11:38] Packet filter: ACL 4:18 Outside
Interface: drop packet in: TCP 199.158.28.65:3807 ->
199.158.28.94:445
[29/Mar/2002 20:11:38] Packet filter: ACL 4:13 Outside
Interface: drop packet in: TCP 199.158.28.65:3808 ->
199.158.28.94:512
[29/Mar/2002 20:11:38] Packet filter: ACL 4:13 Outside
Interface: drop packet in: TCP 199.158.28.65:3809 ->
199.158.28.94:513
[29/Mar/2002 20:11:38] Packet filter: ACL 4:13 Outside
Interface: drop packet in: TCP 199.158.28.65:3810 ->
199.158.28.94:514
```

All rules ACLs that were placed on the outside interface for dropping specific ports show that the traffic was dropped.

Using UDP Flooder this time we sent UDP packets at speed of 50 packets per second on ports 135 and 139 to validate those rules.

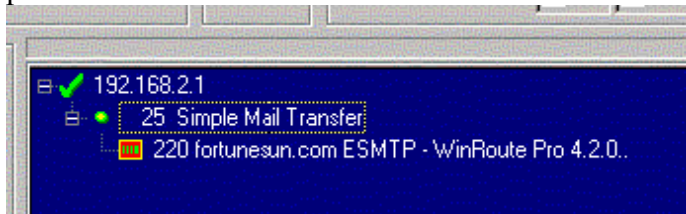


The firewall reported the following for all 50 packets with no detriment to throughput that was noted. We also increased to “LAN speed” of 250 packets per second with the same results.

```
[29/Mar/2002 20:22:21] Packet filter: ACL 4:15 Outside
Interface: drop packet in: UDP 199.158.28.65:3817 ->
199.158.28.94:135
[29/Mar/2002 20:22:22] Packet filter: ACL 4:15 Outside
Interface: drop packet in: UDP 199.158.28.65:3817 ->
199.158.28.94:135
```

Inside Interface:

We now directed the scanner at the inside interface of the firewall. We wanted to allow outbound traffic from the Office address group, using an Office address, to the Internet for port 80, 443 and FTP. We also want to ensure that the interface is passing traffic on port 25.



The result from SuperScan shows that port 25 is passing traffic from the Office Address Group to the Mail Server running on the firewall.

```
[29/Mar/2002 20:47:46] Packet filter: ACL 6:4 Internal Network:
permit packet in: TCP 192.168.4.7:3842 -> 192.168.2.1:20
```

```
[29/Mar/2002 20:47:46] Packet filter: ACL 6:4 Internal Network:
permit packet in: TCP 192.168.4.7:3843 -> 192.168.2.1:21
```

Traffic is permitted to pass thru the internal interface at 192.168.2.1 from the Office computer at 192.168.4.7 destined for port 20 and 21.

```
[29/Mar/2002 20:47:46] Packet filter: ACL 6:2 Internal Network:
permit packet in: TCP 192.168.4.7:3846 -> 192.168.2.1:80
```

```
[29/Mar/2002 20:47:46] Packet filter: ACL 6:3 Internal Network:
permit packet in: TCP 192.168.4.7:3847 -> 192.168.2.1:443
```

Traffic is permitted to pass on ports 80 and 443 as well.

```
[29/Mar/2002 20:47:46] Packet filter: ACL 6:4 Internal Network:
permit packet in: TCP 192.168.4.7:3842 -> 192.168.2.1:20
```

```
[29/Mar/2002 20:47:46] Packet filter: ACL 6:4 Internal Network:
permit packet in: TCP 192.168.4.7:3843 -> 192.168.2.1:21
```

```
[29/Mar/2002 20:47:47] Packet filter: ACL 6:3 Internal Network:
permit packet in: TCP 192.168.4.7:3847 -> 192.168.2.1:443
```

Using FScan: C:> FScan -p 20, -p 21 -p 80 -p 443 192.168.2.1

Results we identical to the above information.

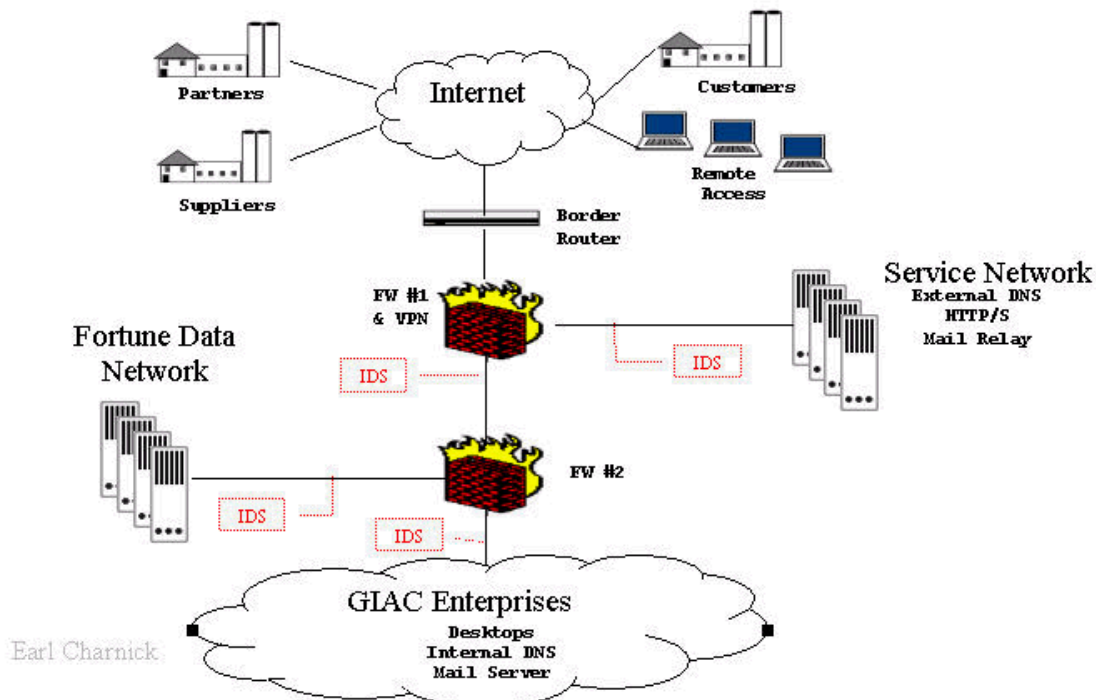
To ensure that no other traffic was passing we tested UDP port 135.

Traffic was not blocked! Recommendation to Add Ruleset to block any unnecessary outbound traffic to mitigate the insider threat. This recommendation extends to all such traffic. The log files of the firewall will be reviewed extensively during the first 3 months of operation to ensure all unnecessary ports are blocked. Robust filtering will also be enabled on the internal router to further mitigate any risk.

Assignment 4: Design Under Fire

The network design that I chose to attack was Earl Charnick and is available at <http://www.giac.org/GCFW.php> Earl_Charnick_GCFW. Mr. Charnick is running Checkpoint Firewall-1 on a Nokia IP 530 appliance as his primary firewall. The Firewall will also act as the VPN access point using VPN-1 SecuRemote.² I conducted my research for vulnerabilities for Checkpoint at a number of sites to include www.securityfocus.com and web searches using Google.

Proposed Architecture



² GCFW IP, Firewall and VPN Practical Version 1.6, Earl Charnick

There are quite a few vulnerabilities listed on the Security Focus web site.

<http://online.securityfocus.com/search> Doing a search for Firewall-1 yielded the following results.

- 2002-03-08: Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability
- 2002-02-19: Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability
- 2001-10-23: Check Point VPN-1 SecuRemote Username Acknowledgement Vulnerability
- 2001-09-12: Check Point Firewall-1 GUI Log Viewer Vulnerability
- 2001-09-08: Check Point Firewall-1 Policyname Temporary File Creation Vulnerability
- 2001-09-08: Check Point Firewall-1 GUI Client Log Viewer Symbolic Link Vulnerability
- 2001-07-18: Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability
- 2001-07-11: Check Point Firewall-1/VPN-1 Management Station Format String Vulnerability
- 2001-07-09: Check Point Firewall-1 RDP Header Firewall Bypassing Vulnerability
- 2001-01-17: Check Point Firewall-1 4.1 Denial of Service Vulnerability
- 2000-12-14: Check Point Firewall-1 Fast Mode TCP Fragment Vulnerability
- 2000-11-01: Checkpoint Firewall-1 Valid Username Vulnerability
- 2000-08-15: Check Point Firewall-1 Session Agent Dictionary Attack Vulnerability
- 2000-08-02: Check Point Firewall-1 Unauthorized RSH/REXEC Connection Vulnerability
- 2000-07-05: Check Point Firewall-1 Spoofed Source Denial of Service Vulnerability
- 2000-06-30: Check Point Firewall-1 SMTP Resource Exhaustion Vulnerability
- 2000-06-06: Check Point Firewall-1 Fragmented Packets DoS Vulnerability
- 2000-03-11: Check Point Firewall-1 Internal Address Leakage Vulnerability
- 2000-03-10: Multiple Firewall Vendor FTP "ALG" Client Vulnerability
- 2000-02-09: Multiple Firewall Vendor FTP Server Vulnerability
- 2000-01-29: Check Point Firewall-1 Script Tag Checking Bypass Vulnerability
- 1999-10-20: Check Point Firewall-1 LDAP Authentication Vulnerability
- 1999-08-09: Firewall-1 Port 0 Denial of Service Vulnerability
- 1999-07-29: FireWall-1, FloodGate-1, VPN-1 Table Saturation Denial of Service Vulnerability
- 1998-09-24: Check Point Firewall-1 Session Agent Impersonation Vulnerability

© SANS Institute 2000 - 2005

The first vulnerability selected is a Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability.

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=4253>

Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability

[info](#) [discussion](#) [exploit](#) [solution](#) [credit](#) [help](#)

bugtraq id 4253
object users.C
class Design Error
cve CVE-MAP-NOMATCH
remote No
local Yes
published Mar 08, 2002
updated Mar 08, 2002
vulnerable Check Point Software Firewall-1 4.0SP8
Check Point Software Firewall-1 4.0SP7
Check Point Software Firewall-1 4.0SP6
Check Point Software Firewall-1 4.0SP5
Check Point Software Firewall-1 4.0SP4
Check Point Software Firewall-1 4.0SP3
Check Point Software Firewall-1 4.0SP2
Check Point Software Firewall-1 4.0SP1
Check Point Software Firewall-1 4.0
Check Point Software Firewall-1 4.1SP5
Check Point Software Firewall-1 4.1SP4
Check Point Software Firewall-1 4.1SP3
Check Point Software Firewall-1 4.1SP2
Check Point Software Firewall-1 4.1SP1
Check Point Software Firewall-1 4.1

By clicking on the discussion tab we find the following information.

[info](#) [discussion](#) [exploit](#) [solution](#) [credit](#) [help](#)

Check Point Firewall-1 is a popular firewall package available from Checkpoint Software Technologies. SecuClient/SecuRemote are VPN-1 implementations for Check Point Firewall-1 products.

It is possible to configure a timeout value for cached user credentials. This value is stored on client systems and can be modified by users of client systems. If security policy includes a time limit on cached credentials, malicious authenticated users may bypass the policy by modifying the value.

Depending on the operating system of the client host, local administrative privileges on the client host may be required to modify the configuration file.

In addition to the timeout values, other sensitive information is reportedly stored on client systems. Further details are not known at this time.

The threat is that a user may be able to change the timeout value of their cached credentials. If a user does this, they will defeat the security policy in place. Mr. Chadwick's paper states that users will be required to change their password every 2 to 3 months. If this is enforced on the client, a user may defeat this policy.

As stated under the Exploit tab, if a user/attacker can read from or write to users.C they can exploit this vulnerability.

As of this writing a Solution is not known, but a workaround proposed is to encrypt the cached user credentials. This is only effective if the user is not allowed to do a SecuRemote topology update.

© SANS Institute 2000 - 2005, Author retains full rights.

The second vulnerability is an HTTP CONNECT TCP tunnel vulnerability.

<http://online.securityfocus.com/bid/4131>

Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability

info	discussion	exploit	solution	credit	help
bugtraq id	4131				
object					
class	Configuration Error				
cve	CVE-MAP-NOMATCH				
remote	Yes				
local	No				
published	Feb 19, 2002				
updated	Mar 04, 2002				
vulnerable	Acme thttpd 2.0 Acme thttpd 2.0.1 Acme thttpd 2.0.2 Acme thttpd 2.0.3 Acme thttpd 2.0.4				

By clicking on the Discussion tab we find that

Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability

info	discussion	exploit	solution	credit	help
------	------------	---------	----------	--------	------

Multiple software and integrated server packages that function as web proxies may be used as open TCP proxies. This is through the usage of the HTTP CONNECT method by default. This method is detailed in RFC 2817, where it is used to build generic Transit Layer Security over HTTP.

Upon receiving a CONNECT request, vulnerable products act as a TCP proxy, tunneling the conversation. This can be used to launch attacks against internal machines or to, for example, use an internal mail server as an open relay.

In many cases, this behavior may be controlled through the server configuration. Often it is related to support for tunneling or SSL related functionality.

This vulnerability represents a preliminary list of vendors which may have vulnerable default configurations. Updates will be made as additional information becomes available.

Check Point Firewall-1 is listed as a vulnerable vendor. A workaround is listed for Firewall-1 under the Solution Tab and is listed below for reference.

Checkpoint has announced that they will include enhanced control of this type of connection in their next product update.

The following workaround has been suggested by Volker Tanger <volker.tanger@discon.de> for CheckPoint Firewall-1 systems:

Fast workarounds:

- Change your resource settings to filter out CONNECT commands, i.e.
 - * disable HTTP tunneling
 - * check that "Other" method is specified NOT to match CONNECT (i.e. remove the default wildcard)
- disallow access from the firewall module (->Properties)
- replace in all your rules containing the service HTTP+Resource this part with plain HTTP. Yes, you loose some content security but at least you don't compromise your other servers

© SANS Institute 2000 - 2005, A

The third vulnerability I have chosen is a network information leak vulnerability.

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3058>

Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability



bugtraq id	3058
object	
class	Configuration Error
cve	CVE-MAP-NOMATCH
remote	Yes
local	No
published	Jul 18, 2001
updated	Jul 18, 2001
vulnerable	Check Point Software Firewall-1 4.0 Check Point Software Firewall-1 4.1SP4 Check Point Software Firewall-1 4.1SP3 Check Point Software Firewall-1 4.1SP2 Check Point Software Firewall-1 4.1SP1 Check Point Software Firewall-1 4.1

The problem here is that older versions of SecuRemote can obtain the entire network topology prior to authentication. This can then be used to gather information prior to an attack. We can attempt this attack by downloading the Perl script that is found under the Exploit tab. <http://downloads.securityfocus.com/vulnerabilities/exploits/sr.pl>

As noted on under the Solution Tab

A workaround for this problem is to use the PolicyEditor configuration tool, and uncheck "respond to unauthenticated topology requests."

This problem has been fixed in recent releases of the software.

So Mr. Chadwick simply needs to maintain an up-to-date system.

A final exploit that was found and can be attempted is the Spoofed Source Denial of Service Vulnerability.

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1419>

VULNERABILITIES

Check Point Firewall-1 Spoofed Source Denial of Service Vulnerability

[info](#) [discussion](#) [exploit](#) [solution](#) [credit](#) [help](#)

bugtraq id	1419
object	
class	Configuration Error
cve	GENERIC-MAP-NOMATCH
remote	Yes
local	No
published	Jul 05, 2000
updated	Jul 05, 2000
vulnerable	Check Point Software Firewall-1 3.0 Check Point Software Firewall-1 4.0 Check Point Software Firewall-1 4.1

Under the Discussion Tab we find that

If Checkpoint Firewall-1 receives a number of spoofed UDP packets with Source IP = Destination IP, the firewall (and likely the machine hosting it) crashes.

This can be exploited by compiling and running the following code found under the Exploit Tab.

<http://downloads.securityfocus.com/vulnerabilities/exploits/cpd.c>

Once downloaded the code can be compiled on a Linux box by running the following command.

```
cc -o cpd cpd.c
```

The attack can then be sent to the Firewall by running the command

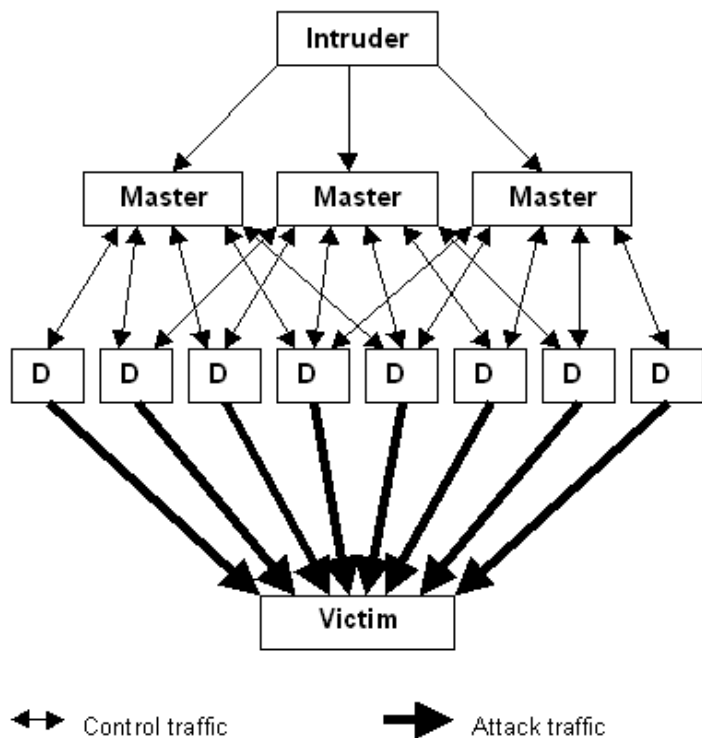
```
./cpd 1.2.3.4 500 53
```

where 1.2.3.4 is the victim IP address, 500 is the number of packets to be sent and 53 is

the destination port number. If this attack is successful, the firewall and possibly the Nokia appliance itself will crash. As noted under the Solution Tab turning on Anti-Spoofing in the firewall ruleset can easily protect against this attack.

Denial of Service

Finally I plan to use a Denial of Service Attack against the network. I found valuable information at http://www.cert.org/incident_notes/IN-99-07.html and http://www.cert.org/reports/dsit_workshop-final.html that detailed both the Trinoo and Tribe Flood Network Tools. Although both are promising, I have chosen to use TFN because it has the ability to generate spoofed source IP addresses, uses encryption to hide the list of compromised systems and has a remote copy capability. Further information on the workings of TFN were found at <http://staff.washington.edu/dittrich/misc/tfn.analysis>. I would attempt to compromise a large number of home systems by sending an email Trojan. I am confident that as the user base for LINUX continues to grow it will not be difficult to find these systems. Once I have several systems running as master controllers, I would then work to compromise user boxes for daemons. With 50 compromised Cable/DSL systems acting as daemons a series of commands would be sent from the master to the compromised daemons.



3

Sending ICMP_ECHOREPLY packets the commands would direct the daemons to use a TCP SYN flood against the GIAC address space or simply against the GIAC web server.

³ http://www.cert.org/reports/dsit_workshop-final.html

Source IP addresses and source ports would be randomized to attempt to conceal the attack. I would then be able to monitor the progress of the attack by attempting to browse to the GIAC web site. The help screen for TFN provides the following usage information:

```
-----
[tribe flood network] (c) 1999 by Mixter

usage: ./tfn <iplist> <type> [ip] [port]

<iplist>      contains a list of numerical hosts that are ready to
flood
<type>        -1 for spoofmask type (specify 0-3), -2 for packet size,
              is 0 for stop/status, 1 for udp, 2 for syn, 3 for icmp,
              4 to bind a rootshell (specify port)
              5 to smurf, first ip is target, further ips are
broadcasts
[ip]          target ip[s], separated by @ if more than one
[port]        must be given for a syn flood, 0 = RANDOM
-----
```

So to send the command to the daemons the command would look something like this:

```
./tfn hosts 2 <GIAC IP> 0
```

GIAC can avoid this type of attack by ensuring that all of their systems are patched. By ensuring that the Service Network IDS has the latest signatures, GIAC can monitor any attempts and follow their response procedures. Finally, stateful packet filtering can also be used to mitigate this risk.

References:

WinRoute Pro Version 4.2 Reference Guide, Kerio Technologies

<http://www.kerio.com/parser/mainpage.php?id=74&lg=1>

CERT/CC

http://www.cert.org/incident_notes/IN-99-07.html

http://www.cert.org/reports/dsit_workshop-final.html

SANS Top 20

<http://www.sans.org/top20.htm>

SANS Top 10 Offenders

<http://www.dshield.org/top10.html>

Permit Enterprise. PERMIT/Gate Model 7520 Version 2.1 Administrator's Guide

Permit Enterprise. Permit/CONFIG Version 2.1 Installation Card: 2

Address Allocation for Private Internets

<http://www.ietf.org/rfc/rfc1918.txt>

Reserved IANA IP Addresses

<http://www.iana.org/assignments/ipv4-address-space>

Exploit Research:

<http://www.securityfocus.com>

Dittrich, David. "Tribe Flood Network." 21 October 1999

<http://staff.washington.edu/dittrich/misc/tfn.analysis> (19 Mar. 2002)

NIST Publications:

Special Publication 800-43, System Administration Guidance For Securing Microsoft Windows 2000 Professional System

Improving Security on Cisco Routers

<http://www.cisco.com/warp/public/707/21.htm#redirect>

Audit Tools

http://www.foundstone.com/knowledge/free_tools.html

© SANS Institute 2000 - 2005, Author retains full rights.