Global Information Assurance Certification Paper

SANS Level 2 GCFW Certification Practical Version 1.5e
Firewalls, Perimeter Protection, and VPNs

Submitted for SANS Baltimore, Maryland By:
Kelvin Tarrance
July 20, 2001

Table of Contents

Assignment 1

Overview of Architecture

All employee traffic to the Internet traverse through a firewall allowing outbound only traffic. All Customer, Supplier, and Partner traffic traverse through a firewall into a DMZ. The DMZ was created to provide secure access to vital information without exposing the internal network. All perimeter defense systems are backed up. See Diagram 1 for network layout.

Perimeter Commonalities

Border Router

Border router used by GIAC Enterprises is a CISCO 3601 using ISO 12.2.

Firewalls

Firewalls used by GIAC Enterprises are Gauntlet Application Proxy firewalls version 5.5. All firewall contain at least two network cards, one for internal and one for external access. All firewalls contain latest firewall patches.

VPNs

VPNs used by GIAC Enterprises are Nortel 4500 VPN version 3.2. All VPN contain at least two network cards, one for internal and one for external.

Operating System (OS)

Each server in Diagram 1 is running on HPUX 10.20 with the latest patches. Each server is running HPUX C2 Level Trusted Systems, which is design to enhance the security of the OS.

Perimeter Defense

Backups

The firewall configuration are encrypted and backed up to the support system on the internal network. A backup will allow for minimum down time if the firewalls are compromised or experience some system hardware failure, which any vendor will tell you never occurs.

Border Router

This device is not only the entry point into GIAC Enterprises Web presents, it is the first point where security filtering can and will be applied. Let's not

forget that device primary job is to route traffic. Therefore, we do not want it loaded down with filters.

Customers, Suppliers, and Partners Web Access

Customers, Suppliers, and Partners will access GIAC Enterprises Web site using http for general browsing while using https for secure browsing. This system is located in the DMZ. The web server queries the database.

DMZ External Firewall

Customers, Suppliers, and Partners pass through firewall fwoutdmz to access GIAC Enterprises data. This firewall allows http, https, and IPSec traffic to pass into the DMZ. If outbound traffic request are initiated in the DMZ for the Internet, they are blocked at the firewall.

DMZ Internal Firewall

Employees pass through firewall fwindmz to access GIAC Enterprises Web site and shared data. This firewall allows http, https, and IPSec traffic to pass into the DMZ. If outbound traffic request are initiated in the DMZ for the internal network, they are blocked at the firewall.

Employee Web Access

Employees will access the Internet through firewall fwintnet, which allows outbound traffic for support analyst and non-support employees to access HTTP, HTTPS, SSH, and Telnet. Because of the insecure nature of ActiveX, it is blocked by this firewall for non-support employees.

External DNS

The external DNS only serves GIAC Enterprises Internet servers. It is unaware of the company's internal network (NOT a splitT DNS). DNS is running in a chrooted environment. Chrooted BIND is not able to access any files outside of its chrooted directory. Lastly, the DNS server will only allow mail relaying from internal IP addresses.

Internal Network

The internal network contains the support server named support, internal DNS, internal mail and various other systems which other organizations should not and do not have access to.

Partners VPN Access

Partners VPN allows IPSec communication with password authentication. The LDAP server handles authentication. The VPN tunnel is established between the Partner's VPN and GIAC's VPN. This allows GIAC's VPN to

know the static IP to permit. The Partners VPN is located in the DMZ.

Physical Security

What is a good network design without some type of physical security? The systems will be located in a locked room.

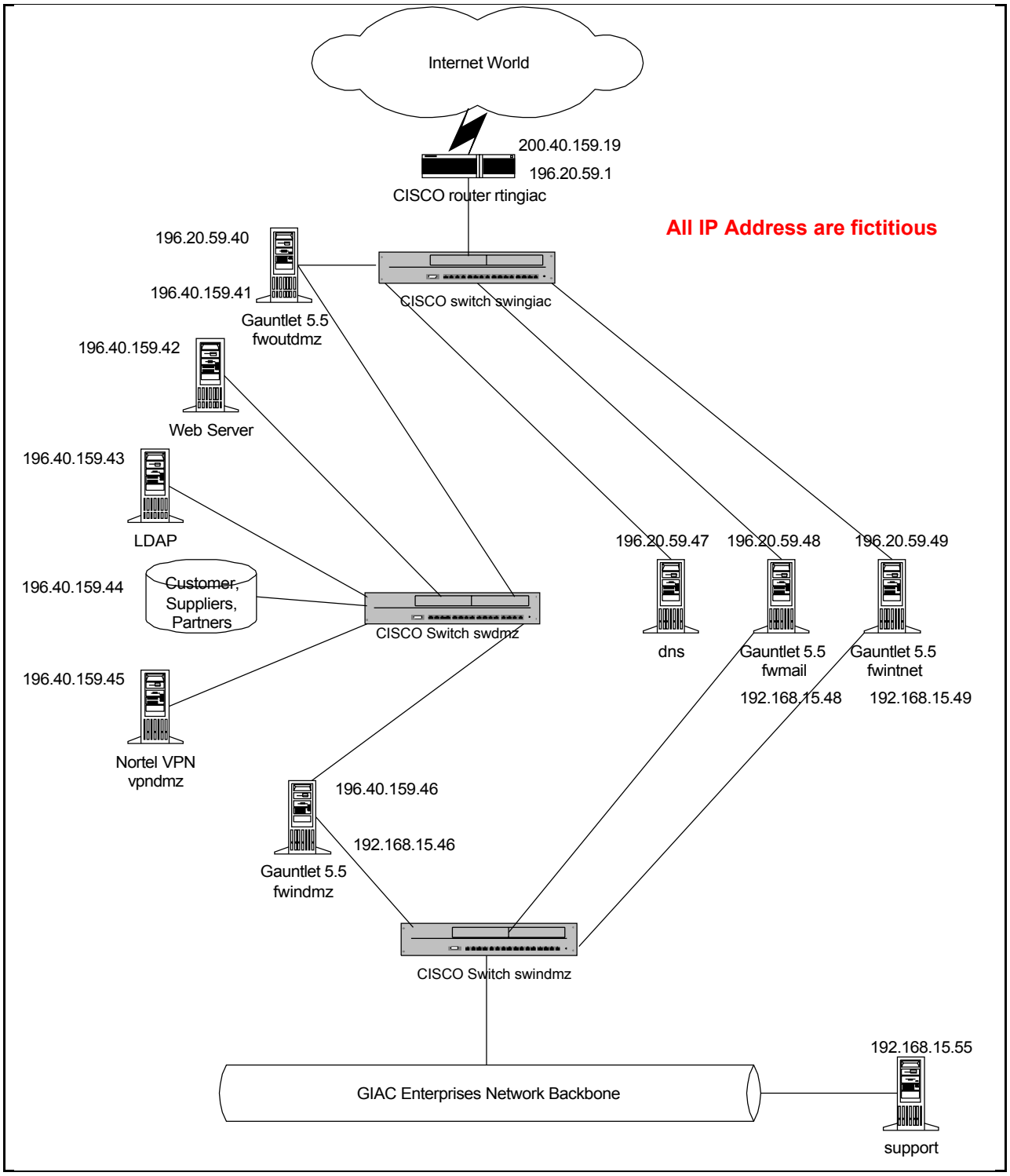
Secure Remote Access

There are several types of secure remote access. Remote partner access is handled by the partner VPN and SSL to the Web server. Customer and Supplier secure remote access is handled by SSL to the Web server. Employee secure remote access is handled by using the Partner VPN and SSL to the Web server. Support analyst secure remote access is handled by SSH.

Security Policy

With all of that hardware we must be secure? Right! Well, the equipment and the staff implementing the hardware are as good as the Security Policy. GIAC Enterprises has a standard policy that outlines how to configure the perimeter hardware, which is above. In addition to perimeter protection, procedures for the following topics: 1. All company computers should have antivirus software. 2. Examples of good passwords are used. 3. Directions on how to use passive FTP because active FTP is not allowed. 4. An Authorize use statement is also included. 5. The punishment for misuse of the hardware and software is specified. 6. Apply updates/patches to workstation and server software. 7. Company computers are close systems and should only contain company issued software. 8. All VPN clients used by Partners should be company supported, which in this case is Nortel VPN Client.

Picture 1



Assignment 2

Overview of Tutorials

Three tutorials are listed below. The tutorials explain how to create rules, ACL, and filters for implementing a security policy on GIAC Enterprises' border router, VPN, and firewall.

Border Router Tutorials

Concepts

- Creating a standard access group with number (0 – 99) of defined access list and in/out parameters which indicate the direction the filter should be tested
- Creating an access list and associate it with an access group
- Keyword permit means to allow
- Keyword deny means not to allow
- Keyword any means match any IP address
- When using access list wildcards, modify the wildcard from left to right, for example 0.0.0.255 means to match the first three octets of the IP address, and 0.0.255.255 means match the first two octets of the IP address
- Remember you get one access list per interface per direction

Using the Command Line Interface and above concepts in configuration mode, we can create ACL similar to the following:

1. Interface Ethernet 0 - Determine the interface for filter
   ip address your_ip_address your_subnet_mask - Address of Ethernet 0 and the subnet mask
   ip access-group number_between_0-99 in/out - Group number and checking in or out checking

2. access_list number_from_access-group permit/deny ip_address/wildcard

Gauntlet Tutorials

The Gauntlet Tutorial does NOT contain actual rules for GIAC Enterprises. The tutorial discusses how to add objects, rules, and packet filters.

Gauntlet is an application proxy firewall. A proxy takes the place of a service (telnet, http, etc) and accepts request then passes them to the other side of the firewall. This action prevents programs on one side from talking directly to a program on the other side of the firewall.

Prior to creating any Gauntlet source or destination rules, a Network object must be created.

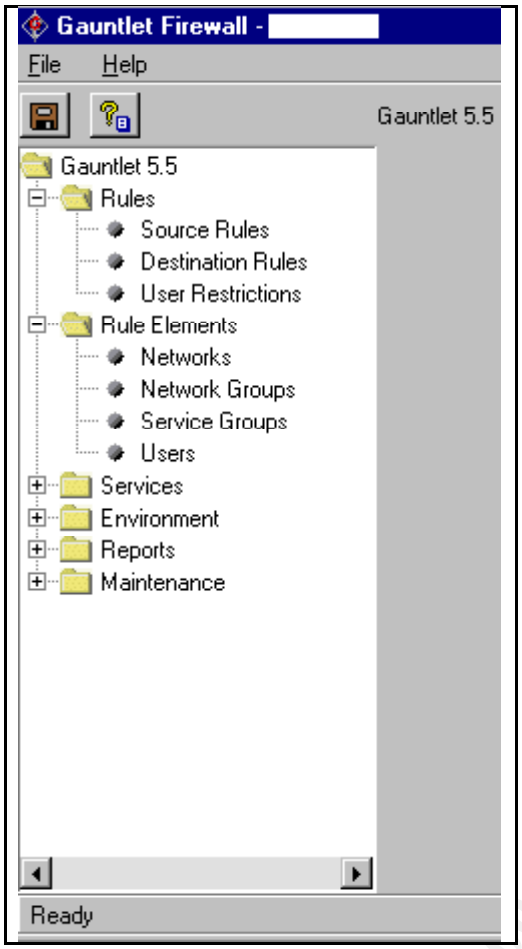
To make administration easier, Network Group objects can be created to group similar network objects, and Service Group objects can be created to group similar service objects. Visualize group objects like filing cabinets.

A network object can contain a single IP or a group of IPs.

A service object can contain a single service or a group of services.

When invoking the Gauntlet GUI, Secure ID is used for authentication. When the GUI is opened, the default screen, Picture 1, is displayed

Picture 1



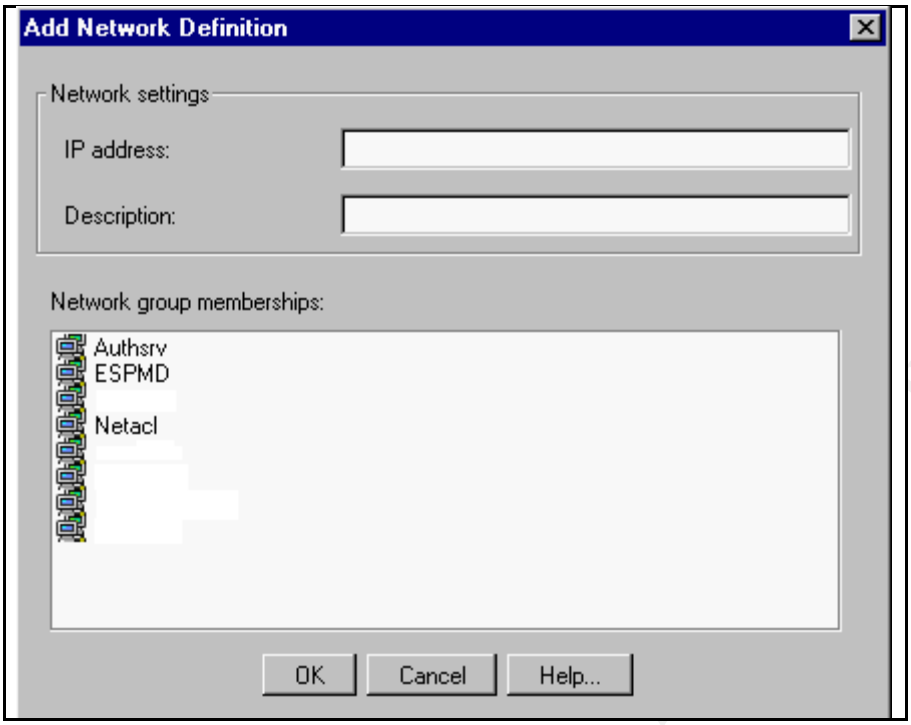
If you want to add a Network Object complete the following steps:

- Using Picture 1, single click on the Networks item under the Rule Elements area
- Single click the Add button
- Picture 2 will appear

Follow the steps below to fill in the screen displayed in Picture 2. The steps do not have to be completed in the listed order.

- Input IP address – can be single IP or something like 192.* for range
- Input Description - not required but a good practice
- Select a group – the group the IP is associated with
- Click the OK button when done

Picture 2



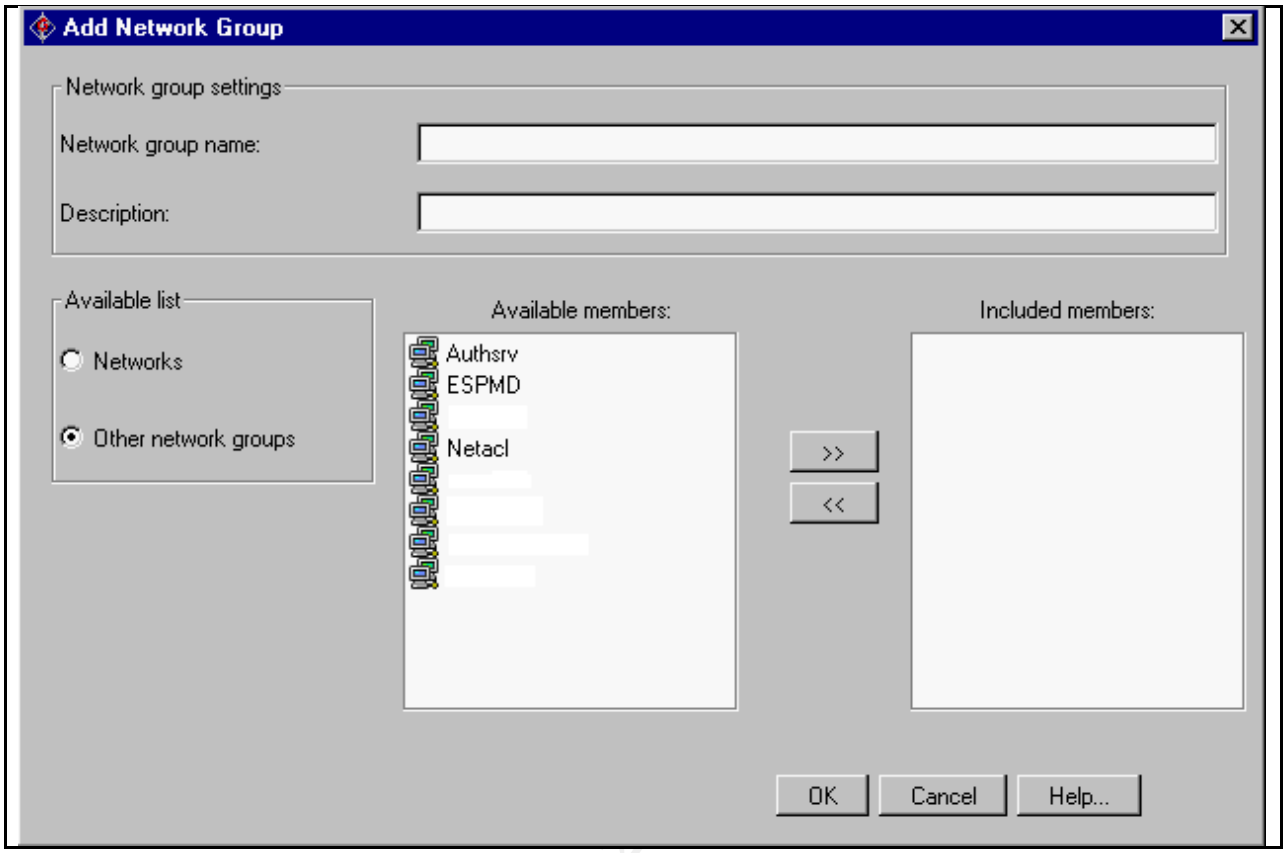
If you want to add a Network Group complete the following steps:

- Using Picture 1, single click on the Network Groups item under the Rule Elements area
- Single click the Add button
- Picture 3 will appear

Follow the steps below to fill in the screen displayed in Picture 3. The steps do not have to be completed in the listed order.

- Input Network group name – in the future, will show up in the Available member section
- Input Description - not required but a good practice
- Select Available list – select from groups or single IPs
- Select Available member – member you wanted included in new group
- Click on ">>" button - to place Available member in Included members section
- Click the OK button when done

Picture 3



If you want to add a Service Group complete the following steps:

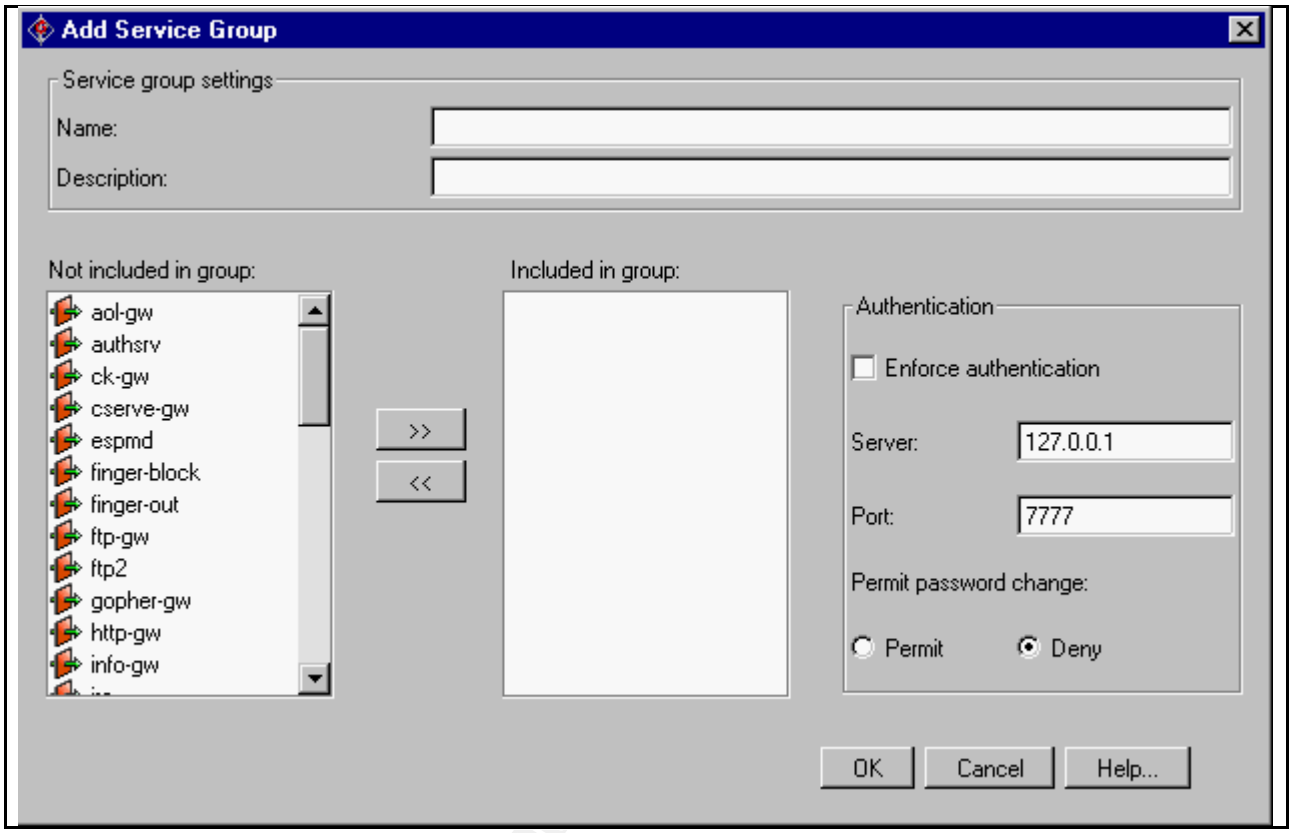
- Using Picture 1, single click on the Service Groups item under the Rule Elements area
- Single click the Add button
- Picture 4 will appear

Follow the steps below to fill in the screen displayed in Picture 4. The steps do not have to be completed in the listed order. Several predefined Services are provided with the software. If a Service is not provided and it uses TCP, you may create a plug proxy. If a Service is not provided and it uses UDP, you may create a packet filter.

- Input Service name – in the future, will show up in the Available member section
- Input Description - not required but a good practice
- Highlight service in Not included in group window
- Click on >> button - to place Available member in Included members section
- Click the OK button when done
- Enforce authentication – check this option when you want to

authenticate a user prior to allowing use of a service group

Picture 4



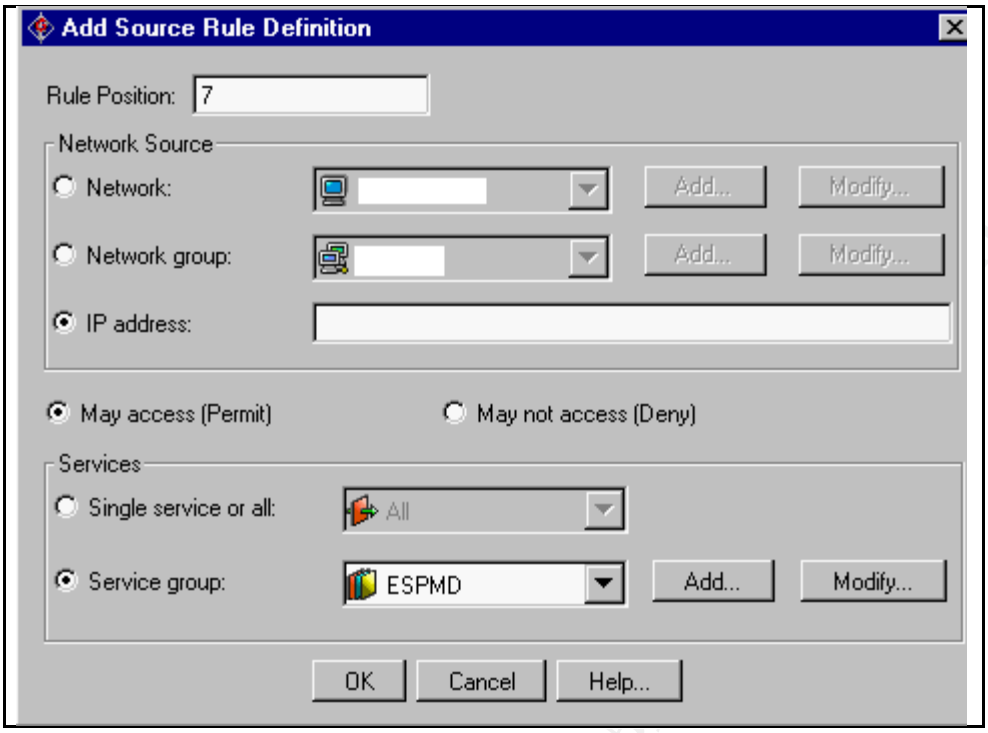
If you want to add Source Rules complete the following steps:

- Using Picture 1, single click on the Source Rules under the Rules area
- Single click on the Add button
- Picture 5 will appear

Follow the steps below to fill in the screen displayed in Picture 5. The steps do not have to be completed in the listed order.

- Enter rule position - the rule will be place in this position in the list
- Select Network Source - can be single network, group of networks, or single IP
- Select May access or May not access – may access will allow the rule to be used and may not access will not allow the rule to be used
- Select Services – can be a single service or a group of services
- Click the OK button when done

Picture 5



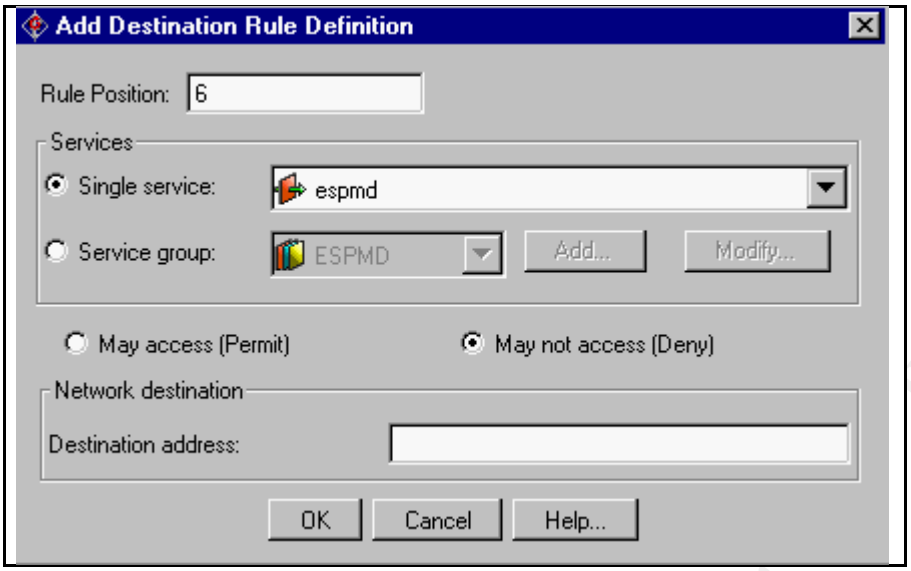
If you want to add Destination Rules complete the following steps:

- Using Picture 1, single click on the Destination Rules under the Rules area
- Single click on the Add button
- Picture 6 will appear

Follow the steps below to fill in the screen displayed in Picture 6. The steps do not have to be completed in the listed order.

- Enter rule position - the rule will be place in this position in the list
- Select Services – can be a single service or a group of services
- Select May access or May not access – may access will allow the rule to be used and may not access will not allow the rule to be used
- Select Network Destination - can be single IP, 207.* for range , or * (wildcard for anything)
- Click the OK button when done

Picture 6



Now that the objects and rules have been created, you can single click on File (use Picture 1) then single click Save to save and apply changes to the firewall.

Unlike Gauntlet source or destination rules, Packet filters do NOT require creating a Network object. Also, Packet filters do NOT have the security that proxies, which are used when building source or destination rules, do.

A packet filter rule is primarily used when there is no proxy available and for speed.

Follow the steps below to create a packet filter:

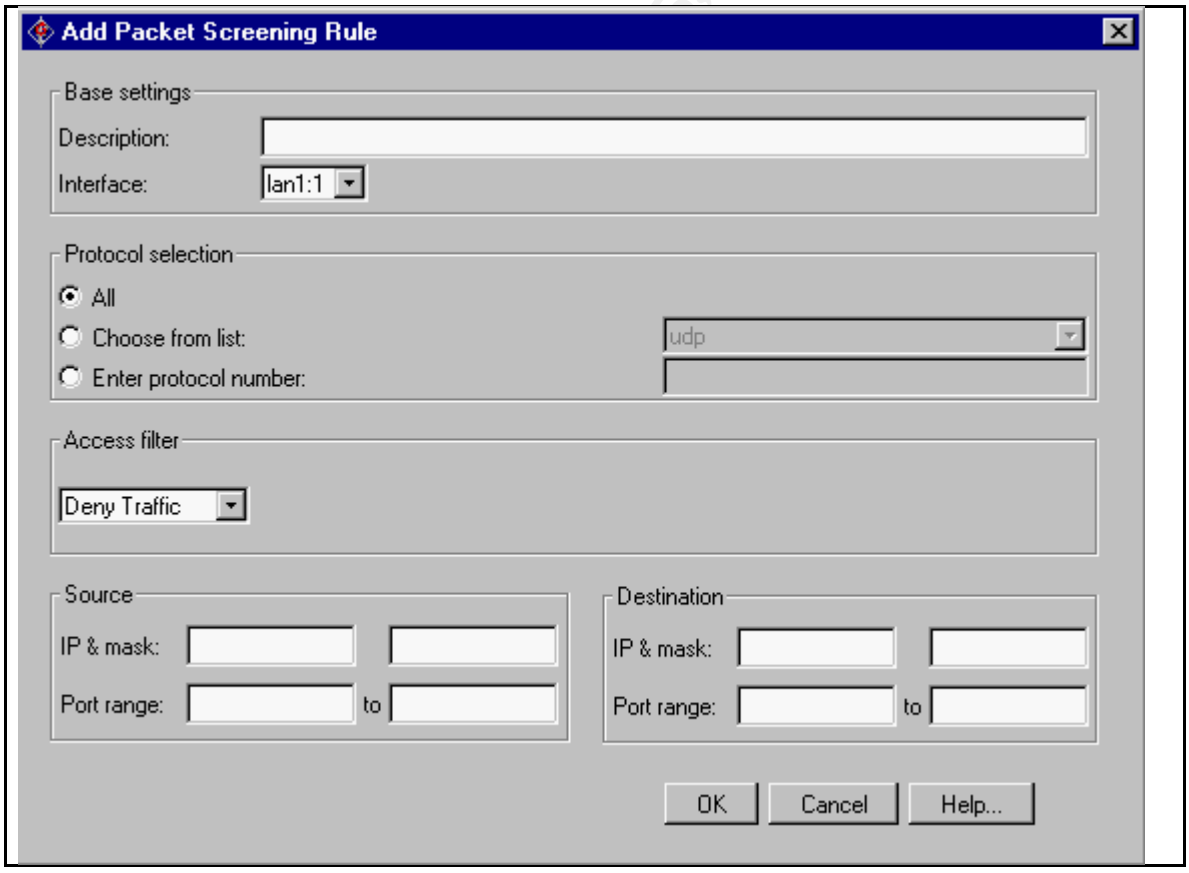
- Using Picture 1, single click on the Fwd Filter Rules under the Environment area – You can create local pack filters – rules destine to the firewall itself, or forward pack filters – rules destine for any host other than the firewall, pack filter rules
- Single click on the Add button
- Picture 7 will appear

Follow the steps below to fill in the screen displayed in Picture 7. The steps do not have to be completed in the listed order.

- Enter Description – not required but a good practice
- Select Interface – interface to apply rule to
- Select Protocol – any, UDP, TCP, ICMP, or protocol number
- Select one of the following Access Filter

    - Deny Traffic – drop and log packet
    - Forward Traffic – deliver the packet to its destination
    - Absorb Traffic – accepts the packet as if it were meant for the firewall and then the service proxy rule is applied, generally used for transparency
    - Forward w/Replies – is just what it says, it delivers the packet to its destination and allows the reply to return to the source, can only be used with UDP and TCP
- Source
    - IP and mask – this is the source IP and net mask of the source
    - Port ranges – numbers or wildcards
- Destination
    - IP and mask – this is the destination IP and net mask of the source
    - Port ranges – numbers or wildcards
- Click the OK button when done

Picture 7



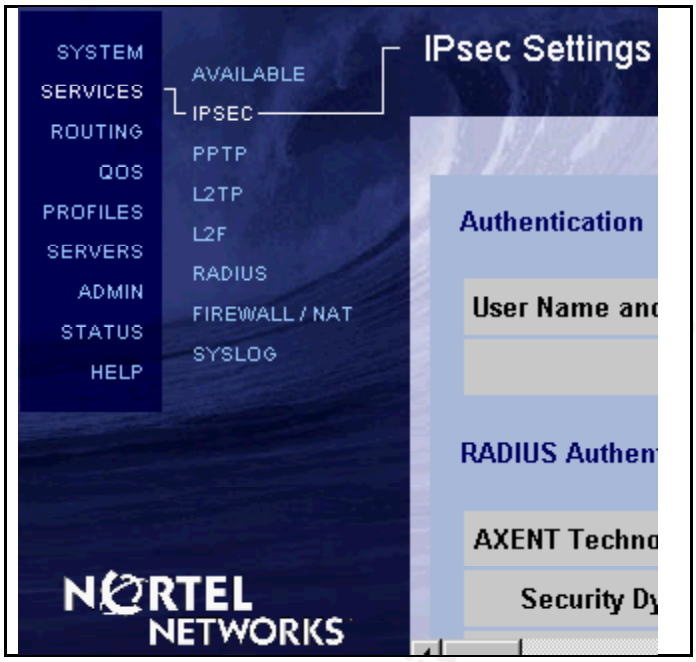
VPN Tutorials

The VPN Tutorial does contain actual IPSec configuration values. The tutorial discusses how to configure IPSec and Contivity Filters.

Prior to creating any Nortel tunnel, we must configure a VPN Protocol.

When the Nortel Administration screen is opened, a screen similar to Picture 8 is displayed. The main navigation for the GUI is listed on the left.

Picture 8

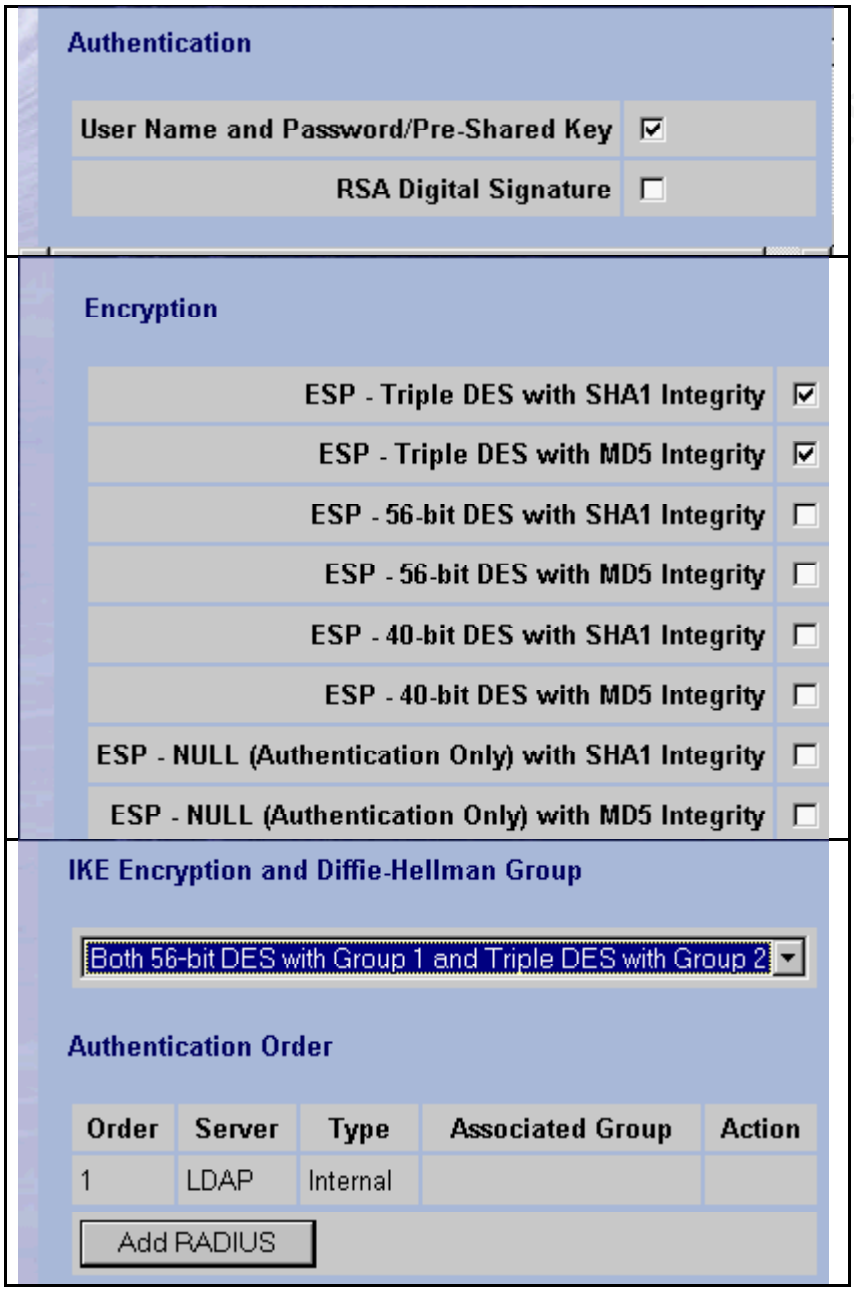


We have selected IPSec for our protocol. To configure, complete the following steps:

- Click on Services in Picture 8
- Click on IPSec

- A screen similar to Picture 9 will appear, omitted are the sections not used
- Click User Name and Password/Pre-Shared Key
- Click ESP – Triple DES with SHA1 Integrity
- Click ESP – Triple DES with MD5 Integrity
- For IKE Encryption, select 56-bit DES with Group1 and Triple DES with Group2
- LDAP is used for authentication

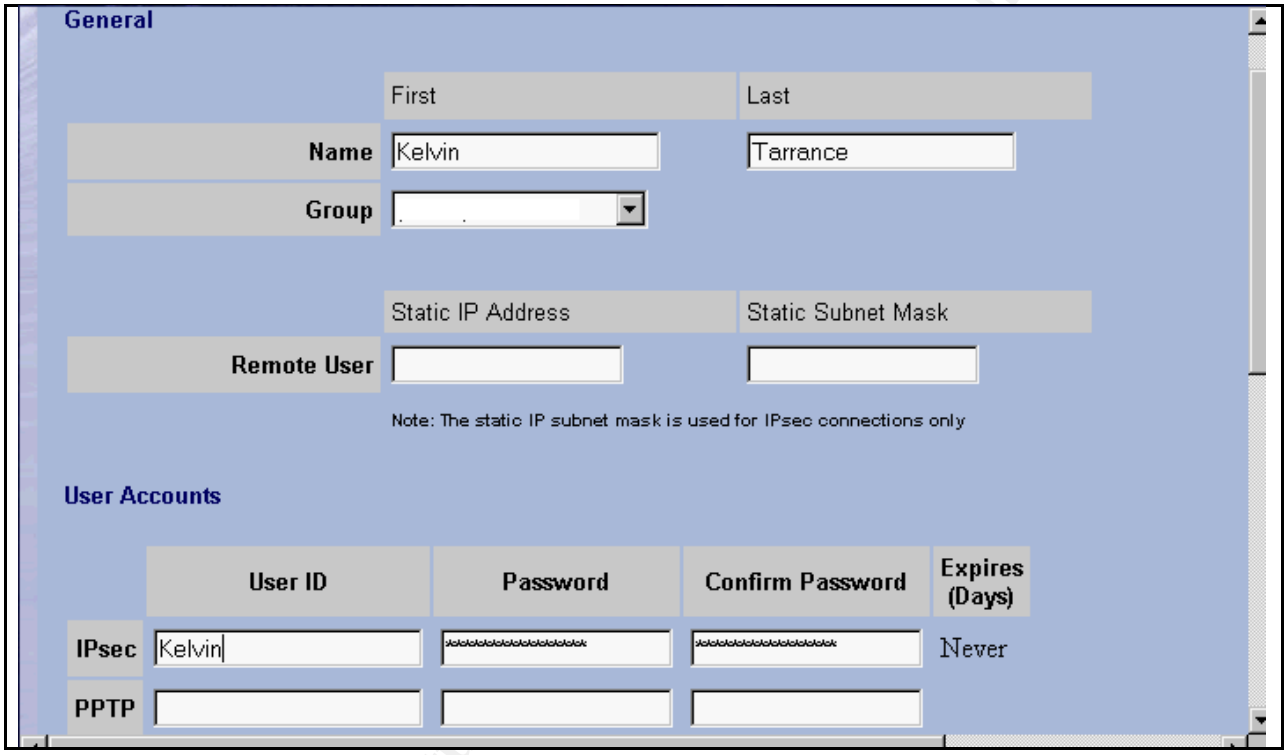
Picture 9



Configure the following Nortel VPN users options: To see what the options are, complete the following steps:

- Click on Profiles in Picture 8
- Click on Profiles then click Users
- A screen similar to Picture 10 will appear

Picture 10



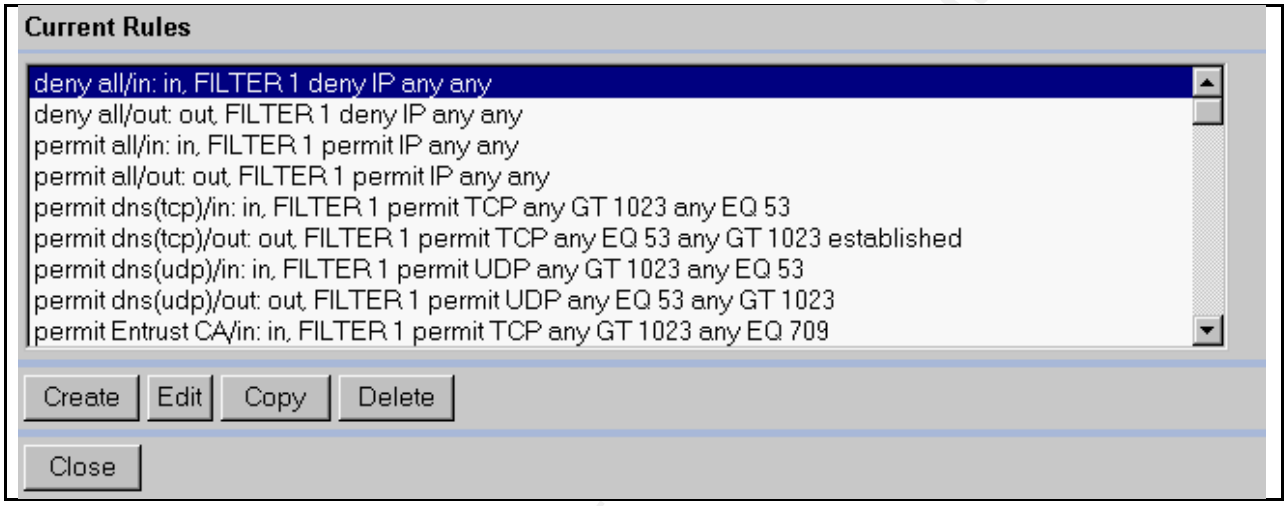
- Name: Enter first and Last
- Group: Select the group the person belongs to
- Static IP Address: If you want the person to receive a static internal IP when they enter the network, assign it here
- Static Subnet Mask: If you enter the static IP, you must enter the static subnet mask
- IPSec: Enter IPSec ID and password, VPN will prompt for these credentials when attempting to connect

The Nortel VPN comes with more default filters and tunnels than GIAC needs. For better security, we need to delete a few of them. To modify them, complete the following steps:

- Click on Profiles in Picture 8

- Click on Filters
- A screen with a Current Contivity Tunnel Filter selection box and Contivity Interface Filter selection box will appear
- To modify the filters, click on Manage Rules under the appropriate selection box
- A screen similar to Picture 11 will appear
- Select the entry to delete and click the Delete button

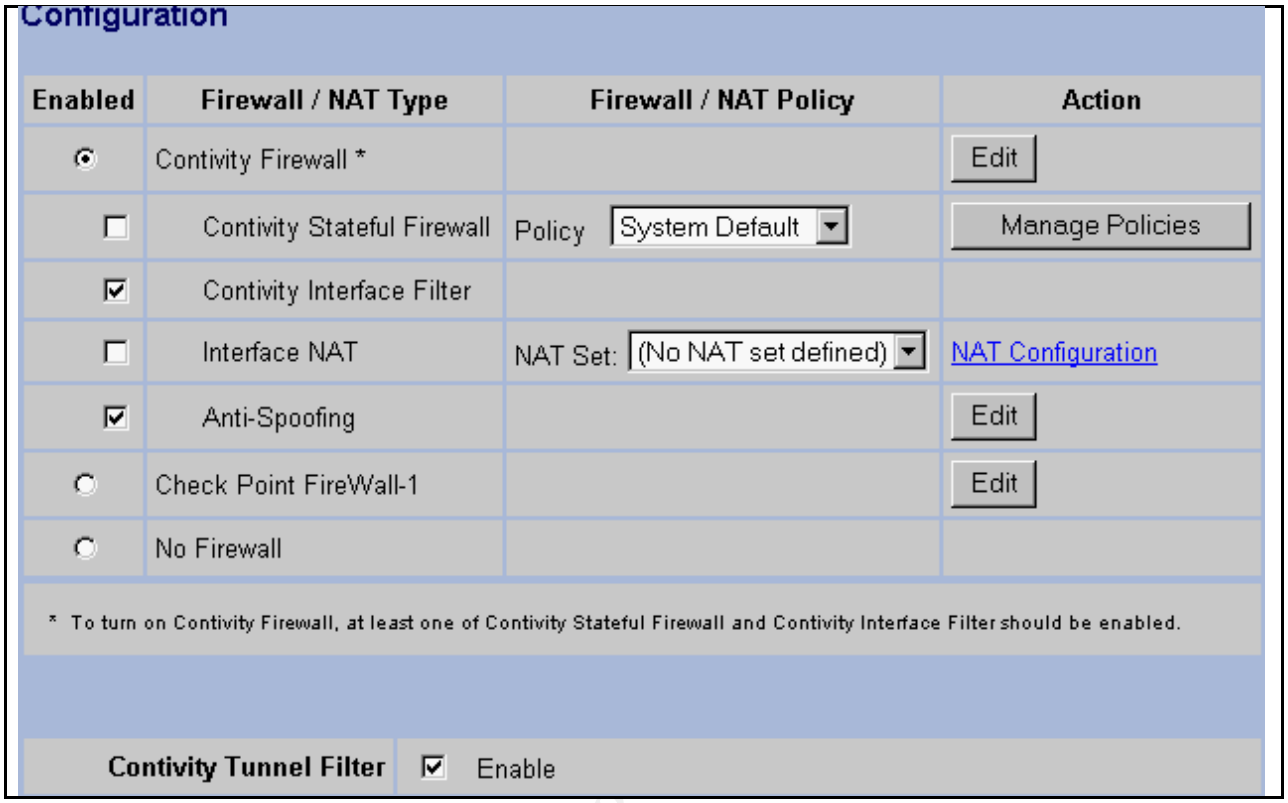
Picture 11



The Nortel VPN has several access options to select from: To see what the options are, complete the following steps:

- Click on Profiles in Picture 8
- Click on Services then click Firewall/NAT
- A screen similar to Picture 12 will appear
- Select whatever options you want to configure
- Click OK when you are finished
- Clicking on Edit for any option will allow more detailed configuration of that option
- Clicking Manage Policies for the Stateful Firewall will allow the Firewall policies to be managed. The version of the JVM (1.3) used by Nortel in this software version is required.

Picture 12



A few important notes to remember about the access options in Picture 12:

- The Contivity Interface Filter and Contivity Tunnel Filter or the Contivity Stateful Firewall must be selected
- If either the Contivity Interface Filter or Contivity Tunnel Filter is selected, the other must be selected
- The Contivity Interface Filter and Contivity Tunnel Filter can be selected without the Contivity Stateful Firewall
- The Contivity Stateful Firewall can be selected without the Contivity Interface Filter and Contivity Tunnel Filter
- All three can be selected and in fact, this is usual until the Stateful Firewall is configured, once the Firewall is configured, the Contivity Interface Filter and Contivity Tunnel Filter can be turned off
- Changing from the Contivity Stateful Firewall to the Contivity Interface Filter and Contivity Tunnel Filter will require the VPN to be rebooted

Overview Rule, Filter, and ACL

Border Router

When the router is set up, everything is allowed. When the first ACL filter is added, the router will deny anything that is not explicitly allowed. All packets are tested as they enter the router thus saving valuable CPU resources. The ACLs are processed in sequential order from one to N

Gauntlet Firewall

All traffic is denied unless explicitly allowed. The source, destination, and packet filter rules are processed in sequential order from one to N. Any unwanted ports found on the firewall will be blocked using a local packet filter.

Nortel VPN

All traffic passes through the VPN based on the Contivity Interface Filter and Contivity Tunnel Filter. By default, the last rule in each filter is denid, but it is not listed.

Border Router ACL and Descriptions

Because a routers primary job is to route traffic, GIAC Enterprises is using Standard access list. This option provides us the greatest routing speed, but not as much security as the Extended access list. Therefore, our access list are simple dealing only with IP spoofs and a few global settings.

GIAC's router does not send out learned entries onto the Internet, which would require a Split Horizon rule.

Configuring a few global settings.

Disable redirects

```
no ip redirects
```

Disable source routing

```
no ip source-route
```

Disable running Cisco Discovery Protocol (CDP)

```
no cdp run
no cdp enable
```

Disable finger

```
no service finger
```

Enable password encryption

```
service password-encryption
```

Disable direct broadcast

```
no ip direct-broadcast
```

Disable small services

```
no service udp-small-servers
no service tcp-small-servers
```

Disable http

```
no ip http server
```

Disable bootp

```
no ip bootp server
```

Disable ICMP unreachables messages

```
no ip unreachables
```

Disable proxy arp

```
no ip proxy-arp
```

Egress filtering

Interface Ethernet 0

```
ipaddress 196.20.59.1 255.255.255.0
ip access-group 13 in
```

Allow anything from internal

```
access-list 13 permit 196.40.159.0 0.0.0.255
access-list 13 permit 196.20.59.0 0.0.0.255
```

Deny spoofed address

```
access-list 13 deny any 127.0.0.0 0.255.255.255
access-list 13 deny any 192.168.0.0 0.0.255.255
access-list 13 deny any 172.16.0.0 0.15.255.255
access-list 13 deny any 10.0.0.0 0.255.255.255
access-list 13 deny any 224.0.0.0 31.255.255.255
access-list 13 deny host 0.0.0.0
```

Deny anything no allowed above, placed here for future logging
access-list 13 deny any

Ingress filtering

Interface Serial 0
ipaddress 200.40.159.19 255.255.255.0
ip access-group 15 in

Deny spoofed address
access-list 15 deny 196.20.59.0 0.0.0.255
access-list 15 deny 196.40.159.0 0.0.0.255
access-list 15 deny any 127.0.0.0 0.255.255.255
access-list 15 deny any 192.168.0.0 0.0.255.255
access-list 15 deny any 172.16.0.0 0.15.255.255
access-list 15 deny any 10.0.0.0 0.255.255.255
access-list 15 deny any 224.0.0.0 31.255.255.255
access-list 15 deny host 0.0.0.0

Allow anything else to GIAC Enterprises
access-list 15 permit any

Gauntlet Rules and Descriptions

Each Gauntlet Firewall has two identical rules: 1. ESPMD allows client GUI software to make secure connections to the firewall, and 2. Netacl allows the capabilities of a TCP wrapper for local services.

All services used are application proxy except ssl-gw, ssh, any packet filters, and the http plug using adaptive proxy.

Refer to the Gauntlet Tutorial for procedures on how to add rules.

Rules for every Firewall

OS Configurations
- DNS configurations are completed through the gauntlet-admin program
- Static routes are completed through the gauntlet-admin program

Network Objects
- Create Networks Object 192.168.15.* GIAC private addresses

- Create Networks Object 127.0.0.1 for local host
- Create Networks Object Any (containing *) for anyone - Note: * is wildcard

- Create Networks Object 192.168.15.10 support analyst IP – Kelvin - Note: Add as many support IP as needed

Network Group
- Create Network Group ESPMD GIAC private IPs with access from GUI
- Create Network Group Netacl localhost IPs
- Create Network Group GIAC GIAC private IPs
- Create Network Group Support Web all support analysts IPs
- Create Network Group Support Connect all support analysts IPs

Service Group
- Note: DENY password word change in Service Group configuration
- Create Services Group ESPMD espmd service for GUIs
- Create Services Group Netacl netacl-telnet-d for local telnet
- Create Services Group Authsrv authsrv service for local authentication
- Create Services Group Support Web http-gw, ssl-gw for support analysts
- Create Services Group Web http-gw, ssl-gw for non-support employees
- Create Services Group Support Connect ssh, tn-gw for support analysts, BIND the telnet proxy and SSH plug to the internal IP address

Users
- Create support users for access to firewall and select secure ID for authentication method

Source Rules – Order is important
1. Create Source Rule for ESPMD – allows GUI access to firewall
    - Rule Position = 1
    - Network Group = ESPMD
    - Select May access (Permit)
    - Select Service group = ESPMD
2. Create Source Rule for Netacl – allows local access and wraps TCP

connections
- Rule Position = 2
- Network Group = Netacl
- Select May access (Permit)
- Select Service group = Netacl

3. Create Source Rule for Authsrv – allows local authentication to firewall
   - Rule Position = 3
   - Network Group = Authsrv
   - Select May access (Permit)
   - Select Service group = Authsrv
4. Create Source Rule for Support Connect – allows members of Support Connect network group access to define services in Support Connect service group
   - Rule Position = 4
   - Network Group = Support Connect
   - Select May access (Permit)
   - Select Service group = Support Connect

Destination Rules – Order is Important

1. Create Destination Rule for Support Connect - allows defined services in Support Connect service group connection to any location
   - Rule Position = 1
   - Service Group = Support Connect
   - Select May access (Permit)
   - Destination address = *

Other Configuration

- Load SSH on the firewall and configure it to listen to the internal IP address of each firewall. Do NOT block SSH connections to the firewall.

Rules for fwintnet

Source Rules – Order is important

5. Create Source Rule for Web – allows members of GIAC network group access to define services in Web service group
   - Rule Position = 5
   - Network Group = GIAC
   - Select May access (Permit)
   - Select Service group = Web

Destination Rules

2. Create Destination Rule for Web - allows defined services in Web service group connection to any location
    - Rule Position = 2
    - Service Group = Web
    - Select May access (Permit)
    - Select Destination address = *

Other Configuration (exception for fwintnet ONLY)

- Load SSH on the firewall and configure it to listen to * address of each firewall. Do NOT block SSH connections to the firewall.

Log Traffic

SSH Traffic coming from the Internet to fwintnet
Jun 26 15:43:51 fwintnet sshd[26843]: User kelvin, coming from hostname.happy.com, authenticated.

SSL Traffic leaving GIAC going to the Internet
Jun 28 13:41:42 fwintnet http-gw[20079]: permit host=nodnsquery/192.168.15.60 use of ssl proxy, mode=Proxy
Jun 28 13:41:42 fwintnet http-gw[20079]: permit host=nodnsquery/192.168.15.60 destination=www.hypersend.com/216.29.193.230 port=443, mode=Proxy
Jun 28 13:41:42 fwintnet http-gw[20079]: permit host=nodnsquery/192.168.15.60 destination=www.hypersend.com port=443, mode=Proxy

HTTP Traffic leaving GIAC going to the Internet
Jun 26 15:45:34 fwintnet http-gw[2676]: exit host=nodnsquery/192.168.15.60 cmds=1 in=198 out=0 user=unauth duration=0, mode=Proxy
Jun 26 15:45:34 fwintnet http-gw[2685]: permit host=nodnsquery/192.168.15.60 use of proxy, mode=Proxy
Jun 26 15:45:34 fwintnet http-gw[2672]: exit host=nodnsquery/192.168.15.60 cmds=1 in=2937 out=0 user=unauth duration=0, mode=Proxy

Rules for fwmail

Service Group

- Create Services Group Mail smap, smapd service accepting and processing mail, sendmail does NOT directly interact with incoming mail

Source Rules – Order is important

5. Create Source Rule for Mail – allows members of Any network group access to define services in Mail service group
    - Rule Position = 5

- Network Group = Any
- Select May access (Permit)
- Select Service group = Mail

Destination Rules – Order is Important

2. Create Destination Rule for Mail Web - allows defined services in Mail service group connection to any location
   - Rule Position = 2
   - Service Group = Mail
   - Select May access (Permit)
   - Select Destination address = *

Log Traffic

Mail coming from the Internet to GIAC

```
Jul 12 15:17:11 fwmail smap[18214]: host=unknown/63.89.85.28 bytes=60127
from=<name@happy.com> to=<name@giac.com> file=xma018214
Jul 12 15:17:11 fwmail smap[18214]: exiting host=unknown/63.89.85.28 bytes=60127
```

Rules for fwoutdmz

Service Group

- Note: DENY password word change in Service Group configuration
- Create Services Group DMZ Web http plug and the ssl-gw plug using adaptive proxy

Source Rules – Order is important

There is NO 3B rule, 3B simply means that this rule would be rule number 4 when applying the general rules to this firewall and general rule 4 would become rule number 5.

3B. Create Source Rule for DMZ Web– allows members of Any network group access to define services in DMZ Web service group
   - Rule Position = 3B
   - Network Group = Any
   - Select May access (Permit)
   - Select Service group = DMZ Web

Destination Rules – Order is Important

2. Create Destination Rule for DMZ Web - allows defined services in DMZ Web service group connection to any location
   - Rule Position = 2
   - Service Group = DMZ Web
   - Select May access (Permit)

- Select Destination address = 196.40.159.42

Packet Filters – Order is Important

1. Create Packet Filter for IPSec Key Exchange
   - Description IPSec
   - Interface lan0
   - Protocol selection udp, Choose from list
   - Access filter Forward Traffic
   - Source IP 0.0.0.0
   - Source IPMask 0.0.0.0
   - Port range 500 to 500
   - Destination IP 196.40.159.45
   - Destination IPMask 255.255.255.255

2. Create Packet Filter for IPSec Key Exchange
   - Description IPSec
   - Interface lan1
   - Protocol selection udp, Choose from list
   - Access filter Forward Traffic
   - Source IP 196.40.159.45
   - Source IPMask 255.255.255.255
   - Port range 500 to 500
   - Destination IP 0.0.0.0
   - Destination IPMask 0.0.0.0

3. Create Packet Filter for IPSec Data Exchange
   - Description IPSec
   - Interface lan0
   - Protocol selection 50, Enter protocol number
   - Access filter Forward Traffic
   - Source IP 0.0.0.0
   - Source IPMask 0.0.0.0
   - Port range * to *
   - Destination IP 196.40.159.45
   - Destination IPMask 255.255.255.255

4. Create Packet Filter for IPSec Data Exchange
   - Description IPSec
   - Interface lan1
   - Protocol selection 50, Enter protocol number
   - Access filter Forward Traffic

- Source IP 196.40.159.45
- Source IPMask 255.255.255.255
- Port range * to *
- Destination IP 0.0.0.0
- Destination IPMask 0.0.0.0

Log Traffic
HTTP Traffic coming from the Internet to GIAC DMZ
Jun 28 13:55:15 fwoutdmz http[26643]: permit host=nodnsquery/34.38.126.139 use of proxy ID=26643811192
Jun 28 13:55:15 fwoutdmz http[26643]: permit destination 196.40.159.42/80 ID=26643811192
Jun 28 13:55:15 fwoutdmz http[26627]: exit host=nodnsquery/209.137.60.146 cmds=0, in=248, out=2043, duration=0, mode=Packet ID=26627846910
Jun 28 13:55:15 fwoutdmz http[26643]: permit host=nodnsquery/209.137.60.146 use of proxy ID=26643811193
Jun 28 13:55:15 fwoutdmz http[26643]: permit destination 196.40.159.42/80 ID=26643811193
Jun 28 13:55:15 fwoutdmz http[26643]: permit host=nodnsquery/209.137.60.146 use of proxy ID=26643811194
Jun 28 13:55:15 fwoutdmz http[26643]: permit destination 196.40.159.42/80 ID=26643811194

SSL Traffic coming from the Internet to GIAC DMZ
Jul 3 14:20:01 fwoutdmz ssl-gw[26601]: exit host=nodnsquery/63.212.99.30 cmds=0, in=672, out=258, duration=0, mode=Packet ID=26601104452
Jul 3 14:20:02 fwoutdmz ssl-gw[26620]: permit host=nodnsquery/171.155.133.187 use of proxy
ID=26620100620
Jul 3 14:20:02 fwoutdmz ssl-gw[26620]: permit destination 196.40.159.42/443 ID=26620100620
Jul 3 14:20:02 fwoutdmz ssl-gw[26606]: exit host=nodnsquery/63.212.99.30 cmds=0, in=668, out=258, duration=1, mode=Packet ID=26606106510

IPSec Traffic coming from the Internet to GIAC DMZ
Jun 28 14:20:54 fwoutdmz http[26590]: exit host=nodnsquery/133.1.1.10 cmds=0, in=500, out=153, duration=0, mode=Packet ID=26590848579
Jun 28 14:20:54 fwoutdmz http[26638]: exit host=nodnsquery/133.1.1.10 cmds=0, in=500, out=153, duration=0, mode=Packet ID=26638832861
Jun 28 14:20:55 fwoutdmz http[26592]: exit host=nodnsquery/133.1.1.10 cmds=0, in=500, out=153, duration=0, mode=Packet ID=26592860083

Note: Unable to capture all of VPN trace but was successful at the VPN. See VPN log section below.

Rules for fwindmz

Source Rules – Order is important
5. Create Source Rule for Support Web – allows members of Support Web

network group access to define services in Support Web service group

- Rule Position = 5
- Network Group = Support Web
- Select May access (Permit)
- Select Service group = Support Web

6. Create Source Rule for Web – allows members of GIAC network group access to define services in Web service group

- Rule Position = 6
- Network Group = GIAC
- Select May access (Permit)
- Select Service group = Web

Destination Rules – Order is Important

2. Create Destination Rule for Support Web - allows defined services in Support WEB service group connection to specific IP

- Rule Position = 2
- Service Group = Support Web
- Select May access (Permit)
- Select Destination address = 196.40.159.42

3. Create Destination Rule for Web - allows defined services in Web service group connection to specific IP

- Rule Position = 3
- Service Group = Web
- Select May access (Permit)
- Select Destination address = 196.40.159.42

Packet Filters – Order is Important

1. Create Packet Filter for IPSec Key Exchange

- Description IPSec
- Interface lan1
- Protocol selection udp, Choose from list
- Access filter Forward Traffic
- Source IP 192.168.15.*
- Source IPMask 255.255.255.0
- Port range 500 to 500
- Destination IP 196.40.159.45
- Destination IPMask 255.255.255.0

2. Create Packet Filter for IPSec Key Exchange
   - Description IPSec
   - Interface lan0
   - Protocol selection udp, Choose from list
   - Access filter Forward Traffic
   - Source IP 196.40.159.45
   - Source IPMask 255.255.255.255
   - Port range 500 to 500
   - Destination IP 192.168.15.*
   - Destination IPMask 255.255.255.0

3. Create Packet Filter for IPSec Data Exchange
   - Description IPSec
   - Interface lan1
   - Protocol selection 50, Enter protocol number
   - Access filter Forward Traffic
   - Source IP 192.168.15.*
   - Source IPMask 255.255.255.0
   - Port range * to *
   - Destination IP 196.40.159.45
   - Destination IPMask 255.255.255.255

4. Create Packet Filter for IPSec Data Exchange
   - Description IPSec
   - Interface lan0
   - Protocol selection 50, Enter protocol number
   - Access filter Forward Traffic
   - Source IP 196.40.159.45
   - Source IPMask 255.255.255.255
   - Port range * to *
   - Destination IP 192.168.15.*
   - Destination IPMask 255.255.255.0

Log Traffic
Note: The HTTP, SSL, SSH traffic would look like the traffic entering and leaving fwintnet and IPSec traffic would look like the traffic entering and leaving fwoutdmz. Unable to capture all of VPN trace but was successful at the VPN. See VPN log section below.

VPN Rules and Description

The VPN is initially configured with a bunch of filters like finger, dns, pcanywhere, ftp, gopher, nntp, snmp, entrust, netbios, etc. Using the Picture 10 in the VPN Tutorial we will delete all but the following Interface and Tunnel filter.

IMPORTANT NOTE: The VPN tutorial contains all of the actual settings for the VPN configuration. The rules are listed below are the only thing NOT accurate in the tutorial.

GIAC is using ESP to encrypt and authenticate. One reason is that adding AH would just be more overhead.

Allow IP protocol into and out of the VPN, this protocol offers a connectionless internetwork service

- Permit all/in: in, FILTER 1 permit IP any any
- Permit all/out: out FILTER 1 permit IP any any

Allow dns UDP queries into and out of the VPN for name resolution

- Permit dns(udp)/in: in, FILTER 1 permit UDP any GT 1023 any EQ 53
- Permit dns(udp)/out: out, FILTER 1 permit UDP any EQ 53 any GT 1023

Allows http request into and out of the VPN for Web browsing

- Permit http/in: in, FILTER 1 permit TCP any GT 1023 any EQ 80
- Permit http/out: out, FILTER 1 permit TCP any EQ 80 any GT 1023 established

Allows ICMP of the VPN

- Permit icmp/out: out, FILTER 1 permit ICMP any any

Allows IKE request out of the VPN for key exchange

- Permit IKE/out: out, FILTER 1 permit UDP any any EQ 500

Allows ldap request into and out of the VPN for authentication

- Permit ldap/in: in, FILTER 1 permit TCP any GT 1023 any EQ 389
- Permit ldap/out: out, FILTER 1 permit TCP any EQ 389 any GT 1023 established

Allows protocol 50 into the VPN for AH and ESP

- Permit PROTOCOL 50: in, FILTER 1 permit 50 any any
- Permit PROTOCOL 51: in, FILTER 1 permit 51 any any

Allows smtp request into and out of the VPN for sending mail

- Permit smtp/in: in, FILTER 1 permit TCP any GT 1023 any EQ 25
- Permit smtp/out: out, FILTER 1 permit TCP any EQ 25 any GT 1023 established

Denys anything not allowed

- Deny all/in: in, FILTER 1 deny IP any any
- Deny all/out: out, FILTER 1 deny IP any any

Note: If a VPN tunnel is established, changing the tunnel filter will not affect the existing connection.

VPN Log

Table 1

Requesting IPSec connection for Kelvin

Security [11] Session: IPSEC[Kelvin] attempting login
06/26/2001 11:11:18 0 Security [01] Session: IPSEC[Kelvin] has no active sessions
06/26/2001 11:11:18 0 ISAKMP [02] Oakley Aggressive Mode proposal accepted from Kelvin (66.4.0.56)
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 SHARED-SECRET authenticate attempt...
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 attempting authentication using LOCAL
06/26/2001 11:11:19 0 Security [11] Session: IPSEC[Kelvin]:108 authenticated using LOCAL
06/26/2001 11:11:19 0 Security [11] Session: IPSEC[Kelvin]:108 bound to group /Base/TEAM/Kelvin Tarrance
06/26/2001 11:11:19 0 Security [00] Account: 7d02438 BwmPolicy: commitedRate=56000 excessRate=128000 action: 0
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 client version 8 (Future Version (ID 8)), push action is: none

Passing connection through filters

06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 OUT FILTER 1 permit IP any any
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 IN FILTER 1 permit IP any any
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 IN FILTER 1 permit TCP any GT 1023 any EQ 53
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 IN FILTER 1 permit TCP any GT 1023 any EQ 53
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 80
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 RESTRICTED FILTER 1 deny TCP any EQ 257 any GT 1023
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 21
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 RESTRICTED FILTER 1 deny TCP any GT 1023 any EQ 20
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 RESTRICTED FILTER 1 permit IP any any
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 OUT FILTER 1 permit IP 66.4.0.56 0.0.0.0 any
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit TCP any GT 1023 any EQ 80
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit ICMP any any 8
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit ICMP any any 0
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit ICMP any any 11
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit ICMP any any 3
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit TCP any GT 1023 any EQ 17
06/26/2001 11:11:19 0 Security [01] Session: IPSEC[Kelvin]:108 LOCAL IN FILTER 1 permit TCP any GT 1023 any EQ 586

Establishing IPSec connection and Assigning Inside IP

06/26/2001 11:11:19 0 Security [11] Session: IPSEC[Kelvin]:108 authorized
06/26/2001 11:11:19 0 Security [12] Session: IPSEC[Kelvin]:108 physical addresses: remote 66.4.0.56 local 196.40.159.45
06/26/2001 11:11:19 0 Security [12] Session: IPSEC[Kelvin]:108 assigned IP address 196.40.159.250, mask 255.255.255.0
06/26/2001 11:11:19 0 ISAKMP [02] ISAKMP SA established with Kelvin (66.4.0.56)
06/26/2001 11:11:19 0 Security [12] Session: IPSEC[Kelvin]:108 physical addresses: remote 66.4.0.56 local 196.40.159.45

Assignment 3

Plan and Description of Audit

Use Picture 1 when reviewing this section.

Prior to starting our Audit, there are several housekeeping things we must do.

First, a meeting must be scheduled with the OS and Firewall personnel to inform them of the particulars of the Audit and discuss any concerns. Lastly, we must review the existing Security Policy to determine what results are expected.

The following components will be scanned using nmap. 1. fwoutdmz, 2. vpndmz, 3. fwindmz, 4. fwmail, and 5. fwintnet. We elected not to scan the gateway router because it is simply blocking spoofed packets and a few other global settings. The gateway router passes everything else through to the firewalls. This is NOT an error but an intentional design.

The Audit will be performed during the middle to late part of second shift (8:00 p.m.). One analyst will scan servers one night. The cost of the Audit will be one week of one analyst's time. The week will include planning, information gathering and exchange meetings, implementation, and writing the Audit report.

To prevent the risk of a real threat going unchecked, it is necessary to tell the OS and Firewall areas what time the scans will start and end. Because minimum work is completed on second shift, there should not be any reports of slow response time from customers, suppliers, or partners.

Prior to, during, or after the scans, the analyst is reviewing procedures and servers. The OS should be checked to make sure that it has actually been harden. Hardening may be identifying who has root access the server and who has logons to the server. Reviewing the backup incident response, escalation, problem resolution, etc. procedures. Actually review the rules on the firewall. Performing the above steps with GIAC's Security Policy in hand is one of the best ways to determine if requirements are being met.

Implementing the Assessment

Nmap commands used to scan all firewalls and Vpns for TCP

```
nmap -sS -O -v -P0 -p 1-65535 -oN /home/kelvin/filename host_IP
```

Nmap commands used to scan all firewalls and Vpns for UDP

nmap –sU -p 1-65535 -oN /home/kelvin/filename host_IP

The defined nmap options below are exact quotes from the nmap MAN pages.

-sS TCP SYN scan: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets.	-O This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtleties in the underlying operating system network stack of the computers you are scanning. It uses this information to create a 'fingerprint' which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file) to decide what type of system you are scanning.
-v Verbose mode. This is a highly recommended option and it gives out more information about what is going on. You can use it twice for greater effect. Use -d a couple of times if you really want to get crazy with scrolling the screen!	-P0 Do not try and ping hosts at all before scanning them. This allows the scanning of networks that don't allow ICMP echo requests (or responses) through their firewall. microsoft.com is an example of such a network, and thus you should always use -P0 or -PT80 when portscanning microsoft.com.
-p <port ranges> This option specifies what ports you want to specify. For example '-p 23' will only try port 23 of the target host(s). ports greater than 60000. The default is to scan all ports between 1 and 1024 as well as any ports listed in the services file which comes with nmap.	-oN write output in human readable form and write it to the specified file name.
-sU UDP scans: This method is used to determine which UDP (User Datagram Protocol, RFC 768) ports are open on a host. The technique is to send 0 byte udp packets to each port on the target machine. If we receive an ICMP port reachable message, then the port is closed. Otherwise we assume it is open.	

Scan of External DMZ Firewall (fwoutdmz)

# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 13:09:17 2001 as: nmap -sS -O -v -P0 -p 1-65535 -oN /home/kelvin/TCP_fwoutdmz 196.20.59.40 Interesting ports on host.domain.com (196.20.59.40): (The 65526 ports scanned but not shown below are in state: closed) Port State Service 22/tcp open ssh 23/tcp open telnet 80/tcp open http 113/tcp open auth 443/tcp open https 8004/tcp filtered unknown 34604/tcp filtered unknown Remote operating system guess: HP-UX 10.20 TCP Sequence Prediction: Class=random positive increments Difficulty=76552 (Worthy challenge) IPID Sequence Generation: Busy server or unknown class # Nmap run completed at Thu Jun 28 13:10:18 2001 -- 1 IP address (1 host up) scanned in 60 seconds	Interesting ports on TCP scan The ssh (22) port is open for secure firewall support access. Authentication is done by public and private key ONLY. Access for this firewall is allowed from internal ONLY. The telnet (23) port is open for firewall support access. Authentication is performed with a Secure ID card. The HTTP (80) is open for internet browsing access. The auth (113) port is open for authentication access. The HTTSP (443) is open for secure (SSL) internet browsing access. Port 8004 is the default port for the Gauntlet GUI. It can be changed. Port 34604 is the default port for HP RAID management. The OS is HP 10.20 IPSec (key exchange and ESP) is configured as a packet filter and packet filter do NOT listen on specific ports. Therefore, they are not listed in the scan.
# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 15:46:48 2001 as: nmap -sU -v -p 1-65535 -oN /home/kelvin/UDP_fwoutdmz 196.20.59.40 Interesting ports on host.domain.com (196.20.59.40): (The 65531 ports scanned but not shown below are in state: closed) Port State Service 123/udp open ntp 514/udp open syslog 34604/udp open unknown # Nmap run completed at Thu Jun 28 15:47:35 2001 -- 1 IP address (1 host up) scanned in 46 seconds	Interesting ports on UDP scan The ntp (123) is used to sync time The syslog (514) port is listening but remote logging is NOT configured. Port 34604 is the default port for HP RAID management.

Scan of VPN in DMZ (vpndmz)

The Nortel VPN Switch has services built in to prevent scanning. Nmap yielded no output.

Scan of External Mail Firewall (fwmail)

# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 14:30:24 2001 as: nmap -sS -O -v -P0 -p 1-65535 -oN /home/kelvin/TCP_fwmail 196.20.59.48 Interesting ports on (196.20.59.48): (The 65528 ports scanned but not shown below are in state: closed) Port State Service 22/tcp open ssh 23/tcp open telnet 25/tcp open smtp 110/tcp open pop-3 113/tcp open auth 8004/tcp open unknown 34604/tcp open unknown Remote operating system guess: HP-UX 10.20 E 9000/777 or A 712/60 with tcp_random_seq = 0 TCP Sequence Prediction: Class=64K rule Difficulty=1 (Trivial joke) IPID Sequence Generation: Busy server or unknown class # Nmap run completed at Thu Jun 28 14:31:41 2001 -- 1 IP address (1 host up) scanned in 77 seconds	Interesting ports on TCP scan The ssh (22) port is open for secure firewall support access. Authentication is done by public and private key ONLY. Access for this firewall is allowed from internal ONLY. The telnet (23) port is open for firewall support access. Authentication is performed with a Secure ID card. SMTP (25) and POP-3 (110) are open for mail transport and access respectively. The auth (113) port is open for authentication access. Port 8004 is the default port for the Gauntlet GUI. It can be changed. Port 34604 is the default port for HP RAID management. The OS is HP 10.20
# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 15:39:01 2001 as: nmap -sU -v -p 1-65535 -oN /home/kelvin/UDP_fwmail 196.20.59.48 Interesting ports on (196.20.59.48): (The 65528 ports scanned but not shown below are in state: closed) Port State Service 123/udp open ntp 514/udp open syslog 34604/udp open unknown # Nmap run completed at Thu Jun 28 15:40:07 2001 -- 1 IP address (1 host up) scanned in 66 seconds	Interesting ports on UDP scan The ntp (123) is used to sync time The syslog (514) port is listening but remote logging is NOT configured. Port 34604 is the default port for HP RAID management.

Scan of External Internet Firewall (fwintnet)

# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 14:27:02 2001 as: nmap -sS -O -v -P0 -p 1-65535 -oN /home/kelvin/TCP_fwintnet 196.20.59.49 Interesting ports on host.domain.com (196.20.59.49): (The 65526 ports scanned but not shown below are in state: closed) Port State Service 22/tcp open ssh 23/tcp open telnet 80/tcp open http 113/tcp open auth 443/tcp open https 8004/tcp filtered unknown 34604/tcp filtered unknown Remote operating system guess: HP-UX 10.20 TCP Sequence Prediction: Class=random positive increments Difficulty=76478 (Worthy challenge) IPID Sequence Generation: Busy server or unknown class # Nmap run completed at Thu Jun 28 14:28:03 2001 -- 1 IP address (1 host up) scanned in 60 seconds	Interesting ports on TCP scan The ssh (22) port is open for secure firewall support access. Authentication is done by public and private key ONLY. Access for this firewall is allowed from internal and external. The telnet (23) port is open for firewall support access. Authentication is performed with a Secure ID card. The HTTP (80) is open for internet browsing access. The auth (113) port is open for authentication access. The HTTSP (443) is open for secure (SSL) internet browsing access. Port 8004 is the default port for the Gauntlet GUI. It can be changed. Port 34604 is the default port for HP RAID management. The OS is HP 10.20
# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 15:26:30 2001 as: nmap -sU -v -p 1-65535 -oN /home/kelvin/UDP_fwintnet 196.20.59.49 Interesting ports on host.domain.com (196.20.59.49): (The 65531 ports scanned but not shown below are in state: closed) Port State Service 123/udp open ntp 514/udp open syslog 34604/udp open unknown # Nmap run completed at Thu Jun 28 15:27:16 2001 -- 1 IP address (1 host up) scanned in 46 seconds	Interesting ports on UDP scan The ntp (123) is used to sync time The syslog (514) port is listening but remote logging is NOT configured. Port 34604 is the default port for HP RAID management.

Scan of Internet DMZ Firewall (fwindmz)

# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 14:40:22 2001 as: nmap -sS -O -v -P0 -p 1-65535 -oN /home/kelvin/TCP_fwindmz 196.20.59.46 Interesting ports on host.domain.com (196.20.59.46): (The 65526 ports scanned but not shown below are in state: closed) Port State Service 22/tcp open ssh 23/tcp open telnet 80/tcp open http 113/tcp open auth 443/tcp open https 8004/tcp filtered unknown 34604/tcp filtered unknown Remote operating system guess: HP-UX 10.20 TCP Sequence Prediction: Class=random positive increments Difficulty=76960 (Worthy challenge) IPID Sequence Generation: Busy server or unknown class # Nmap run completed at Thu Jun 28 14:41:23 2001 -- 1 IP address (1 host up) scanned in 60 seconds	Interesting ports on TCP scan The ssh (22) port is open for secure firewall support access. Authentication is done by public and private key ONLY. Access for this firewall is allowed from internal and external. The telnet (23) port is open for firewall support access. Authentication is performed with a Secure ID card. The HTTP (80) is open for internet browsing access. The auth (113) port is open for authentication access. The HTTSP (443) is open for secure (SSL) internet browsing access. Port 8004 is the default port for the Gauntlet GUI. It can be changed. Port 34604 is the default port for HP RAID management. The OS is HP 10.20
# nmap (V. 2.54BETA25) scan initiated Thu Jun 28 15:36:31 2001 as: nmap -sU -v -p 1-65535 -oN /home/kelvin/UDP_fwintnet 196.20.59.46 Interesting ports on host.domain.com (196.20.59.46): (The 65531 ports scanned but not shown below are in state: closed) Port State Service 123/udp open ntp 514/udp open syslog # Nmap run completed at Thu Jun 28 15:37:15 2001 -- 1 IP address (1 host up) scanned in 46 seconds	Interesting ports on UDP scan The ntp (123) is used to sync time The syslog (514) port is listening but remote logging is NOT configured. Local syslog is enable.

Perimeter Analysis

VPN in DMZ (vpdmz)

To make device vpndmz more secure, GIAC Enterprises should implement certificate base authentication.

External DNS (dns)

Although we are NOT using a split DNS and running it in a chrooted environment, it could be secured better by placing a firewall on it or to save money, place dns in the DMZ.

External Mail Firewall (fwmail)

The nmap scan revealed that the randomness of the fwmail firewall is a joke. Correct this so that it will be a worth challenge like the other firewalls.

External Internet Firewall (fwintnet)

External SSH communication could be replaced with VPN IPSec communication. This would allow greater flexibility with accessing internal applications.

Additional Security Enhancements

An email virus scanning gateway could be placed between the External Mail Firewall and the mail server on the corporate backbone to scan Internet email.

The Internal DMZ Firewall could be another product. Something like Raptor or CheckPoint. If the DMZ was breached, this would provide a different road block than the first one which was smashed.

Because of our router design, it is mandatory that we add Intrusion Detection ASAP. Looking at picture 1, a Network IDS tap would be placed behind the router, behind fwmail, fwintnet, fwoutdmz, and fwindmz. This will allow centralize monitoring.

The support server, used by the support analyst, should have a firewall loaded on it.

As the use of GIAC's VPN grows, they can request that all Partner's accessing the VPN install personal firewalls on the client machines.

Assignment 4

Overview Design Under Fire

I have decided to use Robert Grill's, http://www.sans.org/y2k/practical/Robert_Grill_GCFW.doc for the Design Under Fire. It is important to understand that actually breaking into an infrastructure take patience.

Robert is using the CISCO 2620 for the border router and CISCO 2620 using Content Based Access Control (CBAC) foe the firewall.

Firewall Attack

Using information collected at SecuriTeam.com's site located at http://www.securiteam.com/exploits/2HUQ9QAQOS.html, it is possible to assume control of the CISCO Border Router. This occurs when running various versions IOS 12.X with NAT implemented. Roberts' version was not included in the exclude list.

Once we have control of the router, we can establish access for ourselves. Once we have consistence access, we can launch attacks at the CISCO firewall.

Using the following information from http://www.american.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml, http://www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml it is possible to force the router to reload. Security scanning software can cause a memory error in Cisco IOS Software that will cause a reload to occur. This occurs when running various versions IOS 12.X. Roberts is using one of the affected IOS versions.

When the router is reloaded, it will allow all traffic. This will give us access to systems behind the firewall.

Denial of Service Attack

Using the following information from http://www.securiteam.com/securitynews/2KUPRQKQ0U.html, it is possible to use nmap and a UDP scan of the syslog port (514) to accomplish a DOS attack. This occurs when running various versions IOS 12.X. Roberts' IOS version was not included in the exclude list.

Internal System Attack

Why am I choosing workstations to hack? Are you kidding me? Microsoft has more security advisories than it rains in some locations.

I would try L0phtCrack, a tool password auditing tool for (NT/98/95). It computes password from the registry. See http://www.securiteam.com/tools/2PUPRR5Q0K.html for more details.

Once the password is obtained, use a program like back-orifice that would allow me to administrator the workstation remotely.

Reference

Books

Benton, Chris; Kessler, Gary; Northcutt, Stephen; Pomeranz, Hal;. GCFW Course Materials, The SANS Institute.

Hewlett Packard Company, Administering Your HP-UX Trusted System HP 9000 Computer Systems. Palo Alto: Hewlett Packard Company, August 1996.

Network Associates Inc, Gauntlet Firewall for UNIX Administrator's Guide version 5.5. Santa Clara: Network Associates Inc., 1996-1999.

Network Associates Inc, Gauntlet Firewall for UNIX User's Guide version 5.5. Santa Clara: Network Associates Inc., 1996-1999.

Nortel Networks, Reference for the Contivity VPN Switch. Billerica, MA: Nortel Networks, 2000.

Nortel Networks, Installing the Contivity Extranet Switch Client. Billerica, MA: Nortel Networks, 2000.

Nortel Networks, Configuring the the Contivity VPN Switch Client. Billerica, MA: Nortel Networks, 2000.

Online

Wunsch, Scott. "Chroot-BIND HOWTO". Version 1.4. http://www.redhat.com/mirrors/LDP/HOWTO/Chroot-BIND-HOWTO.html (July 16, 2001).

Ronald McCarty "R.I.P. RIP?" http://www.samag.com/articles/2001/0103/0103j/0103j.htm.

Sans Institute Online http://www.sans.org/newlook/home.htm.