Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment

Version 1.6

SANS Parliament Hill, Ottawa

August 2001

Tom Fast
October 2001

Security Architecture

GIAC Enterprises is an e-business dealing in the online sales of fortune cookie sayings. To protect their business and provide access for customers, suppliers, partners and employees they are implementing the following security architecture.

Assumptions:

The security architecture has been done using the following assumptions about GIAC Enterprise.

- GIAC is running a Novell 5.1 IP network OS.
- The desktops and servers are a mix of NT, W2K, and Linux.
- The team brought in to develop the web site and associated database is using Linux.
- All the servers, routers and components of the firewall are in a single location that has been assessed to be physically secure.
- GIAC has a 10Mb ethernet connection to their ISP.
- GIAC has been given a class C public network address space by their ISP.

Policy:

In order to design and implement a security architecture a policy should first be developed and approved by upper management. This ensures that the design will have the proper balance between business needs and security risks.

GIAC Enterprise Firewall Policy

All data going to and from the screened subnets must be encrypted and sent over a secure connection

All servers, routers, VPNs and networking gear must be kept at the most recent release/patch level

Employees needing Internet access will do so through the main firewall. Any other access (i.e.: dialup) is not allowed.

Partners, suppliers and employees needing external access to the GIAC network will do so over a secure VPN using client software, personal firewalls and virus protection supplied by GIAC. Access to resources through the VPN will be controlled and limited by the VPN appliance. The level of access within the resource will be controlled by user name and password privileges within the OS or application running on the resource.

All email will go through the company email server(s). All incoming/outgoing email and attachments will be scanned for viruses and known exploits.

Routers and firewalls will be configured to their maximum security potential. Taking into account that performance and business needs must be factored in.

Only those services and ports necessary to conduct GIAC business will be allowed through the firewall.

Where ever possible and practical logging will be enabled and logs will be sent to a log server. Log files will be analyzed on a daily basis.

Internal firewalls will be deployed to protect sensitive data servers.

IDS systems will be deployed to monitor network traffic.

The firewall will be audited yearly by an external auditing company..

Internal audits will be done monthly by the IS staff.

This policy is a living document and is subject to revision to meet the security and business requirements of GIAC.

GIAC Enterprises Network Layout:

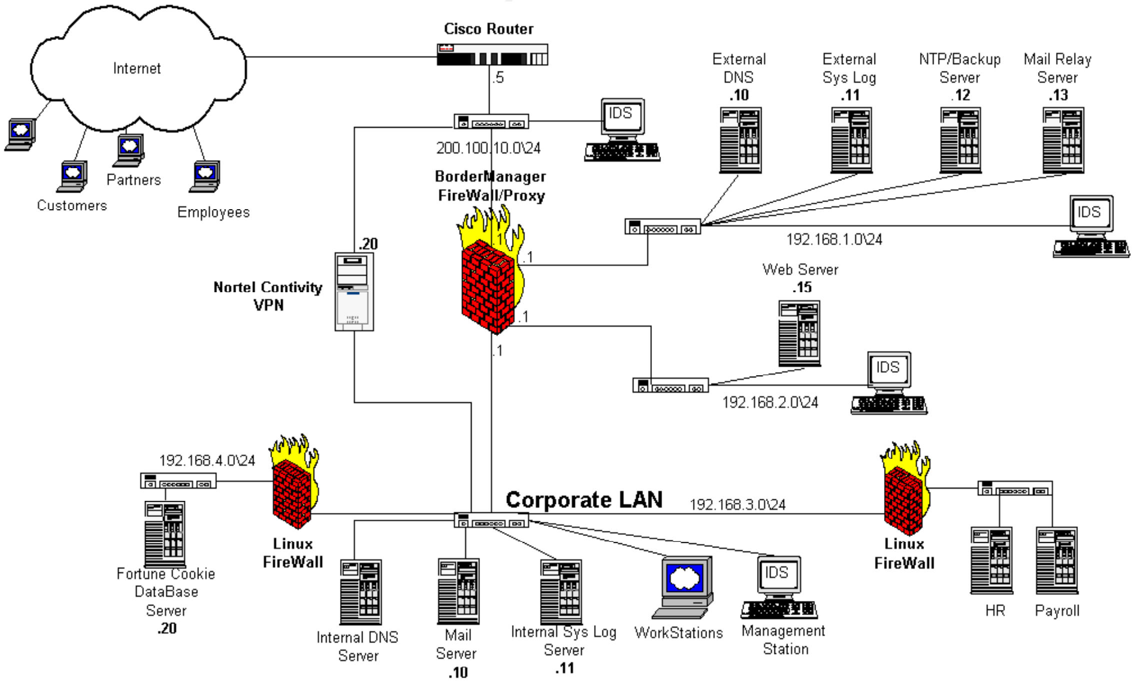


Figure 1

** To avoid diagram clutter the lines connecting the IDS PCs to the management station are not shown.

Defense Components:

Router:

The router is the first line of defense in the GIAC firewall implementation. The router will use a reflective ACL for the incoming and out going traffic. The router will also send log files to a Sys Log server where they will be scanned for any suspicious traffic. A Cisco 3640 series router running IOS 12.1,with dual ethernet interfaces will be used. The 3640 was chosen to insure that there would be enough CPU power to process the ACLs with out dropping packets as well as having expandability options for possible future connections.

Firewall:

The second line of defense and the main firewall is Novells BorderManager 3.6. It will be running on a Novell 5.1 server. There are 4 ethernet interfaces to accommodate the DMZ, two screened subnets and the corporate LAN. Internet access for each server on the screened subnets will be a through NAT. Rules allowing only the necessary services between the Internet, screened subnets and the corporate LAN will be implemented on the server. HTTP and FTP Internet access for the employees from the corporate LAN will be through BorderManagers application proxy. Authentication and control for employee Internet access will be done through BorderManagers access rules using Novells NDS.

The four ethernet interfaces will be assigned as follows.

Eth0: Public interface. This will be the DMZ with a routable Class C network.
Eth1: Screened subnet 1. This will have the Web server for customer access and ordering
Eth2: Screened subnet 2. This will be the service subnet that has the eternal DNS server, the External Sys Log server, the NTP server and the Mail Relay server.
Eth3: Private interface. Connected to the corporate LAN

VPN:

The VPN solution for the GIAC firewall is a Nortel Contivity 1600. The VPN will be used to give partners and suppliers access to the fortune cookie database on the corporate LAN. It will also provide remote access to the network for GIAC employees. All users of the VPN will be supplied with the Contivity client as well as Black Ice personal firewall and McAfee virus scanner. The public interface will connect to the Cisco router through a switch. The private interface will connect to the corporate LAN.

Internal Firewall:

The internal firewalls are servers running Red Hat Linux 7.1 using IP tables. On installation the kernel is modified and recompiled to only include the services that are necessary. Linux was chosen as an alternative to BorderManager servers to provide defense in depth through using a different OS and firewall setup.

Other Components:

All applications running on the servers, will be at the latest release levels with all relevant patches applied. Any unnecessary services and applications will be removed.

All subnet servers and IDS PCs are running Linux Red Hat 7.1. The OS will be kept at the latest release and patch levels. The kernel will be modified and recompiled to eliminate any unnecessary services.

Web Server:

To accommodate client access and on line purchases an Apache web server will be set up. On install the OS will be hardened and patched to the latest level. The front end web applications to show the product and collect customer input information will be developed in house. The customer will browse the products through an HTTP connection and when ready to make a purchase or make a change to their customer information they will be redirected to an HTTPS page. GIAC has purchased a VeriSign 128-bit Global Server ID to accommodate customers world wide to connect using a 128 bit SSL connection. Customer purchases will be made with a credit card or purchase order number for established customers . No credit card information will be stored on the server. The web application will use PGP encryption to encrypt the credit card information and send it to the Credit Company immediately after entry. Upon approval/denial of the credit card, the purchase information will then be encrypted and written to a job file to be retrieved by the main database application. Only minimal customer information will be stored on the server. The main database application will, on a preset interval, query the web server for any jobs waiting and also update the web server with any relevant changes. When an approved customer purchase has been made the database application will post the fortune cookie sayings to a secure directory on the Web Server and email the customer the URL. The customer will access the URL using their customer user name and password. The web server will have it's own tape backup installed and backups will be run nightly.

IDS PCs:

The IDS PCs will be running Snort (www.snort.org). Each PC will have two NICs. One NIC will connect to the switch on the network it is monitoring. This NIC will not have an IP address. The second NIC will tie back into the management station running on the corporate LAN.

NTP/Backup Server:

Running on the service subnet the NTP server will get its time sync from the ISP's time server and will provide all the defense components and servers with a standard time. In the event of a compromise this will ensure that all log entries have been synced to the same clock and the compromise can be tracked in the proper chronological order. This server will also have the backup tape drives and software for backing up all systems on the service subnet. Backups, an essential part of a security architecture, will be run nightly.

DNS Servers:

GIAC is running a split DNS server setup. The external DNS server is the Primary server for the GIAC domain and GIACs ISP is hosting the secondary DNS server. The server will be configured to only allow zone transfers from the ISP DNS server and filters will be in place to enforce transfers to a single IP address. The internal DNS server is only used to resolve internal addresses and has no contact with the external DNS server. Because the employees only access the Internet through the BorderManager Proxy server, BorderManager handles all external DNS lookups for the employees.

Mail Relay Server:

The mail relay server is running BIND. The server is configured to relay company external incoming and outgoing email. There is no email stored on the server.

External Sys Log Server:

Running on the service subnet, the external sys log server will hold the logs generated by the Cisco router, Mail Relay server and the GIAC Web server. The log files will be copied on a preset interval to the internal Sys Log server over a SSH connection initiated by the internal Sys Log server.

Internal Sys Log Server:

The internal sys log server will hold the logs generated by the Nortel Contivity VPN, the BorderManager server, the IDS systems and the internal firewalls. As well it will copy the log files from the external Sys Log server using an automated copy on a preset interval. An automated log file scanner will be installed and configured to generate alerts. A modem, set to dial out only, will be installed so any alerts can be sent directly to security personal pagers and cell phones

Management Station:

The management station will be used to manage the IDS PCs. Two NICs will be installed in the PC. One will for the IDS network and one for the corporate LAN. All alerts and logs from the IDS systems will be forwarded to the management station. The management station will forward the logs to the internal Sys Log server. A modem, set to dial out only, will be installed so any alerts can be sent to security personal pagers and cell phones.

Switches:

Switches will be used wherever multiple connections are required. This is to prevent the possibility of an intruder installing a packet sniffer on a compromised machine to obtain information that is crossing the network. The switches will be managed switches so that port monitoring can done on the port that connects from the Cisco router in the DMZ and the BorderManager interfaces on the screened subnets.

Security Policy:

Cisco Router:

The router is the first line of defense for GIAC Enterprises. In order to maximize this defense the router will use an ACL filter in and a reflective ACL filter out. As much as possible the rules will try to be host specific. The access-list will be built on a policy of deny all and then open ports and services as needed.

The order of the extended access-list is important. In the incoming filter the permit statement “ permit any host xxx.xxx.xxx.xxx” is often used. This makes it important to first deny any addresses that may be spoofed or illegal. Because the incoming and outgoing packets are compared to the rules in the order they are entered, putting the rules that will have the most hits closer to the top of the rule set is recommended.
Using a reflective access list enables the router to create a matching return rule for outgoing traffic. When the router detects that the connection is over, the incoming rule is removed. For UDP, which is connectionless, the router has a timer. If there is no traffic over that connection after the time period specified then the incoming filter is removed. The default time is set to 300 seconds. Using the command “ip reflective-list timeout (time in seconds)” you can change this timeout period.

Ethernet 0/0 is connected to the ISP (Public) network and Ethernet 0/1 is connected to the GIAC (200.100.10.0) network.

Incoming Access-List

```
ip access-list extended filterin

        # Block any packets with the GIAC internal Public network number
                deny   ip 200.100.10.0  0.0.0.255 any  log

        # Block any packets with private addresses
                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

# Block any packets with the loop-back address
          deny   ip 127.0.0.0  0.255.255.255 any log

# Block any packets with the multicast address
          deny   ip 224.0.0.0  15.255.255.255 any log

# Block any packets with an illegal address
          deny   ip host 0.0.0.0 any log

# Allow Web server HTTP and HTTPS Traffic In to DMZ
           permit tcp any 200.100.10.15 eq www
           permit tcp any 200.100.10.15 eq 443

# Allow esp encrypted packets to the Nortel Contivity VPN
          permit esp any host 200.100.10.20
          permit udp any host 200.100.10.20 eq isakamp

# Allow SMTP mail to Mail Relay server
          permit tcp any host 200.100.10.13 eq smtp

# Allow DNS Zone Transfers and large queries from ISP hosted Secondary server
          permit tcp  host 150.200.100.50 host 200.100.10.11 any eq domain

# Allow DNS queries
          permit udp any host 200.100.10.11 any eq domain

# Allow limited ICMP traffic to WEB Server and log
          permit icmp any host 200.100.10.15 echo log

# Create incoming access rules for the filterout reflect statements. This statement must be
here for the reflective list to work.
          evaluate packets

#Deny all other incoming IP traffic and log
          deny ip any any log
```

This access-list is applied to Eth0 as follows.

```
Router# config t
          Router# (config)Config int f0/0
                    Router (config-if)# ip access-group filterin in
```

Outgoing Access-List

```
ip access-list extended filterout

        # Allow any tcp established connection above 1023
                permit tcp any any gt 1023 established

        # Allow any udp connection above 1023
                permit udp any any gt 1023

        # Allow out going HTTP and create matching return filter for Web Server and GIAC
        employee web access and for # WEB server to send PGP encrypted data to the Credit
        Company.
                permit tcp any any eq www reflect packets

        # Allow out going HTTPS and create matching return filter
                permit tcp any any eq 443 reflect packets

        # Allow out going esp encrypted packets and isakamp from the Nortel Contivity VPN
                permit esp  host 200.100.10.20 any
                permit udp  host 200.100.10.20 any eq isakamp

        # Allow out going SMTP from Mail Relay Server and create matching return filter
                permit tcp host 200.100.10.13 any eq smtp reflect packets

        # Allow DNS Zone Transfers to ISP Secondary, large queries and create matching return
        filter
                permit tcp host 200.100.10.13  host 150.200.100.50 eq 53 reflect packets

        # Allow DNS Queries create matching filter
                permit udp any any eq 53 reflect packets

        # Allow FTP client to server initial connection and create matching return filter
                permit tcp any any eq 21 reflect packets

        # Allow out going NTP to ISP's NTP server
                permit udp host 200.100.10.12 host 150.200.100.55 eq 123 reflect packets

        # Allow limited outgoing ICMP from Web Server
                permit icmp host 200.100.10.15 any echo-reply
                permit icmp host 200.100.10.15 any unreachable
                permit icmp host 200.100.10.15 any packet-too-big
                permit icmp host 200.100.10.15 any time-exceeded

        # Deny all other IP traffic and log
                deny ip any any log
```

This access-list is also applied to Eth0 as follows.

```
Router# config t
          Router# (config)Config int f0/0
                    Router (config-if)# ip access-group filterout out
```

When using extended reflective access lists and trying to be host specific there are a few drawbacks.

- extended reflective lists take up more processing power. If you have a large access list make sure your router can handle the load
- being host specific can be an administration nightmare. Often you need more rules than when you use a general “any”. The more rules the more opportunities to make mistakes.

Armoring the router:

To better secure the router the following commands are entered in the router configuration mode.

```
# Block the ability of a packet to tell the router which way to send the return packet.
          no ip source route

#Turn off the non-routing services
          no service tcp-small-servers
          no service udp-small-servers

# Turn off the following services
          no service finger
          no http server
          no snmp
          no ip bootp server

# Stop the router from responding to an ICMP request with a Host Unreachable message
          no ip unreachables

# Disable forwarding of directed broadcasts
          no ip directed-broadcast

# Allow telnet from only the specified addresses
          build access-list
                    access-list 50 permit xxx.xxx.xxx.123
                    access-list 50 permit xxx.xxx.xxx.231
          apply access-list to vty 0 4
                    Router(config)#line vty 0 4
                              Router(config-line)#access-class 50 in
```

```
#  Define the access banner
           banner / WARNING: Unauthorized access is forbidden /

# Put in Sys Log server address
          logging 200.100.10.11

# Save some processing power
          no logging console
```

BorderManager Server:

General Rule Syntax for BorderManager:

BorderManager uses packet-filtering rules that examine ports, protocols, source and destination interfaces and source and destination addresses. The filter can be a one way or stateful. A stateful filter sets up a filter for the return traffic then removes the filter after the it detects the conversation is over. In the case of UDP it removes the return filter after a certain period of conversation inactivity. You can't change the timeout period.

When applying a rule to interfaces that go through a NAT the rule is applied after the NAT translation so the rule has to be applied to the internal host address. This also applies for the outbound NAT.

When the BRDCFG.nlm is run BorderManager applies some default rules that block all traffic from the public interface and all private interfaces in both directions. Also rules are applied that block almost all of the traffic from the Internet to the public interface. Routing updates, TCP and UDP traffic are all blocked at the public interface. It also creates some filter exceptions that allow services that you may have set up. These might be the Proxy service or VPN. You can run it again to recreate the default rules but be aware that it won't modify any exceptions you may have made that defeat the default filters.

The default filters do not block traffic between private interfaces, only from private to public. Therefore, to only allow the traffic you want between your screened subnets you will first have to set up filters that block all traffic going out of each subnet. Then you create the exception rules that allow the traffic you want to pass between the subnets.

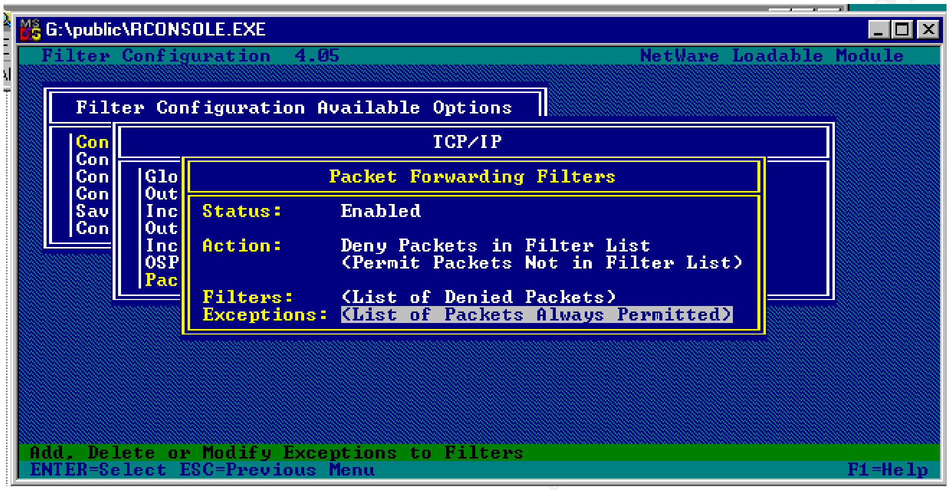
When creating a filter or exception rule BorderManager adds the rule to the list after you create it. The order of the rules does not matter and there is no way, or reason to change the order in the list.

To get to the filter rule and filter exception lists run the FILTCFG.nlm. Chose the following menu choices until you reach the screen shown in Figure 2.

Configure TCP/IP Filters

Packet Forwarding Filters (Make sure the Status is Enabled)

You are now at the Packet Forwarding Filters menu and you can then chose to create a filter or a filter exception.



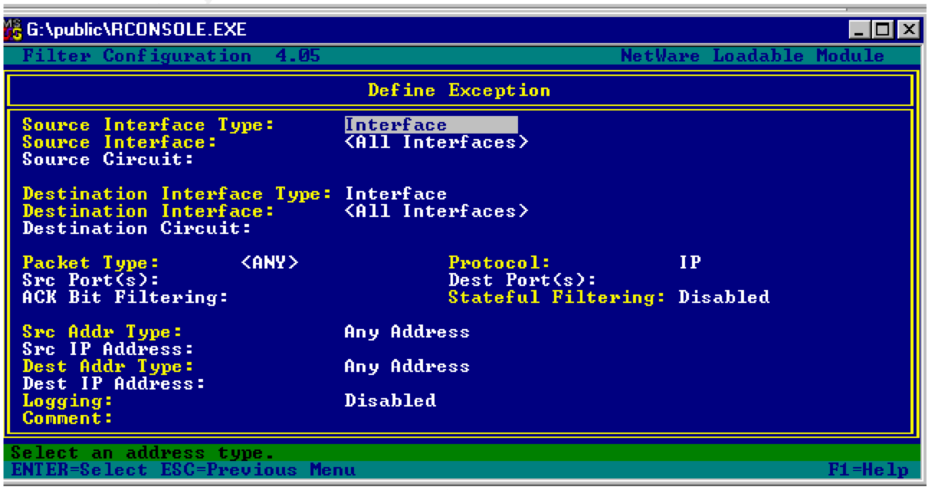
```
G:\public\RCONSOLE.EXE
 Filter Configuration  4.05                           NetWare Loadable Module

   Filter Configuration Available Options
   Con      TCP/IP
   Con
   Con  Glo    Packet Forwarding Filters
   Con  Out
   Sav  Inc  Status:      Enabled
   Con  Out
        Inc  Action:      Deny Packets in Filter List
        OSP               (Permit Packets Not in Filter List)
        Pac
             Filters:     (List of Denied Packets)
             Exceptions:  (List of Packets Always Permitted)

 Add, Delete or Modify Exceptions to Filters
 ENTER=Select  ESC=Previous Menu                                        F1=Help
```

Figure 2

Figure 3 shows the setup screen for creating a filter exception. After adding filters to block all traffic between the subnets there you now at the point of deny all traffic. You can then let traffic through as needed. Letting the traffic through is done through the filter exception screen.



```
G:\public\RCONSOLE.EXE
 Filter Configuration  4.05                           NetWare Loadable Module
                              Define Exception

 Source Interface Type:       Interface
 Source Interface:            <All Interfaces>
 Source Circuit:

 Destination Interface Type:  Interface
 Destination Interface:       <All Interfaces>
 Destination Circuit:

 Packet Type:        <ANY>             Protocol:           IP
 Src Port(s):                          Dest Port(s):
 ACK Bit Filtering:                    Stateful Filtering: Disabled

 Src Addr Type:               Any Address
 Src IP Address:
 Dest Addr Type:              Any Address
 Dest IP Address:
 Logging:                     Disabled
 Comment:

Select an address type.
ENTER=Select  ESC=Previous Menu                                         F1=Help
```

Figure 3

The parts of the filter/filter exception are as follows:

Source Interface:
Chose the interface where the packet is coming in from. It can be also be left at all interfaces if this is required.

Destination Interface:
Chose the interface where the packet is heading out. It can also be all interfaces.

Packet Type:
Select Packet Type and hit enter. The screen will come up and you can chose from a pre-defined list of filter definitions. If you can't find one that meets your requirements you can create your own definition. To create your own hit Insert and the screen in Figure 4 will come up.

The parts of the filter definition are as follows:

Name:
Give the filter a description. (This is the name that will show up as the packet type in the previous screen.)

Protocol:
Hitting Insert will bring up a list of protocols. Highlight one and hit enter.

Source Port:
Enter the source port. You can also enter a port, range of ports as in 1024-65535 or leave it at ALL.

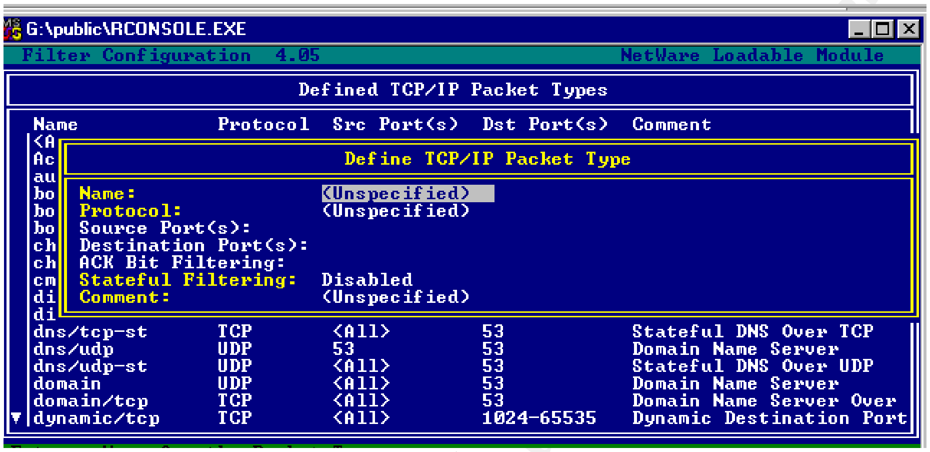
Destination Port:
Enter the destination port, range or leave it at ALL.

Ack Bit Filtering:
Enable or Disable. This will check if the Ack bit is set in a TCP packet. This can be used to allow only an established connection back in. Not needed if you are doing stateful filtering.

Stateful Filtering:
Enable if you want BorderManager to auto create the return filter needed when the criteria is met by the outgoing packet. Recommended.

Comment:

Add a comment if you wish.



```
G:\public\RCONSOLE.EXE
 Filter Configuration  4.05                           NetWare Loadable Module

                          Defined TCP/IP Packet Types

 Name                Protocol  Src Port(s)  Dst Port(s)  Comment
 <A
 Ac                     Define TCP/IP Packet Type
 au
 bo  Name:                  <Unspecified>
 bo  Protocol:              <Unspecified>
 bo  Source Port(s):
 ch  Destination Port(s):
 ch  ACK Bit Filtering:
 cm  Stateful Filtering:    Disabled
 di  Comment:               <Unspecified>
 di
 dns/tcp-st          TCP       <All>        53           Stateful DNS Over TCP
 dns/udp             UDP       53           53           Domain Name Server
 dns/udp-st          UDP       <All>        53           Stateful DNS Over UDP
 domain              UDP       <All>        53           Domain Name Server
 domain/tcp          TCP       <All>        53           Domain Name Server Over
▼dynamic/tcp         TCP       <All>        1024-65535   Dynamic Destination Port
```

Figure 4

Chose the filter definition you want and hit enter. The rest of the fields in the Packet Type section will fill in from the filter definition that was chosen.

Src Address Type:
You can chose to enter the Source IP addresses, a Network or leave it at Any Address. You can not specify a range of addresses.

Destination Address Type:
You can chose to enter the Source IP address, a Network or leave it at Any Address. You can not specify a range of addresses.

Logging:
Chose enabled or disabled. When you enable logging for a rule a popup screen warning you to only enable logging for a short period as it slows down the servers performance. This may be left over from previous versions when servers didn't have the CPU power they do today. BorderManager does not give you a way of sending the logs to a Sys Log server. You have to create a job to periodically copy the log files. It's probably best to start with logging only the essentials then monitor the server performance and enable more logging if the performance is acceptable.

Comment:
If you wish add a comment to the exception for future reference.

Applying the Rule:

The filter exception has now been created. As soon as you hit enter the exception is added to the list and is active.

GIAC Enterprises BoarderManager Rule Set:

The Interfaces on the BorderManager server:

Eth0: Public interface. Connected to the DMZ.
Eth1: Screened subnet 1. This will have the Web server for customer access and ordering
Eth2: Screened subnet 2. This will be the services subnet that has the eternal DNS server, the External Sys Log server, the NTP server and the mail relay server.
Eth3: Private interface. Connected to the corporate LAN

Hosts on the BorderManager subnets that need access through the firewall:

Public DMZ (200.100.10.0 /24)
200.100.10.5 - Cisco Router DMZ Interface
200.100.10.1 - BorderManager Public DMZ Interface

Sub Net 1 (192.168.1.0 /24)
192.168.1.10 - External DNS server
192.168.1.11 - External Sys Log server
192.168.1.12 - NTP server
192.168.1.13 - Mail Relay server

Sub Net 2 (192.168.2.0 /24)
192.168.2.15 - GIAC Web server

Database Server behind Internal firewall (192.168.4.0 /24)
192.168.4.20 - GIAC Fortune Cookie Data Base server

Corporate LAN (192.168.1.0 /24)

192.168.3.10 - Mail server
192.168.3.11 - Internal Sys Log server

The 200.100.10.x addresses were added as secondary addresses on the public NIC. Then the following NATs were created to forward traffic from the subnets to the public NIC.

192.168.1.10 - 200.100.10.10 External DNS server

192.168.1.11 - 200.100.10.11	External Sys Log server
192.168.1.12 - 200.100.10.12	NTP server
192.168.1.13 - 200.100.10.13	Mail Relay server
192.168.2.15 - 200.100.10.15	GIAC Web server

Other servers referred to in the Rule Set

Credit server -	Credit company server where credit card info is forwarded to
ISP DNS -	ISP's trusted DNS servers

BorderManager Filter Rule Set

	Source	Dest.		Source	Destination						
Rule	Intrface	Intrface	Prot.	Port	Port	Stateful	Source	Address	Destination	Address	Log
#1*	ALL	E0	IP				ANY		ANY		Y
#2*	E0	ALL	IP				ANY		ANY		Y
#3	E1	ALL	IP				ANY		ANY		
#4	E2	ALL	IP				ANY		ANY		
#5	E3	ALL	IP				ANY		ANY		

* Added by BorderManager when BRDCFG.nlm is run

These 5 rules form the deny all traffic base of the firewall. As needed, holes are then made using the filter exception rules.

Rule #1

Added by BorderManager to block all incoming traffic to the public interface.

Rule #2

Added by BorderManager to block all out going traffic from the public interface.

Rule #3

Block all traffic from the first screened subnet to any other interface on the firewall.

Rule #4

Block all traffic from the second screened subnet to any other interface on the firewall.

Rule #5

Block all traffic from the Corporate LAN to any other interface on the firewall

BorderManager Filter Exception Rule Set

Rule	Source Intrface	Dest. Intrface	Protocol	Source Port	Destination Port	Stateful	Source	Address	Destination	Address	Log
#1*	Any	E0	IP			N	HOST	200.100.10.1	ANY		
#2*	E0	ANY	TCP	ALL	1023-65535		ANY		HOST	200.100.10.1	
#3*	E0	ANY	UDP	ALL	1023-65535		ANY		HOST	200.100.10.1	
#4	E3	ANY	TCP	1023-65535	22	Y	ANY		ANY		Y
#5	E3	E1	TCP	ALL	25	Y	HOST	192.168.3.10	HOST	192.168.1.13	
#6	E1	E3	TCP	ALL	25	Y	HOST	192.168.1.13	HOST	192.168.3.10	
#7	E1	E0	TCP	ALL	25	Y	HOST	192.168.1.13	ANY		Y
#8	E0	E1	TCP	ALL	25	Y	ANY		HOST	192.168.3.13	Y
#9	E1	E0	UDP	ALL	123	Y	HOST	192.168.1.12	ANY	ISP NTP	
#10	E0	E1	UDP	ALL	123	Y	HOST	200.100.10.5	HOST	192.168.1.12	
#11	E2	E1	UDP	ALL	123	Y	HOST	192.168.2.15	HOST	192.168.1.12	
#12	E3	E1	UDP	ALL	123	Y	ANY		HOST	192.168.1.12	
#13	E0	E2	TCP	ALL	80	Y	ANY		HOST	192.168.2.15	
#14	E0	E2	TCP	ALL	443	Y	ANY		HOST	192.168.2.15	
#15	E3	E2	TCP	ALL	80	Y	ANY		HOST	192.168.2.15	
#16	E3	E2	TCP	ALL	443	Y	ANY		HOST	192.168.2.15	
#17	E2	E0	TCP	ALL	80	Y	HOST	192.168.2.15	HOST	Credit server	Y
#18	E3	E2	TCP	1023-65535	5234	Y	HOST	192.168.4.20	HOST	192.168.2.15	Y
#19	E1	E0	TCP	ALL	53	Y	HOST	192.168.1.10	HOST	ISP DNS	Y
#20	E0	E1	TCP	ALL	53	Y	HOST	ISP DNS	HOST	192.168.1.10	Y
#21	E1	E0	UDP	ALL	53	Y	HOST	192.168.1.10	ANY		
#22	E0	E1	UDP	ALL	53	Y	HOST	ISP DNS	HOST	192.168.1.10	
#23	E1	E0	UDP	ALL	53	Y	HOST	ISP DNS	HOST	192.168.1.13	
#24	E0	E1	UDP	ALL	514	Y	HOST	200.100.10.5	HOST	192.168.1.11	
#25	E2	E1	UDP	ALL	514	Y	HOST	192.168.2.15	HOST	192.168.1.11	
#26	E0	E2	ICMP			Y	ANY		HOST	192.168.2.15	Y

* Added by BorderManager when BRDCFG.nlm is run

Rule #1

Added by BorderManager this allows all TCP outgoing from the public IP address to the public interface. This exception is needed in order for the proxies to work.

Rule #2

Added by BorderManager this allows all incoming TCP traffic with a destination port >1023 from the public interface to the public IP address. This allows returning TCP traffic for the proxies.

Rule #3

Added by BorderManager this allows all incoming UDP traffic with a destination port >1023 from the public interface to the public IP address. This allows returning UDP traffic for the proxies.

Rule # 4

Allows port 22 SSH from the corporate LAN to any of the other interfaces on the BorderManager server. The filter is stateful so the connection can only be initiated from the LAN. SSH is used for all remote management and file transfers from the sub-net servers. SSH is an encrypted service. Using telnet or ftp for file transfer and remote management leaves your passwords and data in clear text. Though SSH is an encrypted service it too has its share of vulnerabilities.

> [1]Specifically: on May 17th, an Apache developer with a SourceForge account logged into a shell account at SourceForge, and then logged from there into his account at apache.org. The ssh client at SourceForge had been compromised to log outgoing names and passwords, so the cracker was thus able get a shell on apache.org. After unsuccessfully attempting to get elevated privileges using an old installation of Bugzilla on apache.org, the cracker used a weakness in the ssh daemon (OpenSSH 2.2) to gain root privileges. Once root, s/he replaced our ssh client and server with versions designed to log names and passwords.

Although there is no need to have SSH going to the Public interface it is blocked by the router and cannot get to the Internet. Using an ANY ANY means one less rule. Without it we would have to have individual rules for each subnet.

Rules #5 - #8

These rules allow SMTP mail traffic in and out of the Internet to be relayed through a server located in a subnet rather then having a direct connection to the Internet. There are many hacks and vulnerabilities using SMTP. An improperly configured mail relay could also be used to by a spammer to cover his tracks and implicate the company running the server. Protecting the company Email is a priority. Email is not stored on the relay server and therefore if the server were compromised the attacker would not have access to the email database.

Rules 5 and 6 make up the set that allows port 25 SMTP to and from the internal mail server and the mail relay server.

Rules 7 and 8 make up the set that allows port 25 SMTP to and from the mail relay server to the external mail servers.

Rule #9

This rule allows the NTP time server to access the ISP NTP server on UDP port 123. NTP is great for time syncing your servers and logs, but be aware that it too can be used by the wiley hacker.

> [2]More seriously, a properly crafted poison packet can cause the targeted system to execute shell commands up to 70 bytes long with the privileges of whatever user that the NTP daemon is running--usually root. As an added bonus for the attacker, the triggering attack packet can be sent from a spoofed address because the NTP protocol runs statelessly on UDP.

Rules #10 - #12

These rules allow UDP port 123 from the Cisco Router and the subnets to go to the NTP server on the .1 subnet. This is needed to in order to time sync the servers, the router and the VPN.

Rules #13 - #14

These rules deal with HTTP and HTTPS traffic to and from the Internet and the GIAC Web server. There are many hacks that have been perpetrated using port 80 to a web server. The real security here has to come from the OS and the applications running on the web server. You can't have a web server and not allow port 80. Up to date code levels, patches for the OS and security conscious programming for the applications are a necessity.

Rule 13 allows HTTP traffic from the Internet to the GIAC Web server for customer access.

Rule 14 allows HTTPS traffic from the Internet to the GIAC Web server for customer access.

Rules #15 - #16

These rules deal with allowing HTTP and HTTPS traffic to the GIAC Web server from the private LAN. This allows the customer service people to access the web site with out going out the Internet and back in.

Rule 15 allows HTTP traffic from the LAN to the GIAC Web server for customer service reps to access the web site.

Rule 16 allows HTTPS traffic from the LAN to the GIAC Web server for customer service reps to access the web site.

Rule #17

This allows the GIAC Web server to send out the PGP encrypted credit card info to the Credit Company server for processing and approval. Logging is enabled.

Rule #18

This rule allows the GIAC main fortune cookie saying Data Base server to communicate with the GIAC Web server to retrieve job files and to update customer information. The rule is stateful and applied from host to host so it can only be initiated from data base server on the Corporate LAN to the WEB server on the screened subnet. The security here lies within the database application. Strong username/password combinations that restrict access levels and security conscious database programming are the key. This keeps out the inside hacker who may have gotten a copy of the database client and knows the port number to connect to. Logging is enabled.

Rules #19 - #22

These rules form the set that allows the DNS server on the .2 subnet to do DNS queries and zone transfers.

Rules 19 and 20 allow TCP 53 between the ISP hosted secondary DNS server and the primary DNS server on the .2 subnet. This allows for zone transfers and large DNS queries between the two servers. Zone transfers can be a major source of information for someone attempting to hack your network. Using the firewall to allow zone transfers only with a trusted server is highly recommended. The server should also be configured to only do zone transfers with the trusted secondary server.

Rules 21 and 22 allow udp 53 between the Primary DNS server and the Internet. In order for Internet users to resolve the GIAC domain opening this port is a necessary evil.

Rule #23

Allow DNS queries to the secondary DNS server on the ISP network

Rules #24 - #25

These rules allow UDP port 514 from the router and the GIAC Web server to the Sys Log server.

Rule 24 allows UDP 514 from the Cisco router to the Sys Log server and sets up the filter needed for the return connection.

Rule 25 allows UDP 514 from the GIAC Web server to the Sys Log server and sets up the filter needed for the return connection.

Rule #26

Allows ICMP traffic from the Internet to the GIAC Web server. While this rule lets in all ICMP traffic from the DMZ, the router filters limit the actual ICMP types that will be allowed. ICMP can be used by a hacker to gain information about the network, or cause a denial of service. In this case GIAC only has one server on the subnet. The server is publicly accessible and GIAC Enterprises would like to be a good Internet neighbor.

Rule Testing:

These are tests for three of the rules implemented on the BorderManager firewall. These tests could be run in a test lab before putting the firewall into production.

Before starting the tests the following commands are run on the BorderManager server.

```
SET TCP IP DEBUG =1.
LOAD CONLOG
```

This will let us view all IP packets that are hitting the server. CONLOG is used to capture the traffic shown on the server console to a text file in the SYS:ETC directory called console.log. The log will show all IP packets that are permitted and discarded.
There is also another command that brings up a menu of TCP filter debugging commands that can be used to be more specific then TCP IP DEBUG when trying to debug a filter. However it is sometimes easier to debug a filter problem when you can see all the IP traffic.

```
SET FILTER DEBUG = ON
```

Testing Rule #25

A test PC is put on the 192.168.2.0 subnet with the IP address of the web server 192.168.2.15. A ping is initiated from the laptop to the test PC. The laptop receives a reply. The console.log is checked and the ping is shown going through the firewall.

The rule is then removed and the test repeated. The laptop does not receive a reply and the console.log shows the packet being dropped.

Testing Rule #13

A device with an http server running is configured with the 192.168.2.15 address and placed on the web server subnet. The laptop on the 200.100.10.0 DMZ then attempts to make a browser connection to the device. The laptop gets the http intro screen from the device. The console.log is checked and the http traffic is shown going through the firewall.

The rule is then removed and the test repeated. The browser on the laptop times out and the console.log shows the packets being dropped.

Testing Rule #18

A laptop is put on the 192.168.2.0 subnet with the IP address of the web server. Port 5324 is opened up with Netcat.

```
nc  -l  -p 5234
```

A PC running Linux is put on the 192.168.3.0 subnet and a Nmap scan on address 192.168.2.15 is started.

```
nmap –sT –p 5000–6000 –v  192.168.2.15
```

The output from nmap shows that the only open port is 5324 and the console.log confirms that all the scan packets where dropped, except for the port 5324 packets. To test that the filter only allows packets initiated from the LAN the laptop and the test PC are swapped and a scan from the web server subnet to the LAN shows that all packets are dropped.

VPN:

Partners and suppliers will connect to GIAC Enterprises through the Nortel Contivity. Through the Contivity group filters their access will be limited to the fortune cookie database only.

Remote access for GIAC Employees will also be though the Nortel Contivity 1600. Employees will have full access to the GIAC network through the VPN.

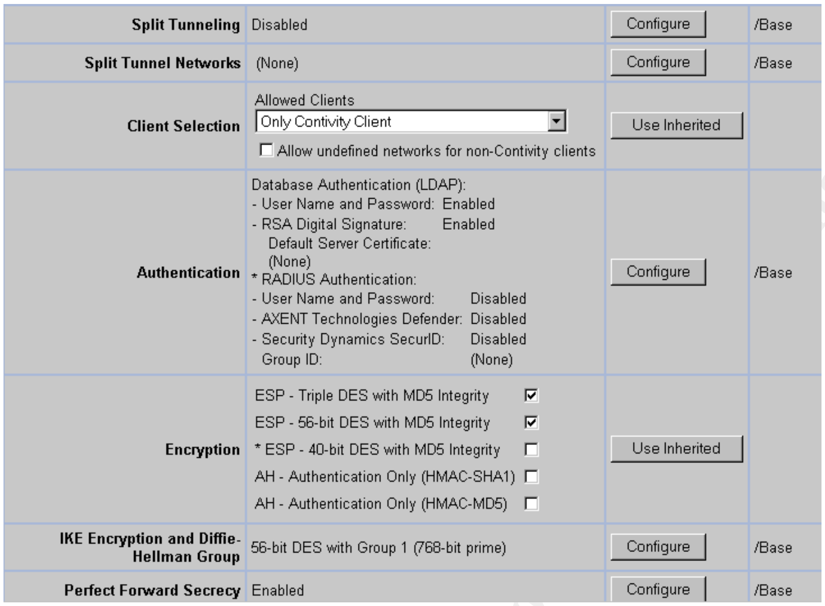
The Contivity will be set up as follows:

Encryption:

The Contivity will try and negotiate the highest possible encryption. If that fails it will then try then next level. Because some of our suppliers/partners are located in countries where we are not allowed to export the 168 bit Triple DES client we will also enable the 56 bit DES.

To accommodate the suppliers, partners and employees that are working from behind a NAT device we will be using ESP encryption.

- ESP Triple DES 168 bit key with MD5 integrity
- ESP DES 56 bit key with MD5 integrity



Split Tunneling	Disabled	Configure	/Base
Split Tunnel Networks	(None)	Configure	/Base
Client Selection	Allowed Clients Only Contivity Client ▾ □ Allow undefined networks for non-Contivity clients	Use Inherited	
Authentication	Database Authentication (LDAP): - User Name and Password: Enabled - RSA Digital Signature: Enabled Default Server Certificate: (None) * RADIUS Authentication: - User Name and Password: Disabled - AXENT Technologies Defender: Disabled - Security Dynamics SecurID: Disabled Group ID: (None)	Configure	/Base
Encryption	ESP - Triple DES with MD5 Integrity ☑ ESP - 56-bit DES with MD5 Integrity ☑ * ESP - 40-bit DES with MD5 Integrity □ AH - Authentication Only (HMAC-SHA1) □ AH - Authentication Only (HMAC-MD5) □	Use Inherited	
IKE Encryption and Diffie-Hellman Group	56-bit DES with Group 1 (768-bit prime)	Configure	/Base
Perfect Forward Secrecy	Enabled	Configure	/Base

Figure 5

User Settings:

- No split tunneling
- Forced logout after 15 minutes of inactivity.
- No saving passwords. The password must be entered at each connection
- Each user will also be assigned an IP address on the GIAC LAN.

General Group Settings:

- Force alpha numeric passwords
- Number of logins set to 1
- Minimum password length set to 8 characters
- Idle timeout set to 15 minutes

Two groups will be set up

Extranet:

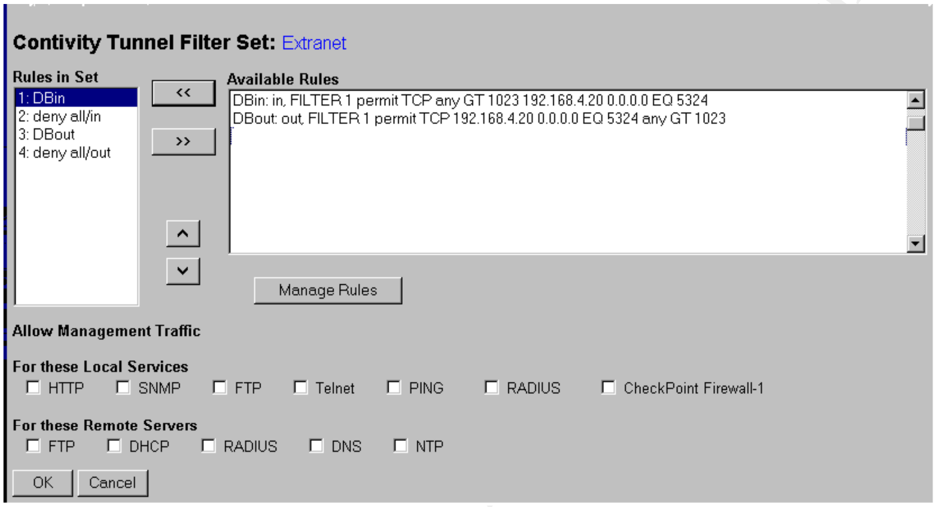
- The partners and suppliers user ID's will be in this group
- A banner stating "Authorized GIAC Extranet Users Only" will appear on login.
- The Extranet filter will be applied to this group (figure 6)

Rules:

Permit DB/in:in, FILTER 1 permit TCP any GT 1023 192.168.4.20 EQ 5234
Permit DB/out:out, FILTER 1 permit TCP 192.168.4.20 EQ 5234 any GT 1023

Rule Set:

1: permit DB/in
2: deny all/in
3: permit DB/out
4: deny all/out



Contivity Tunnel Filter Set: Extranet

Rules in Set

1: DBin
2: deny all/in
3: DBout
4: deny all/out

Available Rules

```
DBin: in, FILTER 1 permit TCP any GT 1023 192.168.4.20 0.0.0.0 EQ 5324
DBout: out, FILTER 1 permit TCP 192.168.4.20 0.0.0.0 EQ 5324 any GT 1023
```

Allow Management Traffic

For these Local Services
☐ HTTP ☐ SNMP ☐ FTP ☐ Telnet ☐ PING ☐ RADIUS ☐ CheckPoint Firewall-1

For these Remote Servers
☐ FTP ☐ DHCP ☐ RADIUS ☐ DNS ☐ NTP

Figure 6

Employee:

- GIAC employees user ID's will be in this group
- A banner stating "Authorized GIAC Employee Use Only" will appear on login.

Audit Your Security Architecture:

The firewall is in place, the rule set has been applied and the servers are up and running. Management has requested that a technical audit be performed to verify the firewall is performing up to spec.

Plan the Audit:

What to Audit:

- A review of the rule set.
- A scan of the firewall from all interfaces to determine that the rule set is performing as required.
- Audit the firewall server for any unnecessary services or NLMs. Because it is a Novell server that ties into the rest of the company's NDS services the NDS access and file rights will also be audited.

****Important****
Be sure to draw up a document outlining the audit and the risks involved. Have upper management sign the document so you are covered if anything goes wrong.

Time of Audit:

GIAC web server is an integral part of the GIAC Enterprises business plan. The site has launched GIAC into a 24 hour, 7-day a week business. Doing a scan on the network has the possibility of bringing down the network. Therefore the time of day the scan is done is important. After consulting with the web development team and going over the statistical data on the site hit counter it is determined that the best time of day to do the firewall scan is between 8:00 PM and 12:00 AM. The log files for this time period will also be smaller than if it was done for during regular business hours. This four-hour window means the scans will have to be carried out over a number of days.
The Novell server audit can be carried out during regular business hours.

Software used:

Nmap -	port scan the firewall
Tcpdump -	capture the UDP scans
Visual Click -	evaluate BorderManager server security from a Novell prospective

Budget costs:

An outside consulting firm will be used to perform the audit. Because the firewall scans will be after regular business hours the overtime rate will apply for that portion of the audit.

Scanning firewall	4 x 4 Hours	$250 / hr	$4000
Sever evaluation	4 Hours	$125 / hr	$500
Evaluate logs, write reports	8 Hours	$125 / hr	$1000
Server evaluation software – Visual Click	1 user / 25 server license		$2500
MIS personal for after hours scans	16 hours	$ 30 / hr	$480
		TOTAL	$8480

Conduct the Audit:
* This network design and testing is theoretical for the purpose of this assignment. While some of the rules were applied and tested the overall design was not.

First the Novell 5.1 server is evaluated.

Using Visual Click software the following is done.

- The NDS security is checked to insure proper rights are assigned to all containers and objects.
- The NLMs and their dependencies are checked to insure that only the ones needed are on the

server.

- A copy of the BorderManager Access Rules is taken for later evaluation.

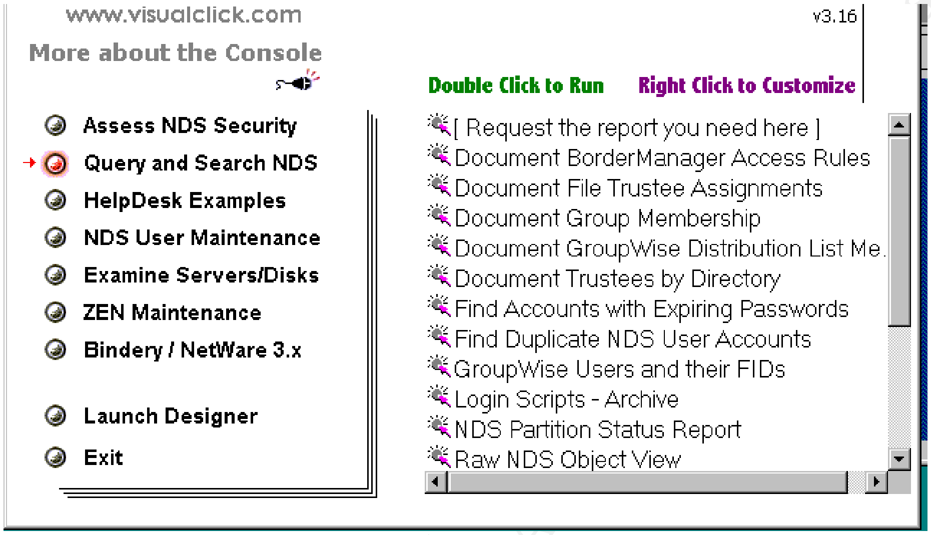

www.visualclick.com
More about the Console
v3.16
Double Click to Run
Right Click to Customize
Assess NDS Security
Query and Search NDS
HelpDesk Examples
NDS User Maintenance
Examine Servers/Disks
ZEN Maintenance
Bindery / NetWare 3.x
Launch Designer
Exit
[Request the report you need here]
Document BorderManager Access Rules
Document File Trustee Assignments
Document Group Membership
Document GroupWise Distribution List Me
Document Trustees by Directory
Find Accounts with Expiring Passwords
Find Duplicate NDS User Accounts
GroupWise Users and their FIDs
Login Scripts - Archive
NDS Partition Status Report
Raw NDS Object View

Figure 7

Scan the FireWall:

Over the next four nights the following scans are done.

From the 200.100.10.0 DMZ :

A laptop with the IP address of 200.100.10.50 is set up to do the scan.

nmap –sT –p 1-65535 –v –n –P0 ‘200.100.10.1, 10-13,15’ –oN bmscan_dmz_tcp.txt
nmap –sU –p 1-65535 –v –n –P0 ‘200.100.10.1, 10-13,15’ –oN bmscan_dmz_udp.txt

The first scan will scan all the TCP ports on the BorderManager primary and secondary IP addresses. No need to be stealthy so –sT is used (The rule set on the IDS should be changed to not alert on any detects from the IP address of the laptop). Scan all ports –p 1-65535 (Takes time but it’s thorough). –P0 tells nmap not to ping before scanning. By default nmap pings the host and if it dosen’t get a reply it will not scan that host. With our firewall setup to not reply to pings(except for the Web server) this is the only way to do a scan.Verbose logging –v. Log in normal fashion to a text file, -oN.

The second scan will similarly scan all the UDP ports. Because UDP is connectionless a scanner can’t expect a reply from a UDP packet sent. How it works is if it gets a ICMP Port Unreachable error message back it marks the port as not open, if it gets no response it marks it open. With our scan we want to determine if the UDP packet is getting through the firewall. To do this we will put a laptop running tcpdump on the subnet that is being scanned. If the packet gets through it will show up in our tcpdump capture.

tcpdump udp –v host 200.100.10.50 > cap_dmzscan_udp.log

This will capture and log the UDP traffic from the laptop doing the scanning from the DMZ.

The following is a capture from tcpdump running on the 192.168.1.0 network while a UDP scan is run from the DMZ on the 200.100.1.10 secondary address. The underlined sections show the port 53 (domain) UDP packet making it through the firewall as it should.

```
[root@localhost /]# tcpdump udp
Kernel filter, protocol ALL, TURBO mode (575 frames), datagram packet
socket
tcpdump: listening on all devices
06:50:15.195654 eth1 < 200.100.10.50.35122 > 192.168.1.10.domain: 0 [0q]
Type0 (Class 0)? . (0)
06:50:15.205654   lo > localhost.localdomain.1025 >
localhost.localdomain.domain: 49189+ PTR? 10.1.168.192.in-addr.arpa. (43)
(DF)
06:50:18.195654 eth1 < 200.100.10.50.35123 > 192.168.1.10.domain: 0 [0q]
Type0 (Class 0)? . (0)
06:50:18.195654 eth1 > 192.168.1.10.domain > 200.100.10.50.35123: 2560 [0q]
(1) (DF)
```

The laptop running tcpdump will have to be moved to the appropriate subnet during the UDP scans.

From the 192.168.1.x subnet:

Scan the second screened subnet. The only IP to scan is the Web server.

nmap –sT –p 1-65535 –v –n –P0 192.168.2.15 –oN bmscan_sn1tosn2_tcp.txt
nmap –sU –p 1-65535 –v –n –P0 192.168.2.15 –oN bmscan_sn1tosn2_udp.txt

Scan the corporate LAN. Because of the number of hosts and the time it would take to scan all ports nmap is left at the default port numbers, which is, to scan ports 1- 1024 as well as the ports listed in the services file which comes with nmap.

nmap –sT –v –n –P0 ‘192.168.3.0/24’ –oN bmscan_sn1tolan_tcp.txt
nmap –sU –v –n –P0 ‘192.168.3.0/24’ –oN bmscan_sn1tolan_udp.txt

From the 192.168.2.x subnet:

Scan the first screened subnet.

```
nmap –sT –p 1-65535 –v –n –P0 ‘192.168.1.10-13’ –oN  bmscan_sn2tosn1_tcp.txt
nmap –sU –p 1-65535 –v –n –P0 ‘192.168.1.10-13’ –oN  bmscan_sn2tosn1_udp.txt
```

Scan the corporate LAN.

```
nmap –sT –v –n –P0 ‘192.168.3.0/24’ -oN  bmscan_sn1tolan_tcp.txt
nmap –sU –v –n –P0 ‘192.168.3.0/24’ –oN bmscan_sn1tolan_udp.txt
```

From the corporate LAN

Scan the first screened subnet.

```
nmap –sT –p 1-65535 –v –n –P0 ‘192.168.1.10-13’ –oN  bmscan_lantosn1_tcp.txt
nmap –sU –p 1-65535 –v –n –P0 ‘192.168.1.10-13’ –oN  bmscan_lantosn1_udp.txt
```

Scan the second screened subnet. The only IP to scan is the Web server.

```
nmap –sT –p 1-65535 –v –n –P0 192.168.2.15 –oN  bmscan_lantosn2_tcp.txt
nmap –sU –p 1-65535 –v –n –P0 192.168.2.15 –oN  bmscan_lantosn2_udp.txt
```

Evaluate the Audit

The audit has been completed and the results are in along with the recommendations of the consulting firm.

Audit results:

- The BorderManager rule base is sound and only the services needed are being allowed through.
- There were no surprises from the nmap scan. It confirmed the rule base is setup and functioning properly.
- The BorderManager server has a number of NLMs that are not needed and should be removed.
- NDS rights to objects and containers checked out OK.

Recommendations:

BorderManager falls short on these points.

- Very limited logging ability
- No alerting for rule base
- Limited ability. BorderManager only does packet filtering and does not interact with any

other systems (i.e. An IDS system changing an access rule when an attack is detected).

BorderManager positives

- NDS security used to give user access rights for Internet access.
- Proxy/caching services for user Internet access.

The recommendation is to replace BorderManager as the main firewall with a Linux firewall. The BorderManager firewall would be the secondary firewall giving GIAC Enterprises more defense in depth. This would also allow GIAC to continue using the proxy/caching services and NDS security for internal user Internet access.

They are also recommending that the LAN side of the Nortel Contivity VPN be run through the firewall. This would enable the unencrypted traffic from the VPN to be logged.

Recommended FireWall Design

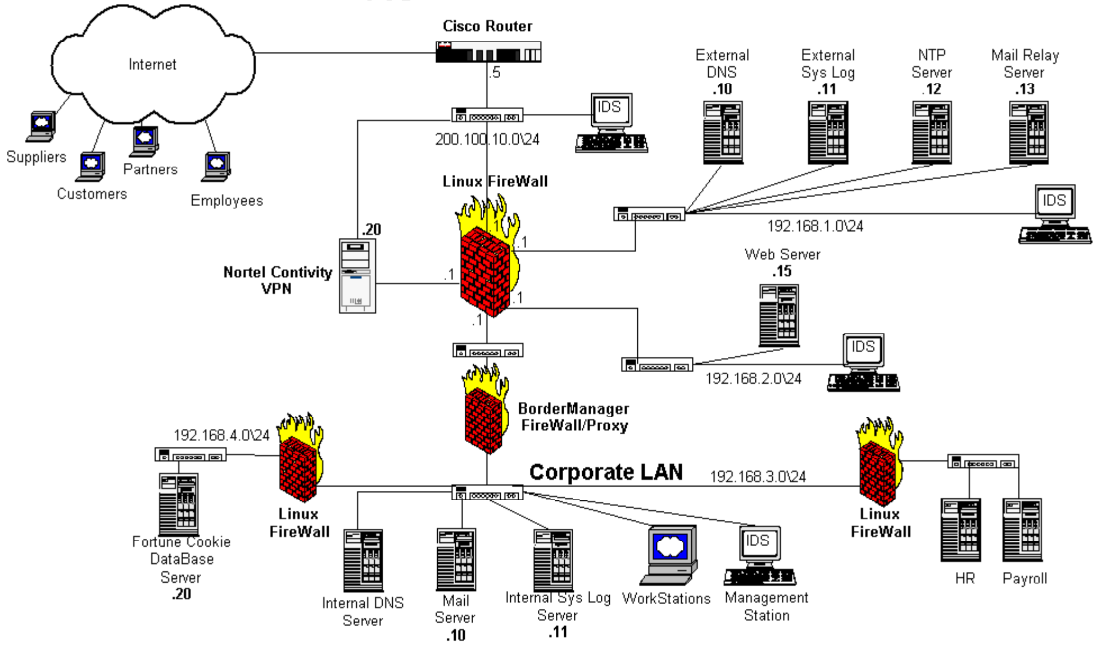


Figure 8

** To avoid diagram clutter the lines connecting the IDS PCs to the management station are not shown.

Design Under Fire:

The network design that I will be using for this section was done by Brett Gordon.

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

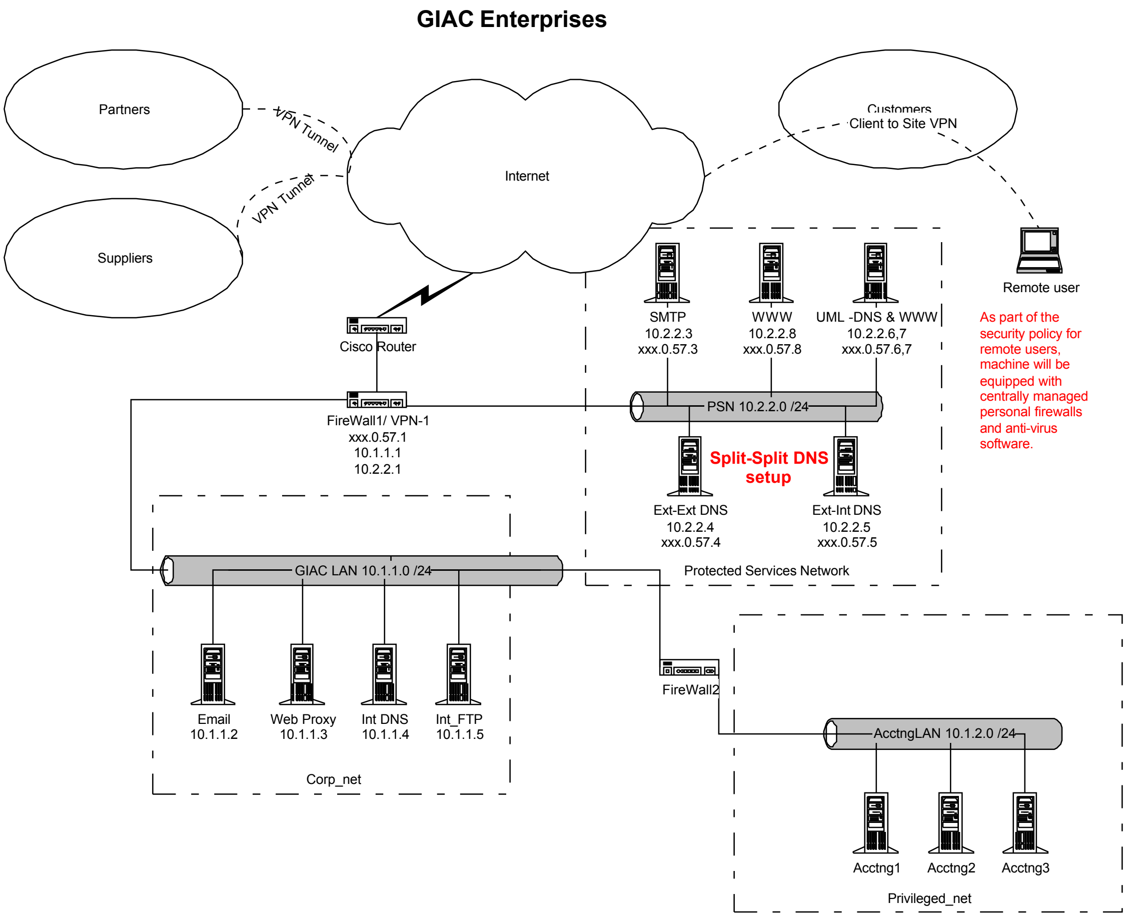


Figure 9

Three FW-1 Vulnerabilities:

Vulnerability 1:

[3]Checkpoint Firewall-1 makes use of a piece of software called SecuRemote (a.k.a. SecureRemote) to create encrypted sessions between users and FW-1 modules. Before

remote users are able to communicate with internal hosts, a network topology of the protected network is downloaded to the client. While newer versions of the FW-1 software have the ability to restrict these downloads to only authenticated sessions, the default setting allows unauthenticated requests to be honored. This gives a potential attacker a wealth of information including IP addresses, network masks, and even friendly descriptions.

Using the Vulnerability to attack:

Downloading a copy of SecureRemote client the attacker attempts a to connect to the Checkpoint Firewall-1 guarding his target. He of course can't connect, but, he doesn't want to, he wants the information that was surrendered by the firewall during the attempted connection. IP addresses, subnet masks and even descriptions of DMZ and subnet servers. Now the attacker doesn't have to run any network scans that might be detected by the security admin. The result of this vulnerability is the attacker can go right to work on hacking into a target. If descriptions are included in the information, he may not even have to scan for OS types or applications. He can be in and out in less time and not run the scans that alert a security admin to a possible attack.

Vulnerability 2

> [4]Check Point uses a protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/FireWall-1 allows RDP packets to traverse firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/FireWall-1 gateway without being explicitly allowed by the rule base.

Vulnerability 3

> [5]FireWall-1 provides a mechanism known as ``fastmode" to allow an administrator to designate certain services as being performance critical. The FireWall-1 kernel module simply passes packets that have a source or destination port of a fastmode service without any additional connection or rule base checking.
>
> Additionally, in fastmode, only SYN packets are verified. This allows an attacker to pass non-SYN TCP packets through the firewall to map the network by setting the source port of her packets to that of the fastmode service. We demonstrated mapping a network using the -g and -sF options in nmap.
>
> [6]If Fast Mode has been enabled in any rule, the following issue applies. If an attacker knows the address of a protected host, or can discover it, unauthorized connection attempts can be made to that host by using a series of specially malformed TCP packet-fragments

At the base of any well-planned exploit is information. The more that an attacker knows about a network the better prepared he/she is to attack. While the attacker may be after a specific target on a network, this vulnerability allows the attacker to learn about other possible targets that may be easier to compromise. A compromised system on the same network as the original target gives an attacker a much better avenue of attack against the original target. Not only could the attacker map the network, they then have a possible avenue to make a connection to a target.

DoS Attack:

Having successfully compromised 50 cable modem machines I am now ready to install my bots and commence my DoS attack on the GIAC Enterprises network. Having followed with interest the DoS attack committed against Gibson Research Corporation (www.grc.com) I decide that a brute force, packet flood is the way to go. I will use the same simple ping command and UDP packet send outlined on grc.com to run the attack. GIAC Enterprises may not have a good relationship with their ISP and by the time that filters can be put in place upstream from GIAC Enterprises I will have tied up their Internet line for an appreciable amount of time.

Having programmed my bots to perform their DoS magic I issue the instruction to start the attack. The bots now run the ping program on the compromised system to start pinging the IP address of the GIAC Enterprises router.

```
ping.exe  xxx.xxx.xxx.GIAC   -l 65500 -t
```

This uses the compromised machines ping program to send continuous pings 65KB in size to the GIAC firewall. By itself this is not a very high-speed attack, as ping waits for a response to its echo request before sending the next ping. However, when all 50 of the compromised machines are pinging at the same time it adds a lot of traffic on the GIAC Enterprises Internet connection.

With the compromised machines using the ping program the installed bot is free to send out continuous maximum sized UDP packets on an likely unused port (port 666 was used in the Gibson attack) to the GIAC Enterprises router as fast as the machine can. As outlined in the Gibson attack as the packets traverse the Internet they will be fragmented into many 1500 byte packets and the resulting packet storm on the GIAC Enterprises Internet line access will be literally shut down.

This type of attack can be very easily constructed, with out having a lot of “hacker” knowledge. To quote Steve Gibson “Nothing more than the whim of a 13-year old hacker is required to knock any user, site, or server right off the Internet.”

Preventing the DoS:

What can be done to counter the flood attack:

> Having a good relationship with your ISP is a top priority. In the case of an all out flood attack the only way to stop the attack is to apply filters upstream at the ISP. Get to know

your ISPs technical contacts before you are hit with a DoS. Find out what you ISPs policies and procedures are on applying blocking filters for their customers. Part of your service agreement might be a set response time to your request to have a filter put in place.

Have a second line to the Internet, from a different ISP if possible. If a flood attack is happening on one line the other line could be used temporarily for all access. This would require reconfiguration of the routers and firewalls. If this option is implemented, all possible configurations need to be mapped out, tested, on file and ready to go.

Have IDS systems in place. Keep the signature files up to date, in order to recognize the different DoS attacks. Install modems in the IDS system (dial out only) to send out alerts to a pager/cell phone. Some IDS firewall combinations can be configured to have the IDS create and apply firewall filters on the fly to try and prevent an incoming DoS. If you don't have a way to identify the addresses and ports that are being used in the attack you can't apply the necessary filters.

Other good practices to help prevent DoS attacks:

Keep your OS, firewall, routers and applications up to date and at the latest patch levels.

Ensure that all possible DoS preventative measures have been taken on your perimeter devices and firewalls.

Review the configuration of your perimeter devices and firewalls periodically to make sure the DoS measures have not been changed or removed.

Have a change request system in place so that all changes made are assessed and documented before the change is implemented.

Applying egress filtering to prevent your Internet connection from being used to DoS someone else.

Attacking an inside machine:

Searching around the Internet for a likely target I come across the GIAC Enterprises web site. I can browse the catalogue, and if I want to make a purchase I am sent to a secure SSL site. At this site it looks like customers can update their information if they have the correct username and password. Possible credit card info or other interesting information can be had here. This is a web site worth hacking.

Having done some simple recognizance by doing a whois lookup on www.giacenterprises.com I found out that the contact is Brett Gordon. Some more digging and I find out that he has a GIAC firewall analyst certification. Knowing this I realize that there's a good chance that the firewalls and servers are running the latest code and patch levels. My plan of action is to attack the web server at the application level. The programming to customize the web site may be sloppy and I can find a way in. Or the application developers may be responsible for the web server software and they may not be a vigilant as Brett Gordon with updates and patches.

The first step will be to try and identify the web server software that GIAC is running. I do some Web server fingerprinting scans and using the HTML pages that I can access I manage to identify the Web server software as IIs 5.0. First I try some basic buffer over flows and directory probes, no luck. Back to searching the Internet and I come across a known vulnerability.

> [7]There is a remotely exploitable buffer overflow in one of the ISAPI extensions installed with most versions of IIS 4.0 and 5.0 (The specific Internet/Indexing Service Application Programming Interface extension is IDQ.DLL). An intruder exploiting this vulnerability may be able to execute arbitrary code in the Local System security context. This essentially can give the attacker complete control of the victim system.

The code to exploit this is freely available and can be run against the server over a web connection. Complete control of the system would allow me to capture credit card numbers and other interesting data. Downloading the code I make a connection to the server and execute the hack. The hack fails and the next time I try connecting to the site it appears that I am being blocked. The latest patches must be installed. Brett must of detected my attempted hack and put in a filter to block my IP address. I'll have to keep an eye on the whois information. Maybe the next person in charge of security won't have had GIAC training.

References

Johnson, Craig - "A Beginner's Guide To BorderManager 3.x"
First Edition May 18, 2001

Johnson, Craig - "BorderManager: A Beginner's Guide to Configuring Filter Exceptions"
First Edition October 27, 1999

Nortel - Reference for the Contivity VPN Switch (.pdf)
Version 3.6, April 2001

Lance Spitzner - Auditing Your Firewall Setup
URL: http://www.enteract.com/~lspitz/audit.html (October 15, 2001)

Scott Winters - Top Ten Blocking Recommendations Using Cisco ACLs
Securing the Perimeter with Cisco IOS 12 Routers
URL: http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm (October 15, 2001)

URL: http://www.visualclick.com/ (October 15, 2001)

URL: http://www.verisign.com/server/rsc/gd/secure-bus/ (October 15, 2001)

URL: http://grc.com/dos/grcdos.htm (October 15, 2001)

[1] http://www.apache.org/info/20010519-hack.html (October 10, 2001)
[2] http://www.infosecuritymag.com/articles/june01/cover.shtml (October 10, 2001)
[3] http://www.securiteam.com/securitynews/5HP0D2A4UC.html (October 9, 2001)
[4] http://www.net-security.org/text/bugs/994716333,17858,.shtml (October 9, 2001)
[5] http://www.securiteam.com/securitynews/5CP0G1P2AE.html (October 9, 2001)
[6] http://www.checkpoint.com/techsupport/alerts/fastmode.html (October 9, 2001)
[7] http://www.cert.org/advisories/CA-2001-13.html (October 15, 2001)