Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment Version 1.8

Kevin Bong
December 8, 2002

Table Of Contents

Table Of Contents **2**
Abstract **5**
Assignment 1: Security Architecture **5**
Access Requirements **5**
Customers 5
Business Operations that need to be supported 5
Proposed Solution including Applications, Services and Protocols Used 6
Access Requirements and Restrictions 6
Suppliers 6
Business Operations that need to be supported 6
Proposed Solution including Applications, Services and Protocols Used 6
Access Requirements and Restrictions 7
Partners 7
Business Operations that need to be supported 7
Proposed Solution including Applications, Services and Protocols Used 7
Access Requirements and Restrictions 8
Internal Employees 8
Business Operations that need to be supported 8
Proposed Solution including Applications, Services and Protocols Used 8
Access Requirements and Restrictions 8
Mobile sales and telecommuters 9
Business Operations that need to be supported 9
Proposed Solution including Applications, Services and Protocols Used 9
Access Requirements and Restrictions 9
Network Administrator 9
Access Requirements and Restrictions 9
Private Network Servers and network infrastructure devices 9
Access Requirements and Restrictions 9
Service Network Servers and network infrastructure devices 10
Access Requirements and Restrictions 10
IP Address Scheme **10**
Network Diagram **11**
Perimeter Defense Components **12**
Border Router 12
Firewall and VPN Concentrator 13
Service Network Switch 13
Service Network IDS Sensor 13
SMTP Gateway 14
Web Server 14
Service Network DNS Server 15
Private Network Switch 15
Private Network IDS Sensor 16
Supplier/Partner Mail Server 16

Syslog Server 16
Corporate Mail Server 17
Assignment 2: Security Policy and Tutorial 17
Border Router Configuration 17
Router Access and Service Configuration Recommendations 19
Access Lists 23
VPN Policy 29
Firewall Policy 30
Private Network Originated Traffic 30
Service Network Originated Traffic 31
Internet Originated Traffic 31
Firewall Implementation Tutorial 31
Overview of steps to implement the firewall 31
Install base OS, service packs, and security patches 32
Configure the network cards 32
Install the Symantec Enterprise Firewall 32
Install any security patches for the Symantec Enterprise Firewall 33
Connect to the Management Console 33
Configuring Routing 35
Configure Remote Management Passwords 38
DNS Configuration 39
Configuring Network Entities 41
Configuring Redirected Services 46
Configuring Rules 48
Configure Custom Protocols 55
Assignment 3: Verify the firewall policy 60
Audit Plan 60
Example 1: Test with Netcat and Internet Explorer of permitted rule 62
Example 2: Test with Netcat of Non-permitted rule 64
Testing the firewall with NMAP 68
Example 3: Private Network User Workstation scan of the Service Network 68
Conclusions 70
Assignment 4 – design under fire 70
Attack 1: An Attack Against the Firewall 71
Probability of success 72
The Attack 73
Protecting against this attack: 73
Attack 2: Denial of Service 74
The Attack 74
Mitigating the attack: 74
Attack 3: Attempt to compromise an internal host 75
The Target 75
The attack 76
Sample Exploit 76
Detecting the attack 77

Countermeasures to prevent this attack 77
References 79

Abstract

The following topics are covered in this paper:

1. A description of a possible security architecture for an imaginary company is presented. The security architecture includes the access requirements for all users, the IP addressing scheme, the network diagram, and a description of all perimeter defense components.
2. The security policies for the border router, the firewall, and the VPN used in the network described above are detailed. A tutorial for implementing the Firewall policies using Symantec Enterprise Firewall is presented.
3. An audit of the firewall policies implemented above is described. The audit is performed in two different ways, first by using Netcat to verify the necessary services are open, and second by using Nmap to scan to see that all unnecessary protocols are blocked.
4. Three attacks are presented against the network detailed in an earlier student's submitted practical. The first attack involves attemtping to exploit a recently disclosed vulnerability in the HTTP proxy service of the Symantec Enterprise Firewall. The second attack describes using the TrinOO denial of service program with a small number of hosts to attack the network. The third attack attempts to gain control of the network's web interface to their email server, which uses the open source program Squirrelmail, which is known to have weaknesses.

Assignment 1: Security Architecture

Background and goal and basic principals
I have been asked to analyze and enhance the perimeter defense of GIAC Enterprises.

Online sale of fortune cookie sayings

Access Requirements

Customers

Business Operations that need to be supported

- Customers will browse GIAC's on-line catalog using non-secure protocols
- Customers will purchase fortunes from GIAC Enterprises securely over the Internet
- Customers should not need special software or configurations to order fortunes

Customers will not need a user ID or password to order. After they complete their first order, they will receive a password on the confirmation screen to use (with their email address as their username) to check the status of their order. The password and any personal customer information will not be sent by email.

Proposed Solution including Applications, Services and Protocols Used

- Customers purchase fortunes on-line from GIAC Enterprises' secure web server in the GIAC Service Network.
- Customers will use a standard web browser (Such as Internet Explorer, Mozilla, Opera, or Netscape) to connect to the web site.
- HTTP (Hyper-Text Transfer Protocol) will be used to browse the GIAC Enterprise On-line Catalog
- SSL (Secure Sockets Layer) protocol will provide encryption, GIAC server identity verification, and data integrity during orders.
- Customers will also be able to communicate with GIAC Enterprises using email (SMTP Protocol)

Access Requirements and Restrictions

- Customers (all addresses on the public Internet) should be permitted access to GIAC Enterprises DNS server on UDP port 53 (DNS). TCP Port 53 access is not required because the GIAC DNS Server will not return responses longer than UDP can support.
- Customers (all addresses on the public Internet) should be permitted access to the GIAC Enterprises Webservers on TCP ports 80 (HTTP) and 443(SSL)
- Customers (all addresses) on the public Internet should be permitted access to GIAC Enterprises mail server on TCP port 25 (SMTP). The mail server will only accept inbound traffic destined for GIAC Enterprises (Mail Forwarding Disabled)

Suppliers

Business Operations that need to be supported

- Receive orders and other secure communications from GIAC Enterprises
- Send invoices and other secure communications to GIAC Enterprises
- Send large electronic files (up to 50 MB) containing fortunes to GIAC Enterprises
- All suppliers have Internet connections, and would like to communicate with GIAC Enterprises over the Internet.
- Suppliers can be supplied with a User ID and password through postal mail prior to their first transaction.
- Suppliers use a wide variety of different technologies for OS, Software, and Internet connection.

Proposed Solution including Applications, Services and Protocols Used

- Each supplier will be provided an account on the dedicated supplier/partner mail server.
- A web interface to the supplier/partner mail server will be housed on the secure web server in the Service Network.

- SSL (Secure Sockets Layer) protocol will provide encryption, GIAC server identity verification, and data integrity.
- Standard web browsers can be used by suppliers, allowing for easy setup of each new supplier. All common platforms (Windows, Unix, and Macintosh) are supported.

Access Requirements and Restrictions

- Suppliers (all addresses on the public Internet) should be permitted access to GIAC Enterprises DNS server on UDP port 53 (DNS). TCP Port 53 access is not required because the GIAC DNS Server will not return responses longer than UDP can support.
- Suppliers (all addresses on the public Internet) should be permitted access to the GIAC Enterprises Webservers on TCP ports 80 (HTTP) and 443(SSL)
- Suppliers (all addresses on the public Internet) should be permitted access to GIAC Enterprises mail server on TCP port 25 (SMTP). The mail server will only accept inbound traffic destined for GIAC Enterprises (Mail Forwarding Disabled) While clear-text SMTP communication is available, suppliers will be urged to use the web based secure mail channel for all communication.

Partners

Business Operations that need to be supported

- Receive invoices and other secure communications from GIAC Enterprises
- Send orders and other secure communications to GIAC Enterprises
- Receive large electronic files (up to 50 MB) containing fortunes to GIAC Enterprises
- All Partners have Internet connections, and would like to communicate with GIAC Enterprises over the Internet.
- Partners can be supplied with a User ID and password through postal mail prior to their first transaction.
- Partners use a wide variety of different technologies for OS, Software, and Internet connection.

Proposed Solution including Applications, Services and Protocols Used

- Each Partner will be provided an account on the dedicated supplier/partner mail server.
- A web interface to the supplier/partner mail server will be housed on the secure web server in the Service Network.
- SSL (Secure Sockets Layer) protocol will provide encryption, GIAC server identity verification, and data integrity.
- Standard web browsers can be used by suppliers, allowing for easy setup of each new supplier. All common platforms (Windows, Unix, and Macintosh) are supported.

Access Requirements and Restrictions

- Partners (all addresses on the public Internet) should be permitted access to GIAC Enterprises DNS server on UDP port 53 (DNS). TCP Port 53 access is not required because the GIAC DNS Server will not return responses longer than UDP can support.
- Partners (all addresses on the public Internet) should be permitted access to the GIAC Enterprises Webservers on TCP ports 80 (HTTP) and 443(SSL)
- Partners (all addresses on the public Internet) should be permitted access to GIAC Enterprises mail server on TCP port 25 (SMTP). The mail server will only accept inbound traffic destined for GIAC Enterprises (Mail Forwarding Disabled) While clear-text SMTP communication is available, partners will be urged to use the web based secure mail channel for all communication.

Internal Employees

Business Operations that need to be supported

- Need to run applications which access the internal database
- Need access to corporate email
- Need ability to access the internet via HTTP, HTTPS, and FTP
- Need to communicate securely with suppliers and partners
- Need to communicate with other pieces of private network infrastructure, such as DHCP servers and DNS servers.

Proposed Solution including Applications, Services and Protocols Used

- Internal Employees will communicate with GIAC's internal systems over the GIAC Local Area Network.
- The GIAC Local area network will be protected from the Internet and Service Network by a firewall
- Internal employees will be allowed outbound access for HTTP, HTTPS, and FTP
- Internal employees can communicate with suppliers and partners through the dedicated vendor/supplier mail server.

Access Requirements and Restrictions

- All traffic between any two hosts on the private network will be permitted.
- Desktops will be permitted outbound HTTP (Port 80), HTTPS (Port 443), and FTP (Port 21)
- Will communicate with suppliers and partners by sending email to the supplier/partner mail server.

Mobile sales and telecommuters

Business Operations that need to be supported

- Need access to corporate email
- Need access to internal applications which interact with the internal database
- Lowest common denominator is 56K dial-up Internet Connection

Proposed Solution including Applications, Services and Protocols Used

- Mobile workers use local ISP's for Internet connectivity
- VPN used to secure data between client PC and GIAC Enterprises
- All hardware provided and managed by GIAC Enterprises
- VPN restricted to connect only to terminal server.
- Company provided laptops run Virus scan and personal firewall software

Access Requirements and Restrictions

- All the same access levels for Customers, Partners, and Suppliers listed above
- The mobile sales force and telecommuters (all addresses on the Internet) will need to access the VPN Concentrator (IPSEC, TCP Port 50 and UDP Port 500)

Network Administrator

Access Requirements and Restrictions

The Network Administrator Workstation has all the right of an internal employee, as well as the following additional privileges for management and troubleshooting.

- SSH (TCP Port 22) to the IDS sensor in the Service Network
- DNS (TCP and UDP port 53) outbound
- Telnet (TCP Port 23) to the border router
- All ICMP traffic to the Service Network and Internet

The network administrator is "trusted" and will be permitted to communicate on all ports and protocols to the DMZ Network and Service Network.

Private Network Servers and network infrastructure devices

Access Requirements and Restrictions

All traffic originating from the server segment of the private network (172.17.10.x) to the Internet or the Service Network will be blocked except the traffic shown below. Responses to the traffic permitted below will also be permitted through the use of stateful analysis on the firewall.

Supplier/Partner Mail Server

- Send mail outbound to the SMTP Gateway in the Service network (Port 25 outbound)

Corporate Mail Server
- Send mail outbound to the SMTP Gateway in the Service network (Port 25 outbound)

Internal DNS Server
- DNS lookups (port 53 TCP and UDP) outbound to the Internet. All other devices on the private network will use this server for DNS requests.

Service Network Servers and network infrastructure devices

Access Requirements and Restrictions

All traffic originating from the service network (172.17.10.x) to the Internet or the Private Network will be blocked except the traffic shown below. Responses to the traffic permitted below will also be permitted through the use of stateful analysis on the firewall.

IDS Sensor
- Syslog traffic permitted to the Syslog server (Port 514 UDP)

SMTP Gateway
- SMTP (port 25 TCP) to the Internet
- SMTP (port 25 TCP) to the Corporate Mail Server on the private network
- HTTP (port 80) to the Internet to download virus definitions

Web Server
- ODBC Calls (Default Port TCP 1433 for Microsoft SQL Server, I will set this to use the custom port TCP 1544) to the Corporate Database
- IMAP Calls (TCP port 143) from the web server to the Supplier/Partner mail server.

DNS Server
- DNS lookups (port 53 TCP and UDP) outbound to the Internet. All other devices on the service network will use this server for DNS requests.

IP Address Scheme

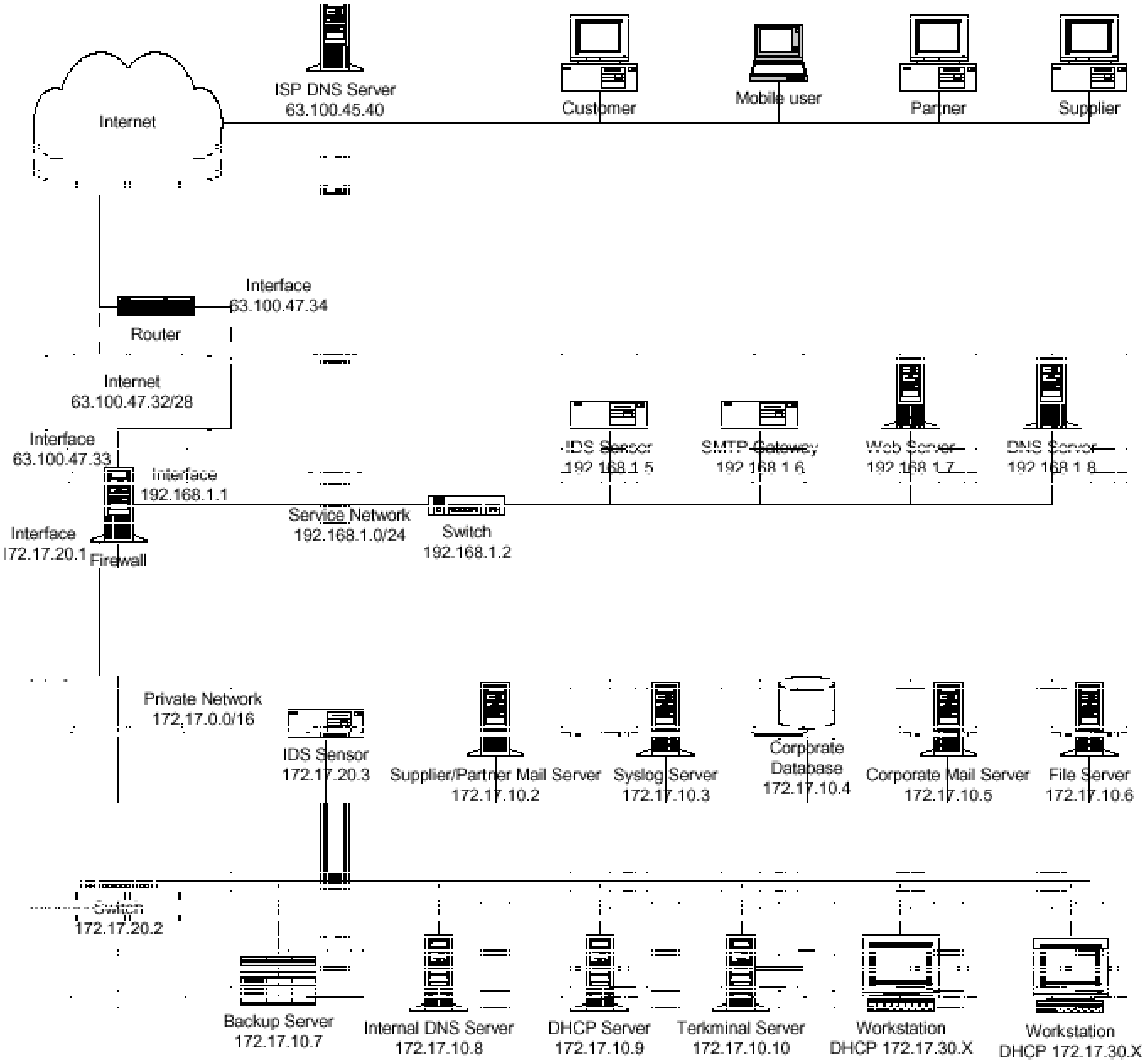
On the public Internet, GIAC Enterprises has been assigned the address range 63.100.47.32/28 by their ISP. This gives them 14 usable IP addresses. The netmask for this address range is 255.255.255.240. For the Serial interface of

the border router, they have been assigned the address 63.100.46.37 by their ISP.

In the Service Network, GIAC Enterprises will use the RFC 1918 private address range of 192.168.1.0/24

On the private network, GIAC Enterprises will use the RFC 1918 private address range of 172.17.0.0/16. Private network infrastructure devices, such as switches, gateways, and IDS sensors will be given static addresses of the form 172.17.20.X. Private network servers will be given static addresses of the form 172.17.10.X. Workstations will be given DHCP assigned addresses of the form 172.17.30.X.

Network Diagram



Perimeter Defense Components

Border Router

IP Addresses:
Serial Interface (Internet): 63.100.46.37 (ISP Assigned)
Ethernet Interface (DMZ Network): 63.100.47.34

Hardware/Software:
The border router will be a Cisco 2610 running Cisco IOS version 12.2. This router has one fixed 10MB Ethernet port and two Wan Interface Card Slots. In WIC Slot 0, I will install a Cisco WIC-1DSU-T1 1-port T1/Fractional T1 DSU/CSU WAN Interface Card. The second Wan Interface Card slot and a single Network Module slot are available for future expansion.

Firewall and VPN Concentrator

IP Addresses:
DMZ Network Interface: 63.100.47.33
Service Network Interface: 192.168.1.1
Private Network Interface: 172.17.20.1

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 2x 18.2 GB SCSI Hard Drives, hardware disk mirroring
- 512 MB RAM

Software:
- Windows 2000 Server Service Pack 3
- Symantec Enterprise Firewall version 7.0
- Symantec Enterprise VPN version 7.0
- Tripwire for Servers

Then firewall will break the network into three segments:
1. The DMZ – the area between the border router and the firewall, untrusted.
2. The Service Network, a semi-trusted segment that con communicate with both the Internet and the Private network. It will hold our Internet servers, such as Web, Mail, and DNS.
3. The Private Network, the trusted are of our network where our users, servers, and data exist.

Service Network Switch

IP Address: 192.168.1.2

Hardware:
HP Procurve 2512 12 port managed switch
Switching improves performance and makes sniffing and spoofing attacks more difficult. This switch includes support for Port monitoring – IDS can view traffic across this segment.

Service Network IDS Sensor

IP Address: 192.168.1.5

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 2x 18.2 GB SCSI Hard Drives, hardware disk mirroring
- 512 MB RAM

Software:
- Redhat Linux 7.3
- Snort 1.9.0 Network IDS software
- Tripwire

The Service Network IDS sensor will monitor all traffic in the Service Network, and report anomalous traffic via syslog to the syslog server on the private network. It is located in the service network and plugged into the monitoring port of the switch.

SMTP Gateway

IP Address: 192.168.1.6
Internet IP Address (Address Redirection done by Firewall): 63.100.47.36

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 2x 18.2 GB SCSI Hard Drives, hardware disk mirroring
- 512 MB RAM

Software:
- Microsoft Windows 2000 Server Service Pack 3
- McAffee Webshield SMTP 4.5
- Tripwire for Servers

The SMTP Gateway scans all inbound and outbound traffic passing through the gateway. The SMTP Gateway checks messages for known virus signatures and does content filtering as well. It can be configured to clean or quarantine email messages passing through it. It exists in the service network because it communicates with both the Internet and Private Network servers. It allows us to block harmful SMTP traffic before it enters our private network.

Web Server

IP Address: 192.168.1.7
Internet IP Address (Address Redirection done by Firewall): 63.100.47.37

Hardware:
- Compaq Proliant DL360

- 1.4 GHz PIII processor
- 2x 18.2 GB SCSI Hard Drives, hardware disk mirroring
- 512 MB RAM

Software:
- Microsoft Windows 2000 Server Service Pack 3
- Microsoft Internet Information Server 5.5
- Tripwire for Servers

The webserver accepts requests for web pages from the Internet. Requests may be clear-text (http) or secured using SSL. The web server may communicate with the private network corporate database using ODBC calls, or with the Supplier/Partner mail server on the private network using IMAP, to pull data needed to fulfill end user requests. No sensitive customer or company data is stored on the web server or elsewhere in the Service Network.

Service Network DNS Server

IP Address: 192.168.1.8
Internet IP Address (Address Redirection done by Firewall): 63.100.47.38

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 2x 18.2 GB SCSI Hard Drives, hardware disk mirroring
- 512 MB RAM

Software:
- Microsoft Windows 2000 Server Service Pack 3
- Tripwire for Servers

GIAC is using split-level DNS. The Service Network DNS server exists in the service network and answers DNS queries from the Internet as well as from other devices in the service network. A separate DNS server in the private network fulfills DNS requests for private network hosts.

Private Network Switch

IP Address: 172.17.20.2

Hardware:
HP Procurve 4000m 40 port managed switch
Switching improves performance and makes sniffing and spoofing attacks more difficult. This switch includes support for Port monitoring – an IDS can view traffic across this segment.
This switch is expandable to 80 ports, to allow room for company growth.

Private Network IDS Sensor

IP Address: 172.17.20.3

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 2x 18.2 GB SCSI Hard Drives, hardware disk mirroring
- 512 MB RAM

Software:
- Redhat Linux 7.3
- Snort 1.9.0 Network IDS software
- Tripwire

The private network IDS sensor scans network traffic for anomalies and sends suspicious traffic alerts to the Syslog server. Is it plugged into a monitoring port on the private network switch.

Supplier/Partner Mail Server

IP Address: 172.17.10.2
Service Network IP Address (Address Redirection done by Firewall): 192.168.1.22

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 3x 18.2 GB SCSI Hard Drives, hardware RAID 5
- 512 MB RAM

Software:
- Windows 2000 Server
- Gordano NT Mail version 6.04
- Tripwire for servers

The supplier/partner mail server contains mailboxes for suppliers and partners. When a supplier or partner wishes to communicate securely with GIAC enterprises, or send data securely, they will log into their mailbox using a web interface on the web server in the Service Network. The mail server is on the private network because this is where the data is held.

Syslog Server

IP Address: 172.17.10.3

Service Network IP Address (Address Redirection done by Firewall): 192.168.1.23
DMZ Network IP Address (Address redirection done by Firewall): 63.100.47.40

Hardware:
- Compaq Proliant DL360
- 1.4 GHz PIII processor
- 3x 18.2 GB SCSI Hard Drives, hardware RAID 5
- 512 MB RAM

Software:
- Redhat Linux 7.3
- Tripwire

The Syslog Server receives and logs Syslog messages as well as SNMP messages (port 162). It resides on the private network to protect the security logs.

Corporate Mail Server

IP Address: 172.17.10.5
Service Network IP Address (Address Redirection done by Firewall): 192.168.1.25

Hardware:
- Compaq Proliant DL360
- Two 1.4 GHz PIII processors
- 3x 18.2 GB SCSI Hard Drives, hardware RAID 5
- 512 MB RAM

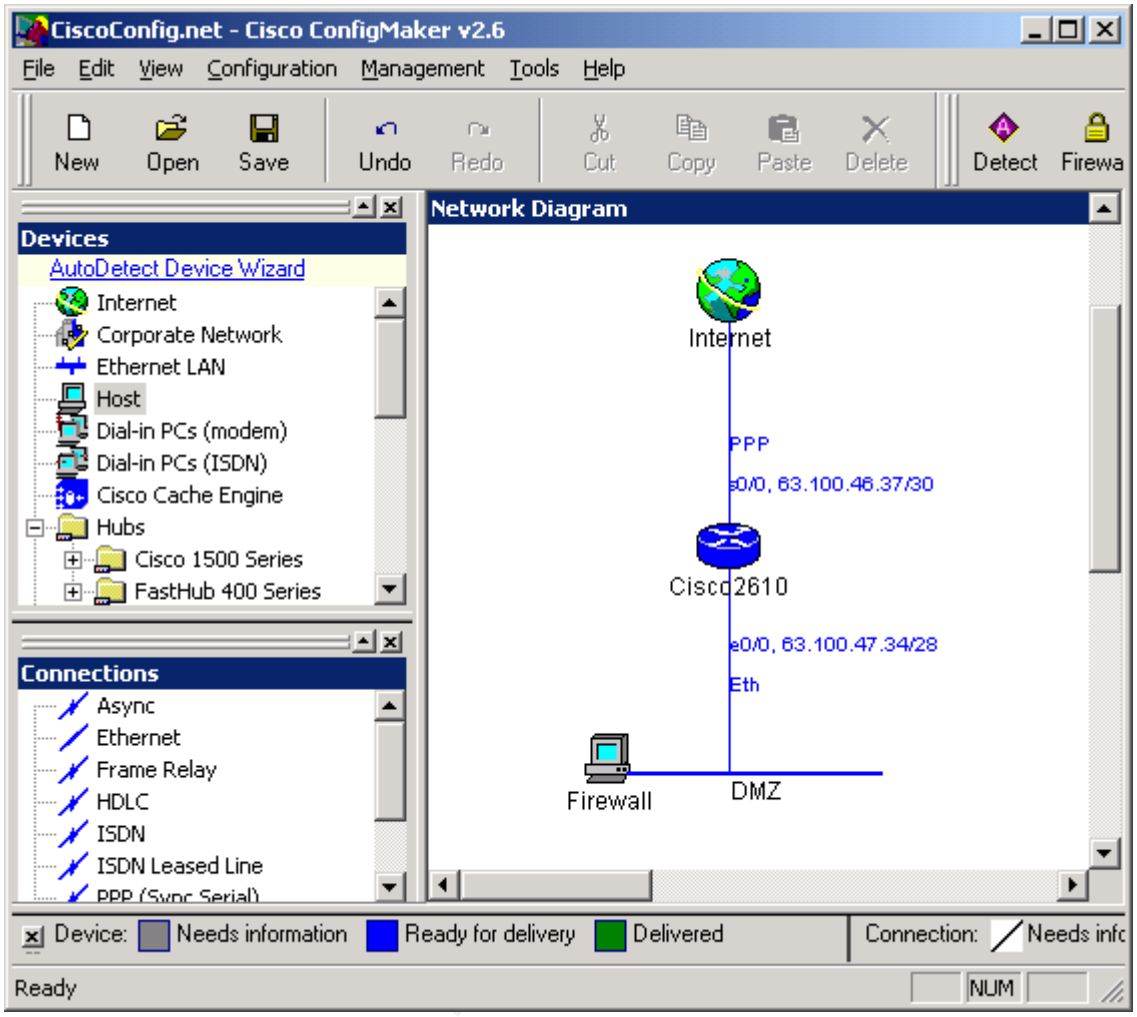
Software:
- Windows 2000 Server
- MS Exchange server Version 5.5

The corporate mail server exists on the private network. All SMTP traffic from the Internet to GIAC Enterprises or from GIAC Enterprises to the Internet goes through the SMTP Gateway in the Service Network.

Assignment 2: Security Policy and Tutorial

Border Router Configuration

First I used Cisco's Configmaker Utility to build the basic Router configuration.



Which generated this router config

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Cisco2610
!
enable password enablepw
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
 description connected to DMZ
 ip address 63.100.47.34 255.255.255.240
 keepalive 10
!
interface Serial 0/0
 no shutdown
```

```
 description connected to Internet
 service-module t1 clock source line
 service-module t1 data-coding normal
 service-module t1 remote-loopback full
 service-module t1 framing esf
 service-module t1 linecode b8zs
 service-module t1 lbo none
 service-module t1 remote-alarm-enable
 ip address 63.100.46.37 255.255.255.252
 encapsulation ppp
!
router rip
 version 2
 network 63.0.0.0
 passive-interface Serial 0/0
 no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0/0
no ip http server
snmp-server community pubcomm RO
snmp-server community privcomm RW
snmp-server location Kevins Cube
snmp-server contact Kevin,X4872,kbong@johnsonbank.com
snmp-server host 63.105.70.72 trapcomm
banner motd #Unauthorized access not permitted.  You will be prosecuted.#
!
line console 0
 exec-timeout 0 0
 password loginpw
 login
!
line vty 0 4
 password loginpw
 login
!
end
```

This I will customize to our desired secure configuration. The first resource used is the "NSA/SNAC Router Security Configuration Guide" available at http://nsa2.www.conxion.com/cisco/guides/. For each recommendation on the guide, determine if it has already been implemented by Cisco Configmaker, and if not, implement it.

Router Access and Service Configuration Recommendations

1. Shut down unneeded servers on the router. These include small services, BOOTP, finger, HTTP, and SNMP. Here are the commands do shut them off:
    - no service tcp-small-servers
    - no service udp-small-servers
    - no ip bootp server
    - no service finger
    - no ip http server
    - no snmp-server

2. Shut down unneeded services on the router. These include CDP, Remote Config, Source Routing, and Classless Routing. To disable these services, use these commands:
    - no cdp run
    - no service config
    - no ip source-route
    - no ip classless
3. Shutdown unused interfaces with this command:
    - shutdown
4. Secure all interfaces from smurf attacks and ad-hoc routing (should be applied to every interface)
    - no ip directed-broadcast
    - no ip proxy-arp
5. Further secure the console, auxiliary line, and virtual terminal with the following commands:
    - ! secure the console
    - line console 0
    - exec-timeout 5 0
    - login
    - transport input telnet
    - ! disable auxiliary line
    - line aux 0
    - no exec
    - exec-timeout 0 10
    - transport input none
    - ! secure the virtual terminal lines
    - line vty 0 4
    - exec-timeout 5 0
    - login
    - transport input telnet
6. Configure the enable-secret password, which is protected by an MD-5 algorithm.
7. Enable secret 0 ta2lymeb4n4n4
8. Use strong (hard to guess or crack) passwords on all interfaces
    - line console 0
    - password goOut2Eat$42
    - line aux 0
    - password giveMe3#Pickle5
    - line vty 0
    - password thisKnif3is2#
9. Provide basic protection for console lines by using “service password-encryption”
    - Service password-encryption
10. Configure Logging to the Private Network syslog server
    - logging on

- logging 63.100.47.40
- logging buffered
- logging console critical
- logging trap debugging
- logging facility local1

11. Configure the router to use time information in the logging
    - service timestamps log datetime localtime show-timezone
    - clock timezone EST –5
    - clock summer-time EDT recurring
    - ntp source Serial0/0
    - ntp server 203.21.37.18
    - ntp server 198.147.37.140

Below is our customized configuration, with details about the purpose for specific lines.

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
!
hostname Cisco2610
!
enable password enablepw
!
! shut down unneeded servers
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
no snmp-server
no ip name-server
!
! shut down unneeded services
no cdp run
no service config
no ip source-route
no ip classless
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0/0
 no shutdown
```

```
 description connected to DMZ
 ip address 63.100.47.34 255.255.255.240
 keepalive 10
 ! no smurf attacks
 no ip directed-broadcast
 ! ad-hoc routing
 no ip proxy-arp

!
interface Serial 0/0
 no shutdown
 description connected to Internet
 service-module t1 clock source line
 service-module t1 data-coding normal
 service-module t1 remote-loopback full
 service-module t1 framing esf
 service-module t1 linecode b8zs
 service-module t1 lbo none
 service-module t1 remote-alarm-enable
 ip address 63.100.46.37 255.255.255.252
 encapsulation ppp
 ! no smurf attacks
 no ip directed-broadcast
 ! ad-hoc routing
 no ip proxy-arp
!
!  Configure Logging to the Private Network syslog server
 logging on
 logging 63.100.47.40
 logging buffered
 logging console critical
 logging trap debugging
 logging facility local1
!
!    Configure the router to use time information in the
logging
 service timestamps log datetime localtime show-timezone
 clock timezone EST -5
 clock summer-time EDT recurring
 ntp source Serial0/0
 ntp server 203.21.37.18
 ntp server 198.147.37.140
!
!
router rip
 version 2
 network 63.0.0.0
```

```
 passive-interface Serial 0/0
 no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0/0
!no ip http server
! snmp server disabled
!snmp-server community pubcomm RO
!snmp-server community privcomm RW
!snmp-server location Kevins Cube
!snmp-server contact Kevin,X4872,kbong@johnsonbank.com
!snmp-server host 63.105.70.72 trapcomm
banner motd #Unauthorized access not permitted.  You will
be prosecuted.#
!
! secure the console
line console 0
 exec-timeout 5 0
 password goOut2Eat$42
 login
 transport input telnet
!
! disable auxiliary line
line aux 0
 no exec
 exec-timeout 0 10
 transport input none
 password giveMe3#Pickle5
!
! secure the virtual terminal lines
line vty 0 4
 exec-timeout 5 0
 password thisKnif3is2#
 login
 transport input telnet
!
end
```

Access Lists

I will apply access lists to our router to get a “first line of defense” in our layered security approach. I use extended access lists because they give us a higher level of control, rather than just testing the IP source. To define an extended access list, use access list numbers between 100 and 199. To control CPU and

memory utilization on our router, I am not going to use reflexive ACLs. Access lists read top to bottom until a match is found to the current packet, so the order of the ACL rules is very important, primarily for the logic to work correctly but also for performance. Rules to deny suspicious and non-permitted traffic come before rules to permit traffic, and our default deny rule comes last. I will not log most permitted packets.

The primary resources for the following ACL configuration are:
SANS Institute coursebook Track 2.3; Firewalls 102: Perimeter Protection and Defense In-Depth, and the Router Security Configuration Guide (National Security Agency), which is are available from
http://nsa2.www.conxion.com/cisco/guides/

Ingress Filtering
Access list 101 will be applied to the external interface, and will filter inbound traffic.

```
! First clear ACL 101
no access-list 101
! deny all packets with an RFC 1918 source address
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
! deny packets from the localhost
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
! deny all packets with a source address of our DMZ network
access-list 101 deny ip 63.100.47.32 0.0.0.15 any log
! deny broadcast
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
! deny default dhcp failed addresses
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
! reject risky protocols – tcpmux
access-list 101 deny ip any any eq 1 log
! reject risky protocols – echo
access-list 101 deny ip any any eq 7 log
! reject risky protocols – discard
access-list 101 deny ip any any eq 8 log
! reject risky protocols – systat
access-list 101 deny tcp any any eq 11 log
! reject risky protocols – daytime
access-list 101 deny ip any any eq 13 log
! reject risky protocols – netstat
access-list 101 deny tcp any any eq 15 log
! reject risky protocols – chargen
access-list 101 deny ip any any eq 19 log
! reject risky protocols – time
```

```
access-list 101 deny ip any any eq 37 log
! reject risky protocols – whois
access-list 101 deny tcp any any eq 43 log
! reject risky protocols – bootp
access-list 101 deny udp any any eq 67 log
! reject risky protocols – tftp
access-list 101 deny udp any any eq 69 log
! reject risky protocols – supdup
access-list 101 deny tcp any any eq 93 log
! reject risky protocols – sunrpc
access-list 101 deny ip any any eq 111 log
! reject risky protocols – loc-srv; netbios
access-list 101 deny ip any any range 135 139 log
! reject risky protocols – xdmpc
access-list 101 deny udp any any eq 177 log
! reject risky protocols – netbios
access-list 101 deny tcp any any eq 445 log
! reject risky protocols – rexec
access-list 101 deny tcp any any eq 512 log
! reject risky protocols – lpr
access-list 101 deny tcp any any eq 515 log
! reject risky protocols – talk
access-list 101 deny udp any any eq 517 log
! reject risky protocols – ntalk
access-list 101 deny dup any any eq 518 log
! reject risky protocols – uucp
access-list 101 deny tcp any any eq 540 log
! reject risky protocols – Microsoft UPnP
access-list 101 deny ip any any eq 1900 log
! reject risky protocols – Microsoft UPnP
access-list 101 deny ip any any eq 5000 log
! reject risky protocols – nfs
access-list 101 deny udp any any eq 2049 log
! reject risky protocols – X windows
access-list 101 deny tcp any any range 6000 6063 log
! reject risky protocols – irc
access-list 101 deny tcp any any eq 6667 log
! reject risky protocols – Netbus
access-list 101 deny tcp any any eq 12345 log
! reject risky protocols – Netbus
access-list 101 deny tcp any any eq 12346 log
! reject risky protocols – Back Orifice
access-list 101 deny ip any any eq 31337 log
! reject unused protocols – finger
access-list 101 deny tcp any any eq 79 log
! reject unused protocols – snmp
access-list 101 deny ip any any 161 log
```

```
! reject unused protocols – snmp trap
access-list 101 deny ip any any eq 162 log
! reject unused protocols – rlogin, who
access-list 101 deny ip any any eq 513 log
! reject unused protocols – rcommands, syslog
access-list 101 deny ip any any eq 514 log
! reject unused protocols – who
access-list 101 deny ip any any eq 550 log
! allow established connections
access-list 101 permit tcp any 63.100.47.32 0.0.0.15
established
! allow access to the specific services allowed on our
servers
! using their redirect addresses
! allow http access to web server, and do not log
access-list 101 permit tcp any 63.100.47.37 eq 80
! allow https access to web server, and do not log
access-list 101 permit tcp any 63.100.47.37 eq 443
! allow SMTP access to mail gateway, and do not log
access-list 101 permit tcp any 63.100.47.36 eq 25
! allow DNS access to dns server, and do not log
access-list 101 permit udp any 63.100.47.38 eq 53
! allow VPN traffic to the VPN gateway
access-list 101 permit esp any host 63.100.47.39 log
access-list 101 permit udp any eq 500 host 63.100.47.39 eq
500 log
! deny certain icmp traffic
access-list 101 deny icmp any any echo log
access-list 101 deny icmp any any redirect log
access-list 101 deny icmp any any mask-request log
access-list 101 permit icmp any any log
! default deny rule
access-list 101 deny ip any any log
```

Egress Filtering

The border router also uses Egress filtering to block some of the traffic headed out to the Internet.

Access List 151 will be used for traffic coming into the internal interface. Many of the same rules that applied to inbound traffic will be used on outbound traffic.

```
! First clear ACL 151
no access-list 151
! deny all packets with an RFC 1918 source address (since the firewall should
! use NAT to convert all addresses
access-list 151 deny ip 10.0.0.0 0.255.255.255 any log
access-list 151 deny ip 172.16.0.0 0.15.255.255 any log
access-list 151 deny ip 192.168.0.0 0.0.255.255 any log
access-list 151 deny ip 192.0.2.0 0.0.0.255 any log
```

```
! deny packets from the localhost
access-list 151 deny ip 127.0.0.0 0.255.255.255 any log
! deny broadcast
access-list 151 deny ip 0.0.0.0 0.255.255.255 any log
! deny default dhcp failed addresses
access-list 151 deny ip 169.254.0.0 0.0.255.255 any log
! reject risky protocols - tcpmux
access-list 151 deny ip any any eq 1 log
! reject risky protocols - echo
access-list 151 deny ip any any eq 7 log
! reject risky protocols - discard
access-list 151 deny ip any any eq 8 log
! reject risky protocols - systat
access-list 151 deny tcp any any eq 11 log
! reject risky protocols - daytime
access-list 151 deny ip any any eq 13 log
! reject risky protocols - netstat
access-list 151 deny tcp any any eq 15 log
! reject risky protocols - chargen
access-list 151 deny ip any any eq 19 log
! reject risky protocols - time
access-list 151 deny ip any any eq 37 log
! reject risky protocols - whois
access-list 151 deny tcp any any eq 43 log
! reject risky protocols - bootp
access-list 151 deny udp any any eq 67 log
! reject risky protocols - tftp
access-list 151 deny udp any any eq 69 log
! reject risky protocols - supdup
access-list 151 deny tcp any any eq 93 log
! reject risky protocols - sunrpc
access-list 151 deny ip any any eq 111 log
! reject risky protocols - loc-srv; netbios
access-list 151 deny ip any any range 135 139 log
! reject risky protocols - xdmpc
access-list 151 deny udp any any eq 177 log
! reject risky protocols - netbios
access-list 151 deny tcp any any eq 445 log
! reject risky protocols - rexec
access-list 151 deny tcp any any eq 512 log
! reject risky protocols - lpr
access-list 151 deny tcp any any eq 515 log
! reject risky protocols - talk
access-list 151 deny udp any any eq 517 log
! reject risky protocols - ntalk
access-list 151 deny dup any any eq 518 log
! reject risky protocols - uucp
```

```
access-list 151 deny tcp any any eq 540 log
! reject risky protocols – Microsoft UPnP
access-list 151 deny ip any any eq 1900 log
! reject risky protocols – Microsoft UPnP
access-list 151 deny ip any any eq 5000 log
! reject risky protocols – nfs
access-list 151 deny udp any any eq 2049 log
! reject risky protocols – X windows
access-list 151 deny tcp any any range 6000 6063 log
! reject risky protocols – irc
access-list 151 deny tcp any any eq 6667 log
! reject risky protocols – Netbus
access-list 151 deny tcp any any eq 12345 log
! reject risky protocols – Netbus
access-list 151 deny tcp any any eq 12346 log
! reject risky protocols – Back Orifice
access-list 151 deny ip any any eq 31337 log
! reject unused protocols – finger
access-list 151 deny tcp any any eq 79 log
! reject unused protocols – snmp
access-list 151 deny ip any any 161 log
! reject unused protocols – snmp trap
access-list 151 deny ip any any eq 162 log
! reject unused protocols – rlogin, who
access-list 151 deny ip any any eq 513 log
! reject unused protocols – rcommands, syslog
access-list 151 deny ip any any eq 514 log
! reject unused protocols – who
access-list 151 deny ip any any eq 550 log
! allow established connections
access-list 151 permit tcp any 63.100.47.32 0.0.0.15
established
! allow http outbound and do not log
access-list 151 permit tcp 63.100.47.32 0.0.0.15 any eq 80
! allow https access outbound and do not log
access-list 151 permit tcp 63.100.47.32 0.0.0.15 any eq 443
! allow ftp access outbound and do not log
access-list 151 permit tcp 63.100.47.32 0.0.0.15 any eq 21
! allow SMTP access to mail and do not log
access-list 151 permit tcp 63.100.47.32 0.0.0.15 any eq 25
! allow DNS access to dns and do not log
access-list 151 permit ip 63.100.47.32 0.0.0.15 any eq 53
! allow ike traffic to the VPN gateway
access-list 151 permit udp 63.100.47.39  eq 500 any eq 500
log
! deny certain icmp traffic
access-list 151 deny icmp any any echo log
```

```
access-list 151 deny icmp any any redirect log
access-list 151 deny icmp any any mask-request log
access-list 151 permit icmp any any log
! default deny rule
access-list 151 deny ip any any log
```

VPN Policy

The VPN will be used by mobile employees and telecommuters to connect to the GIAC enterprise's network. Users will only be permitted to connect to the Terminal Server on the private network, which will then allow them access to all the services that a desktop user on the private network would have. Here is how the VPN will be configured:

User Accounts:
User accounts for VPN access will be created on the firewall. This will give us firm control over who has access to the VPN. The VPN password will be different from the user's network password, so that an intruder would need to guess both passwords to gain access to network resources.

Security Gateway Address
The address of the security gateway on the firewall will be 63.100.47.39

Protocols
The VPN will use IPSEC
The VPN will use IKE for key exchange.

Access Restrictions
Clients connecting to the VPN gateway will only be allowed to communicate with the Private Network Terminal Server, at 172.17.10.10.

Policy Detail
Encapsulation Protocol: IPSEC/IKE
Data Integrity Protocol: MD5
Data Privacy Protocol First Preference: 3DES
Data Privacy Protocol Second Preference: DES
Data Compression: LZS
Session Lifetime Timeout: 8 hours
Inactivity Timeout: 30 minutes
Encapsulation Mode: Tunnel
Data Integrity will be only applied to the data portion of the packet (ESP)

VPN Client
VPN Clients will use the Symantec SEVPN Client software to connect to the security gateway.

Private Network Originated Traffic

The firewall will by default deny all traffic passing through it. The following are the only traffic types permitted.

Purpose	Source IP	Source Port	Destination IP	Destination Port/Protocol	Base Protocol
Web browsing	172.17.30.*	*	All Internet Ips	HTTP (80)	TCP
Secure Web browsing	172.17.30.*	*	All Internet Ips	HTTPs (443)	TCP
Web browsing of GIAC server	172.17.30.*	*	192.168.1.7	HTTP (80)	TCP
Secure Web browsing of GIAC server	172.17.30.*	*	192.168.1.7	HTTPs (443)	TCP
File Transfer	172.17.30.*	*	All Internet Ips	FTP (21)	TCP
Web browsing	172.17.10.10	*	All Internet Ips	HTTP (80)	TCP
Secure Web browsing	172.17.10.10	*	All Internet Ips	HTTPs (443)	TCP
Web browsing of GIAC server	172.17.10.10	*	192.168.1.7	HTTP (80)	TCP
Secure Web browsing of GIAC server	172.17.10.10	*	192.168.1.7	HTTPs (443)	TCP
File Transfer	172.17.10.10	*	All Internet Ips	FTP (21)	TCP
Outbound SMTP	172.17.10.5	*	192.168.1.6	SMTP (25)	TCP
Outbound SMTP	172.17.10.2	*	192.168.1.6	SMTP (25)	TCP
DNS Queries	172.17.10.8	*	All Internet Ips	DNS (53)	TCP and UDP
Network Management Traffic	172.17.20.4		All Internet Ips		ICMP
Network Management Traffic	172.17.20.4		192.168.1.*		ICMP
Network Management Traffic	172.17.20.4		63.105.70.*		ICMP
Network Management Traffic	172.17.20.4	*	192.168.1.*	*	TCP
Network Management Traffic	172.17.20.4	*	192.168.1.*	*	UDP
Network Management Traffic	172.17.20.4	*	63.105.70.*	*	TCP
Network	172.17.20.4	*	63.105.70.*	*	UDP

Management Traffic					

Service Network Originated Traffic

The firewall will by default deny all traffic passing through it. The following are the only traffic types permitted.

Purpose	Source IP	Source Port	Destination IP	Destination Port/Protocol	Base Protocol
IDS Alerts	192.168.1.5	*	172.17.10.3	Syslog (514)	UDP
Inbound SMTP	192.168.1.6	*	172.17.10.5	SMTP (25)	TCP
Outbound SMTP	192.168.1.6	*	All Internet Ips	SMTP (25)	TCP
DNS Queries	192.168.1.8	*	All Internet Ips	DNS (53)	TCP and UDP
Database Queries from Web Server	192.168.1.7	*	172.17.10.4	1544 (Custom)	TCP
IMAP Queries from webserver	192.168.1.7	*	172.17.10.2	IMAP(143)	TCP
SNMP Alerts	192.168.1.*	*	172.17.10.3	SNMP (161)	TCP

Internet Originated Traffic

The firewall will by default deny all traffic passing through it. The following are the only traffic types permitted.

Purpose	Source IP	Source Port	Destination IP	Destination Port/Protocol	Protocol
Router SNMP Alerts	63.100.47.34	*	172.17.10.3	SNMP (161)	UDP
Inbound SMTP	All Internet Ips	*	192.168.1.6	SMTP (25)	TCP
DNS Queries	All Internet Ips	*	192.168.1.8	DNS (53)	TCP
Web Requests	All Internet Ips	*	192.168.1.7	HTTP (80)	TCP
Secure Web Requests	All Internet Ips	*	192.168.1.7	HTTPS (443)	TCP

Firewall Implementation Tutorial

Overview of steps to implement the firewall

1. Install base OS, service packs, and security patches
2. Configure the network cards
3. Install Symantec Enterprise Firewall
4. Check for and install any service packs and security patches for the Symantec firewall
5. Launch the Management console and login to the firewall administration interface
6. Configure Routing
7. Configure Remote Management Passwords

8. Configure DNS
9. Configure Network Entities
10. Configure Redirected Services
11. Configure Custom Protocols
12. Configure Rules

Install base OS, service packs, and security patches

Install windows 2000 server with required components, but do not install unnecessary services such as Internet Information Server or Remote Access Services. Upgrade to the latest service pack, and then check http://www.microsoft.com/technet/security/ for the latest OS security patches.

Configure the network cards

Configure the network card that will be the external interface with the following settings:
IP Address: 63.100.47.33
Subnet Mask: 255.255.255.240
Gateway: 63.100.47.34

Configure the network card that will be the Service Network interface with the following settings:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: None

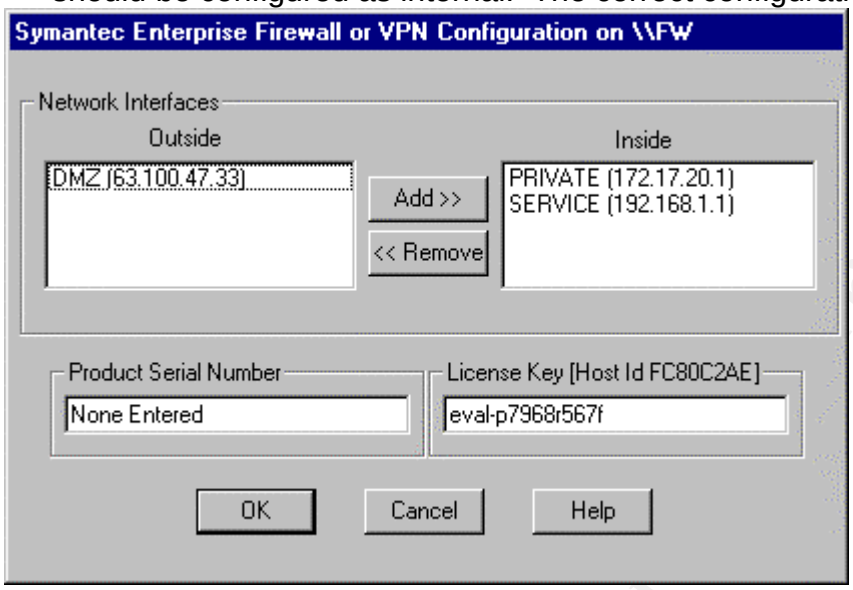
Configure the network card that will be the Private Network interface with the following settings:
IP Address: 172.17.20.1
Subnet Mask: 255.255.0.0
Gateway: None

Important: The only interface with a default gateway should be the external interface.

Install the Symantec Enterprise Firewall

1. Download the Symantec Enterprise Firewall software from the Symantec Website.
2. Unzip the archive. The folder C:\SymantecSW will be created.
3. Navigate to the folder C:\SymantecSW\SEF_SEVPN_70\DES\SYMC_fw_vpn\DES\ and launch the program Setup.exe
4. Follow the installation steps, including accepting the license agreement, entering you license key, and choosing the installation folder.

5. On the Interface configuration screen, the only interface that should be configured as an “external” interface is the one that has an IP address assigned by the service provider. All interfaces with RFC 1918 addresses should be configured as internal. The correct configuration is shown:

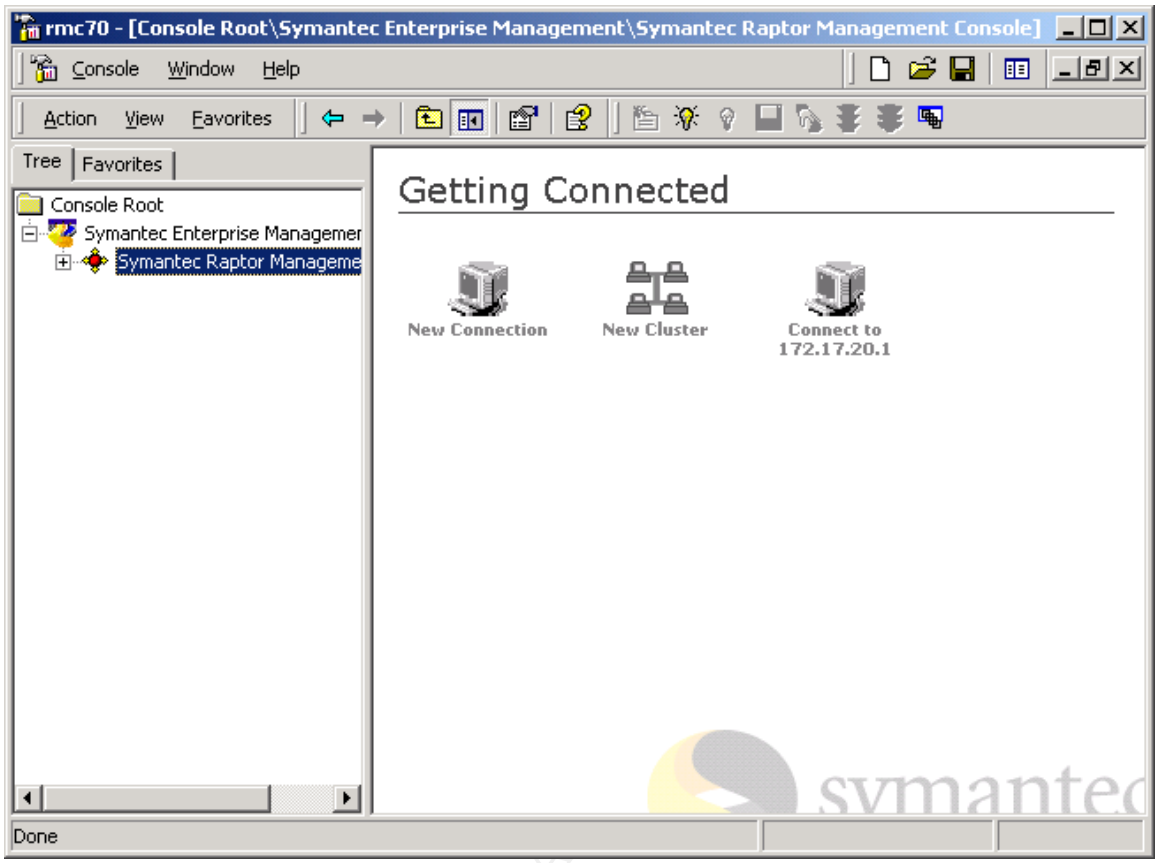


Install any security patches for the Symantec Enterprise Firewall

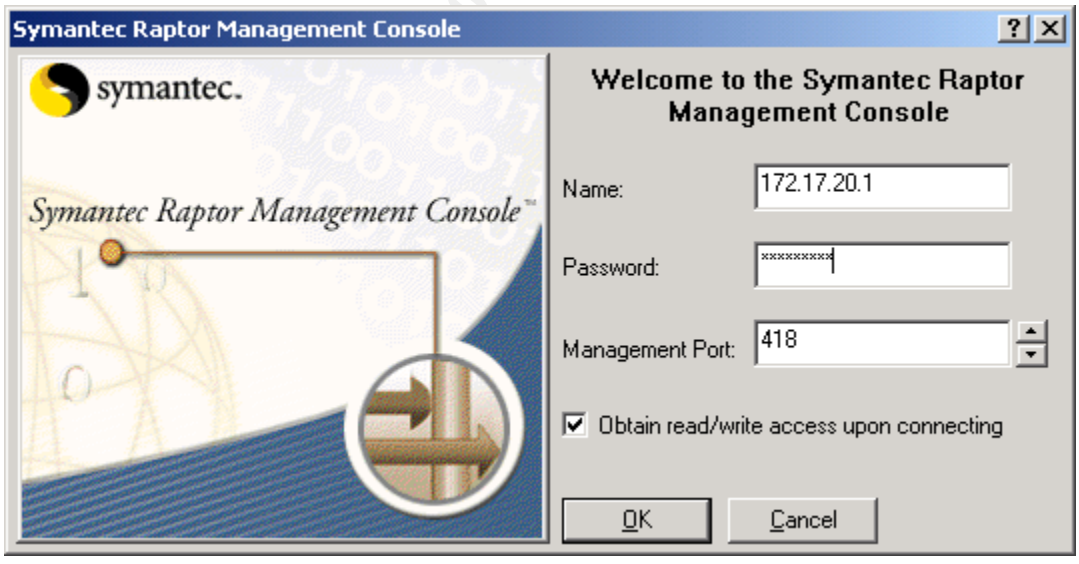
Go to http://www.symantec.com/techsupp/enterprise/ and search for the latest hotfixes available for the version of the firewall software you are running.

Connect to the Management Console

Click on the ‘Symantec Raptor Management Console” icon to launch the management application. You will see a screen similar to the following:

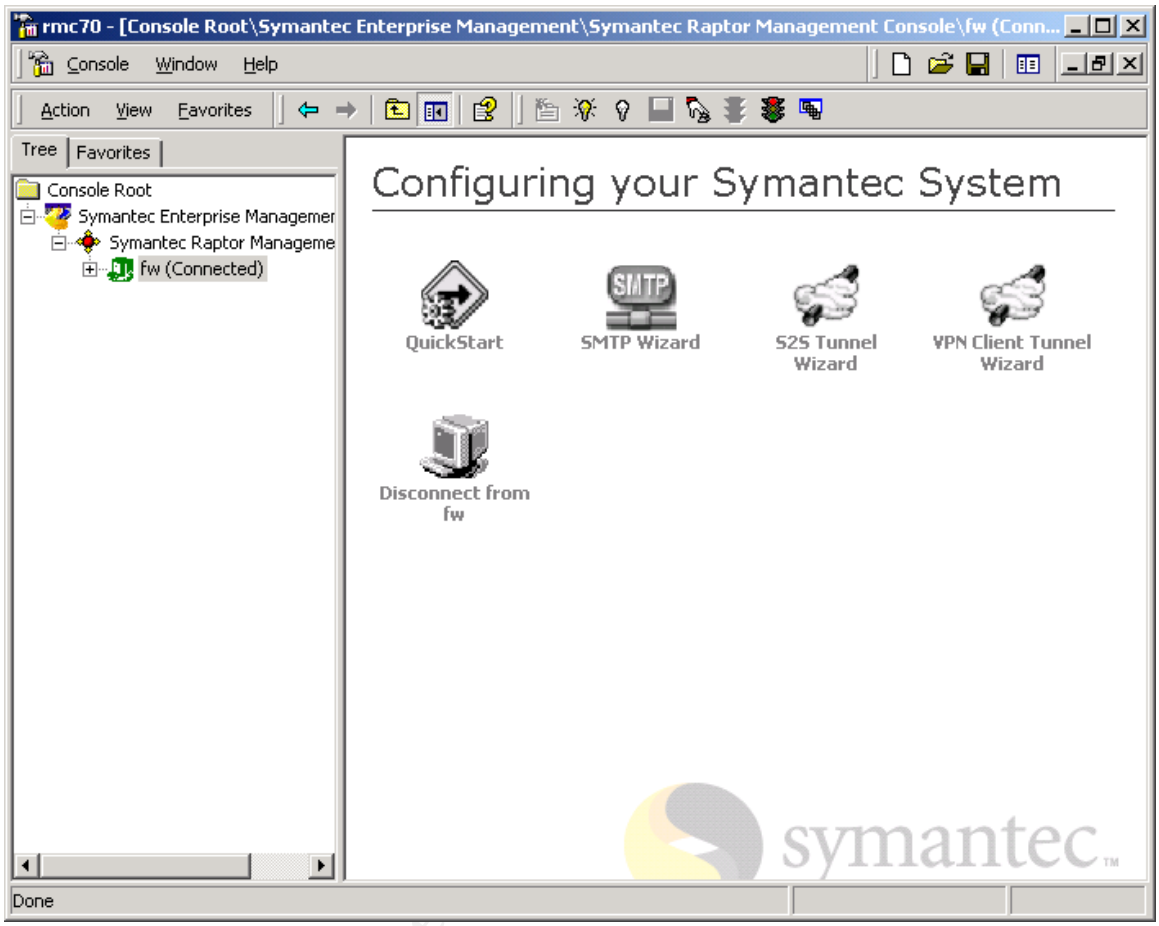


Click on “New Connection” and you will get the following dialog:



Enter the password that you entered when you installed the Raptor software and click OK.

Once you connect, the firewall icon turns green



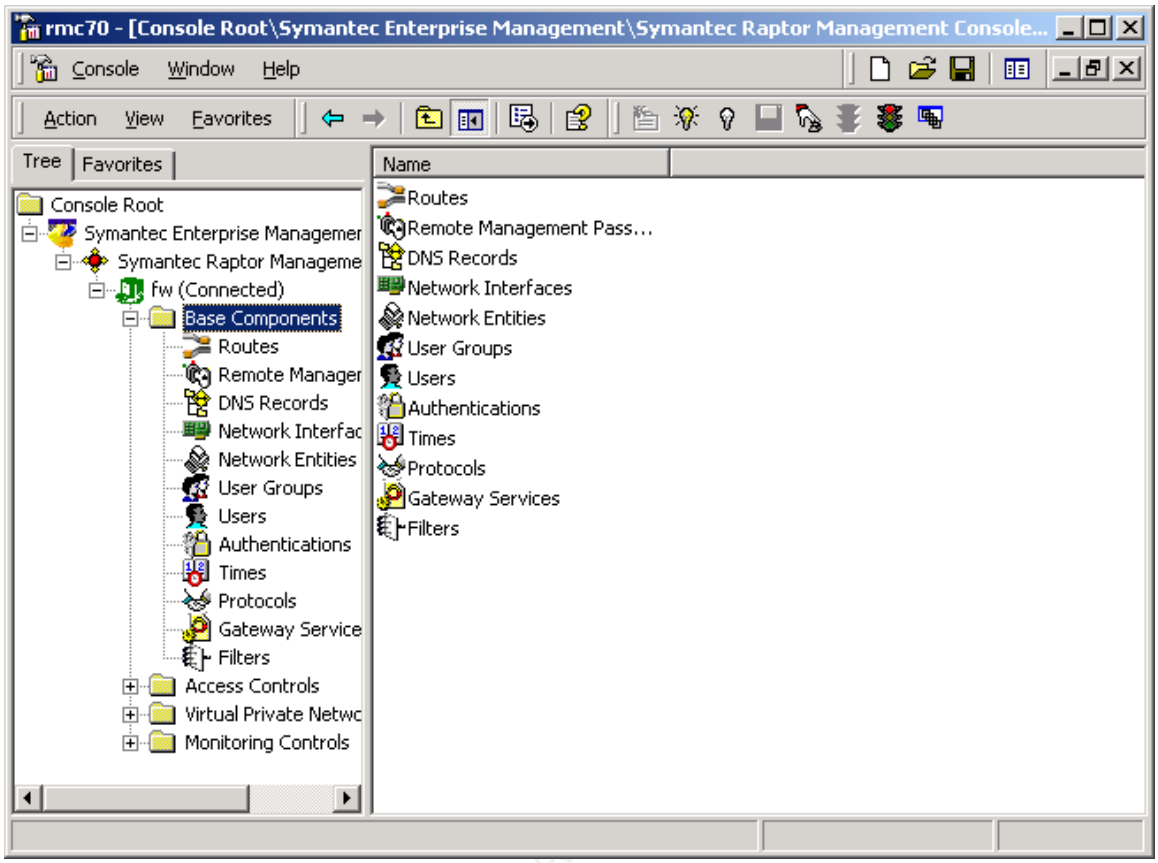
Configuring Routing

The first step after connecting is to set up our routes. The internal routing table on the security gateway must be manually configured, it does not support dynamic routing.

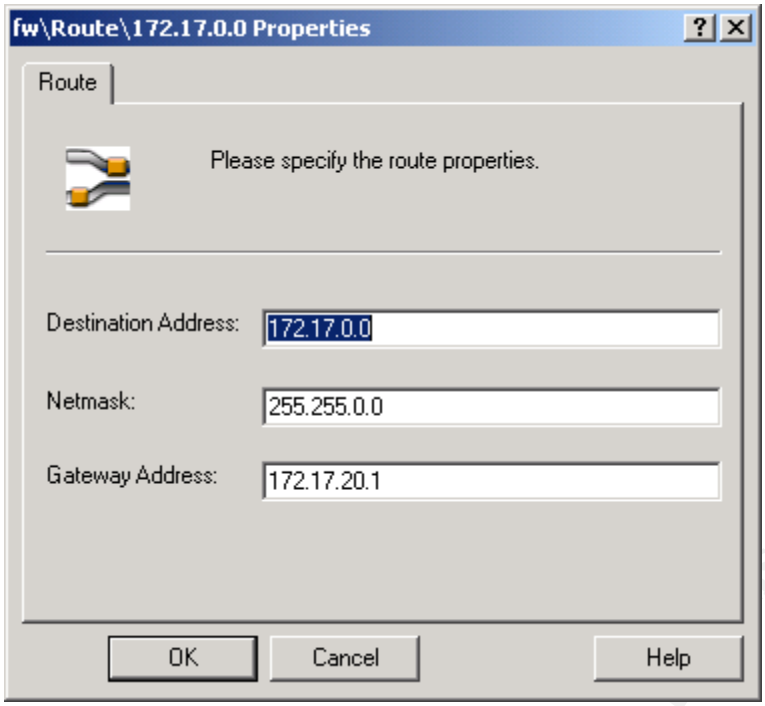
Use the Network Control Panel to set the default route on the external interface:

Once that is done, configure the routes within the firewall using the Symantec Remote Management Console. You need to configure a route that says all traffic destined for the 172.17.x.x network goes through the Private network interface. To do this, follow these steps:

1. In the Symantec Enterprise Management Console, expand the Firewall and then expand the “Base Components” folder.



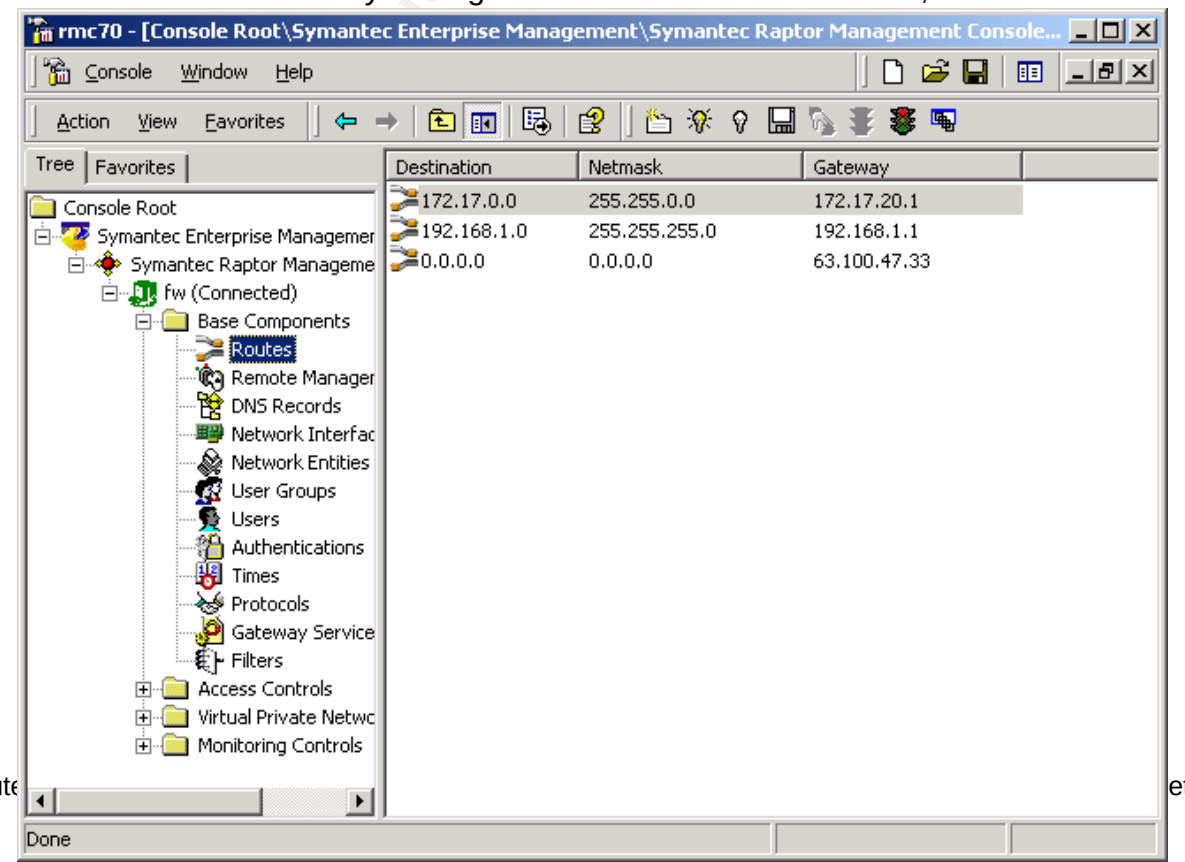
2. Right click on Routes and Click “New” Then “Route”



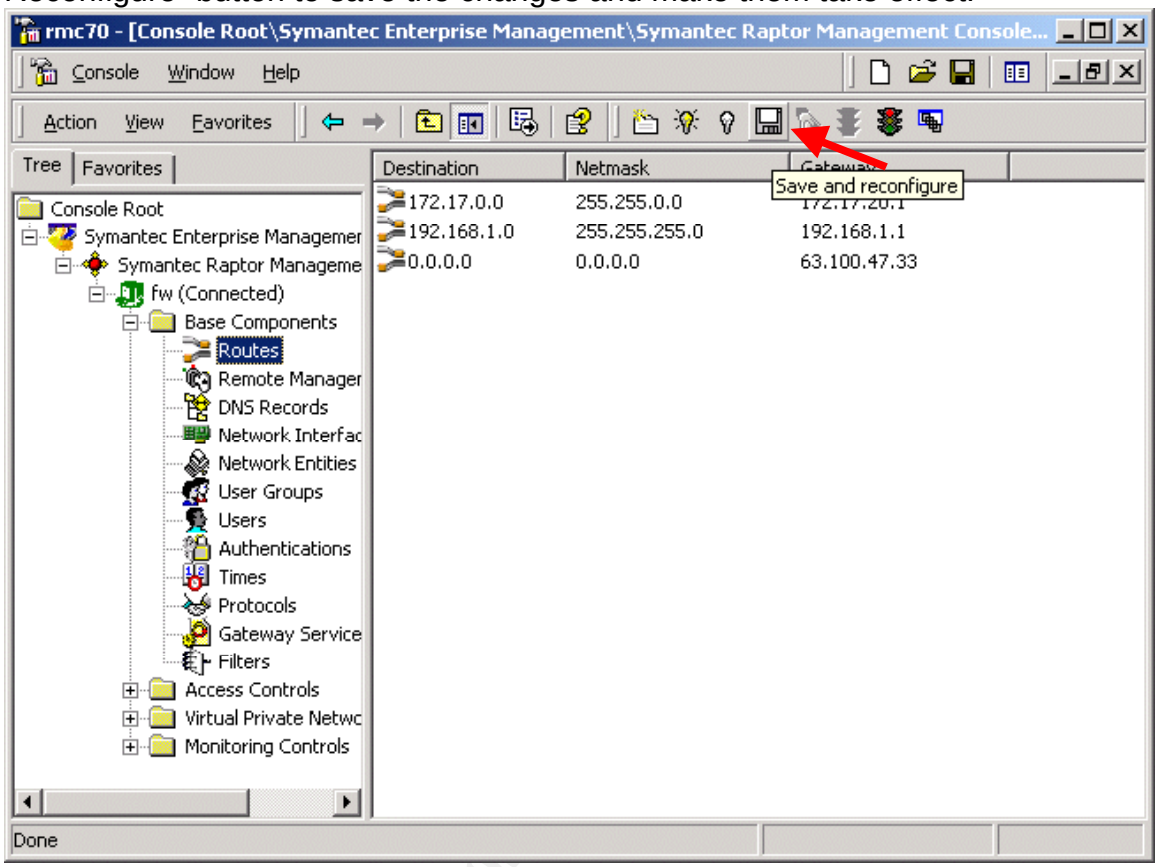
3. For the Destination address, enter the “172.17.0.0” network. The subnet is “255.255.0.0”, and the Gateway Address is the Private Network Firewall Interface, or 172.17.20.1.

You also need to add a route for the Service Network addresses. Follow the same steps as above, using a Destination address of 192.168.1.0, Subnet of 255.255.255.0, and a Gateway of 192.168.1.1.

Finally, you need to add a route that says to send all other traffic out the external interface. This is done by adding a route for the network 0.0.0.0, Subnet



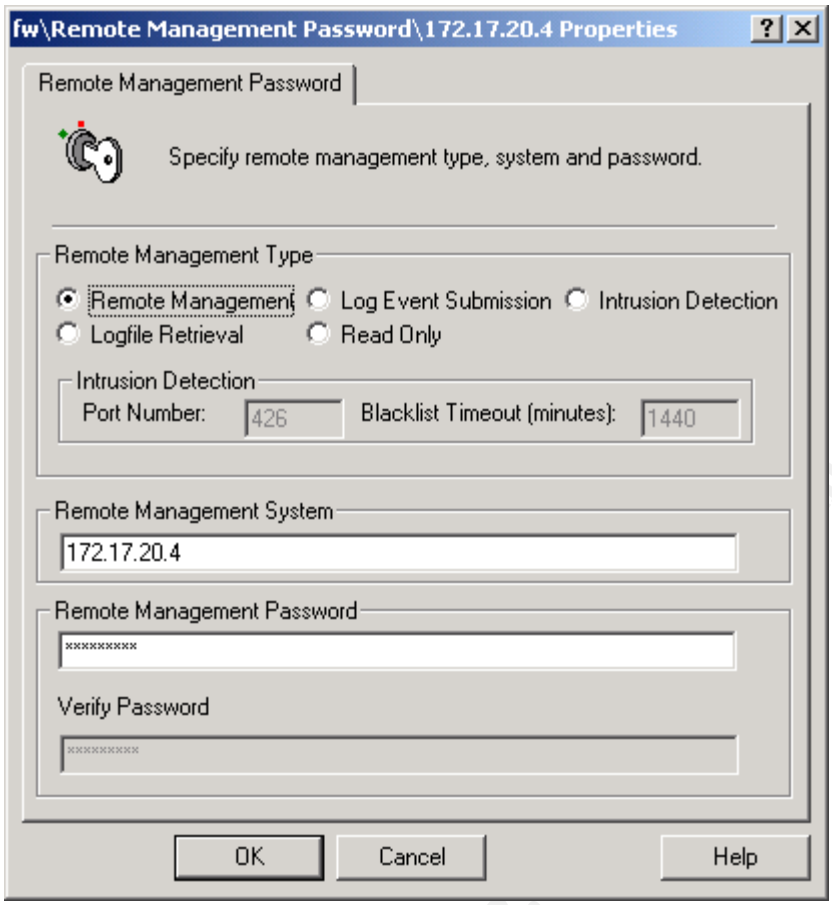
After making any changes to the firewall, you need to press the “Save and Reconfigure” button to save the changes and make them take effect:



Configure Remote Management Passwords

Remote Management Passwords allow us to set up management stations that are allowed to connect to and configure the firewall using the Symantec Raptor Management Console application.
Follow these steps to add a remote management workstation:

1. Expand the “Base Components” folder of the firewall in the Management Console.
2. Right- click on “Remote Management Passwords” and choose New..Management Password
3. The following dialog will display:



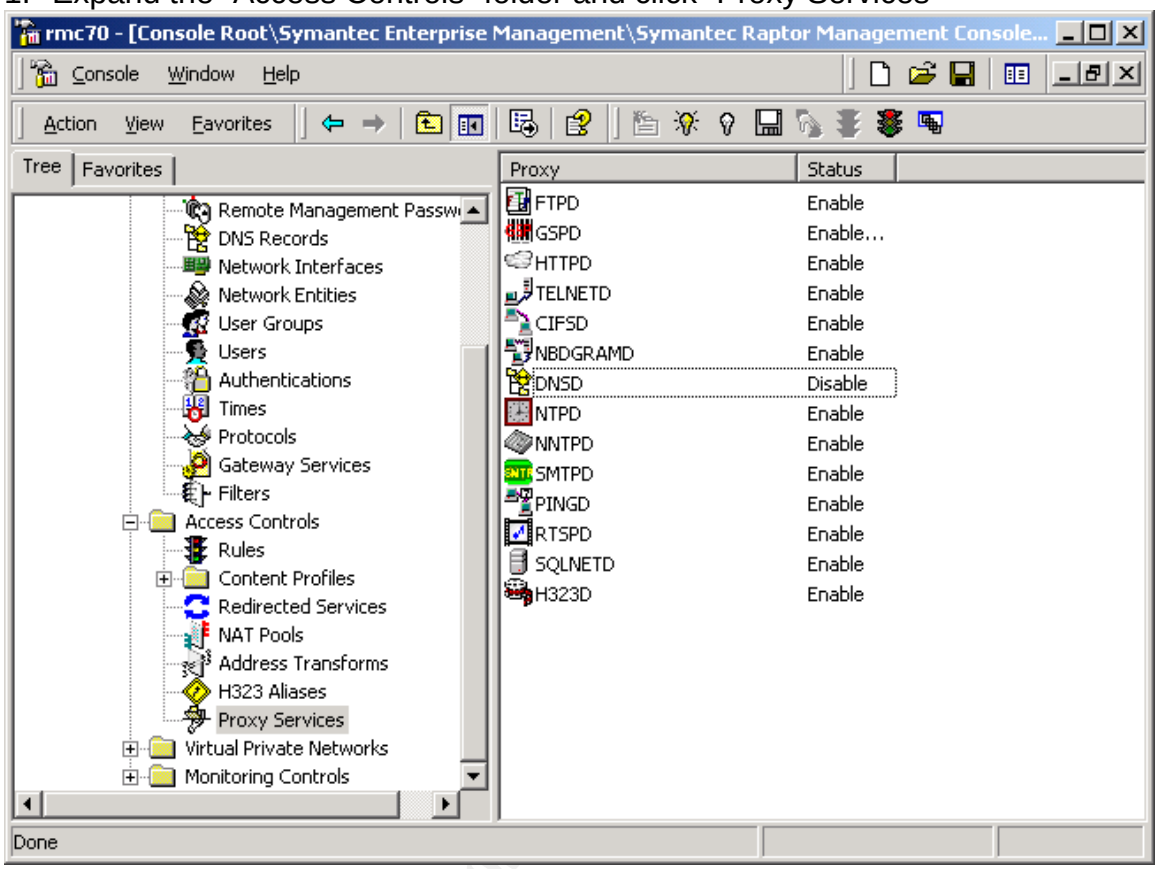
4. Under “Remote Management System” add the IP Address of the Network Manager’s Workstation (172.17.20.4)
5. Enter the Remote Management password twice to verify it is typed in correctly.
6. The default selection “Remote Management” is kept. This will allow Network Administrator to configure the firewall settings from her workstation.
7. Click OK, then click “Save and reconfigure” to save changes.

DNS Configuration

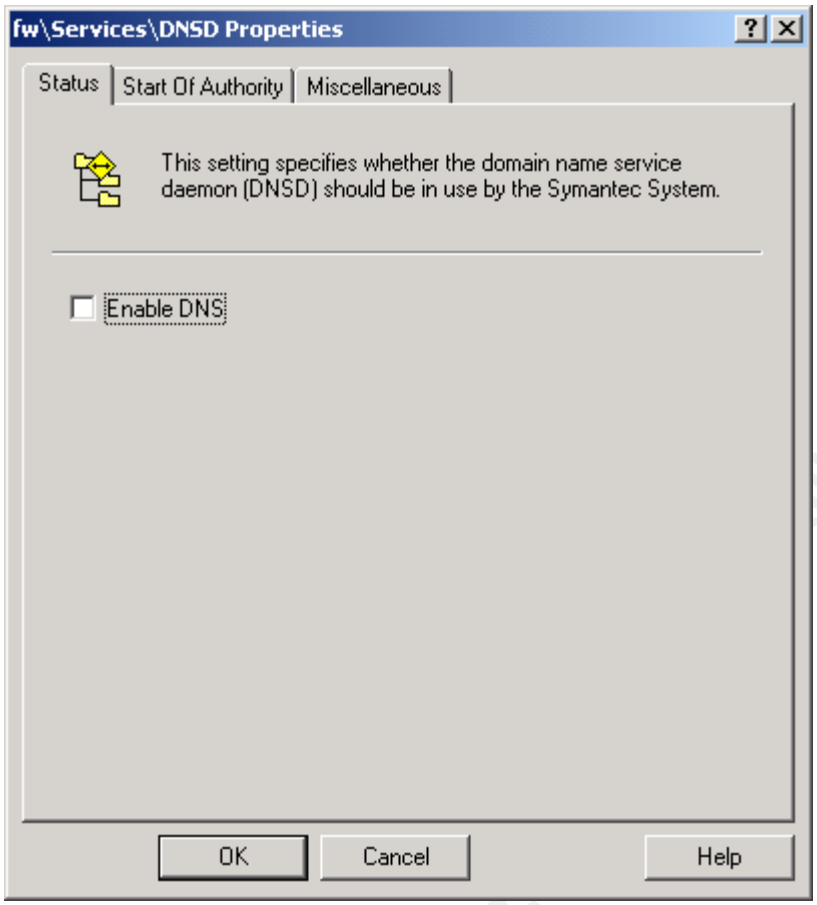
The firewall can act as a DNS server, but GIAC has opted to instead use its DNS servers in the Service Network and Private Network to be the authoritative name servers. GIAC is using a split-level DNS, the Service Network DNS server is authoritative for the domain GIAC.com and services devices in the service network and requests from the Internet. The Private Network DNS server is authoritative for the domain GIAC.com and services only devices on the private network.

Since they are not using the firewall’s built in DNS service, it will need to be disabled.

1. Expand the “Access Controls” folder and click “Proxy Services”



2. Right Click on “DNSD” and choose Properties.
3. Uncheck the “Enable DNS” box. Click Ok, and then click “Save and Reconfigure” to save changes.



The rules to allow DNS traffic to pass through the firewall will be configured later.

Configuring Network Entities

A network entity is a host or group of hosts which will pass data through the firewall. We must configure a network entity for each system or group of systems that will have unique rules for passing data through the firewall.

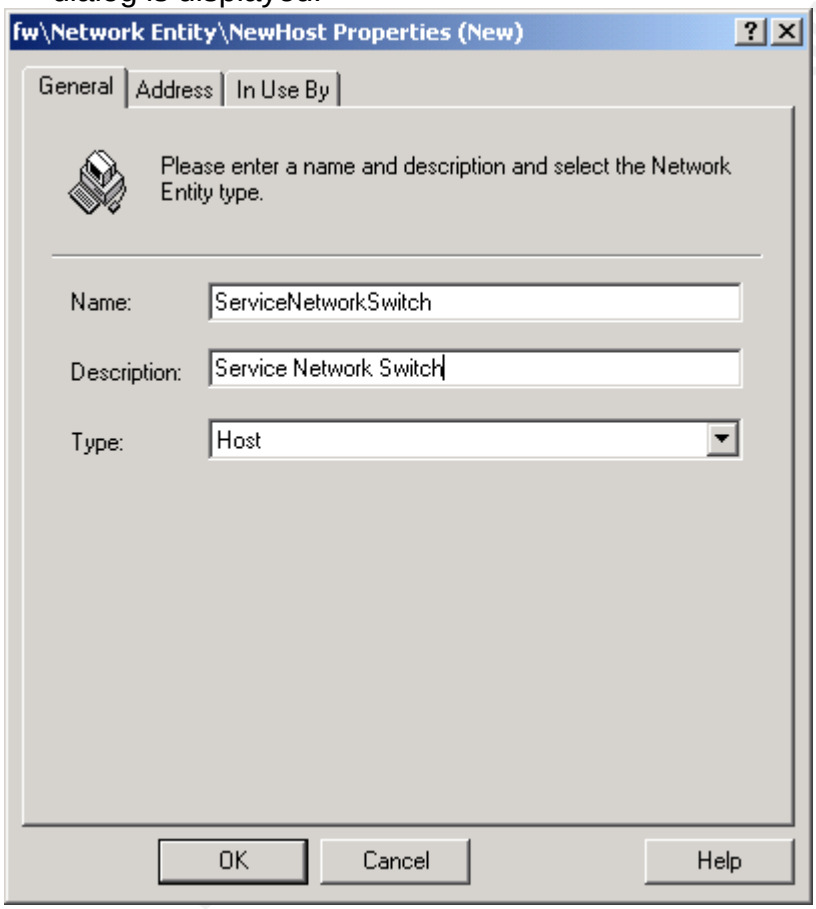
Our list of network entities is as follows:

- Service Network Switch
- Service Network IDS Sensor
- Service Network SMTP Gateway
- Service Network Web Server
- Service Network DNS Server
- Private Network Administrator Workstation
- Private Network Supplier/Partner Mail Server
- Private Network Syslog Server
- Private Network Corporate Database
- Private Network Corporate Mail Server

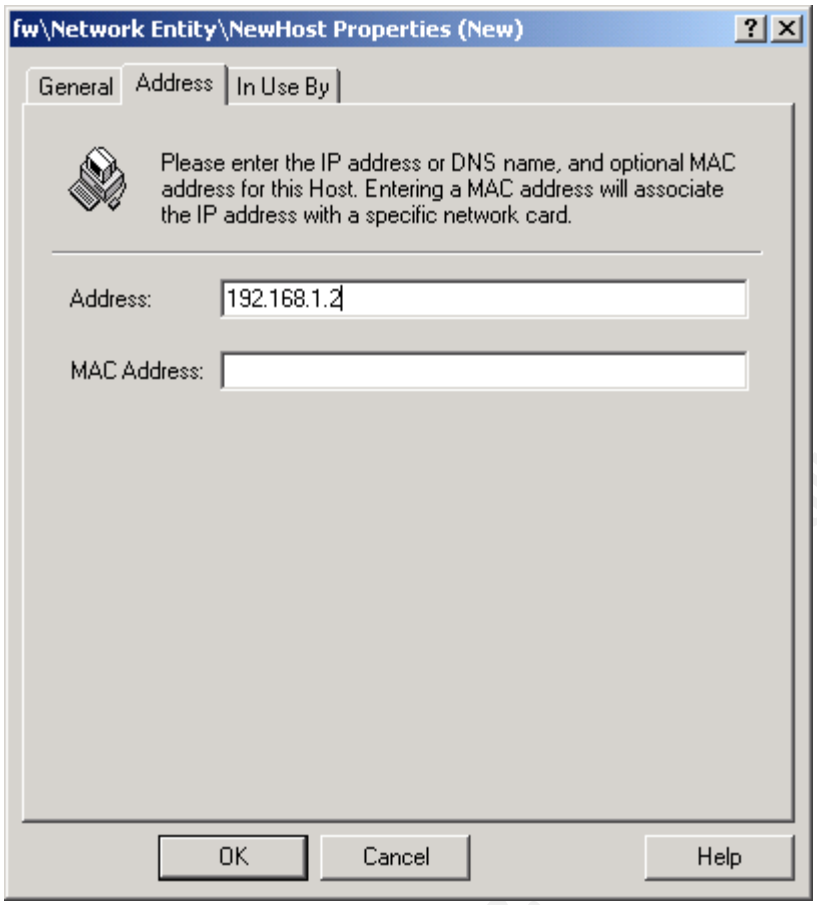
- Private Network Internal DNS Server
- Private Network Network Administrator station
- Private Network all user workstations
- Private Network Terminal Server
- All Internet Addresses
- Border Router Internal Interface

To configure a single network entity:

1. Expand the “Base Components” folder
2. Click on “Network Entities”
3. Right Click on “Network Entities” and choose “New Host”. The following dialog is displayed:



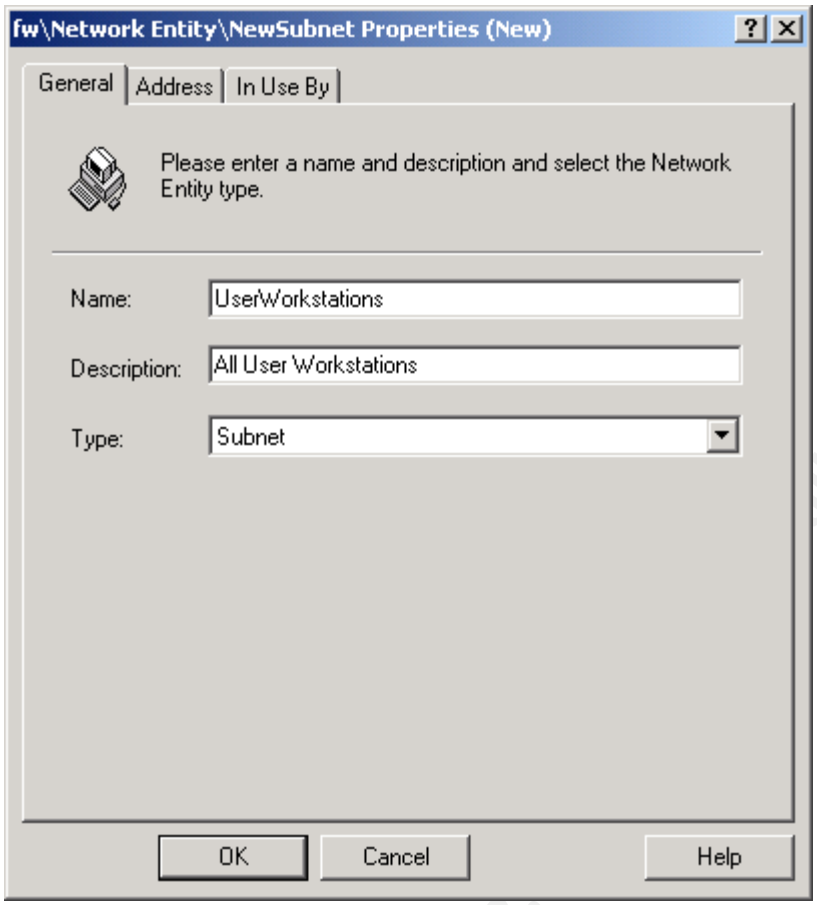
4. The name of the first host is the “Service Network Switch”. It is of type host.
5. Click on the Address tab and enter the IP address for the device. The IP address of the switch is 192.168.1.2. The MAC address is not required, but can be entered for additional security.



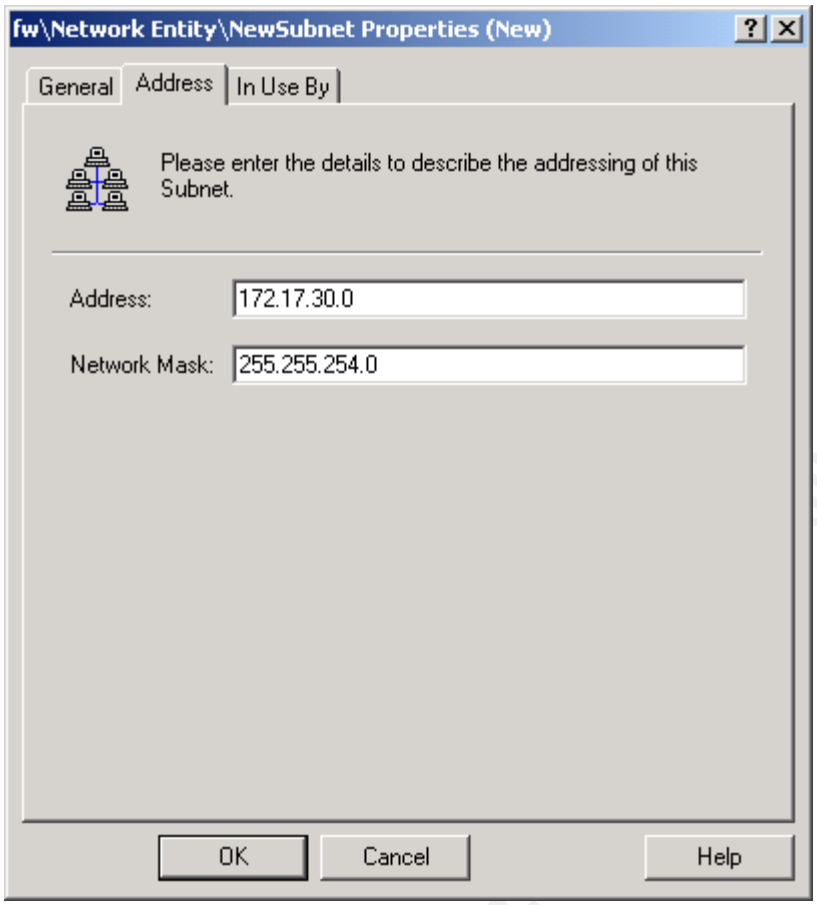
6. Click OK.

Since all of our user workstations will have the same rules applied, and all lie on the same network, we can add them as a group rather than each individually. To add a group of all hosts on the same network, follow these steps:

1. Expand the “Base Components” folder
2. Click on “Network Entities”
3. Right Click on “Network Entities” and choose “New Subnet”. The following dialog is displayed:

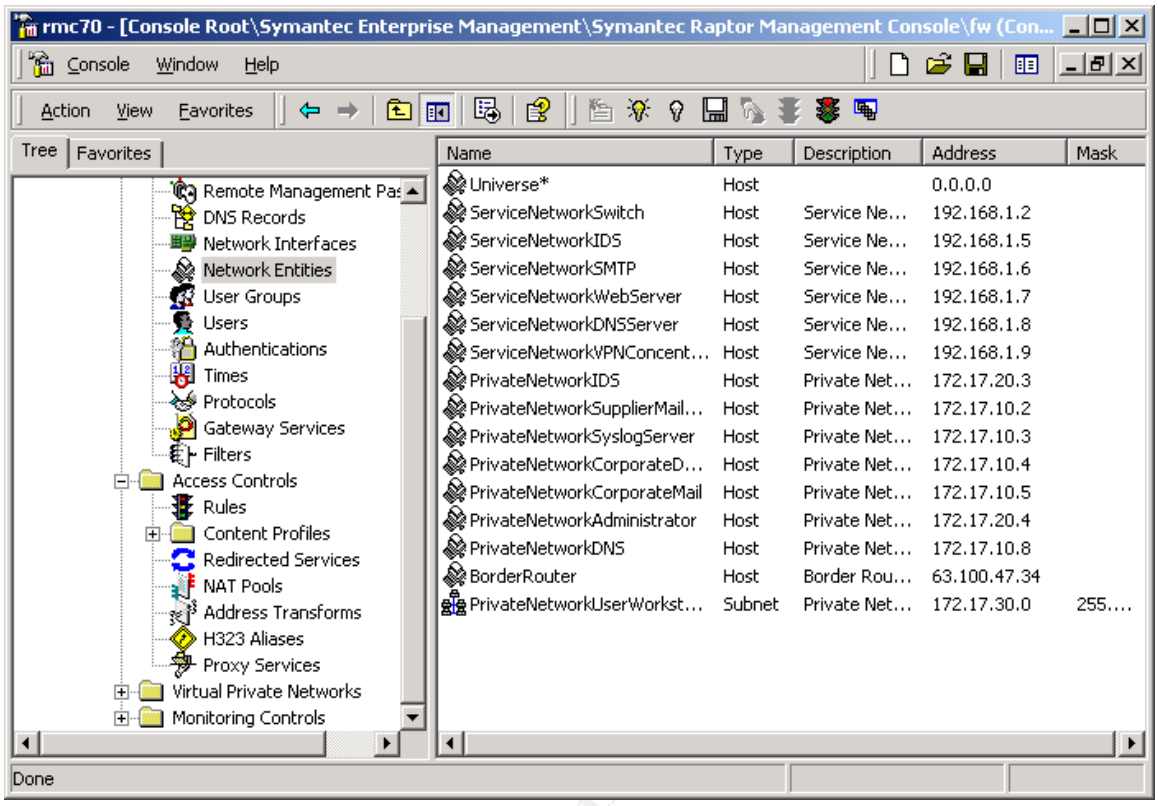


4. Click on the Address Tab.



5. The Address for our User Workstation subnet is 172.17.30.0, and the Network Mask is 255.255.255.0.
6. Click Ok.

Follow this process to add all applicable hosts to the system. When complete, remember to click “Save and reconfigure”.



Configuring Redirected Services

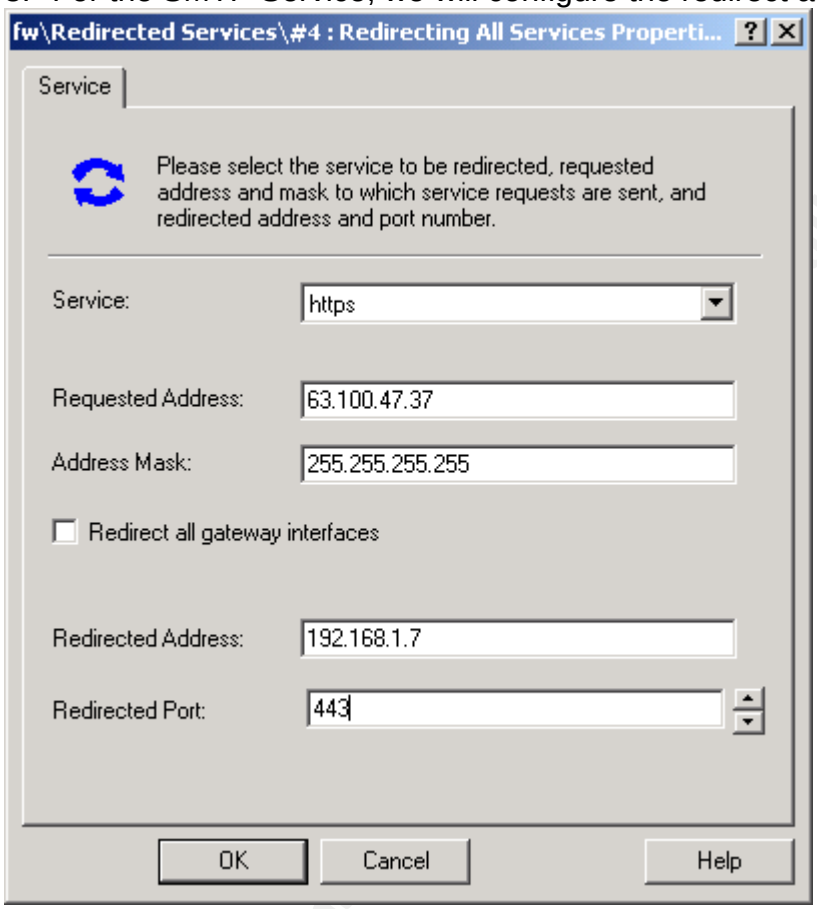
Since we are using non-routable addresses on our service network devices, but these devices are running services that will be available to Internet hosts, we need the firewall to redirect traffic destined for Internet Routable addresses to the Service Network. As we saw above, the following addresses need to be redirected:

Service	**Internet Address**	**Redirects to Service Network Address**
SMTP	63.100.47.36	192.168.1.6
HTTP/HTTPS	63.100.47.37	192.168.1.7
DNS	63.100.47.38	192.168.1.8
Service	**Internet Address**	**Redirects Private Network Address**
Syslog for border router	63.100.47.40	172.17.10.3
Service	**Service Network Address**	**Redirects to Private Network Address**
SMTP to mail server	192.168.1.25	172.17.10.5
Syslog	192.168.1.23	172.17.10.3
Corporate Database ODBC	192.168.1.24	172.17.10.4

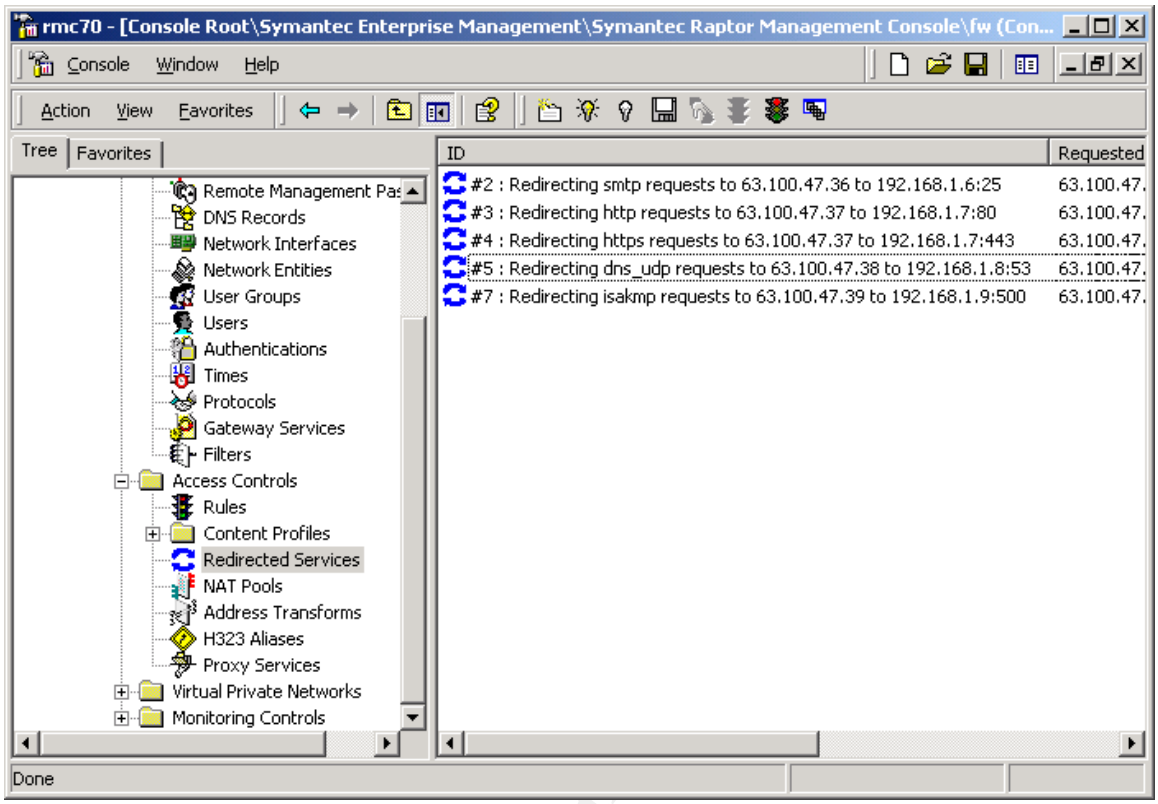
IMAP to mail server	192.168.1.22	172.17.10.2

To configure the firewall to redirect an address:

1. Expand the “Access Controls” folder
2. Right Click on “Redirected Services” and choose “New”..”Redirected Service”
3. For the SMTP Service, we will configure the redirect as shown:



Follow the same process to create each redirected service.



Configuring Rules

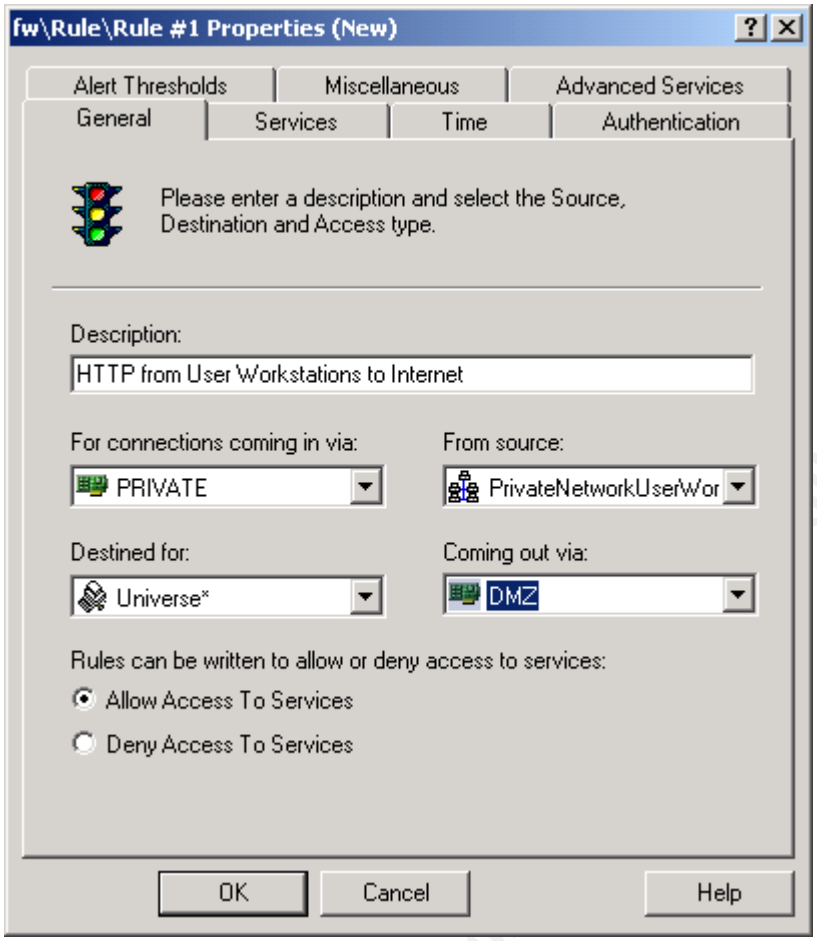
Now we are ready to create the rules that will allow traffic to pass through the firewall.
Our firewall will be configured as default “Deny All”, and then permit specific services as necessary.

The Symantec firewall orders rules based on how specific they are. Rules dealing with a specific host are tested before rules that apply to a subnet. Subnet rules are tested before domain rules, and domain rules are tested before rules that apply to the entire universe.

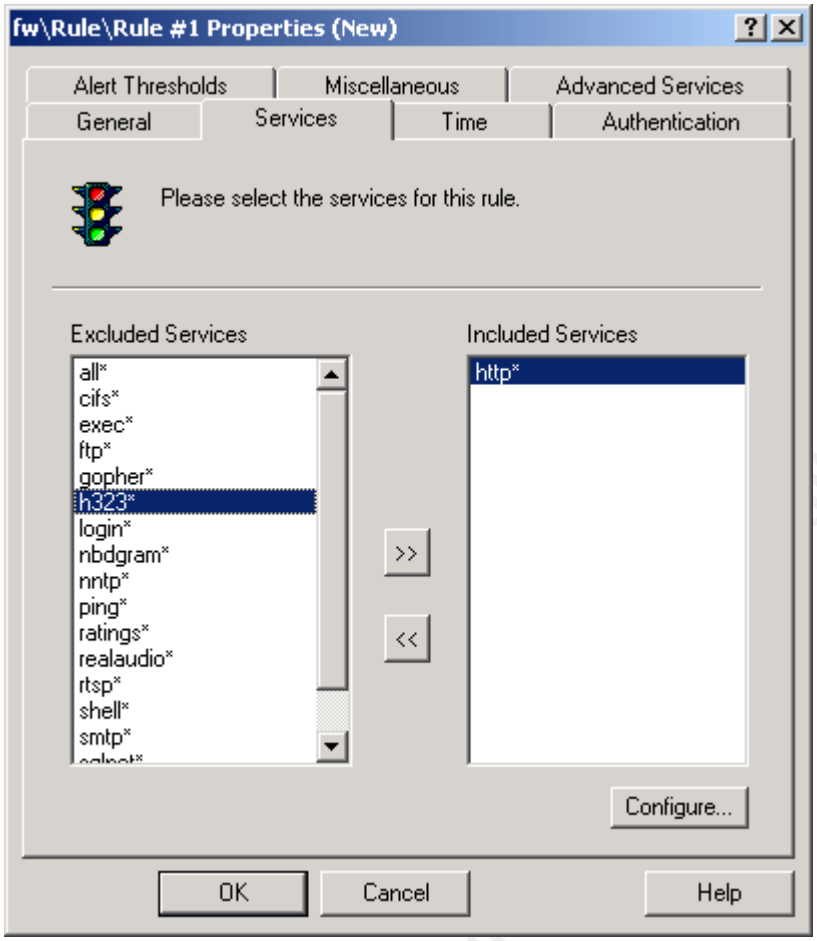
Important – Rules should always be created using the true IP address of a device. A virtual or redirected IP address should never appear in a rule (if the address was redirected by the same firewall that contains the rule.)

Looking at our firewall policy above, our first rule is to allow web browsing (HTTP Traffic) by all internal network workstations. To Create the rule to allow this traffic:

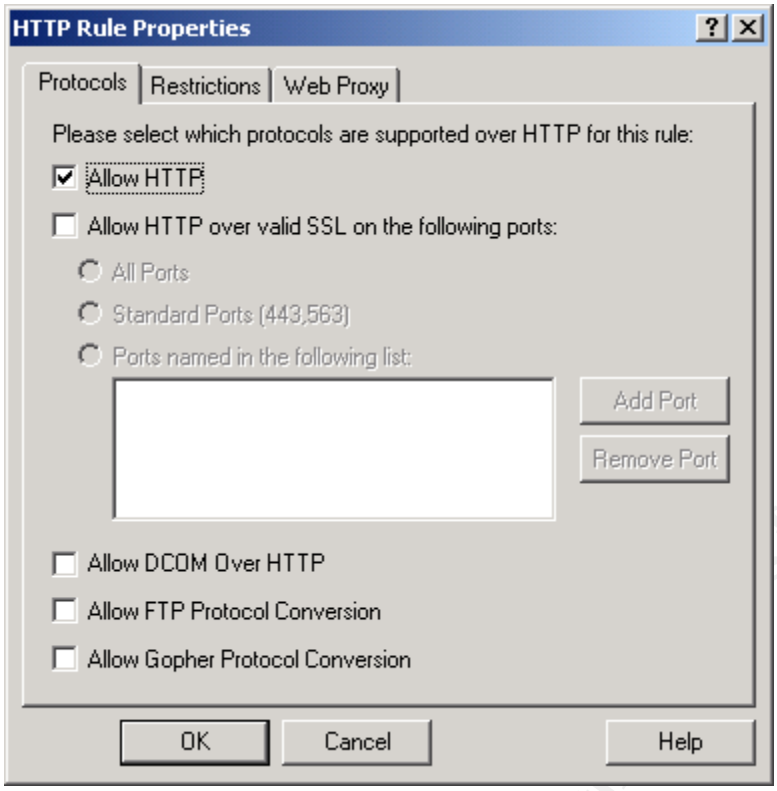
1. Expand the “Access Controls” folder
2. Right-click on Rules and choose “New..Rule”



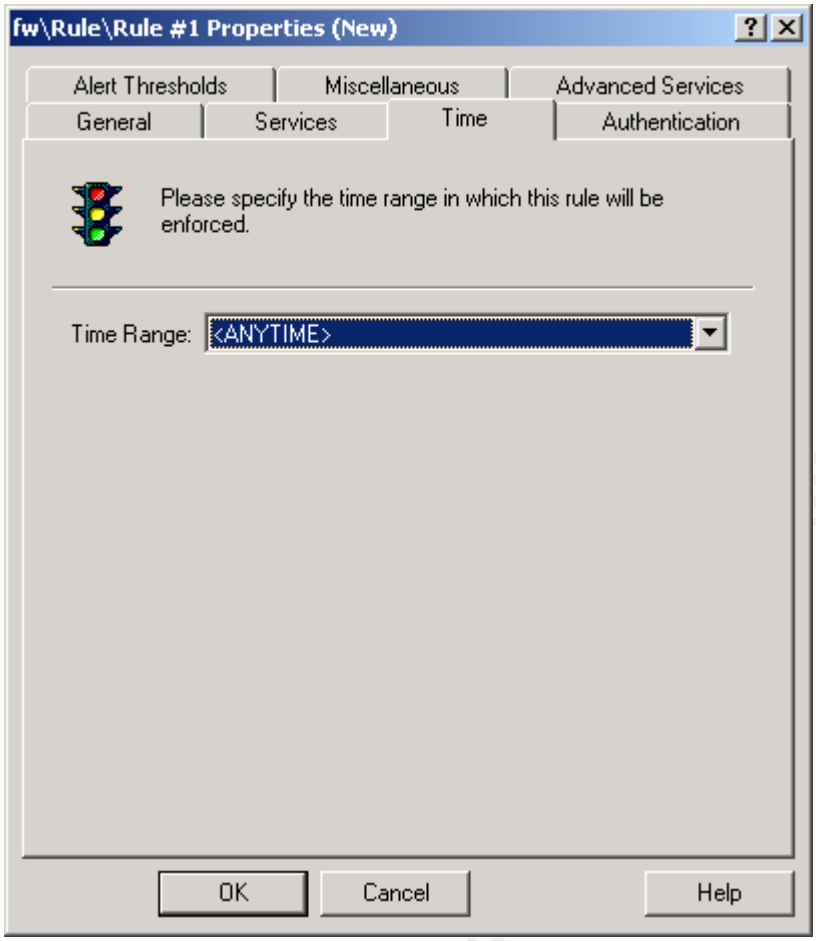
3. For a description, we enter “HTTP from User Workstations to Internet
4. Choose the “Private” interface as the “connection coming in via”
5. The source is our subnet “PrivateNetworkUserWorkstations”
6. The Destination is All IP Addresses
7. Coming our via the “DMZ” interface
8. Our default rule is to deny, so all subsequent rules will be to allow.
9. Click on the “Services” tab



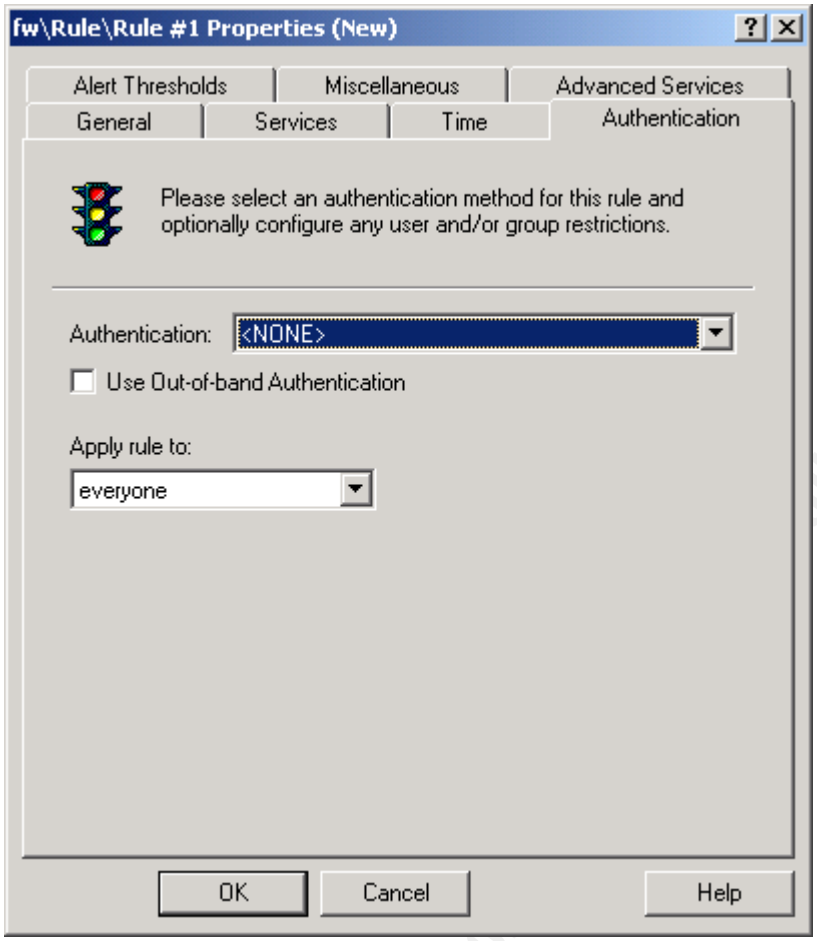
10. Here we choose the “http” service.
11. The http service has some special configuration options, choose “configure” to view and set.



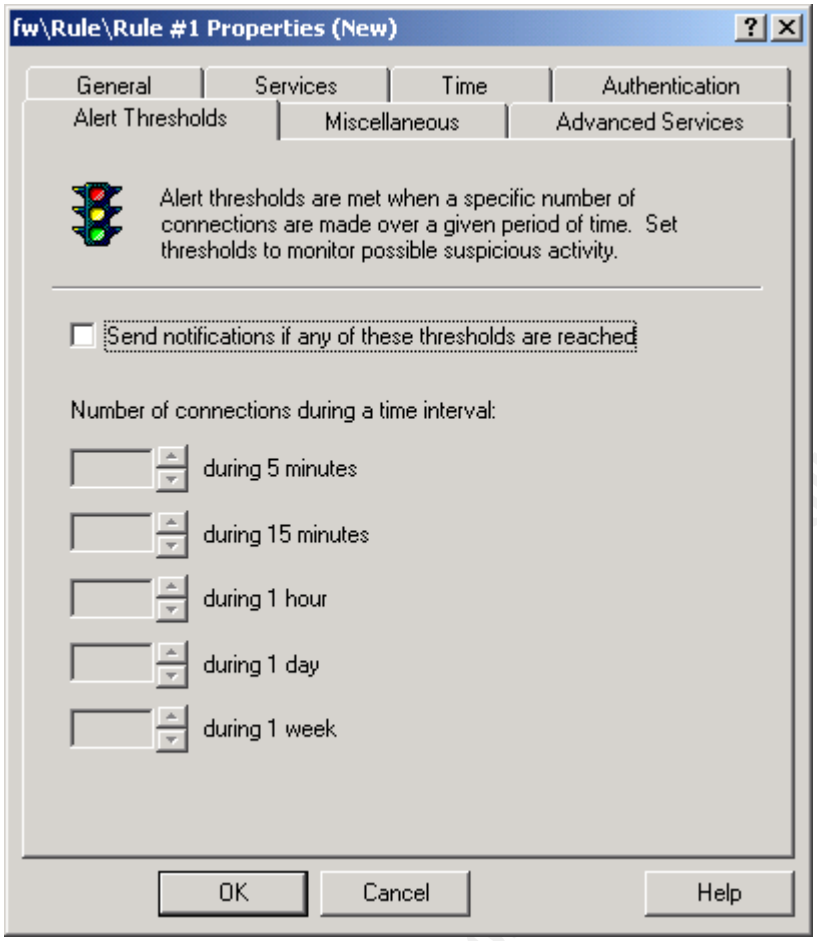
12. We will click to enable SSL over the standard ports.
13. Click on the “Time” tab.



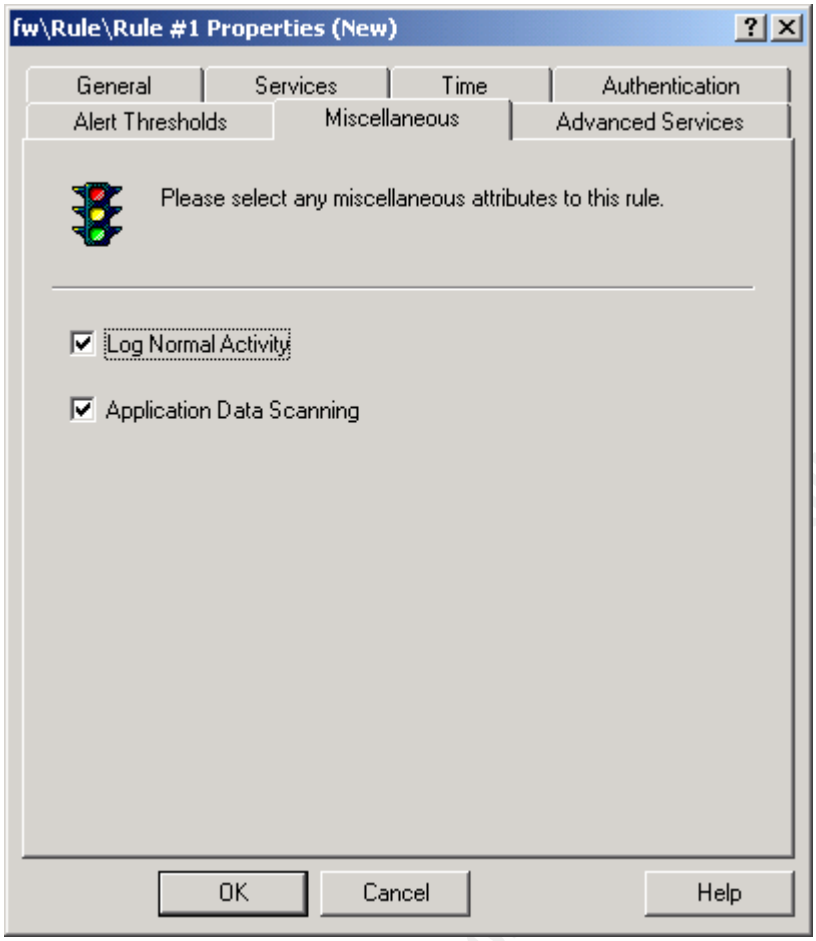
14. We have the ability to configure a time range when this rule is active. Leave this set at “Anytime”
15. Click on the “Authentication” tab



16. We have the ability to force users to authenticate to activate this rule. We will not use Authentication.
17. Click on the “Alert Thresholds” tab.



18. We have the ability to configure an alert to be generated if a certain number of connections is reached in a certain time period. We will not configure a threashold.
19. Click on the “Miscellaneous” tab.



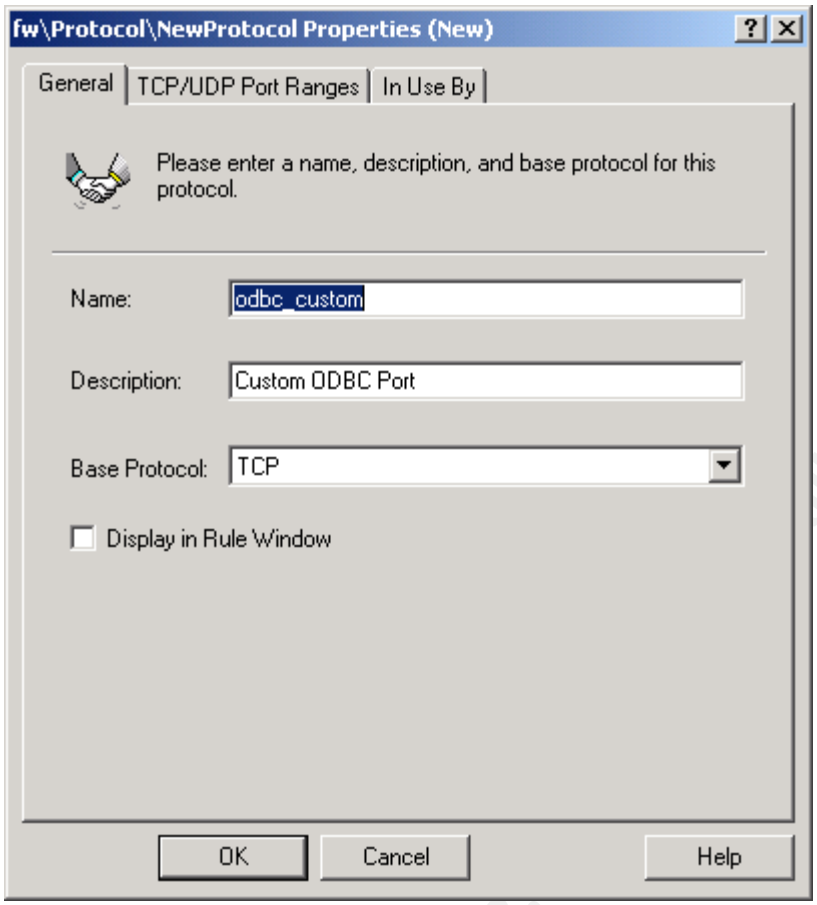
20. Here we have the ability to choose to log activity and scan the data sent by the application. We will do both. With application data scanning, the firewall acts like a proxy firewall, reading in the entire request to see if it is valid before passing it to the target system. If application data scanning is disabled, the firewall acts like a packet filtering firewall, and passes each packet of the request to the target system without verifying it is a valid request for the configured service.
21. Click Ok to save the new rule

Use this same process to configure all of the other rules.

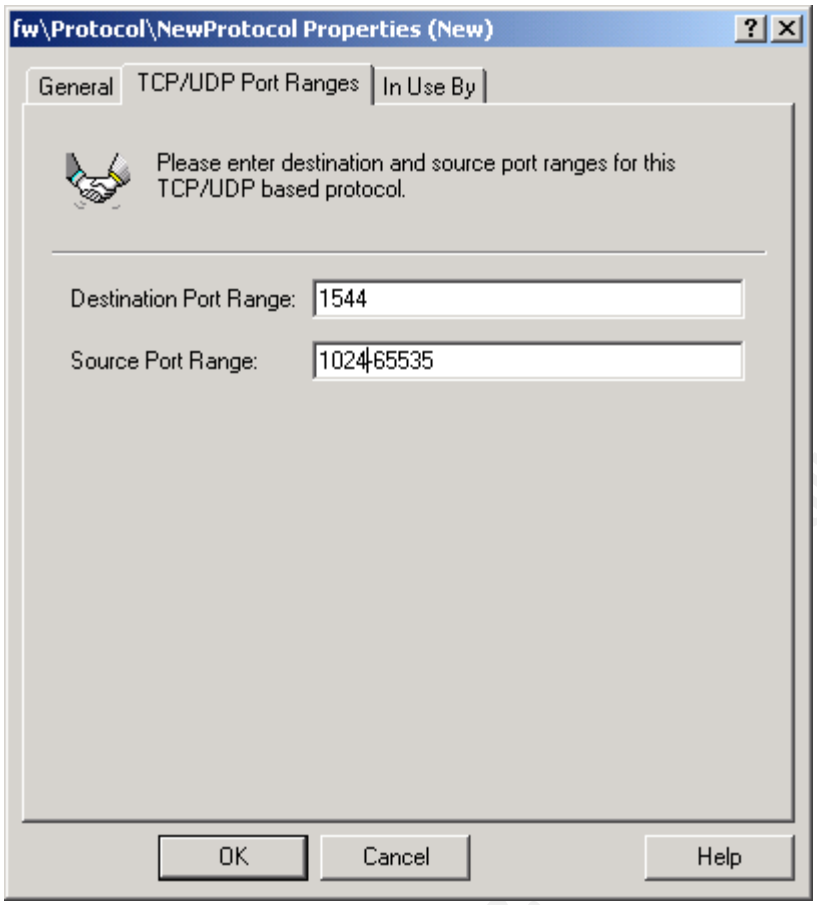
Configure Custom Protocols

If a rule does not have a pre-configured service or protocol listed (such as our custom ODBC port for communication between the web server and the database) the protocol will need to be added prior to adding the rule. Follow this process to add a protocol:

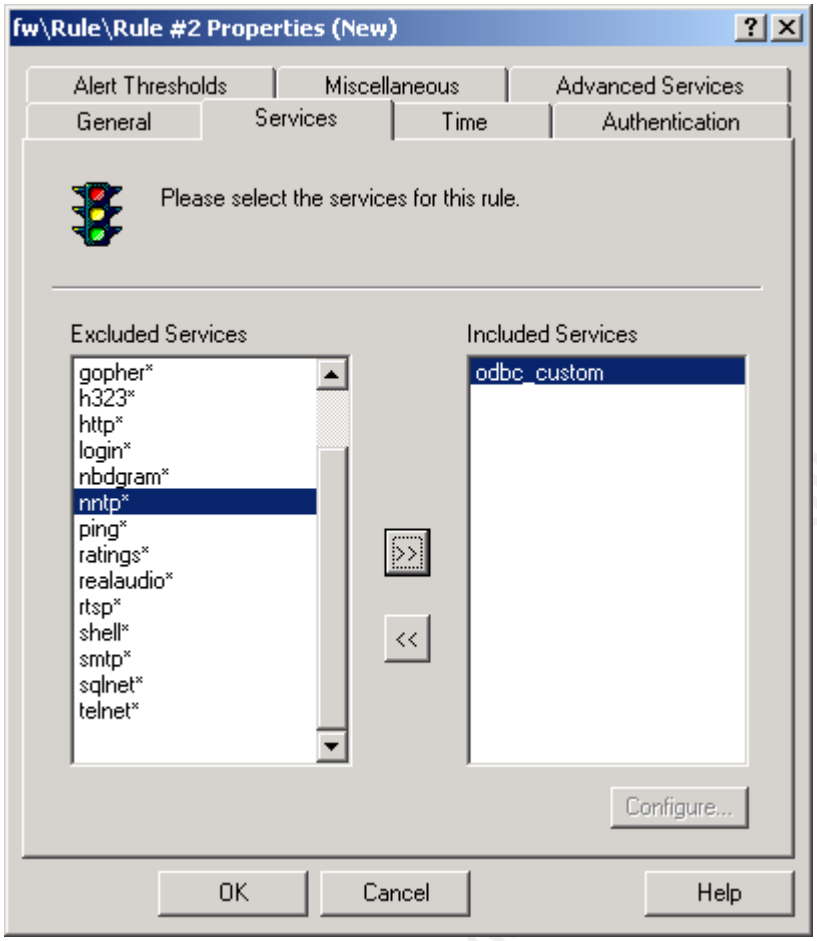
1. Expand the “Base Components” folder
2. Right-click on “Protocols” and choose “New”..”Protocol”



3. The name of our protocol is “odbc_custom”
4. The Base Protocol is TCP. It should be displayed in the Rule Window.
5. Click on TCP/UDP Port Ranges

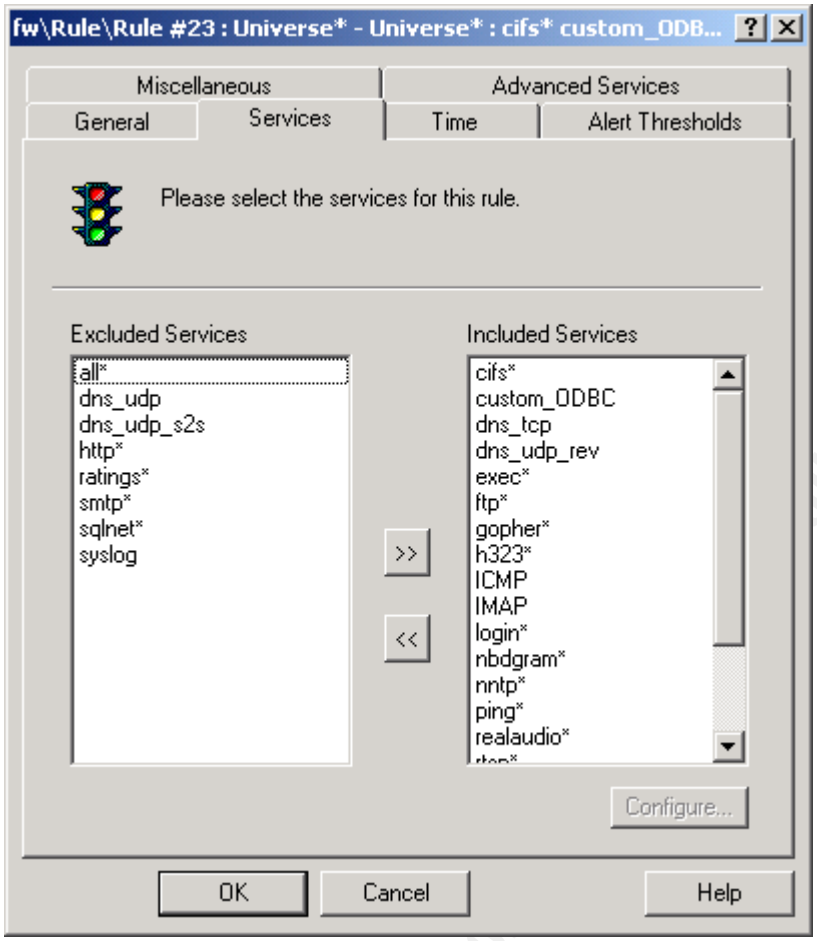


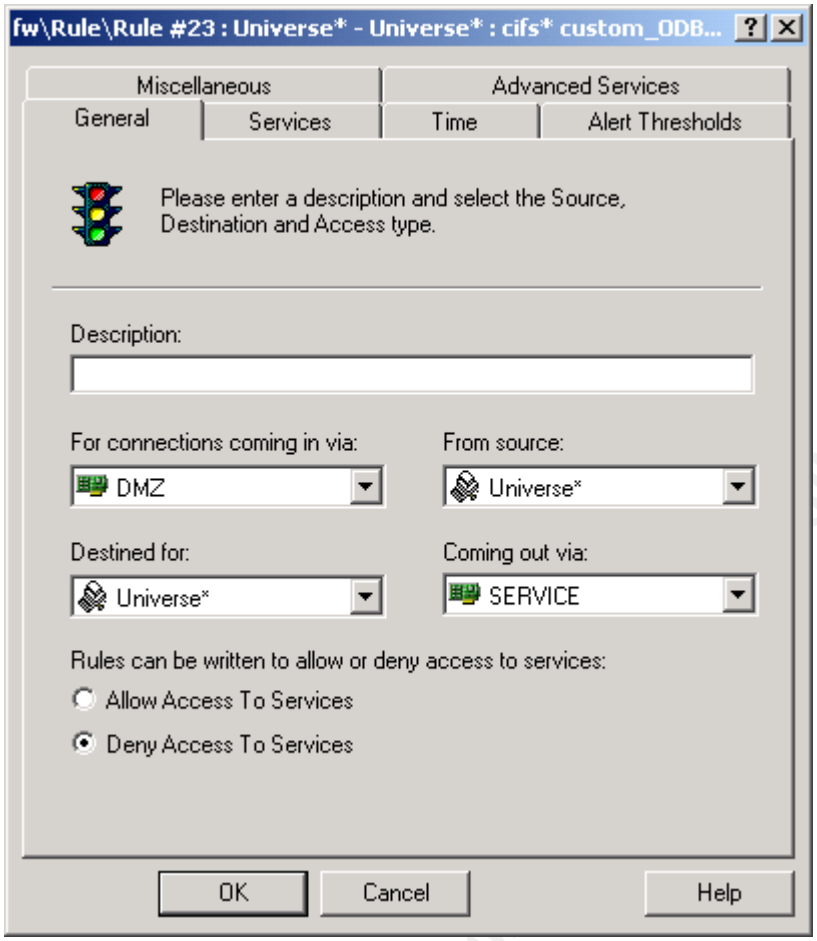
6. The Destination Port Range is the custom port 1544. Our source port is any of the ephemeral ports, or 1024-65535.
7. Click OK. Now our custom service is available in the “Services” window of the “Add Rule” dialog.



Deny Rules

Deny rules are added in the same way as permit rules. The following screenshots show a deny rule to deny all unused services from passing through the firewall from the Internet to the Server Network.





Assignment 3: Verify the firewall policy

Audit Plan

We will use three tools to test the firewall configuraton:
NetCat
Ethereal
NMap

There are two ways we will test the firewall.

First will will use NetCat to determine if traffic is permitted to the appropriate servers.
For each type of traffic that is to be permitted, we will do the following:

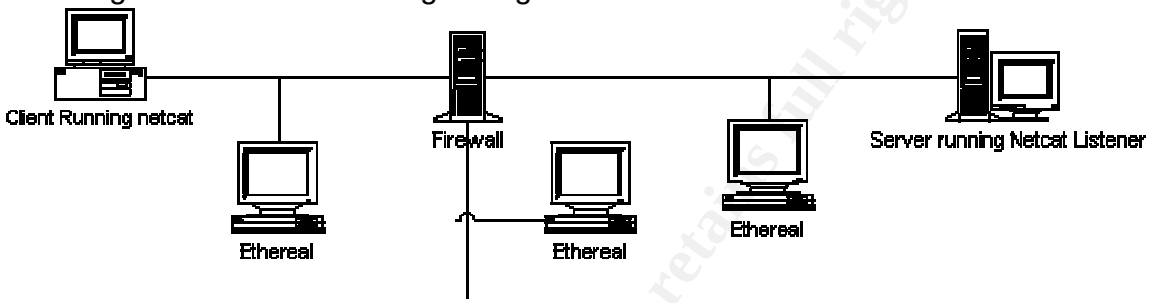
1. Set up a listening service on the specified port on the server that is supposed to receive the traffic. For example, if we want to set up a listener on port 25 TCP (pretending to be an SMTP server), we will use the following command on the server:

nc –l –p 25

The “-l” switch tells netcat to run in listen mode.
The “-p” switch tells netcat to use port 25
The default behavior is to use TCP

2. We will run Ethereal on all three network segments during the test to capture any packets. This will show us that the firewall is routing traffic to the appropriate segments.

This diagram shows the testing configuration:



3. We will then go to the client machine and attempt to connect to the server machine using netcat:

nc server_ip 25

If the connection is successful, we should be able to type characters into the netcat instance on either the client or the server, and have the characters show up on the other machine.
One thing to keep in mind, the Symantec Enterprise Firewall acts as a proxy for many well known services, such as HTTP and SMTP. To successfully pass traffic through the firewall on these services, the traffic must be a valid request or response for that type of traffic. To accomplish this, we can either paste valid traffic into NetCat, or use a web or smtp client to generate the traffic.

Netcat can be used to test services using both TCP and UDP. To test UDP services, use the same commands as above, but use the –u switch.

We will check the Ethereal log on all three segments to see if any additional traffic was generated.

This testing can be performed at any time of day, because we do not have any rules that are time-based.

The cost to perform this testing will be minimal, because we are using freely available tools. The effort/time to perform the test will be a couple of days. This

is because we are testing each permitted rule individually, and also testing each interface using NMAP from a number of different source hosts.

Example 1: Test with Netcat and Internet Explorer of permitted rule

corporate database on our custom port 1544, but that it is not allowed to communicate with the syslog server on that same port.

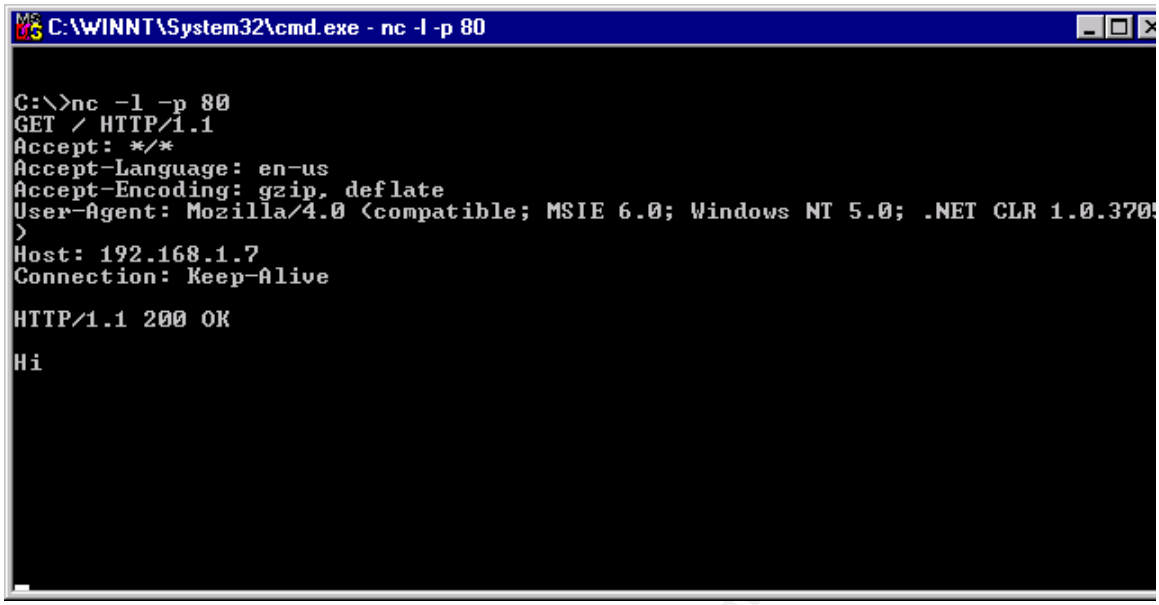
1. For this test, we configure a device to act as the web server in the service network.
IP Address: 192.168.1.7
Subnet: 255.255.255.0
Gateway: 192.168.1.1
And we plug it into the Service Network switch.

2. We also configure a device to act as the user workstation
IP Address: 172.17.30.5
Subnet: 255.255.0.0
Gateway: 172.17.20.1
And we plug it into the private network switch.

3. Now we start Ethereal on both ofn the above workstations.

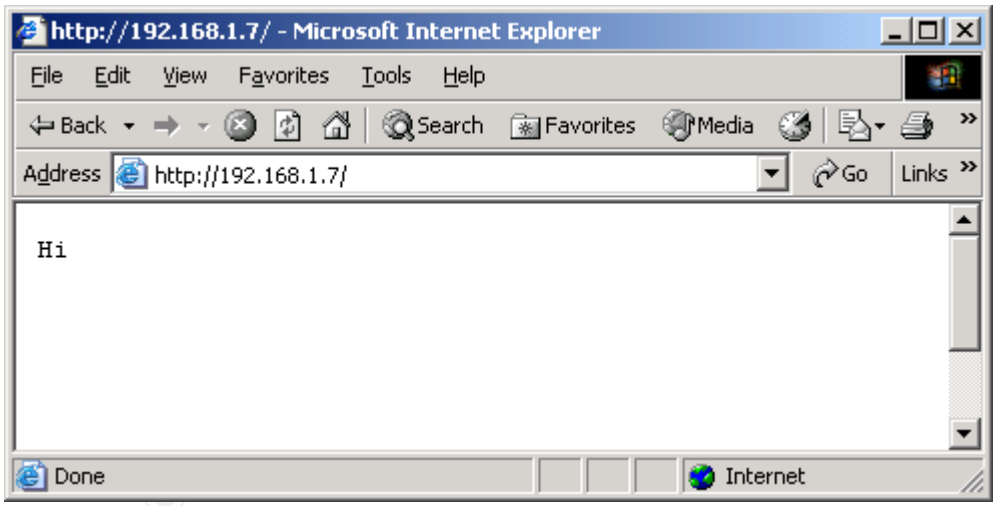
4. Now start a listener on the “web server” using the following command:
- nc –l –p 80

5. Since we are using the HTTP proxy on the Firewall, we will need to send a valid HTTP request or the firewall will block it. The easiest way to do this is to launch Internet Explorer and use it to send the request. We launch Internet Explorer on the “User Workstation” and type the web server address 192.168.1.7 into the address bar.
6. We see the HTTP request in the NetCat session on the “Web Server”, so the firewall permitted our request to go through.

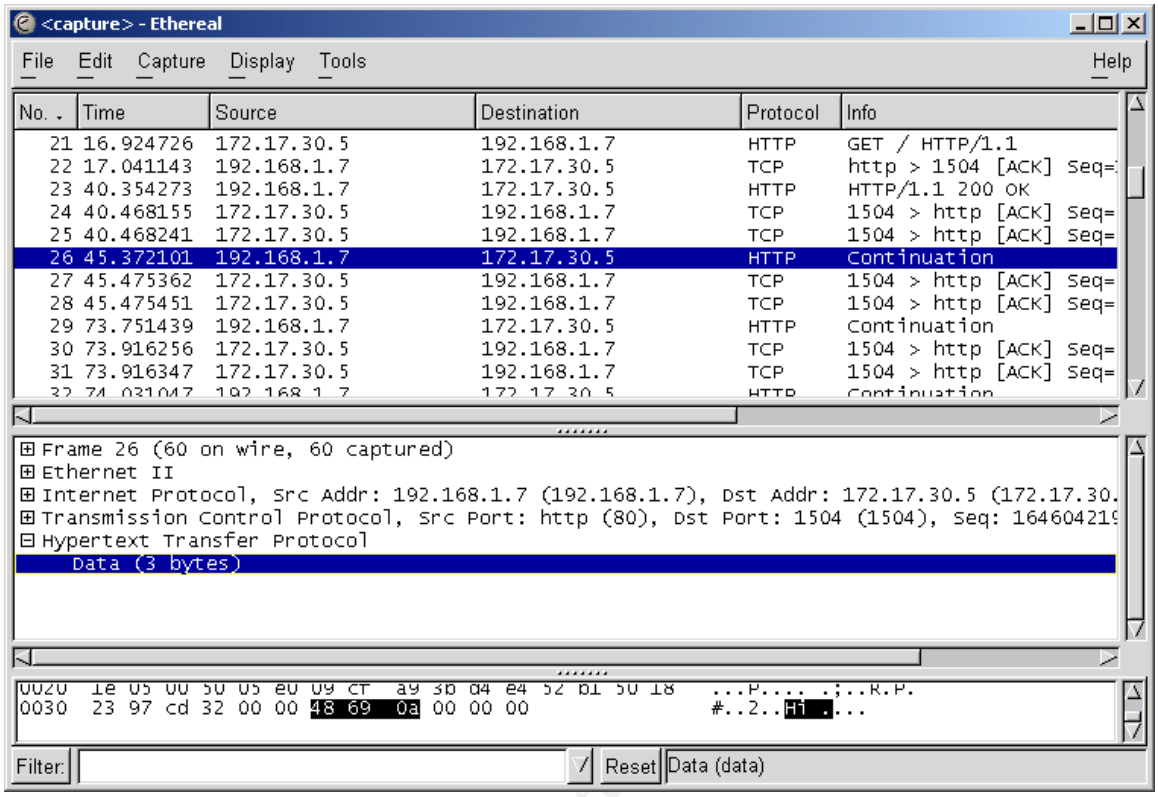


7. To test that our response is also permitted to go through the firewall, we type the following three lines into Netcat on the webserver:
   HTTP/1.1 200 OK\n
   \n
   Hi\n

   This sends a valid HTTP header and the content “Hi” back to the browser:



Ethereal picked up the expected network traffic and no other traffic:



We can follow this same process to verify that every service we expect to be open is open. We can also verify that non-expected services are not open.

Example 2: Test with Netcat of Non-permitted rule

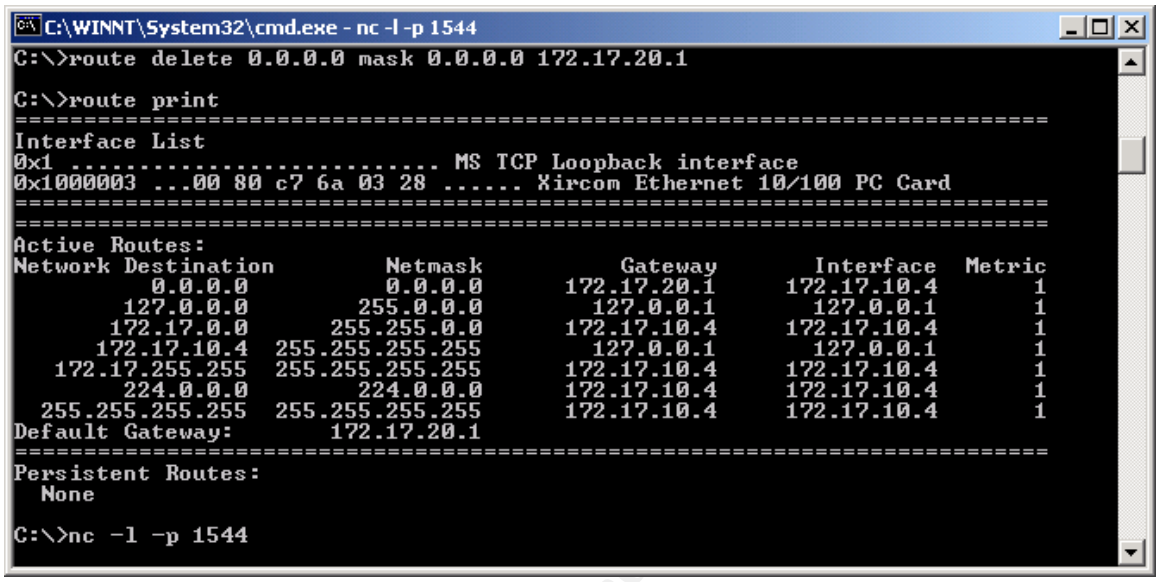
In this example, we are going to test that the web server is allowed to communicate with the corporate database on our custom port 1544, but that it is not allowed to communicate with the syslog server on that same port.

1. For this test, we configure a device to act as the web server in the service network.
IP Address: 192.168.1.7
Subnet: 255.255.255.0
Gateway: 192.168.1.1
And we plug it into the Service Network switch.

2. We also configure a device to act as the database
IP Address: 172.17.10.4
Subnet: 255.255.255.0
Gateway: 172.17.20.1
And we plug it into the private network switch.

3. Now we start Ethereal on both of the above workstations.

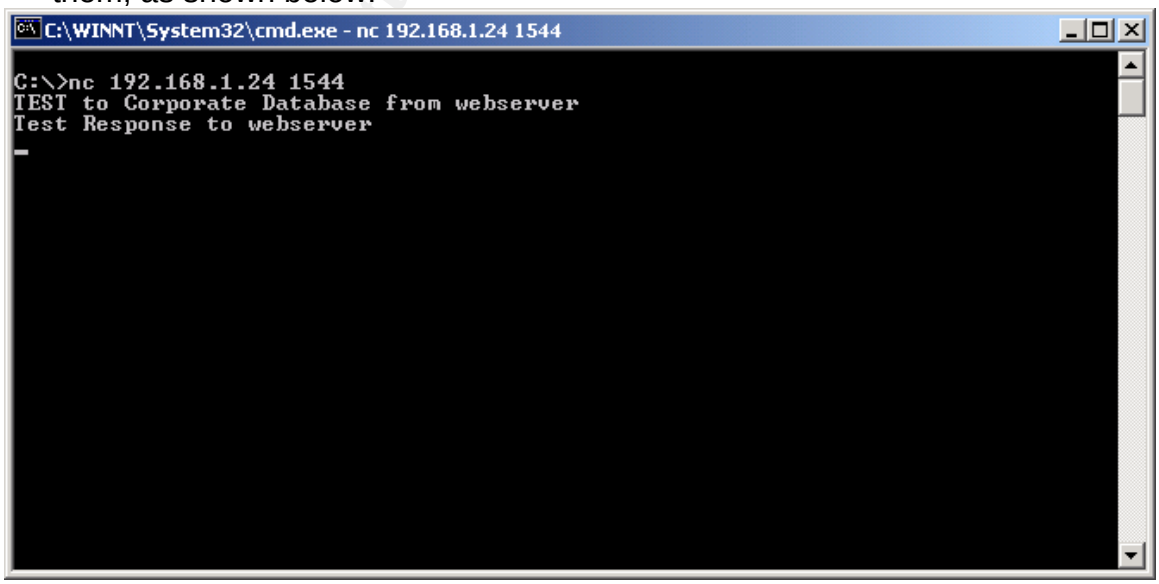
8. Now start a listener on the “database” using the following command:
- nc –l –p 1544

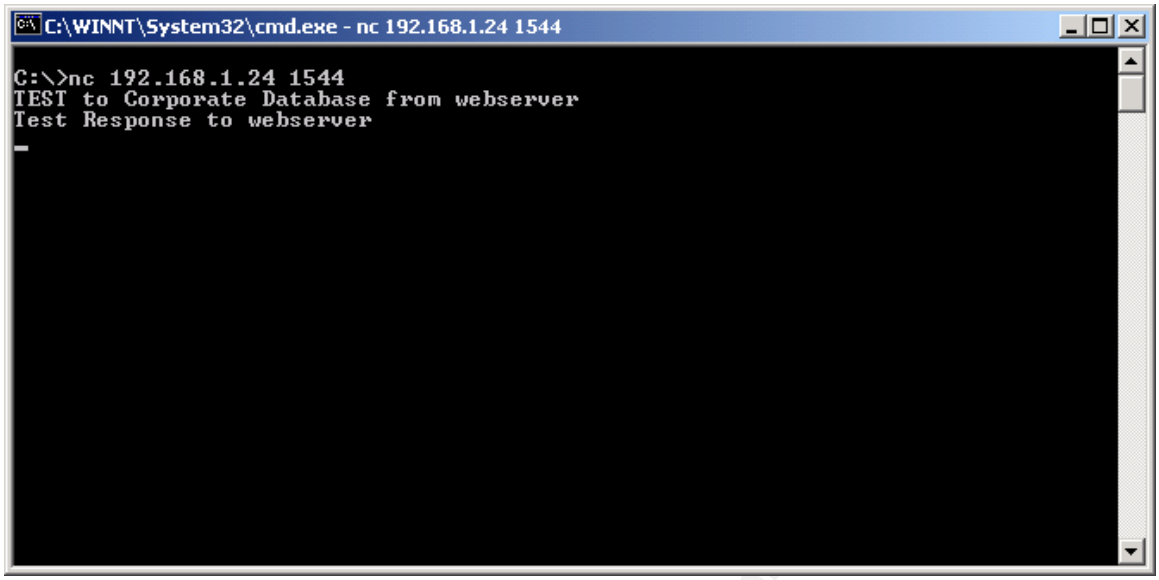


9. Now attempt to connect to the listener on the “database” from the “web server” using the following command:
   - nc 192.168.1.24 1544

   Note that since we are communicating from the Service Network into the private network, we use the “redirect” address of 192.168.1.24, rather than the true IP address of the device, 172.17.10.4.

   You can now move between the two computers and send traffic between them, as shown below.





Ethereal shows no additional network traffic.

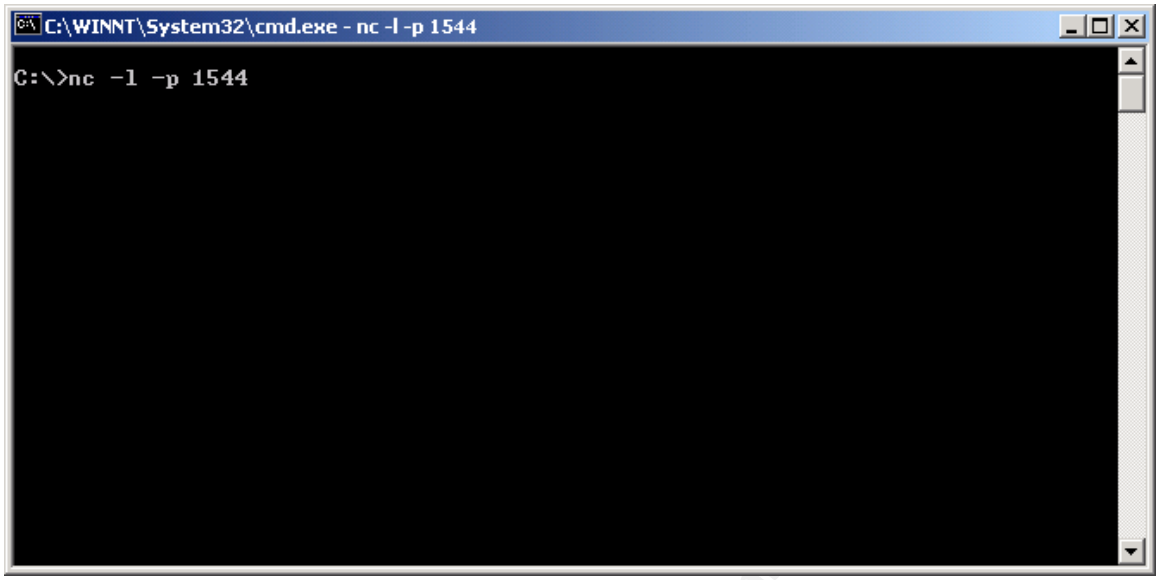
The second part of this test involves attempting to connect from the webserver to the Syslog server on the custom port 1544. This traffic should be denied.

1. For this test, we configure a device to act as the web server in the service network.
IP Address: 192.168.1.7
Subnet: 255.255.255.0
Gateway: 192.168.1.1
And we plug it into the Service Network switch.

2. We also configure a device to act as the syslog server
IP Address: 172.17.10.3
Subnet: 255.255.255.0
Gateway: 172.17.20.1
And we plug it into the private network switch.

3. Now we start Ethereal on both of the above workstations.

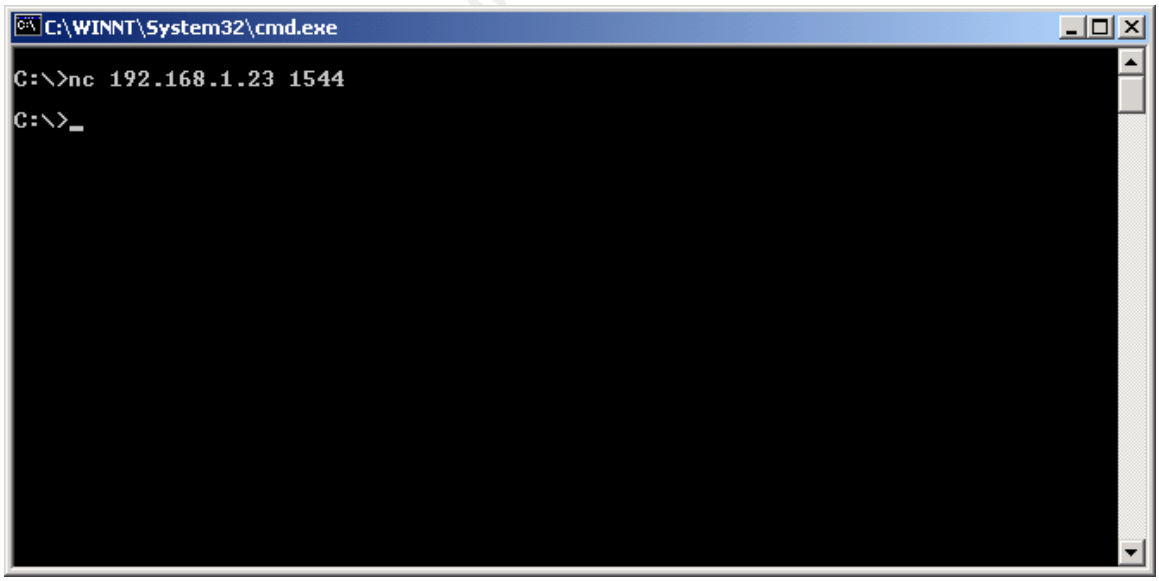
10. Now start a listener on the “syslog server” using the following command:
- nc –l –p 1544



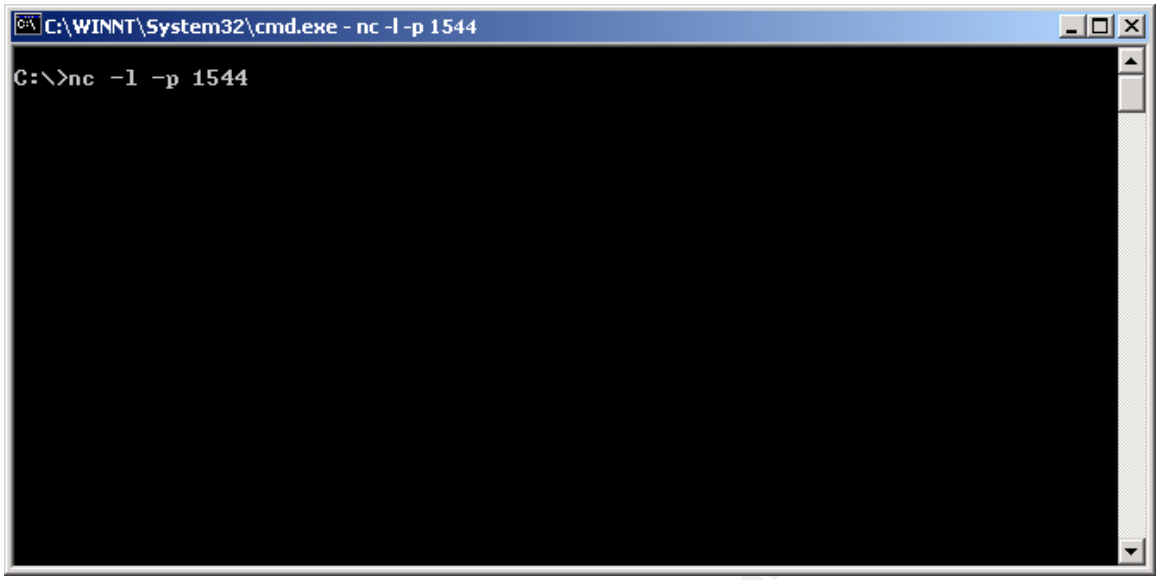
11. Now attempt to connect to the listener on the “syslog server” from the “web server” using the following command:
    - nc 192.168.1.23 1544

    Note that since we are communicating from the Service Network into the private network, we use the “redirect” address of 192.168.1.23, rather than the true IP address of the device, 172.17.10.3.

    The connection attempt fails, we are returned to the command prompt after a short timeout.



No indication of a connection is shown in the listener.



Testing the firewall with NMAP

The second way we will verify the firewall policy is to run nmap against each of the interfaces and verify that the appropriate ports are open. The allowed services are different depending on the source of the traffic, so we will need to run the scan from a number of different source addresses.

Some of the options of nmap we will use are:
-sS TCP Syn scan
-P0 (do not ping hosts before scanning) because our firewall blocks ICMP echo traffic
-oN <logfilename> - log results to a file
-S <ipaddress> - select the IP address to use. We will bind each used IP address to the network card before it is used so that we grab the response traffic.
-n do not resolve DNS addresses
-v verbose mode

Example 3: Private Network User Workstation scan of the Service Network

1. Set the NMAP machine to the IP address of a workstation – 172.17.30.5
2. Place the Ethereal sniffer in the Service Network
3. Run the following command:

Nmap –sS –p0 –S 172.17.30.5 –n –v 192.168.1.7 > test.txt
(for this example we scanned only the webserver, 192.168.1.7. We could scan the whole range using the form 192.168.1.0/24)

Here is the contents of test.txt:
Starting nmap V. 3.00 (www.insecure.org/nmap)
Host (192.168.1.7) appears to be up ... good.

```
Initiating SYN Stealth Scan against  (192.168.1.7)
Adding open port 514/tcp
Adding open port 21/tcp
Adding open port 1521/tcp
Adding open port 512/tcp
Adding open port 554/tcp
Adding open port 119/tcp
Adding open port 1720/tcp
Adding open port 80/tcp
Adding open port 23/tcp
Adding open port 25/tcp
Adding open port 443/tcp
Adding open port 70/tcp
Adding open port 139/tcp
Adding open port 7070/tcp
Adding open port 513/tcp
The SYN Stealth Scan took 216 seconds to scan 1150 ports.
Interesting ports on  (192.168.1.7):
(The 1135 ports scanned but not shown below are in state: filtered)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
70/tcp     open        gopher
80/tcp     open        http
119/tcp    open        nntp
139/tcp    open        netbios-ssn
443/tcp    open        https
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
554/tcp    open        rtsp
1521/tcp   open        oracle
1720/tcp   open        H.323/Q.931
7070/tcp   open        realserver

Nmap run completed -- 1 IP address (1 host up) scanned in 216 seconds
```

This is a strange response to get. It shows that services such as gopher, telnet, oracle, and realserver are open on the firewall. A scan of any address through the Symantec firewall returns this same list of “open” ports. A TCP Connect scan using NMAP also returns the same list.

These open ports correspond to the “Proxy” services that Symantec Firewall has built-in and enabled by default. We have no rules to permit activity on the majority of these services, and in fact, all of the unused ones are explicitly set to

"deny" in our deny rule. However, it appears that the Proxy Services on the Symantec Enterprise Firewall allow the client to complete the TCP three-way handshake, and waits to see what data the client sends to the proxy before deciding to which rule to apply and to terminate the connection.

We will need to use another means, such as the Netcat connection attempt shown above, to verify whether any of the "open" ports listed above would actually allow a transaction.

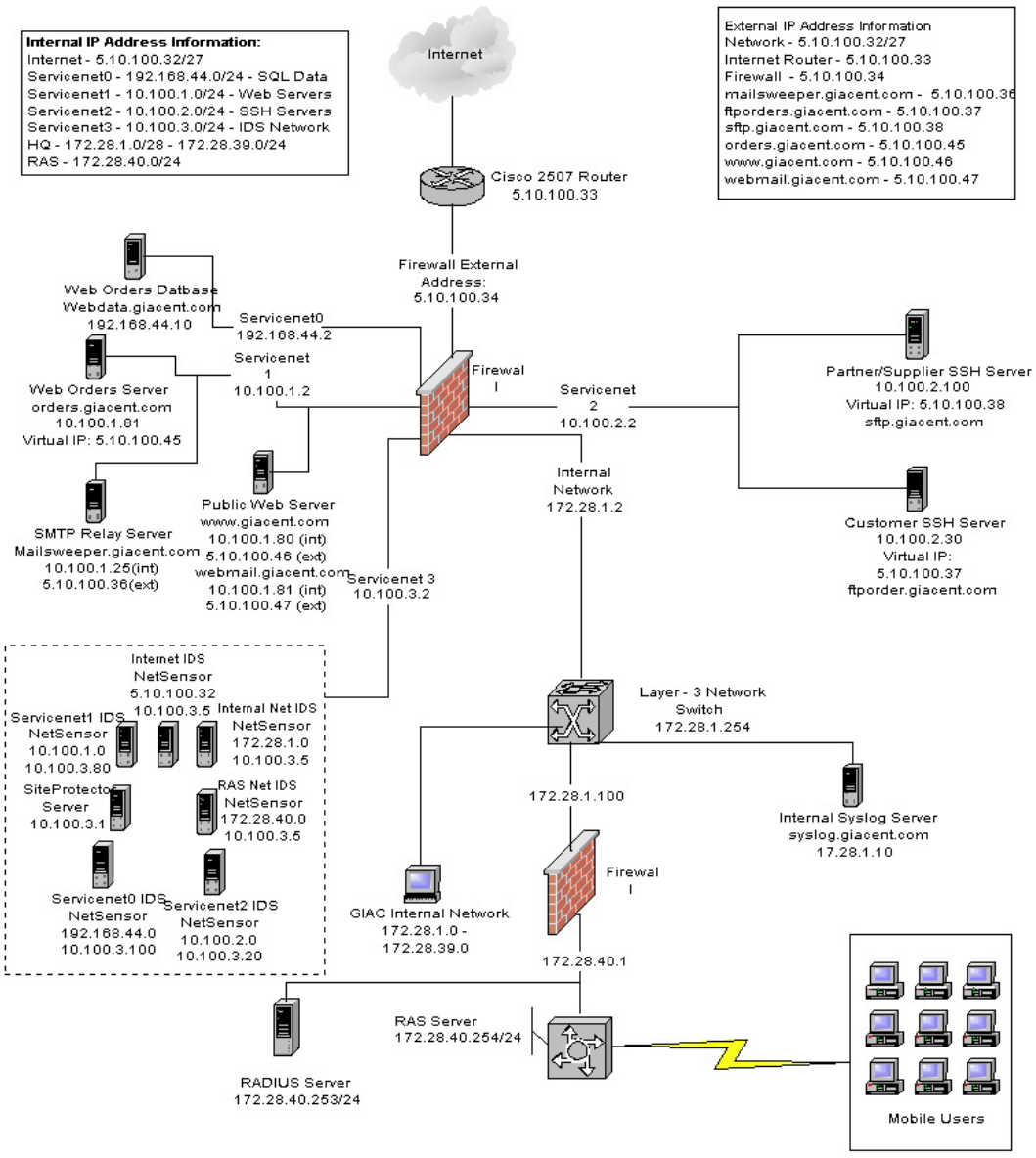
Conclusions

The configuration of the Symantec Firewall permits the traffic appropriately according to the rules we created.
The Symantec immediately blocks denied traffic by not even completing the three-way handshake. The exception to this are any of the services for which the Symantec Firewall has a proxy built and enabled. For these services, it completes the three-way handshake for every request, and then waits to see the session data before checking the rulebase and terminating the connection.
Recommendation: GIAC should go back into the Raptor Management Console and disable any unused proxy services. Even though there should not be a risk, because there are no rules permitting traffic on these services, the fact that the server completes a three-way handshake on these ports could expose a vulnerability.
The proxy services that should be disabled are:

- 70/tcp - gopher
- 119/tcp - nntp
- 139/tcp - netbios-ssn
- 512/tcp - exec
- 513/tcp - login
- 514/tcp - shell
- 554/tcp - rtsp
- 1521/tcp - oracle
- 1720/tcp - H.323/Q.931
- 7070/tcp - realserver

Assignment 4 – design under fire

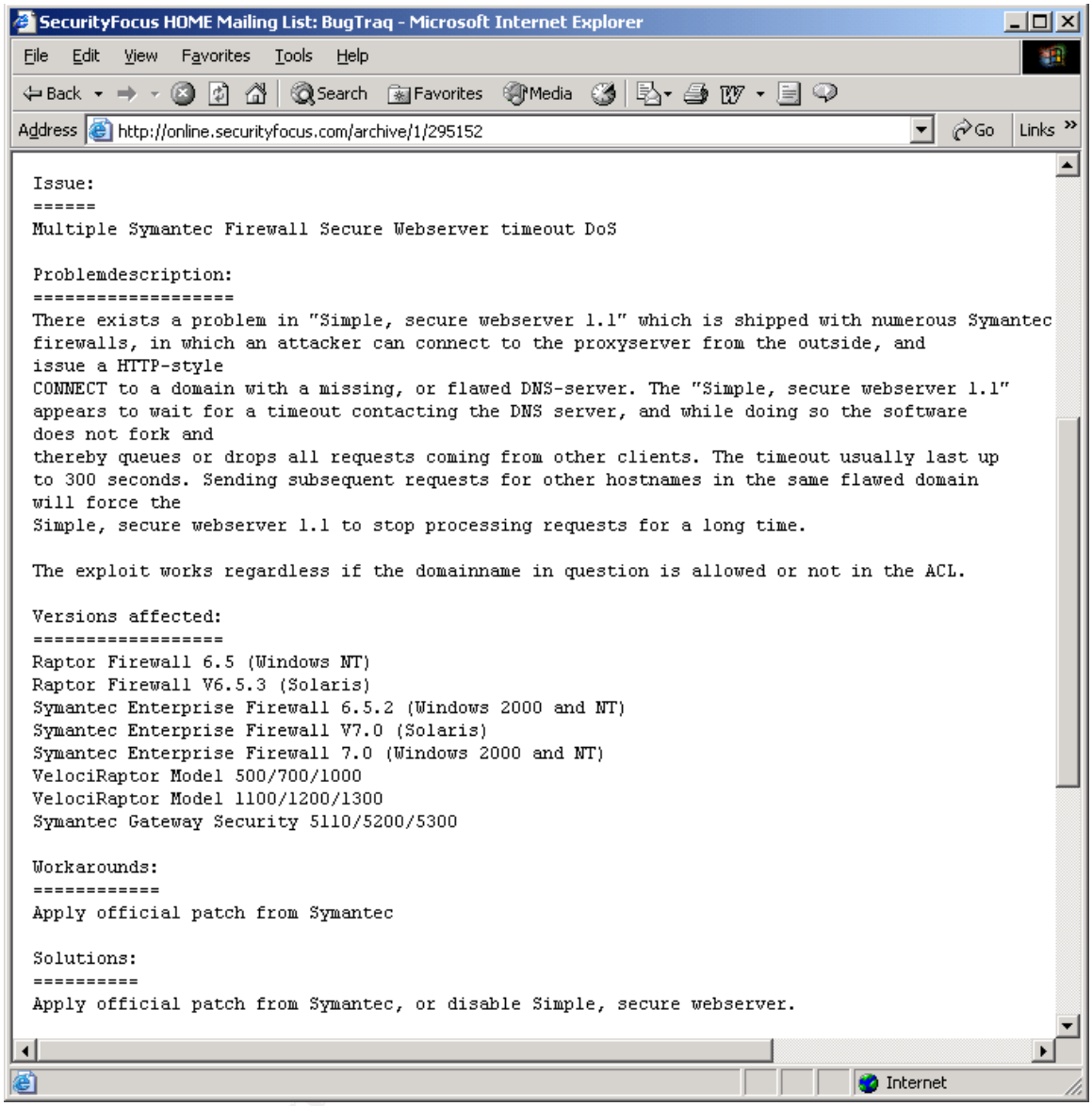
For this assignment, I chose to analyze Greg Surla's practical, available at http://www.giac.org/practical/Greg_Surla_GCFW.doc . Here is Greg's Network Diagram:



Attack 1: An Attack Against the Firewall

Greg is using a Symantec Enterprise Firewall Version 7.0.

A search of Bugtraq (http://online.securityfocus.com/archive/1) reveals the following recently discovered vulnerability:



The Symantec Firewall uses a HTTP Proxy service to handle web requests. The exploit above indicates that a certain type of request to the proxy service will force the service to wait for a timeout, and multiple requests will cause the proxy service to stop processing requests for a significant period of time.

Probability of success

Before attempting the exploit, we need to evaluate if it is likely to be successful against Greg's configuration.

- The vulnerability and fix was made public fairly recently, many network administrators have likely not applied the fix yet.
- This is a denial-of-service vulnerability, and does not allow anyone additional levels of access or put GIAC data at risk. For this reason, this fix is considered less critical and is not widely publicized.

- Greg is using the HTTP proxy service to handle requests to his protected web servers.

Based on this information, it is likely that the attack will be successful.

The Attack

To exploit the vulnerability against Greg's setup we do the following:

1. Find a domain name with a non-responding DNS server, or create the situation. Many registrars do not test to see if a Domain Name Server is functional before allowing you to set it as the authoritative server for a domain, so we simply need to find a non-responding internet address, and configure a domain name to point at that address. As a number of networks configure their routers as "Black Holes" (meaning they do not return ICMP Unreachable messages) a random scan of the Internet should turn up a usable address in short order.
2. Configure the domain name to point to the non-responding internet address. For our example, we will assume we have configured "sample.com" to have it's domain name server set as 140.104.1.1
3. Now we need to connect to the HTTP proxy on Greg's firewall and issue a http connect request for our domain. We will use netcat. From the diagram above, the external address for Greg's webserver is 5.10.100.46

First Command:

```
nc 5.10.100.46 80
```

This connects us to the web server

Second Command:

```
GET / HTTP/1.1
Host:  test1.sample.com
```

This command will cause the GIAC Firewall proxy to send a DNS request to the sample.com DNS server. Since the name server does not send any response to dns queries, the http proxy on the firewall will wait for up to 300 seconds before timing out and proceeding to the next request.

The attack can be made more effective by scripting the GET request, to repeatedly query the HTTP proxy with different servers in the domain sample.com.

Protecting against this attack:

If the firewall is vulnerable, the patch should be applied immediately. It is available from http://www.symantec.com/

Attack 2: Denial of Service

The goal of this attack is to perform a distributed denial of service attack against the above network.

The Attack

Step 1: Gain control of 50 client machines and install the DDOS client. For this attack I have chosen to use TrinOO. I chose TrinOO because it has a windows client. One of the easiest targets for machines to use to lauch DDOS attacks are new or novice home DSL/Cable users, who are often running windows, may have not applied patches, may not be running antivirus software, and may be likely to open email attachments or install software from untrusted sources. TrinOO can be found and downloaded from various hacker tool sites.

The structure of TrinOO is a Master and Daemons. The TrinOO daemon is installed on each controlled host that will attack the final victim. The single TrinOO master sends commands to multiple TrinOO daemons to launch a coordinated attack. The hacker controls the TrinOO master using netcat or telnet.

Step 2: Install the TrinOO master component on one or two compromised machines

Step 3: Install the TrinOO daemon on the rest of the controlled hosts. TrinOO daemon is installed by running the compiled W32.DoS.Trin00 software on the host. When this program is run, TrinOO copies itself to the windows/system folder and modifies the registry to load the program at startup. The daemon will then send the string *Hello* to the master on port 31335 to register itself. The Daemon will now be listening on port 34555

Set 4: Send the command to the TrinOO masters to being the attack.
This is as simple as connecting to the masters with Netcat on port 27665 TCP, sending the password (144adsl), and then sending the command to DOS the host – "**dos 5.10.100.34**"

The TrinOO master now sends the command to the controlled TrinOO daemons to begin attacking the address 5.10.100.34. The Daemons send out large numbers of UDP packets in an attempt to use up network bandwidth and firewall resources.

Mitigating the attack:

A Denial of Service Attack is very difficult to stop. Some things that could be done to mitigate the attack include:

- Contact the ISP and attempt to have them block the attacking hosts

- Configure the border router to block the offending traffic if possible, to reduce resource utilization on the firewall
- Configure the border router and firewall to not send ICMP unreachables, so that we are not sending responses to each attack packet, thereby increasing the bandwidth used by the attack.

References for this section:
Brumley, David. "Denial Of Service". http://crypto.stanford.edu/cs155/lecture-ddos.ppt

Bowden, Eric J. "Toolkits for DOS Attacks". http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2645417-3,00.html. October 30, 2000.

Attack 3: Attempt to compromise an internal host

The Target

I would attempt to compromise the "Web-based E-Mail Server" webmail.giacnt.com. I chose this host because

- Controlling this system would be a great foothold into the network. I may be able to read user's email, capture user IDs or passwords, and attack other hosts from this system.
- This system has an open service to the Internet, the secure web port (443)
- This system is running SquirrelMail. Squirrelmail is an open source mail web interface package that is known to have major security flaws in earlier versions, and although the known ones have been fixed, there may be unknown ones we could exploit. Since the source is available, we could search the source for new vulnerabilities.
- Squirrelmail requires PHP. PHP's default configuration leaves many vulnerabilities if strict coding standards are not carefully followed.
- Squirrelmail requires temporary mailbox, attachment, and configuration directories which need to be write-able by the apache web service. This means there is may opportunity to write or overwrite data on the server.

Previous Vulnerabilities in Squirrelmail involved exploiting the following attributes:

1. Many variables are not declared or initialized before they are used.
2. There are a number of shared "library" files that are called from the Squirrelmail PHP scripts. These library files are not meant to be called directly by the web user, but the default configuration allows them to be.
3. PHP includes functions that allow for reading or executing code pulled from other sources. If these functions are used without carefully checking their input, they can be exploited.
4. File Upload saves to a temporary file on disk before processing the script. Allows the attacker to write attack code to disk.

The attack

To attempt this attack, I would first connect to the webmail.giacnt.com site and save the code returned for some of the screens viewed. Then I would download the source code for the most recent versions of Squirrelmail, and compare it to the responses received, to determine which version of Squirrelmail they are running. Once I know which version they are running, I would check the Squirrelmail mailing list and the BugTraq list to see if there are any known vulnerabilities in that version. If that fails, I would then install the same version that GIAC is running on a local server, and attempt to configure that server as close as I can to what I believe is the configuration of GIAC's server. Then I would begin to go through the Squirrelmail source code looking for bits of code that use the features listed above, which are known to often cause vulnerabilities.

Sample Exploit

A sample exploit of a vulnerability that existed in Squirrelmail 1.0.4 is shown here as a sample attack. An attack on a more recent version would likely be similar

This vulnerability in Squirrelmail allows an attacker to read information from any file to which the web server user account has rights without logging in to the server. Here are the attributes of the Squirrelmail code that work together to allow this to happen:

1. Many variables are not declared or initialized before they are used.
2. There are a number of shared "library" files that are called from the Squirrelmail PHP scripts. These library files are not meant to be called directly by the web user, but the default configuration allows them to be.

Here is a block of code from one of the library files, "load_prefs.php":

```
38 if ((isset($chosen_theme)) && (file_exists($chosen_theme))) {
39 require("$chosen_theme");
40 } else {
41 if (file_exists($theme[0]["PATH"])) {
42 require($theme[0]["PATH"]);
43 } else {
```

If the library file "load_prefs.php" is called directly by the web browser, $theme[0]["PATH"] is not initialized before it is used here. Since PHP allows us to create a globally-scoped variable simply by passing that variable as an HTTP GET or POST parameter, or even a cookie value, it is easy for the user to initialize this variable to any value.

Inspection of additional code in "load_prefs.php" reveals that one must also provide the following variables to get the code above to execute by directly calling load_prefs.php.

- $username (can be anything)

- $config_php = true
- $data_dir = the directory of the Squirrelmail data directory. This could be guessed, or there are vulnerabilities in Squirrelmail that will provide this information. This vulnerability can be found in *Remote command execution vulnerabilities in Squirrelmail* (http://www.securereality.com.au/sradv00010.txt).

We use the above information to craft a specific URL to send to Squirrelmail. This URL can be loaded using any web browser, such as Internet Explorer.

http://webmail.giacnt.com/squirrelmail/src/load_prefs.php?username=nobody&config_php=true&theme[0][PATH]=/etc/passwd&data_dir=/var/www/html/squirrelmail/data

When the web server loads this URL and parses the script, the PHP variable $theme[0][PATH] is set to "/etc/passwd".
When the script executes "42 require($theme[0]["PATH"]);", the contents of /etc/passwd will be pushed to the screen. If a different file that contained PHP code had been specified, that PHP code would have been executed.

Detecting the attack

The following pieces of the security architecture would not have been effective in stopping or detecting the attack for the following reasons:
Border Router – the border router would not have blocked the attack, it is configured to permit this web traffic to pass.
Firewall – The firewall permits access to the GIAC webserver on the secure web port. We are sending normal web requests, our attack information is part of our querystring or form parameters, so it will not rais suspicion. Also, the firewall cannot decrypt the SSL data, so it would not be able to see the attack parameters
IDS – The IDS would not see that attack for the same reason as the firewall, it is encrypted using SSL. If the attack were not encrypted, an IDS would still likely not detect it, because the form and querystring parameters are not unusual.
Tripwire – Tripwire would not have detected the attack. The folders required by squirrelmail for configuration, temporary data, and attachments have dynamic content, and would be configured to be ignored by Tripwire during scans.
Webserver logfiles – the attack would not likely be noticeable in the webserver logfiles. We are sending normal-looking requests to valid web pages.

Countermeasures to prevent this attack

Do not use the default configuration of PHP, secure the PHP application. This will break some of the functioinality of Squirrelmail, but the source code is available and the broken functions can be fixed.

These settings are stored in the php.ini file. Here are some of the settings that can be changed:

- Set safe_mode to TRUE
  By default, safe_mode is set to false. Setting safemode to true does the following:

1. Restricts running external programs on the web server from PHP
2. Restricts the use of dangerous functions, like include(), ReadFile(), fOpen(), etc.
3. Restricts access to files based on authentication information
4. Disables file upload
   While this setting renders your PHP site much more secure, most PHP software, such as Squirrelmail, will not function with safe_mode set to TRUE

- Set register_globals to FALSE
  This setting will cause PHP not to create a global variable for each URL GET, POST, or Cookie parameter. While this restricts an attacker from initializing your script variables, most PHP software is developed with the assumption that register_globals is set to TRUE.

- Set open_basedir
  The open_basedir setting limits which directories files can be read from. This will keep the user from reading files outside of the PHP script directories.

- Set allow_url_fopen to off
  This setting disables the remote file include feature of PHP

References for this section:

Clowes, Shaun. “A Study in Scarlet: Exploiting Common Vulnerabilities in PHP Applications” SecureReality, http://www.securereality.com.au/studyinscarlet.txt

Bong, Kevin “Exploiting Vulnerabilities in Squirrelmail”. http://www.giac.org/practical/Kevin_Bong_GCIH.doc

References

Antoine, Vanessa, et al. *"Router Security Configuration Guide".* National Security Agency. March 25, 2002. <http://nsa2.www.conxion.com/cisco/guides/>

Bowden, Eric J. *"Toolkits for DOS Attacks"*. December 4, 2002. <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2645417-3,00.html>

Bong, Kevin. *"Exploiting Vulnerabilities in SquirrelMail"*. SANS Institute GCIH Practical. December 5, 2002 <http://www.giac.org/practical/Kevin_Bong_GCIH.doc>

Brumley, David. *"Denial Of Service".* December 4, 2002 <http://crypto.stanford.edu/cs155/lecture-ddos.ppt>

Clowes, Shaun. *"A Study in Scarlet: Exploiting Common Vulnerabilities in PHP Applications"*. SecureReality, December 6, 2002 <http://www.secureReality.com.au/studyinscarlet.txt>

"Multiple Symantec Firewall Secure Webserver timeout DoS". BugTraq/Security Focus. December 1, 2002. < http://online.securityfocus.com/archive/1/295152 >

"Remote command execution vulnerabilities in Squirrelmail ". Secure Reality Pty Ltd. December 5, 2002. <http://www.secureReality.com.au/sradv00010.txt>

Surla, Greg. "*Giac Certified Firewall Analyst Practical"* <http://www.giac.org/practical/Greg_Surla_GCFW.doc>

Symantec Enterpise Firewall and Symantec Enterprise VPN; Configuration Guide. Symantec Corporation. November 10, 2002. < http://www.symantec.com/ >

"Track 2 – Firewalls, Perimeter Protection, and VPNs" Coursebooks. SANS Institute.