GIAC ENTERPRISES

GCFW Practical Assignment

Version 1.7

Prepared by:

Robert K. Alley

10-17-2002

Revised
12-11-2002

GCFW Practical Assignment
A Recipe for Good Fortune

Version 1.7

GIAC Enterprises

Abstract:

This is a submission based on the version 1.7 requirements for the GCFW Practical Assignment.
The material of this document covers the measures used to protect a fictitious company called GIAC Enterprises as they connect to the Internet and begin using the services it provides. It also simulates an attack on a network design from a previous practical.
A description of GIAC Enterprises is given, along with an examination of their business practices, connectivity requirements, network design, and a cost justification.
The security policies of the network components are described, a tutorial for one of the components is given, and an audit of the design is performed and evaluated.

The design of a previous practical is analyzed for possible weaknesses and is then subject to an attack on the firewall itself, a Denial of Service attack, and an attack on a machine on the internal network. The attacks are planned, implemented, and then the results are used to create recommendations for improvement.

Table of Contents:

Table of Contents: (cont.)

Assignment 1:

Security Architecture (15 Points)

GIAC: the Company

GIAC is a small family owned company that has unwillingly embraced the information age. With sales dropping, the determination was made that it must become a ".com" company in order to compete with what had become a global list of competitors. After deciding that the benefits of connecting the company to the internet, if properly done, outweighed the dangers, a list of objectives was decided upon:

1) Implement secure web-based access for it's customers
2) Improve communications with suppliers
3) Better access to information shared with partners
4) Allow employee access to the internet
5) Provide secure connectivity to the mobile users and telecommuters
6) Secure the network from outside attack

The company currently has a physical presence in a renovated warehouse building in the "Old City" part of the business district. This has been beneficial in that the rent has been low and that the phone company has a central office (CO) nearby. The close proximity of the CO has allowed the company to take advantage of using a low cost DSL connection for access to and from the Internet.

The staff consist of four (4) full time employees, and six (6) part time/contract employees:

Employee	Hours	Role
Owner	Full	Owner/President of the Company In charge of In-House Sales
Owner's Husband	Full	Vice President Book keeping
Daughter	Full	In House Sales Maintaining the Web Site
Son	Full	Outside Sales
Grandson	Part	Information Systems
Local Writer	Part	Write Fortunes
Web Based Writers (4)	Part	Write Fortunes

Assignment 1:

Security Architecture
----
(2)

GIAC has established partnerships with other companies throughout the world. These companies create localized (translated) fortunes from those supplied to them by GIAC.

Access Requirements and Restrictions

- Customers: The class of user that will be accessing the GIAC Website to place orders or look up their account information.
- Suppliers: The class of user or entities that deliver fortune cookie sayings to GIAC.
- Partners: Companies with the need for real-time access to GIAC resources
- Internal Employees: User Class that is within the firewall.
- Sales and Mobile Workers: Those individuals who are employees and will be accessing internal resources from the public side of the firewall.

Class of User	Access Requirements	Restrictions
Customers	Account Info Email Online Catalog	No access to internal resources except those supplied through the web site Must have a Certificate to place email orders
Suppliers	Email	No access to internal resources
Partners	Database Email Terminal Service VPN	Limited access to internal resources - Controlled through Access Controls (Permissions/Rights)
Internal Employees	Database Email Internet Printer	No access to company banned web sites (none at this time)
Sales and Mobile Workers	Database Email Internet Printer Terminal Service VPN	No access to company banned Web sites through Local Network (via VPN) (none at this time)

Assignment 1:

Security Architecture
----
(3)

Business Operations

Starting from the point of view of a Customer there are three methods to interface with the staff of GIAC: (placing an order)

1. Call or Fax
   a. This is the preferred method of many of the customers who have a history with GIAC.
   b. The procedures are in place to do this and have been for many years.
   c. Procedure:
      i. The customer places and order
      ii. A Credit Card, P.O. Number, or Check Number is received by the GIAC staff.
      iii. The information is entered into the ordering system.
      iv. A work order is generated.
      v. The work order is filled, by placing the information onto the media the customer has requested. (see Shipping Procedure)

2. Email
   a. This method has been available, but has only recently been expanded to include new customers. Prior to using certificates to authenticate the identity of a user, only emails from trusted clients were accepted.
   b. Procedure:
      i. The customer can view the web site and decide upon what they would like to purchase (there is a downloaded form they can attach to their email).
      ii. They may call and then place the order later through email.
      iii. They may have placed orders previously and already know what they would like.
      iv. Once received and the email is authenticated (either through certificates, or staff knowledge of the individual), the information is keyed into the ordering system
      v. A work order is generated.
      vi. The work order is filled. (see Shipping Procedure)

3. Web Form
    a. The customer can do everything through the online store.
    b. Procedure:
        i. The customer views the online catalog and selects their purchase by placing items into their "shopping cart".
        ii. The customer then chooses to "check out" and is prompted for delivery method and payment options.
        iii. The backend system enters the information into the database.
        iv. A work order is generated.
        v. The work order is filled. (see Shipping Procedure)

The Suppliers deliver their product in one of the following ways:

1. Email
    a. This method is used by the supplier to either send the fortune cookie sayings:
        i. In the body of the message
        ii. As an attachment
2. FTP
    a. Not used as frequently
    b. Can be access directly or through a link on the Supplier section of the web page.
3. Physical Media
    a. The information is placed onto either a floppy disk, or a CDROM and delivered to GIAC.

Companies that GIAC has partnered with (companies that translate and sell the fortunes in other countries) have two options of accessing the database of sayings:

1. Terminal Services
    a. Through this method, they can access the database of sayings and then update the records with the proper translation.
    b. When complete, they can email themselves a copy of the translated text from within the database application or save the translations to files that can be sent as email attachments

2. VPN
    a. The database is accessed directly by the computers at the Partner's company. The employees (at the partner company) can update the records and then save the results locally.

Assignment 1:

Security Architecture

----

(5)

The Internal Employees are located on the local area network and have very few restrictions with respect to the internal resources. There are a few limitations on external websites that may be visited, and these are configured using the “site and content” rules of ISA server.
From the Internal Employees point of view, they have a need to access the following to perform their daily duties:

1) Database
    a. This is a SQL2000 based system.
    b. It has a set of forms or screens to access the company data and is the business system for the company.
    c. Has Modules for Accounts Receivable, Accounts Payable, Ordering/Purchasing, Shipping, Inventory, and Work Orders.
    d. Employees access this for all normal business activities
2) Email
    a. Outlook is the program used to view and send email.
    b. Customer/Supplier communications that are not handled with the telephone, or ones that need more clarity or follow-up can be done this way.
    c. It is also used for internal communications between the employees
3) Internet
    a. Accessing content from the Internet is accomplished using Internet Explorer
    b. It has mainly been seen as a side benefit of allowing public access to the web server.
    c. The only restriction that employees find when browsing is that the namespaces of some pop-up advertisement sites have been blocked.
4) Printers
    a. Are used by the employees to create the Packing List, Invoices, and other print-based communications used by the company.
    b. These are network-based printers.

The Mobile, Sales and Teleworkers are all part of the same category of users that require access to internal resources, but are located outside of the network perimeter. Dial-up, DSL, Cable, and ISDN are used by the individuals to connect to the Internet and then to GIAC. This difference in speed has made different connectivity methods a must.
From the External Employees point of view, they have a need to access one or more of the following to perform their daily duties:

Assignment 1:

Security Architecture

----

(6)

a. Database
   a. Access to the database requires that a VPN first be established to the internal network.
   b. This is a SQL2000 based system.
   c. It has a set of forms or screens to access the company data and is the business system for the company.
   d. Has Modules for Accounts Receivable, Accounts Payable, Ordering/Purchasing, Shipping, Inventory, and Work Orders.
   e. Only certain External Employees access this for their business activities and it is not their normal method. It is used only for temporary or special needs.

b. Email
   a. It can be accessed through the VPN or through a connection to the Exchange server via POP3.
   b. Outlook is the preferred program used to view and send email, although some external users have chosen other pop mail readers.
   c. Customer/Supplier communications that are not handled with the telephone, or ones that need more clarity or follow-up can be done this way.
   d. It is also used for internal communications between the employees.

3) Internet
   a. Accessing content from the Internet is typically accomplished using Internet Explorer and the Internet connection they originally established to connect to GIAC.

4) Printers
   a. Can be accessed remotely if the employee has established a VPN.
   b. May also be accessed from a Terminal Service session.
   c. These are network-based printers.

5) Terminal Service
   c. Used when direct connectivity is not required or
   d. A slow connection has been established to the Internet (dial-up).

Assignment 1:

Security Architecture
----
(7)

Connectivity (To GIAC)

Class of User	Connectivity	Ports
Customers	HTTP HTTPS	80 443
Suppliers	Email	25
Partners	Database	1433 via VPN
	Email	25
	Terminal Server	3389 (UDP) (via VPN), 3389 (TCP) (via VPN)
	VPN	1723 PPTP
Sales and Mobile Workers	Internet	80, 443
	Database	1433 via VPN,
	Email	25, 110
	Terminal Server	3389 (UDP) (via VPN), 3389 (TCP) (via VPN)
	VPN	1723 PPTP

Connectivity (From GIAC)

Class of User	Services	Applications	Protocol/Port
Internal Employees	Internet	Web Browser	80, 443
	Database	SQL	1433
	Email	Email Client (Outlook)	25, 110, 143
	FTP	FTP	20/21
	Printer	Windows OS	
Sales and Mobile Workers	Internet	Web Browser	80, 443
	Email	Email Client	25, 110
	Printer	Windows OS	

Architecture Design

The following table lists the components and the service or function they perform (see appendix C for Custom Security Template information)

Public	
GIACRTR Cisco 2600 IOS Version 12.2 (5d) DSL card	Border/Filtering Router

Assignment 1:

Security Architecture

----

(8)

Internal Network	
Item	**Use**
GIACCORP 1 Windows 2000 Server (w/SP2) Custom security template applied	Main Server for the company Global Catalog Server/DC PDC / Relative ID Master (RID) DNS/DHCP
GIACIDS2 Windows 2000 Pro (w/SP2) Custom security template applied	Host Operating System for Snort
GIACTERM Windows 2000 Server (w/SP2) Custom security template applied	Windows 2000 Terminal Service
GIACSQL Windows 2000 Server (w/SP2) SQL 2000 Custom security template applied	Database server to support queries from the GIACWEB web server Domain Controller Infrastructure Master DHCP (secondary)

Perimeter	
GIACWEB Windows NT4.0 Server (w/SP6a) Internet Information Server Custom security template applied	Storefront with shopping cart and checkout. GIAC main web site
W2KISA1 Windows 2000 Server (w/SP2) ISA Server w/SP1 Custom security template applied	External Perimeter Firewall Perimeter VPN Endpoint
W2KISA2 Windows 2000 Server (w/SP2) ISA Server w/SP1 Custom security template applied	Internal Perimeter Firewall Internal VPN Endpoint
GIACIDS1 Windows 2000 Pro (w/SP2) Custom security template applied	Host Operating System for Snort
GIACMAIL Windows 2000 Server (w/SP2) Exchange 2000 w/SP2 Custom security template applied	Mail Server

Filtering Routers

- Cisco 2600 w/DSL card
    - This purpose of this component is as a connectivity point to the outside world.
    - It is placed between the External Firewall and the Internet.
    - Access lists (the rules that control how traffic flows through the router) are limited to the following:
        - Access list 10 - Needed to remove "noise" from the Internet. In this case, all of the unused/unassigned address space, the loopback address, the private IP address ranges, the APIPA (169.254) range, the multicast range, and any internal address ranges.
        - Access list 110 - Allows only internal addresses to get out.
        - Access list 20 – Used to secure the router itself. This is a list that is applied to restrict telnet to a specific host or hosts.
    - Appendix A of the SANS/FBI Top 20 list will be addressed at the external firewall and not the border router.
    - The standard access list applied (access list 10) does not allow for port or protocol blocking, but it has the benefit of requiring fewer router resources than an extended access list.

<u>External Firewall</u>

- Microsoft ISA Server – Standard Edition
    - This component is used as the primary defense against outside attacks. It also serves the purpose of a reverse-proxy for external access to the GIAC web server.
    - It is placed between the Border router and the Perimeter network (DMZ)
    - The Operating System has been hardened (see configuration section later in this document)
    - Rules are configured that:
        - Address Appendix A of the SANS/FBI Top 20 list. Only required ports are allowed

list. Only required ports are allowed.
        - Allow traffic to the Web server (through server publishing)
        - Allow traffic to the FTP server (through server publishing)
        - Allow email traffic to the Exchange Server (through mail server publishing)
        - Allow Terminal Service traffic on port 3389 (this is done through the VPN connection)
        - VPN connectivity is implemented using PPTP
        - All other external traffic is blocked
    - See the ISA server configuration section later in the document

<u>VPN</u>

- Microsoft ISA Server – Standard Edition
    - The External and Internal firewalls serve this role through a combined effort.
        - The User establishes a VPN connection to the external firewall
        - The VPN connection is given an IP address valid on the perimeter network (DMZ). DMZ resources are then available, or….
        - The user then establishes another VPN connection. This one is to the Internal firewall via the first VPN
        - The second VPN is given an IP address valid on the internal network
        - The user can now access internal resources
    - Placement will be considered to be the two endpoints of the VPN, or the DMZ and the Internal Network. (see VPN config later in this document)
    - The method describe in an article at the ISAServer.org website was used:
      VPN Access in a back to back ISA configuration:
      http://www.isaserver.org/pages/article.asp?id=212

<u>Internal Firewall</u>

- Microsoft ISA Server – Standard Edition
    - Serves as the final endpoint for the VPN connections as well as being the protection for the internal

network.
    - It is placed between the Perimeter Network (DMZ) and the Internal Network.
    - Ports are opened to allow access from:
        - Web Server to the SQL Server (1433)
        - From the internal network to common web services (DNS:53, HTTP:80, HTTPS:443, POP3:110, IMAP:143, Telnet:23, FTP:20/21)
        - From the Terminal Server to the Internal Network

<u>Additional Secure Remote Access</u>

- Microsoft Terminal Service
    - This component is used for its ability to work with slow connections (28.8 bps) and because it can be used to access company resources without giving the user direct connectivity to the internal network
    - It allows for a layered approach to access
        - Partners and employees can connect here to gain indirect access to company resources. (faster for anything that does not require data transfer)
        - Partners and employees can use the above listed VPN method to gain direct access to internal resources.
    - It is placed on the perimeter Network
    - User authentication is through Active Directory
    - Connectivity to the Terminal server from offsite is through the VPN connection to the External Firewall

<u>Intrusion Detection System</u>

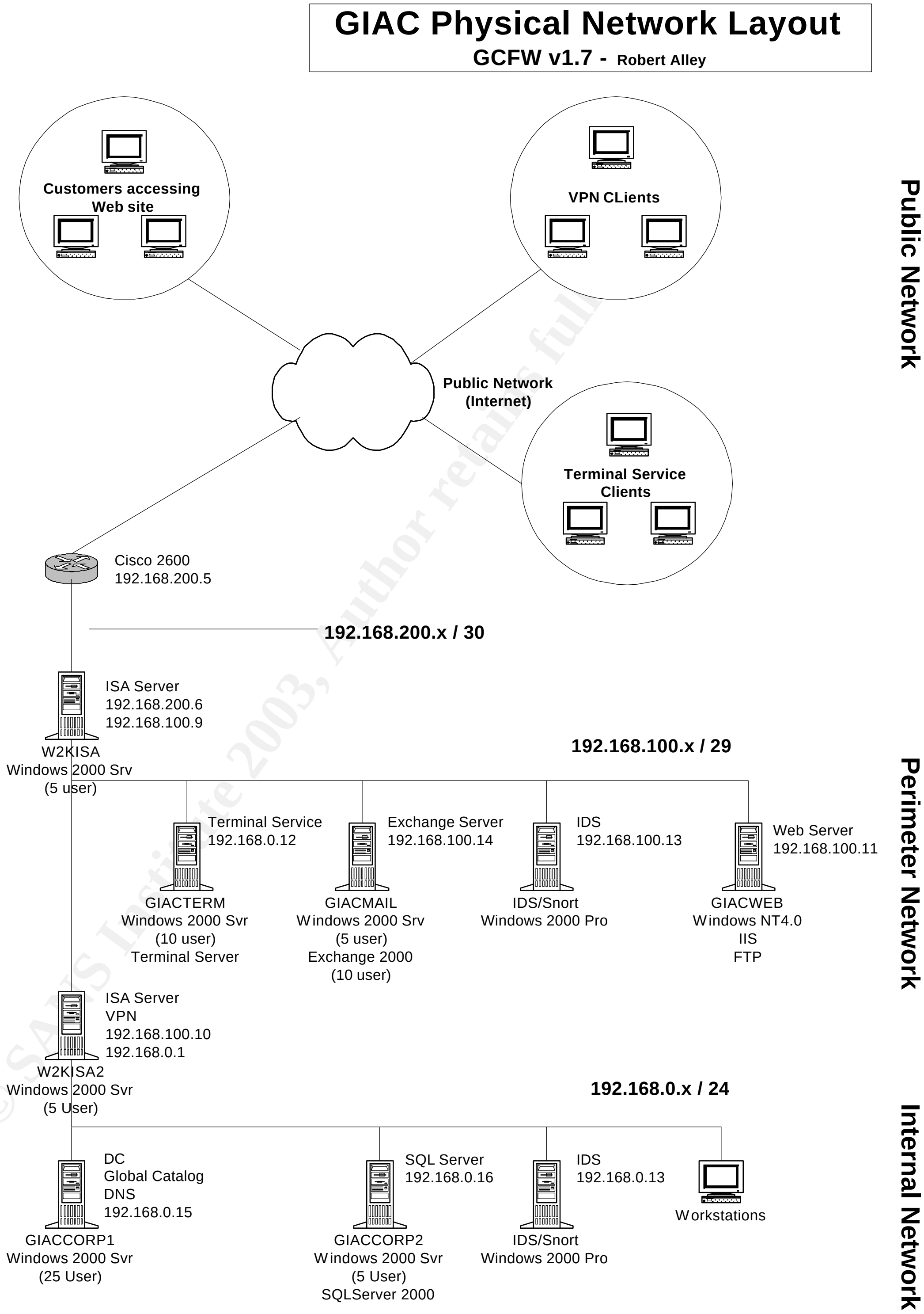
- Snort 1.8.x for Win32
    - This component is used to detect and alert if there is suspicious activity on the network.
    - GIACIDS1 is placed on the DMZ and is used to detect possible attacks and unwanted traffic to the Web, Email, and Terminal Servers.
    - GIACIDS2 is placed on the Internal Network and is used to detect unwanted activity (network traffic). This traffic may come from the Internet, VPN clients, or from compromised (infected) internal clients.

Assignment 1:

Security Architecture

----

(12)



Assignment 1:

Security Architecture
----
(13)

Cost Justification

Software

Item	Qty	Cost	Total Cost
Windows 2000 Server – 5 user	4	$900.00	$3600.00
Windows 2000 Server - 25 User	1	$1500.00	$1500.00
ISA Server – Standard Edition	2	$1300.00	$2600.00
Exchange 2000 – 5 user	1	$1100.00	$1100.00
Exchange 2000 – addition 5 user license	1	$50.00	$50.00
Windows 2000 Professional	2	$270.00	$540.00
			$9060.00

Hardware

Item	Qty	Cost	Total Cost
Cisco 2600 Router (used)	1	$935.00	$935.00
WIC-1DSU-T1 DSL module (auction)	1	$312.00	$312.00
2U Dual PIII 550 Mhz Rack Server w/ 512 meg RAM, 9.1GB HD (auction)	5	$335.00	$2010.00
2U Dual P3 1 GHz w/ 1GB RAM, 73GB HD (auction)	3	760.00	$2280.00
			$5537.00

Due to there not being a budget allocated to implement this project, one of the goals in securing GIAC was to keep the cost at a minimum and still supply a degree of protection. In adhering to this goal the following occurred:

The software for the firewall design was purchased retail and the costs listed represent a low-end estimate of several suppliers.

The hardware was purchased from an online auction service, and therefore reduced the cost of implementation dramatically. The three 1GHz computers will be used for the two ISA servers and the SQL Server (GIACCORP2).
The total cost for Hardware and Software is **$14,597.00.**

Security Policies

Border Router

The following lines are used to discard any traffic that may be from one of the private IP address ranges, the reserved range, multicast, or loopback. This is the initial order of these rules. The logs can be audited periodically and the rules that are used most often can be moved higher in the list to make it more efficient.

```
access-list 10 deny 10.0.0.0 0.255.255.255            < private
access-list 10 deny 172.16.0.0 0.15.255.255           < private
access-list 10 deny 192.168.0.0 0.0.255.255           < private
access-list 10 deny 169.254.0.0 0.0.255.255           < private (APIPA)
access-list 10 deny 224.0.0.0 31.255.255.255          < multicast
access-list 10 deny 127.0.0.0 0.255.255.255           < loopback
access-list 10 deny 0.0.0.0 0.255.255.255             < reserved
access-list 10 deny 1.0.0.0 0.255.255.255
access-list 10 deny 2.0.0.0 0.255.255.255
access-list 10 deny 5.0.0.0 0.255.255.255
access-list 10 deny 7.0.0.0 0.255.255.255
access-list 10 deny 23.0.0.0 0.255.255.255
access-list 10 deny 27.0.0.0 0.255.255.255
access-list 10 deny 31.0.0.0 0.255.255.255
access-list 10 deny 36.0.0.0 0.255.255.255
access-list 10 deny 37.0.0.0 0.255.255.255
access-list 10 deny 39.0.0.0 0.255.255.255
access-list 10 deny 41.0.0.0 0.255.255.255
access-list 10 deny 42.0.0.0 0.255.255.255
access-list 10 deny 49.0.0.0 0.255.255.255
access-list 10 deny 50.0.0.0 0.255.255.255
access-list 10 deny 58.0.0.0 0.255.255.255
access-list 10 deny 59.0.0.0 0.255.255.255
access-list 10 deny 60.0.0.0 0.255.255.255
access-list 10 deny 70.0.0.0 0.255.255.255
access-list 10 deny 71.0.0.0 0.255.255.255
access-list 10 deny 72.0.0.0 7.255.255.255
access-list 10 deny 82.0.0.0 31.255.255.255
access-list 10 deny 197.0.0.0 0.255.255.255
access-list 10 deny 201.0.0.0 0.255.255.255
access-list 10 deny 222.0.0.0 0.255.255.255
access-list 10 deny 223.0.0.0 0.255.255.255
access-list 10 deny 240.0.0.0 15.255.255.255          < reserved
access-list 10 permit any                       < allow everything else
```

Assignment 2: Security Policy and Tutorial
----
(2)

This is applied to the DSL port as an incoming (ingress) filter.

```
interface ATM0/0
ip access-group 10 in
```

(see tutorial)

This next section list the lines used to allow the internal networks to pass through to the public network. It also has restrictions for NetBIOS traffic to prevent it from passing through. Finally, it has a line to deny all other traffic.

```
access-list 110 deny udp any any eq 138                 < netbios
access-list 110 deny udp any any eq 137                 < netbios
access-list 110 permit ip 192.168.0.0 0.0.0.255 any     < internal network
access-list 110 permit ip 192.168.100.0 0.0.0.255 any   < internal network
access-list 110 permit ip 192.168.200.0 0.0.0.255 any   < internal network
access-list 110 deny ip any any log                     < deny any other IP
                                                          traffic and log it
```

This access list is applied to the Ethernet interface as an incoming filter.

```
interface fa0/0
ip access-group 110 in
```

(see tutorial)

This section list the lines used to restrict vty (telnet) access to the router. It is configured to only allow access from the network administrator's computer host (192.168.0.55) on the inside of the router.

```
 access-list 20 permit 192.168.0.55  0.0.0.0            < internal networks
```

This access list is applied to the vty lines 0 through 4 as an incoming filter

```
 line vty 0 4
 ip access-class 20 in
```

(see tutorial)

Assignment 2: Security Policy and Tutorial
----
(3)

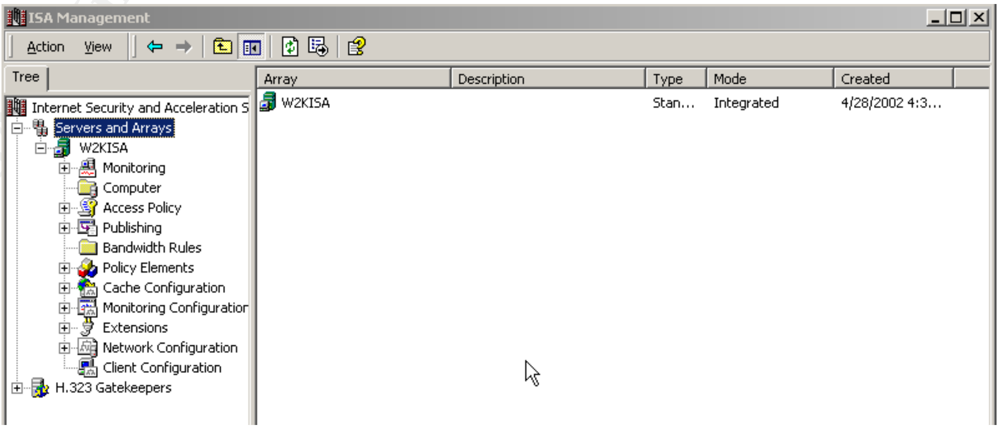
External Perimeter Firewall

Incoming Traffic (allowed)					
Protocol	Source Address	Source Port	Destination Address	Destination Port	Note
HTTP	Any	Any	192.168.100.11	80	
HTTPS	Any	Any	192.168.100.11	443	SSL
FTP	Any	Any	192.168.100.11	21	Ctrl
FTP	Any	Any	192.168.100.11	20	Data
SMTP	Any	Any	192.168.100.14	25	
POP3	Any	Any	192.168.100.14	110	
IMAP	Any	Any	192.168.100.14	143	
VPN	Any	Any	192.168.200.6	1723	PPTP

Note: Terminal Service uses port 3389 TCP and UDP for access but these will not be passed by the firewall. Connectivity to the Terminal Server will be through the VPN connection.

Web Server

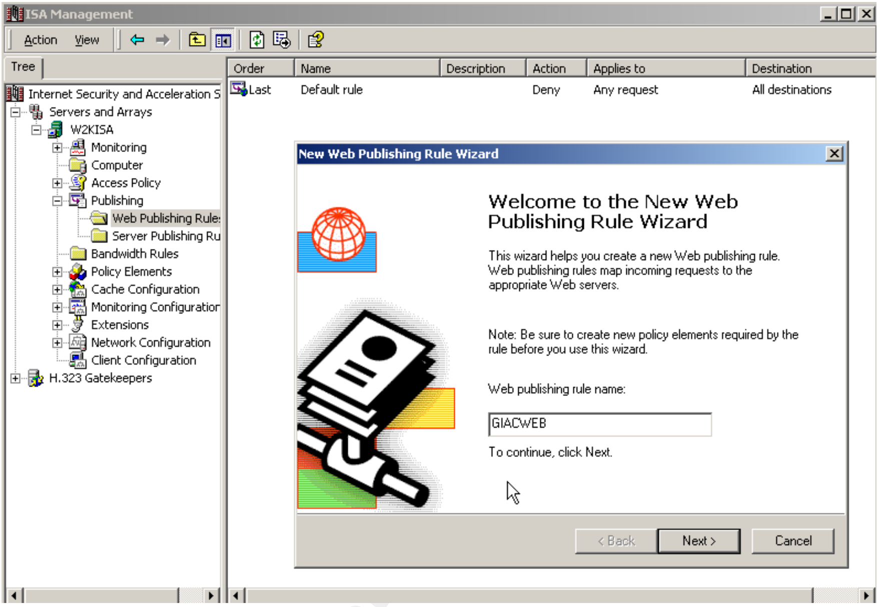
Web Server access from the Internet is accomplished by using the Web Server Publishing feature of the ISA Server. Microsoft has supplied a Wizard that creates the necessary rules to pass port 80, and port 443 traffic to an internal address. This can be accomplished by starting the ISA Management Console (below) and expanding the publishing tab (Figure WP2). A name is given to the rule-set and then <NEXT> is selected.



Array	Description	Type	Mode	Created
W2KISA		Stan...	Integrated	4/28/2002 4:3...

Figure WP1 (ISA Management Console)

Assignment 2: Security Policy and Tutorial
----
(4)



Welcome to the New Web Publishing Rule Wizard

This wizard helps you create a new Web publishing rule. Web publishing rules map incoming requests to the appropriate Web servers.

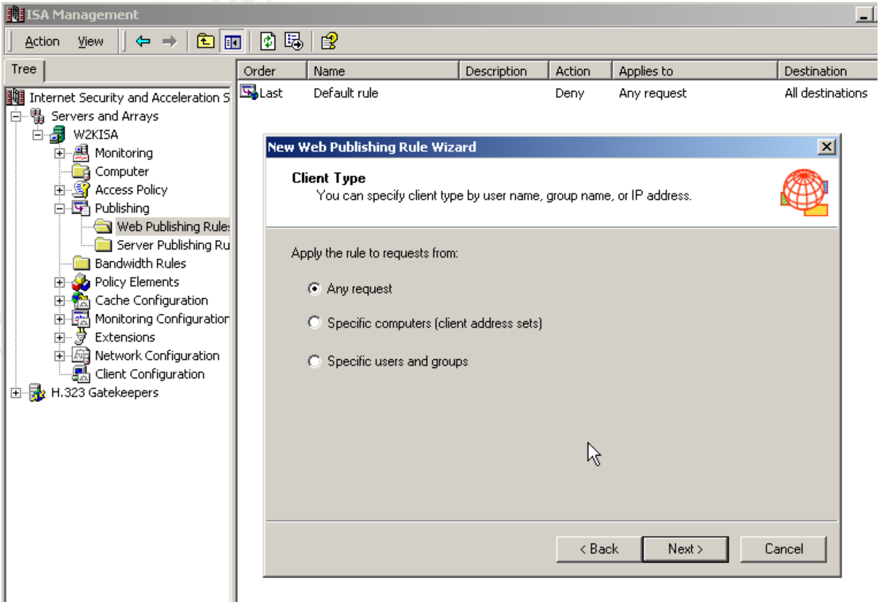
Note: Be sure to create new policy elements required by the rule before you use this wizard.

Web publishing rule name: GIACWEB

To continue, click Next.

Figure WP2 (Naming the Rule-Set)

The External clients that will be accessing the web server are selected. In this case, all of the hosts on the Internet. (Figure WP3)



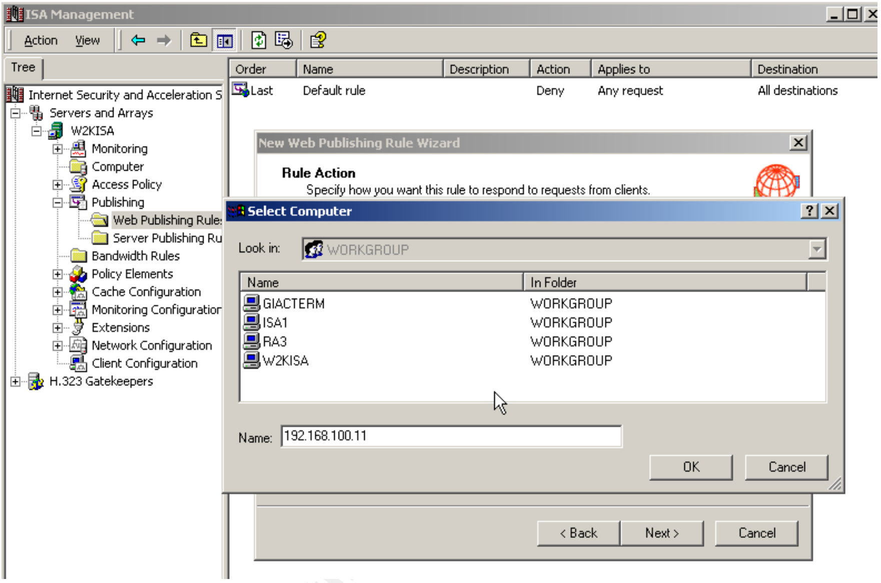
Client Type
You can specify client type by user name, group name, or IP address.

Apply the rule to requests from:

● Any request
○ Specific computers (client address sets)
○ Specific users and groups

Figure WP3 (Setting up access to the web server)

Once the external clients are configured, the Web server to be published can be chosen from a list of available servers, or the IP address can be typed in manually. (Figure WP4)



Order	Name	Description	Action	Applies to	Destination
Last	Default rule		Deny	Any request	All destinations

Rule Action
Specify how you want this rule to respond to requests from clients.

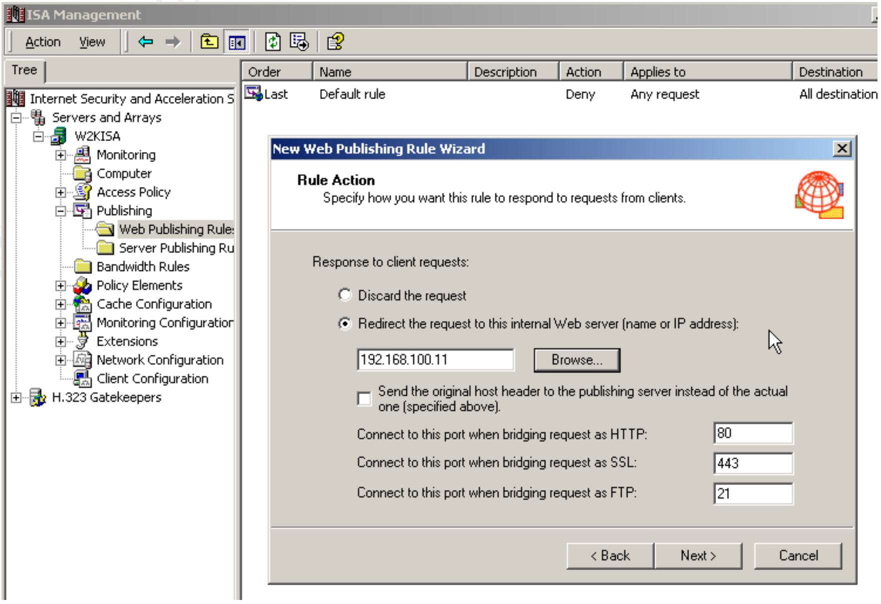
Look in: WORKGROUP

Name	In Folder
GIACTERM	WORKGROUP
ISA1	WORKGROUP
RA3	WORKGROUP
W2KISA	WORKGROUP

Name: 192.168.100.11

Figure WP4 (Selecting the Web Server)

Redirection options are then available. The defaults of ports 80, 443 and 21 are used to bridge (redirect) the requests to the internal web server. (Figure WP5)



Order	Name	Description	Action	Applies to	Destination
Last	Default rule		Deny	Any request	All destination

Rule Action
Specify how you want this rule to respond to requests from clients.

Response to client requests:

○ Discard the request
● Redirect the request to this internal Web server (name or IP address):
192.168.100.11

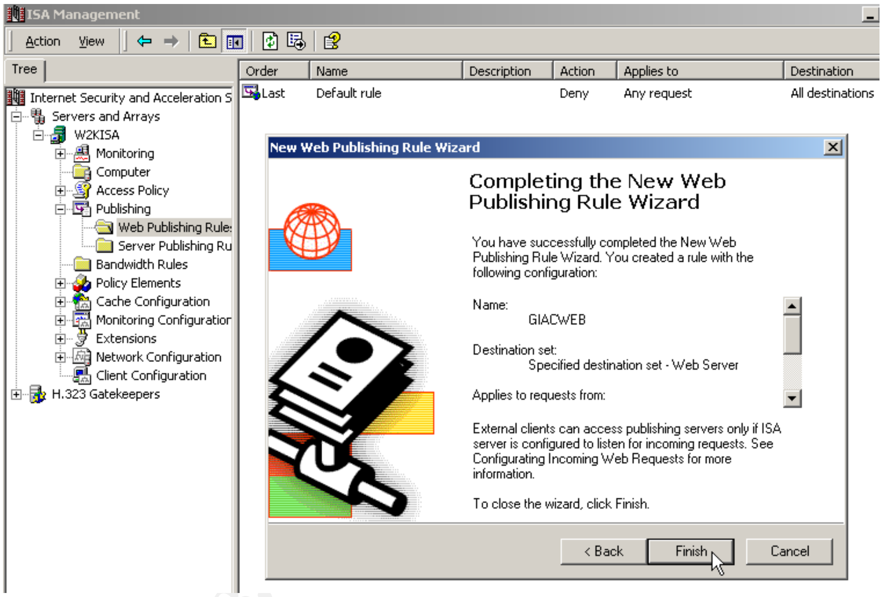
☐ Send the original host header to the publishing server instead of the actual one (specified above).

Connect to this port when bridging request as HTTP: 80
Connect to this port when bridging request as SSL: 443
Connect to this port when bridging request as FTP: 21

Figure WP5 (Redirecting the requests to the web server)

Assignment 2: Security Policy and Tutorial
----
(6)

Configuration is now complete and the Wizard presents a closing screen that displays what has been done. (Figure WP6)



Order	Name	Description	Action	Applies to	Destination
Last	Default rule		Deny	Any request	All destinations

Completing the New Web Publishing Rule Wizard

You have successfully completed the New Web Publishing Rule Wizard. You created a rule with the following configuration:

Name:
GIACWEB

Destination set:
Specified destination set - Web Server

Applies to requests from:

External clients can access publishing servers only if ISA server is configured to listen for incoming requests. See Configurating Incoming Web Requests for more information.

To close the wizard, click Finish.

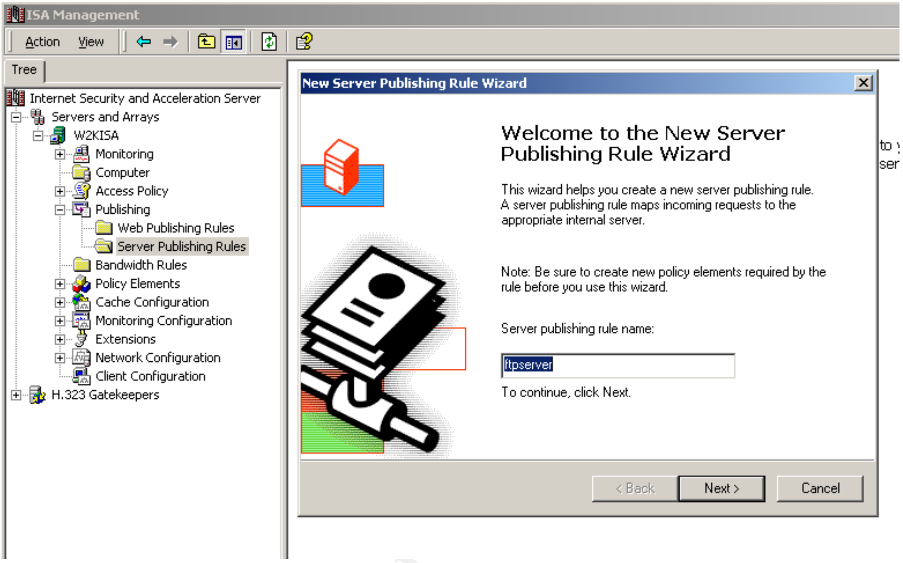
Figure WP6 (The completion screen)

The Web Server is now accessible from the Internet. <Hint> Remember, The IP Address registered with the DNS services will be the external address of the ISA Server and not the DMZ address of the Web Server. <End Hint>

<ins>FTP Server</ins>

Access to FTP services (ports 20 and 21) is accomplished through the Server Publishing Wizard. This wizard has a list of services to choose from during the configuration process. Similar to the Web Publishing wizard, the ftp services are actually redirected from the external interface to the internal FTP server.

The Publishing tab is again selected, followed by Server Publishing Rules. The caption to name the rule-set is the first option of the wizard (Figure FS1). This is followed by the internal IP address of the server to be published, as well as, the external address of the ISA server (Figure FS2).



Welcome to the New Server Publishing Rule Wizard

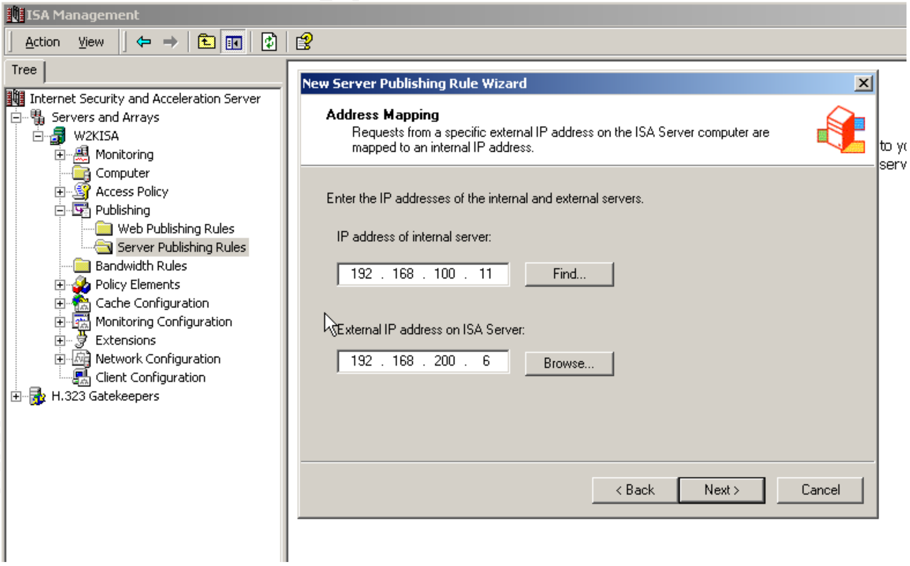
This wizard helps you create a new server publishing rule. A server publishing rule maps incoming requests to the appropriate internal server.

Note: Be sure to create new policy elements required by the rule before you use this wizard.

Server publishing rule name: ftpserver

To continue, click Next.

Figure FS1 (Naming the Server Rule)



Address Mapping

Requests from a specific external IP address on the ISA Server computer are mapped to an internal IP address.

Enter the IP addresses of the internal and external servers.

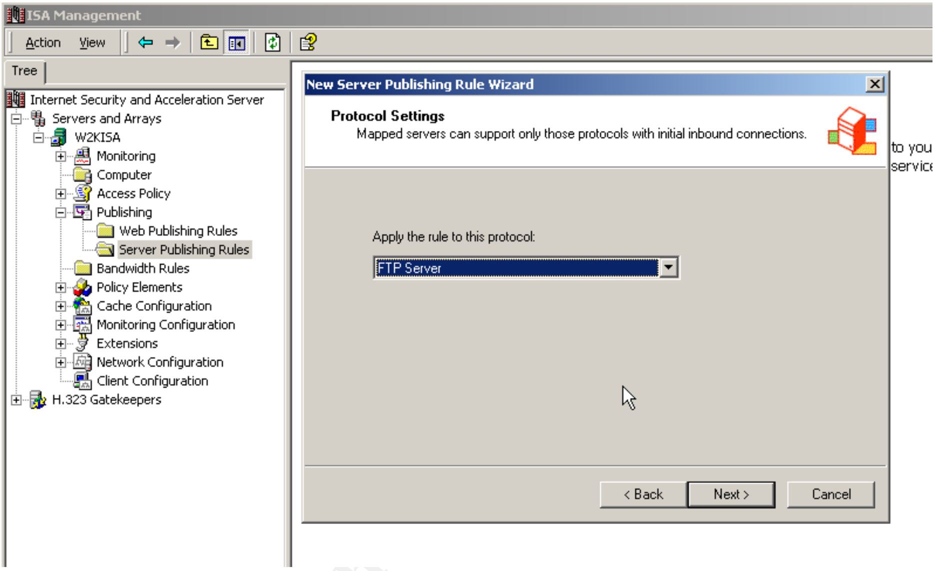
IP address of internal server: 192 . 168 . 100 . 11

External IP address on ISA Server: 192 . 168 . 200 . 6

Figure FS2 (Setting IP addresses)

The wizard then gives an option of the Microsoft defined protocols that can be chosen. All of the major services are listed when the drop down box is clicked on, and from here the FTP server is selected (Figure FS3). This will open up Port 21 (FTP Control) and Port 20 (FTP Data) on the external interface. FTP traffic is then redirected to the internal address of the FTP server. The responses will be redirected back through the ISA Server and to the external host somewhere on the Internet.

to the external host somewhere on the Internet.



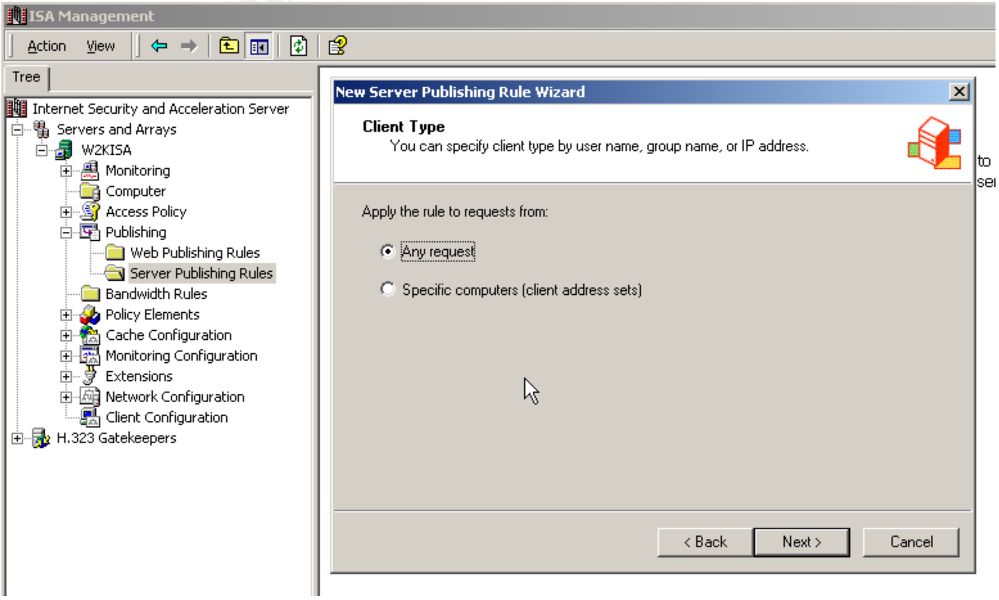
New Server Publishing Rule Wizard

Protocol Settings
Mapped servers can support only those protocols with initial inbound connections.

Apply the rule to this protocol:
FTP Server

Figure FS3 (Selecting a Server type)

Next, access to the appropriate clients is granted. In this case it is applied to any request from the internet (Figure FS4).

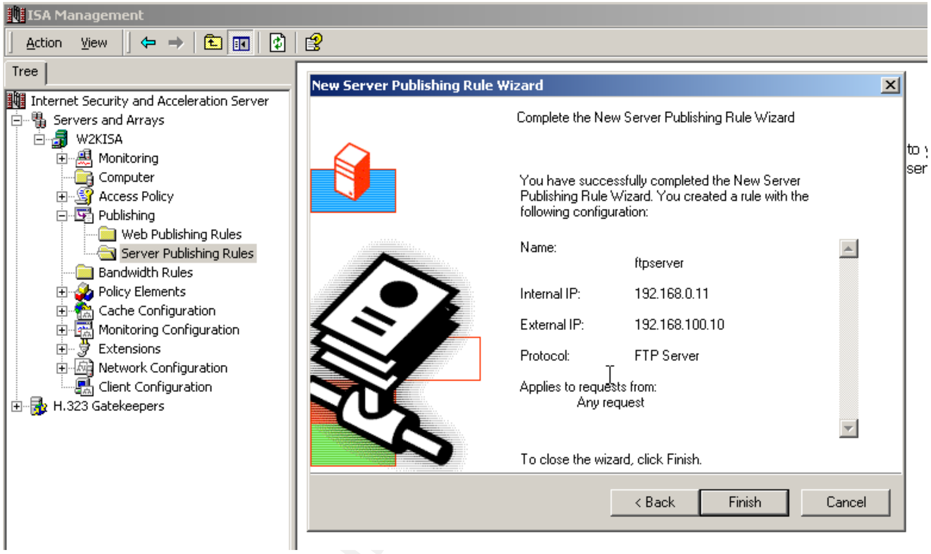


New Server Publishing Rule Wizard

Client Type
You can specify client type by user name, group name, or IP address.

Apply the rule to requests from:
● Any request
○ Specific computers (client address sets)

Figure FS4 (Setting up client access)



Complete the New Server Publishing Rule Wizard

You have successfully completed the New Server Publishing Rule Wizard. You created a rule with the following configuration:

Name: ftpserver
Internal IP: 192.168.0.11
External IP: 192.168.100.10
Protocol: FTP Server
Applies to requests from:
Any request

To close the wizard, click Finish.

Figure FS5 (

The ending screen shows the chosen configuration and can now be closed by selecting <FINISH>. The FTP server setup is now complete and the internal ftp server will now receive requests. <Note> Remember that the IP address listed in the public DNS record must be that of the external interface of the ISA server and not the IP address of the FTP server located on the DMZ.

Email

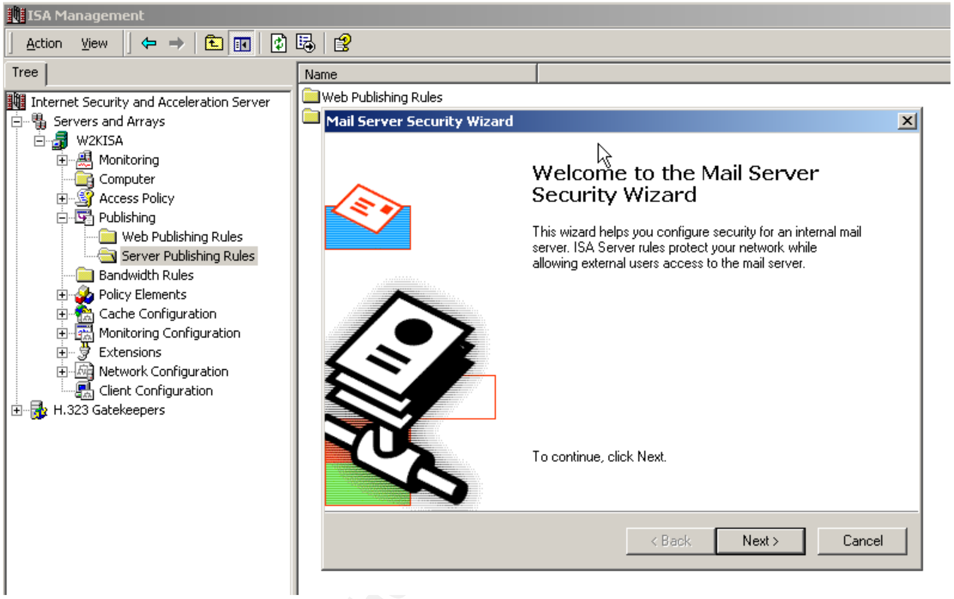
The Mail services are configured using the Secure Mail Publishing Wizard. This wizard will redirect ports 25,100, and 143 to the mail server located on the DMZ.

The first option after starting the wizard (Figure MS1) is to select the appropriate protocols for the site. SMTP, POP3 and MS Exchange are selected (Figure MS2). The MS Exchange option opens up the Exchange server to RPC, so caution and possibly a risk analysis should be conducted. Selecting <NEXT> will advance to the next screen of the wizard.

Assignment 2: Security Policy and Tutorial

----

(10)

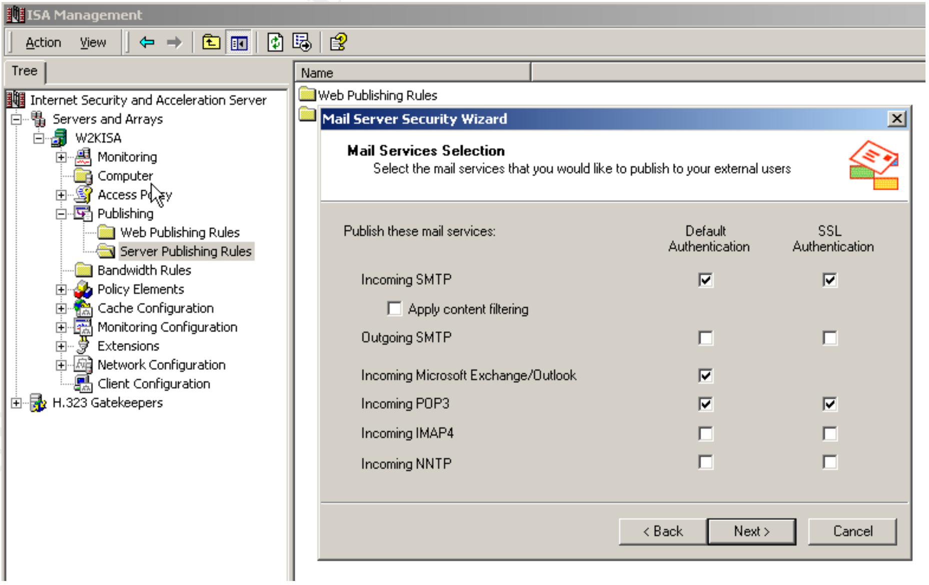


Welcome to the Mail Server Security Wizard

This wizard helps you configure security for an internal mail server. ISA Server rules protect your network while allowing external users access to the mail server.

To continue, click Next.

Figure MS1 (Starting the Mail Wizard)



Mail Services Selection
Select the mail services that you would like to publish to your external users

Publish these mail services:	Default Authentication	SSL Authentication
Incoming SMTP	☑	☑
☐ Apply content filtering		
Outgoing SMTP	☐	☐
Incoming Microsoft Exchange/Outlook	☑	
Incoming POP3	☑	☑
Incoming IMAP4	☐	☐
Incoming NNTP	☐	☐

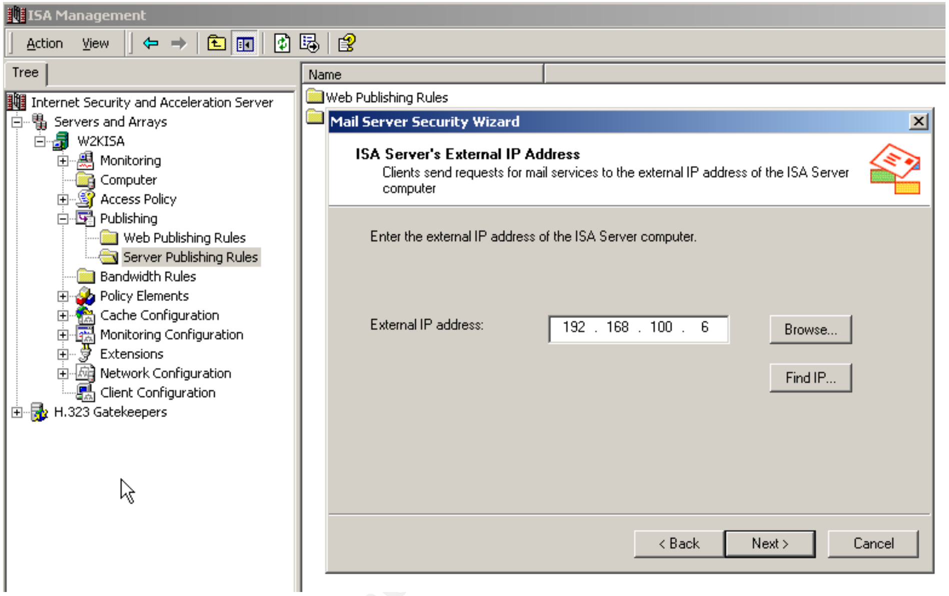
Figure MS2 (Selecting the Protocols)

The IP address of the ISA Server's external interface is then selected from the next screen (Figure MS3), and the IP address of the internal mail server is entered into the one following (Figure MS3).

Assignment 2: Security Policy and Tutorial

----

(11)



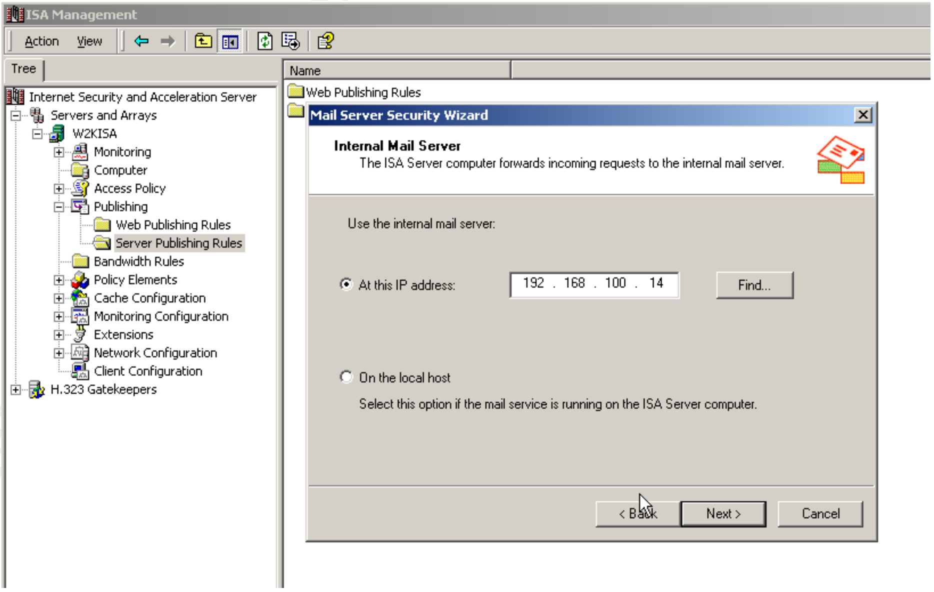
ISA Server's External IP Address

Clients send requests for mail services to the external IP address of the ISA Server computer

Enter the external IP address of the ISA Server computer.

External IP address: 192 . 168 . 100 . 6

Figure MS3 (Selecting the ISA Server's External Address)



Internal Mail Server

The ISA Server computer forwards incoming requests to the internal mail server.

Use the internal mail server:

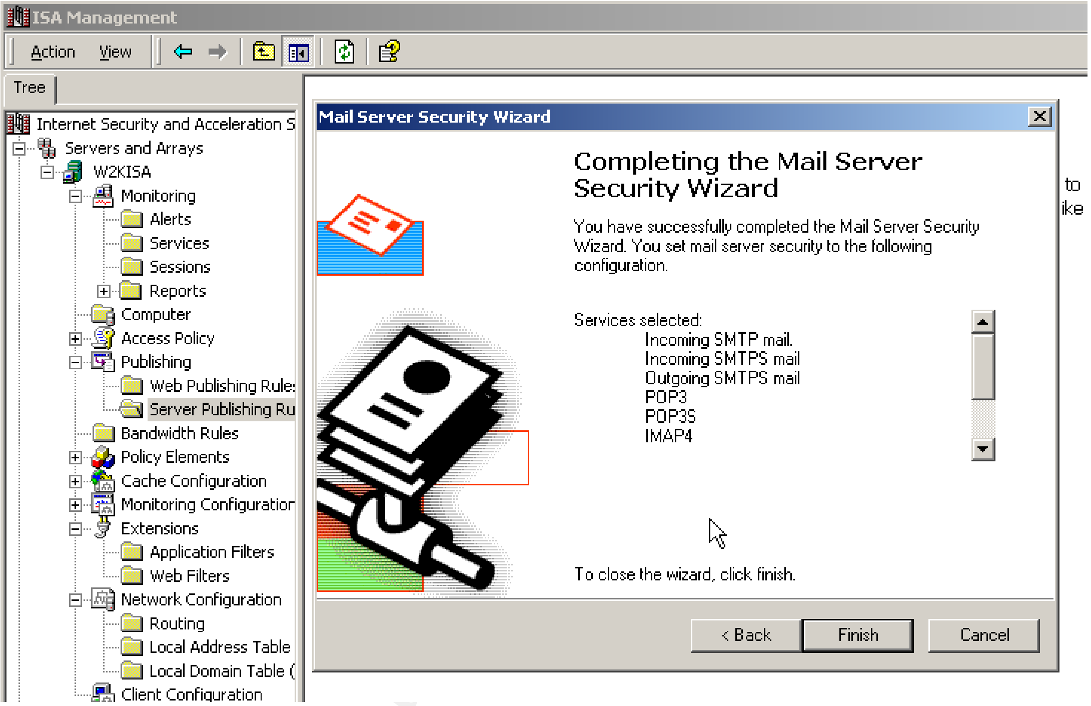
● At this IP address: 192 . 168 . 100 . 14

○ On the local host

Select this option if the mail service is running on the ISA Server computer.

Figure MS4 (Internal Mail Server selection)

The closing screen of the Wizard shows the protocols that were selected. After selecting <FINISH> (Figure MS5), the screen will now show the rule-sets created to support email traffic (Figure MS6).



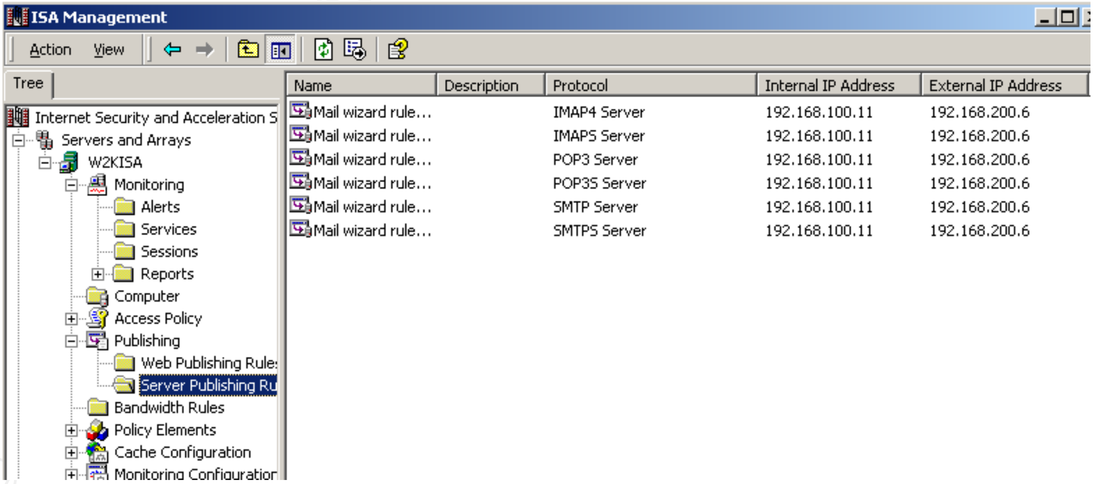
Completing the Mail Server Security Wizard

You have successfully completed the Mail Server Security Wizard. You set mail server security to the following configuration.

Services selected:
Incoming SMTP mail.
Incoming SMTPS mail
Outgoing SMTPS mail
POP3
POP3S
IMAP4

To close the wizard, click finish.

Figure MS5 (Mail Wizard closing screen)



Name	Description	Protocol	Internal IP Address	External IP Address
Mail wizard rule...		IMAP4 Server	192.168.100.11	192.168.200.6
Mail wizard rule...		IMAPS Server	192.168.100.11	192.168.200.6
Mail wizard rule...		POP3 Server	192.168.100.11	192.168.200.6
Mail wizard rule...		POP3S Server	192.168.100.11	192.168.200.6
Mail wizard rule...		SMTP Server	192.168.100.11	192.168.200.6
Mail wizard rule...		SMTPS Server	192.168.100.11	192.168.200.6

Figure MS6 (Mail Wizard rule-set)

Terminal Server

The Terminal Server will not need to be set up using the server publishing wizard since it will be accessed through A VPN connection to the DMZ. If the Terminal Server was to be accessed through the Firewall, the Server Publishing Wizard could be used to select TCP and UDP port 3389.

Outgoing Traffic (allowed)					
Protocol	Source Address	Source Port	Destination Address	Destination Port	Note
HTTP	192.168.0.0	Any	Any	80	
HTTPS	192.168.0.0	Any	Any	443	SSL
FTP	192.168.0.0	Any	Any	21	Ctrl
FTP	192.168.0.0	Any	Any	20	Data
SMTP	192.168.0.0	Any	Any	25	
POP3	192.168.0.0	Any	Any	110	
IMAP	192.168.0.0	Any	Any	143	
SMTP	192.168.100.14	Any	Any	25	
DNS	192.168.100.14	Any	Any	53	TCP

The External Firewall is set up to allow traffic from the internal network (192.168.0.0) to reach the Internet. HTTP, HTTPS, and FTP traffic is passed from the Internal ISA Server to the External ISA Server, therefore rules do not need to be created to pass these. The easiest way to configure for the remaining protocols is to use the same "Inet Rule" that was created for the Internal Firewall. The email rules can be retained and the others deleted. (see the Inet rule-set configuration below)

Incoming email (ports 25, 110, 143) and the responses are automatically handled by the Secure Email Publishing rules. The outgoing email will require SMTP port 25 to be passed, and the rule for this was created automatically by the Secure Email Wizard that was run earlier. DNS queries over TCP Port 53 will also need to be opened to allow the Exchange Server to resolve MX records for email domains. <NOTE> Exchange Server uses TCP and not UDP for DNS queries. <End NOTE>

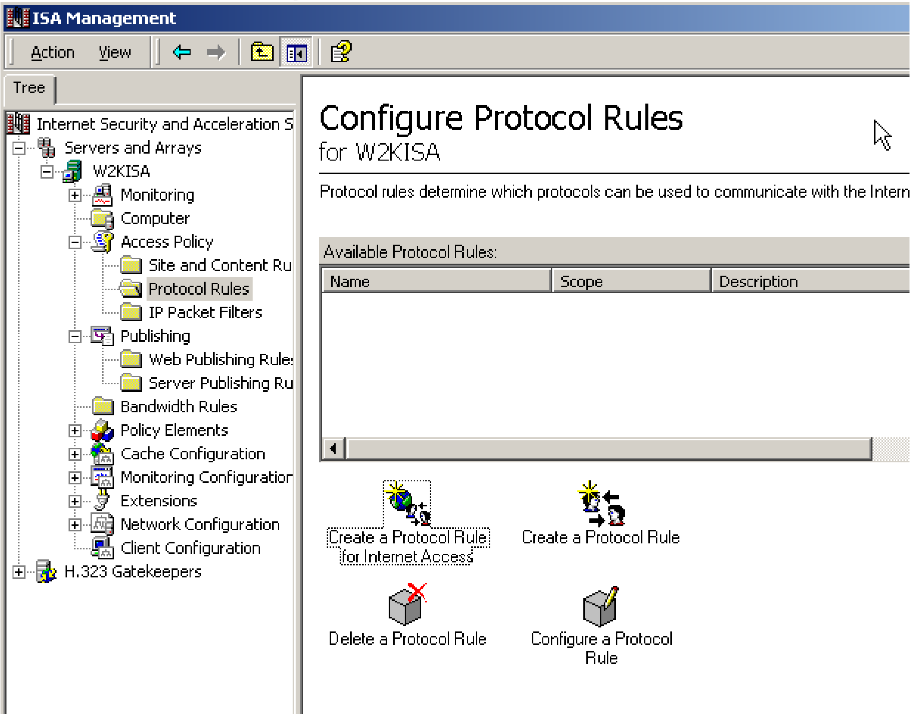
Internal Perimeter Firewall

Incoming Traffic (allowed)					
Protocol	Source Address	Source Port	Destination Address	Destination Port	Note
SQL	192.168.100.11	Any	192.168.0.16	1433	Data
Any	192.168.100.12	Any	192.168.0.15	Any	Data

The only traffic that is allowed into the internal network is from the Web Server (192.168.100.11) to the SQL Server (192.168.0.15), and from the Terminal Server (192.168.100.12) to the internal network. All other traffic is blocked. These exceptions are handled by publishing the SQL server and by creating a protocol rule for the Terminal Server.

Outgoing Traffic (allowed)					
Protocol	Source Address	Source Port	Destination Address	Destination Port	Note
HTTP	192.168.0.0	Any	Any	80	
HTTPS	192.168.0.0	Any	Any	443	SSL
FTP	192.168.0.0	Any	Any	21	Ctrl
FTP	192.168.0.0	Any	Any	20	Data
SMTP	192.168.0.0	Any	Any	25	
POP3	192.168.0.0	Any	Any	110	

There exist a handy wizard (Create a Protocol Rule for Internet Access) for creating the basic Internet connectivity (Figure PR1)

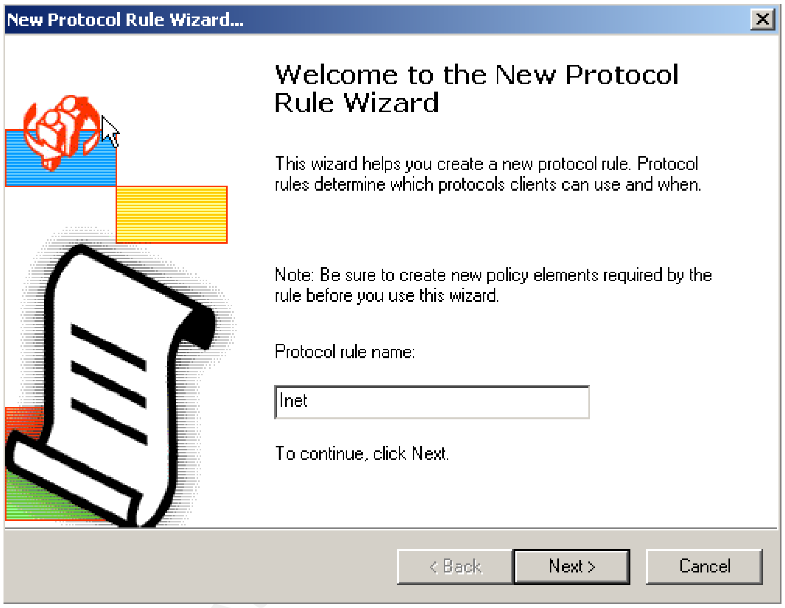


Configure Protocol Rules
for W2KISA

Protocol rules determine which protocols can be used to communicate with the Intern

Figure PR1 (The Internet Access Wizard)

As with all of Microsoft's Wizard's, the first thing that needs done, is to give the protocol rule a name (Figure PR2). In this case: "Inet"



Welcome to the New Protocol Rule Wizard

This wizard helps you create a new protocol rule. Protocol rules determine which protocols clients can use and when.

Note: Be sure to create new policy elements required by the rule before you use this wizard.

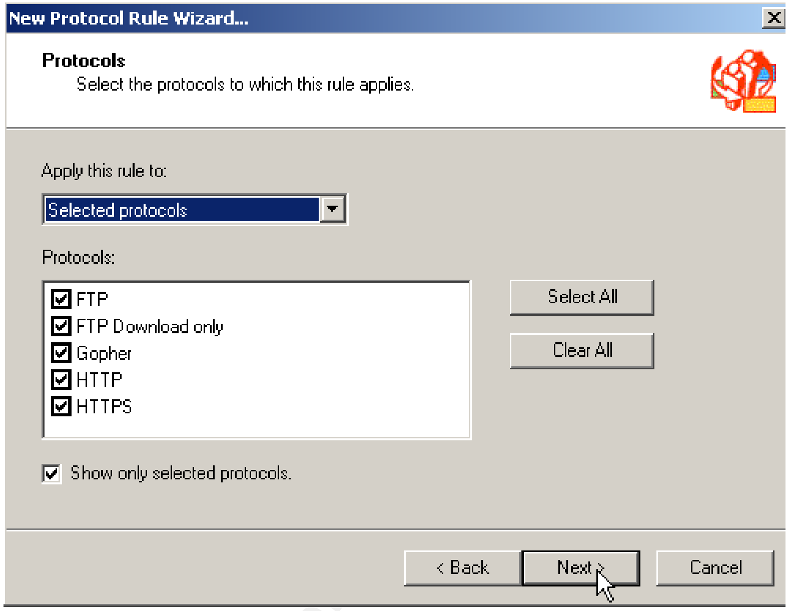
Protocol rule name: Inet

To continue, click Next.

Figure PR2 (Naming the Protocol Rule)

By default, the wizard will automatically select FTP, FTP Download, Gopher, HTTP, and HTTPS. Gopher should be deselected, as well as the "Show only selected protocols option" (Figure PR3).
Once the "Show only selected protocols" option is deselected, the wizard will a long list of available protocols (Figure PR4). The additional protocols that need selected are SMTP, POP3 and, IMAP.

This area left blank for formatting reasons



Protocols
Select the protocols to which this rule applies.

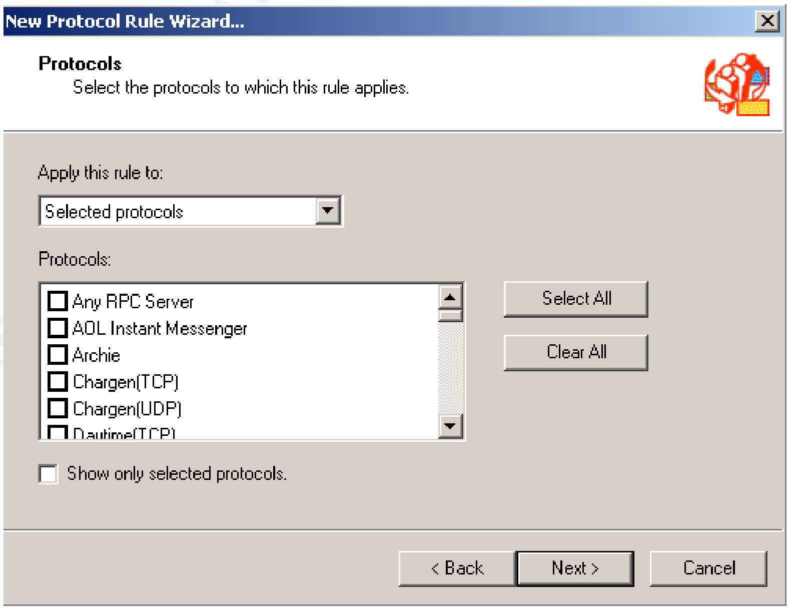
Apply this rule to: Selected protocols

Protocols:

- ☑ FTP
- ☑ FTP Download only
- ☑ Gopher
- ☑ HTTP
- ☑ HTTPS

☑ Show only selected protocols.

Figure PR3 (The default protocols)



Protocols
Select the protocols to which this rule applies.

Apply this rule to: Selected protocols

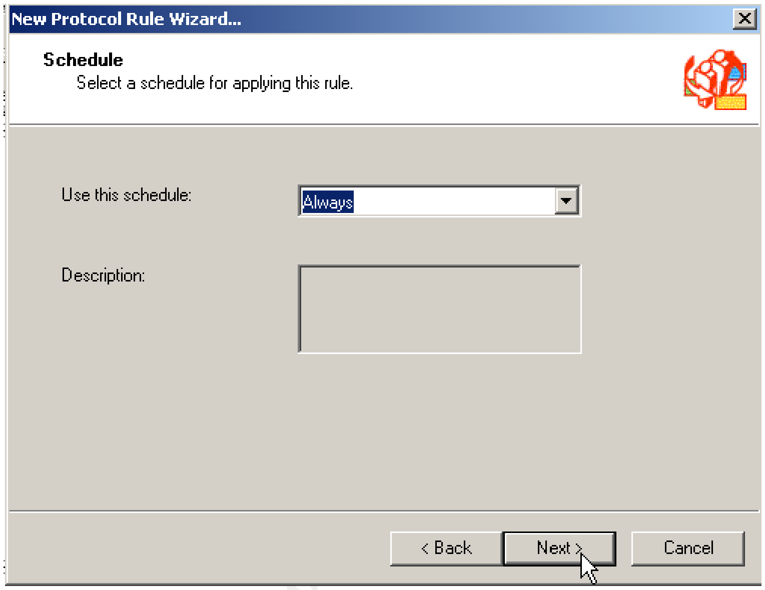
Protocols:

- ☐ Any RPC Server
- ☐ AOL Instant Messenger
- ☐ Archie
- ☐ Chargen(TCP)
- ☐ Chargen(UDP)
- ☐ Daytime(TCP)

☐ Show only selected protocols.

Figure PR4 (Adding additional protocols)

The Schedule to which this rule applies is the next option, and the default (always active) will be taken. This means that these protocols will always be available to the internal clients. (Figure PR5)



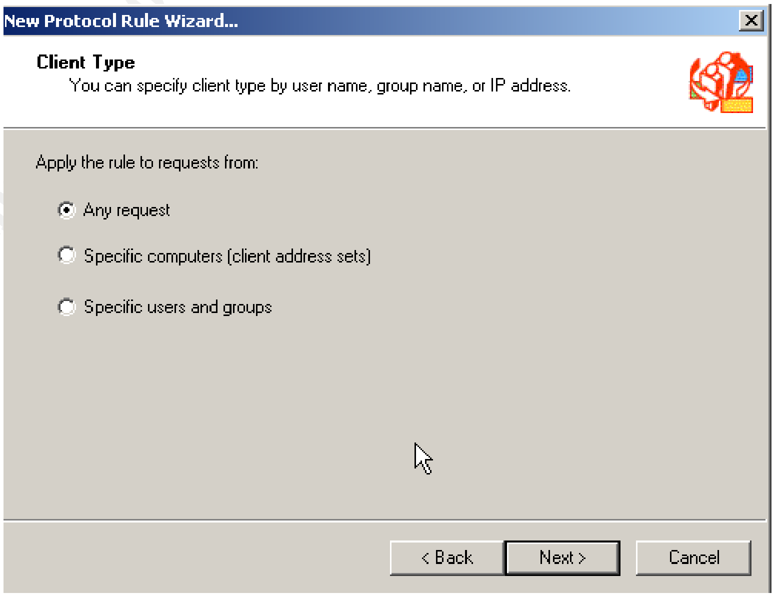
Schedule
Select a schedule for applying this rule.

Use this schedule: Always

Description:

Figure PR5 (Selecting the schedule)

The client (the computers to which this rule applies) is left at the default of “any request”. This will apply to all internal computers (192.168.0.0) (Figure PR6).



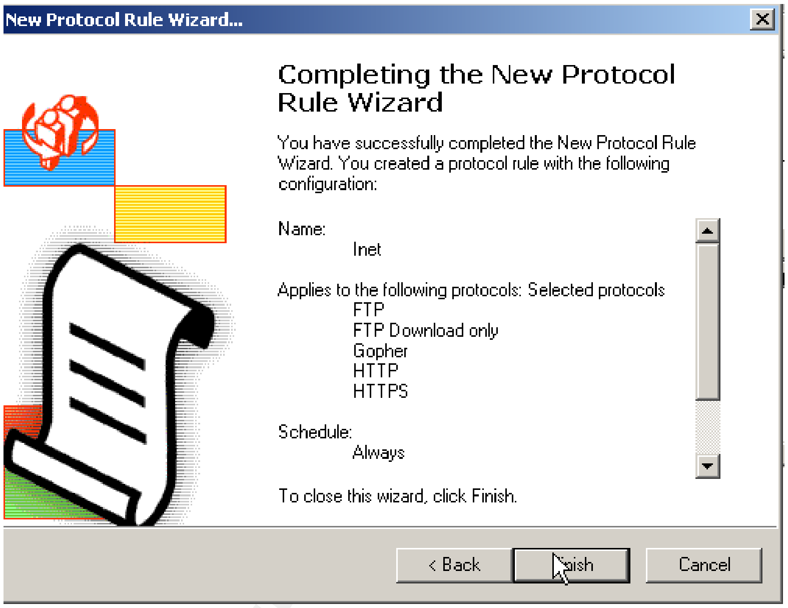
Client Type
You can specify client type by user name, group name, or IP address.

Apply the rule to requests from:

- ● Any request
- ○ Specific computers (client address sets)
- ○ Specific users and groups

Figure PR6 (Selecting the clients)

The final option is the wizard completion screen (Figure PR7).



Completing the New Protocol Rule Wizard

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

Name:
Inet

Applies to the following protocols: Selected protocols
FTP
FTP Download only
Gopher
HTTP
HTTPS

Schedule:
Always

To close this wizard, click Finish.

Figure PR7 (Completing the Wizard)

VPN

As mentioned earlier, VPN connectivity is achieved by first establishing a VPN connection to the external firewall, and then tunneling through that VPN to establish a connection to the internal firewall. PPTP is used instead of L2TP in this initial configuration to get the system up and running and supply some level of security. The L2TP configuration would require a Certificate Authority and the distribution of the certificates to the employees and partners. The use of L2TP has been placed on the list of future enhancements to the network and will be considered when more time and funding are available.

The first VPN creates a connection through the Internet to the external firewall and secures the traffic through the use of PPTP, the result of this connection is:

- A secure channel through which employees and partners can access the Terminal Server.
- A path to the internal firewall through which employees and partners can create a second PPTP session.

The second VPN is created to make use of the first VPN and is established through it to the internal firewall. The result of this VPN is that:

through it to the internal firewall. The result of this VPN is that:

- A secure channel is created all the way to the internal network by using PPTP.
- Direct access to the database from outside the network is accomplished.
- Only employees and partners with a need to access the internal resources are allowed.

The VPN Wizard supplied with ISA server simplifies the VPN setup. From the ISA Management screen, right click network configuration and then select the Allow VPN Client Connections option.

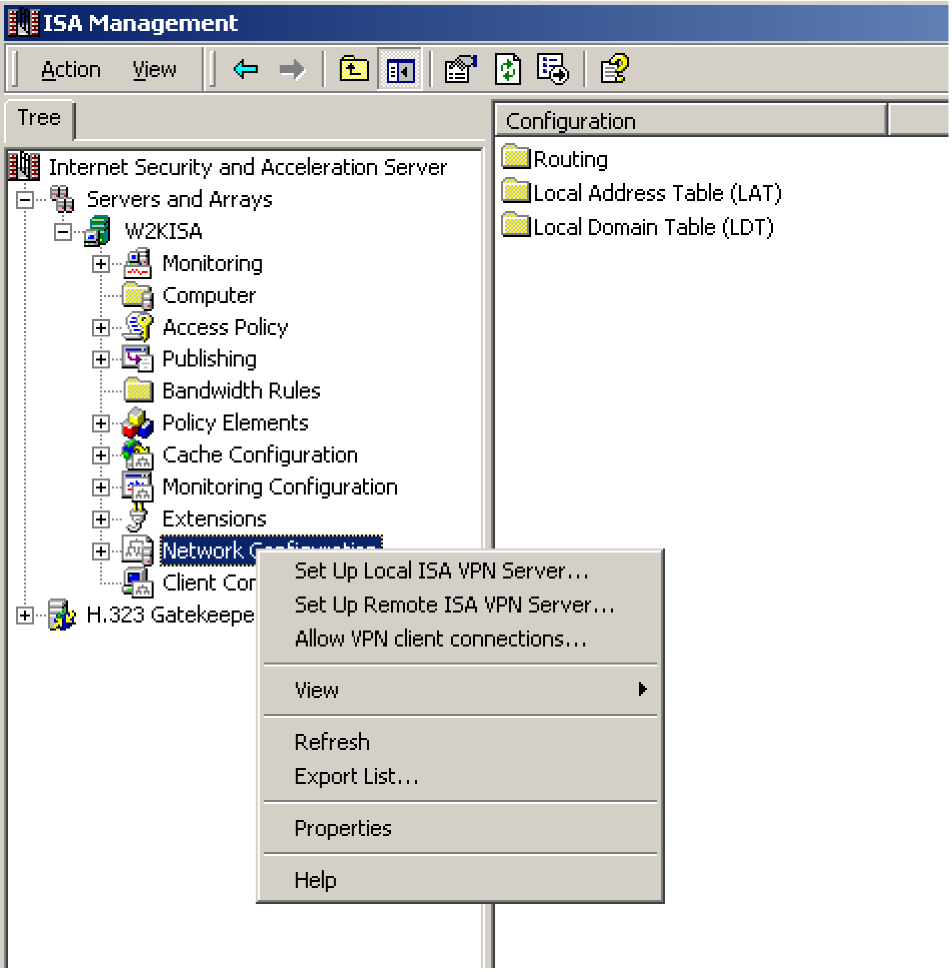
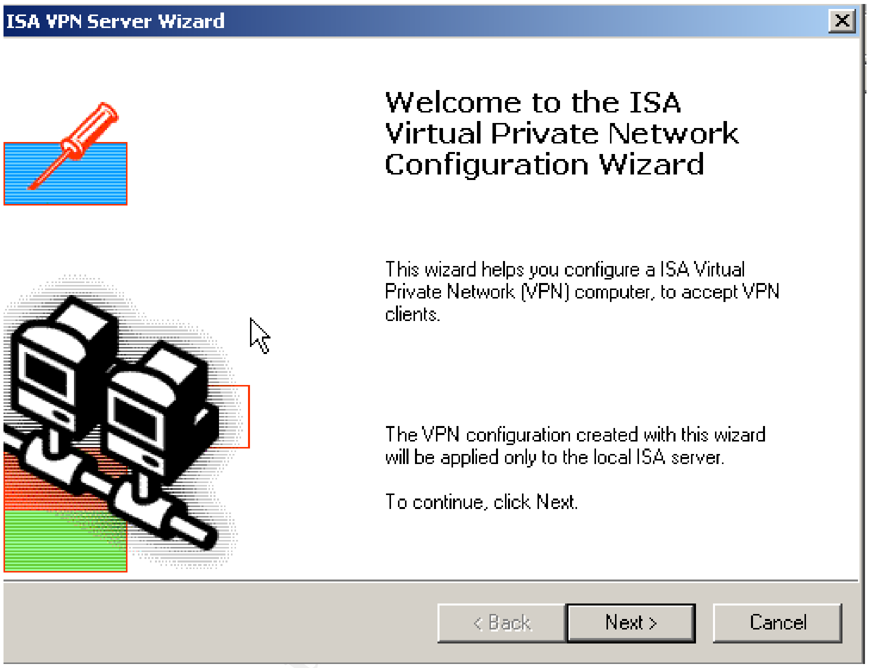


Figure VPN1

The wizard will then begin.



Welcome to the ISA Virtual Private Network Configuration Wizard

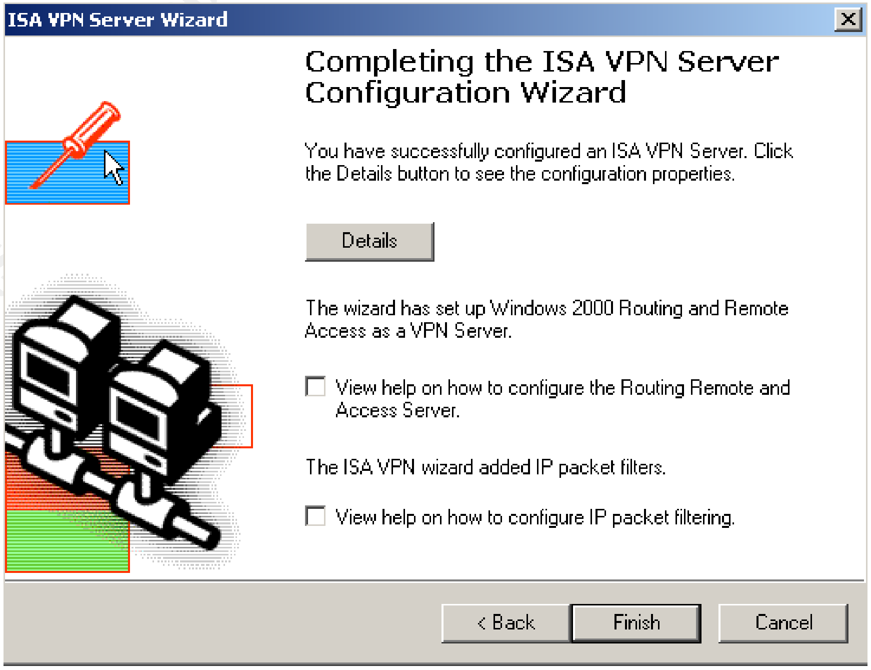
This wizard helps you configure a ISA Virtual Private Network (VPN) computer, to accept VPN clients.

The VPN configuration created with this wizard will be applied only to the local ISA server.

To continue, click Next.

Figure VPN2

Continue to click Next until the wizard is complete.



Completing the ISA VPN Server Configuration Wizard

You have successfully configured an ISA VPN Server. Click the Details button to see the configuration properties.

The wizard has set up Windows 2000 Routing and Remote Access as a VPN Server.

☐ View help on how to configure the Routing Remote and Access Server.

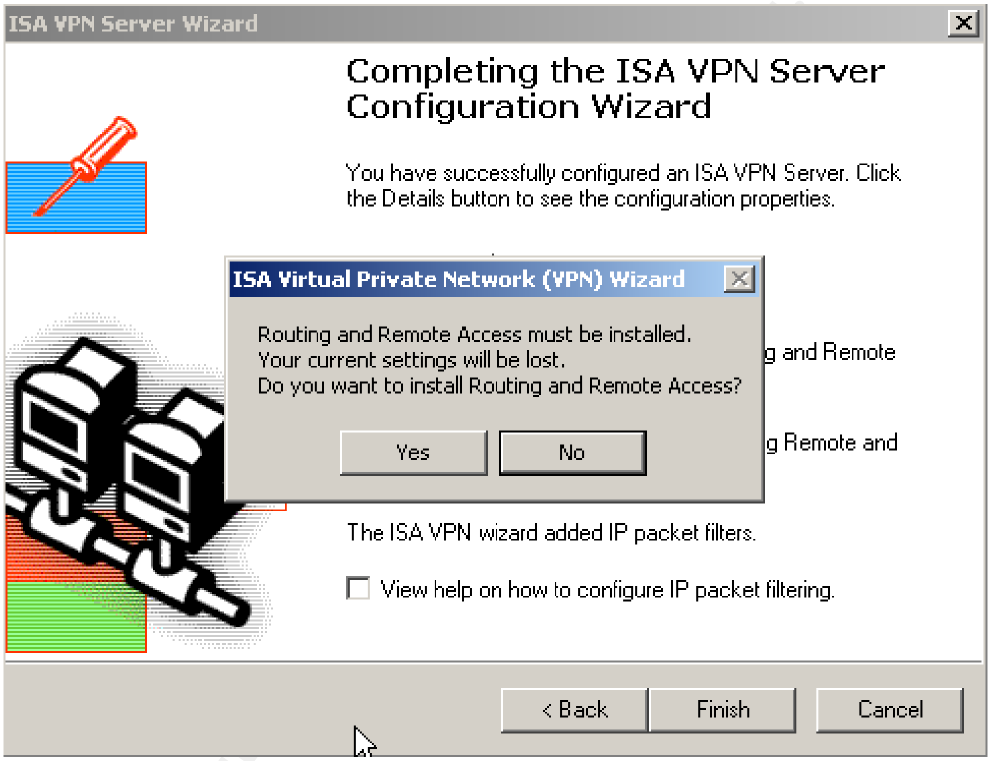
The ISA VPN wizard added IP packet filters.

☐ View help on how to configure IP packet filtering.

Figure VPN3

Assignment 2: Security Policy and Tutorial
----
(21)

At this point, Microsoft Windows 2000 Routing and Remote Access Service will be installed if it has not been done so before. Answer "yes" when asked to set up RRAS and to start/restart the service.



Completing the ISA VPN Server Configuration Wizard

You have successfully configured an ISA VPN Server. Click the Details button to see the configuration properties.

g and Remote

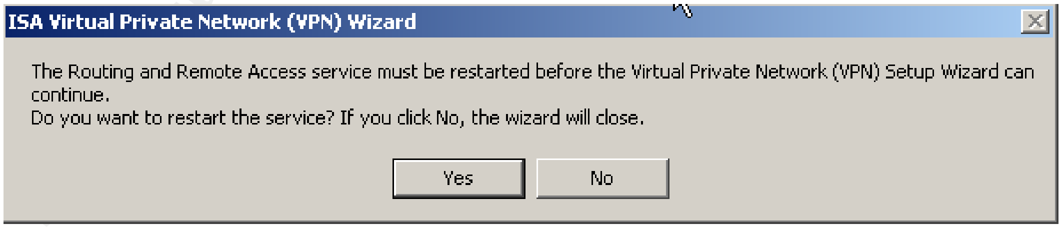
g Remote and

The ISA VPN wizard added IP packet filters.

☐ View help on how to configure IP packet filtering.

Routing and Remote Access must be installed.
Your current settings will be lost.
Do you want to install Routing and Remote Access?

Figure VPN4



The Routing and Remote Access service must be restarted before the Virtual Private Network (VPN) Setup Wizard can continue.
Do you want to restart the service? If you click No, the wizard will close.

Figure VPN5

This is all that is required to set up the VPNs.

The following are the individual configurations for each firewall.

External Firewall (for VPN):

Most of the settings have already been configured when the firewall was originally set up. The following charts show network settings.

External Interface	**Setting**	**Note**
Address	192.168.200.6	
Subnet Mask	255.255.255.252	
Default Gateway	192.168.200.5	Address of Cisco router
DNS	216.32.200.6	DNS Server of ISP
WINS	none	

Internal Interface	**Setting**	**Note**
Address	192.168.100.9	
Subnet Mask	255.255.255.248	
Default Gateway	192.168.100.10	Address of Internal Firewall
DNS	none	
WINS	none	

Internal Firewall (for VPN):

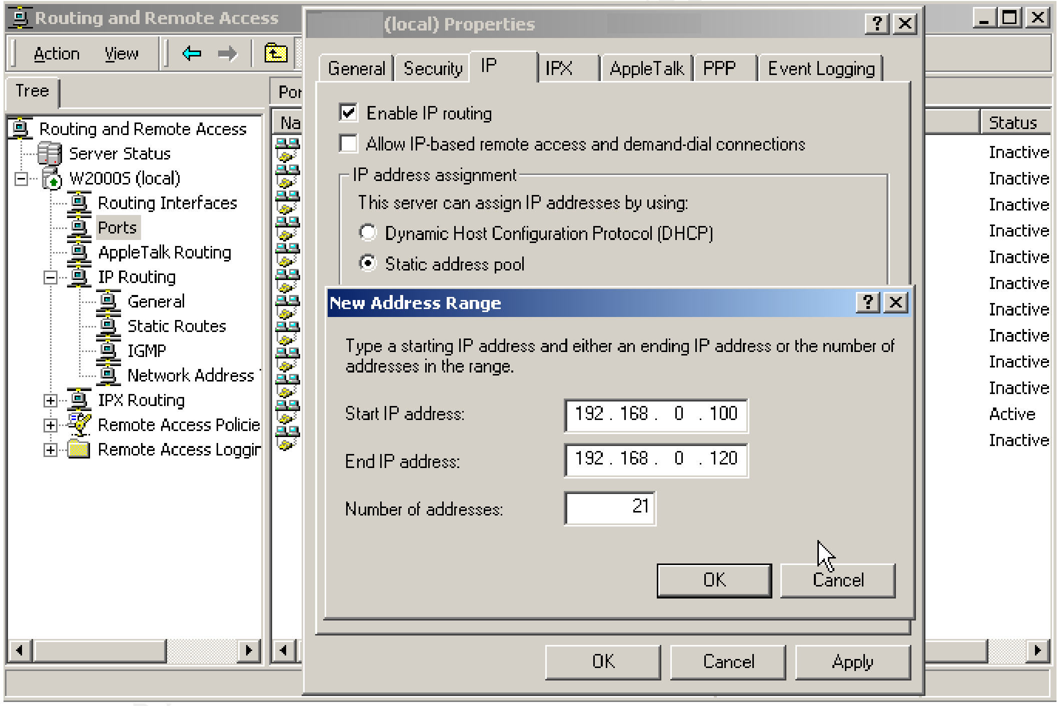
Most of the settings have already been configured when the firewall was originally set up. The following charts show network interface settings.

External Interface	**Setting**	**Note**
Address	192.168.200.6	
Subnet Mask	255.255.255.252	
Default Gateway	192.168.200.5	Address of Cisco router
DNS	216.32.200.6	DNS Server of ISP
WINS	none	

Internal Interface	**Setting**	**Note**
Address	192.168.100.9	
Subnet Mask	255.255.255.248	
Default Gateway	192.168.100.10	Address of Internal Firewall
DNS	none	
WINS	none	

The RRAS Service must now be set up for the VPN Clients:

- Under Start > Settings>Administrative Tools> Routing and Remote Access select "Properties".
- Set up a range of Static IP address to be assigned and complete the setup.



☑ Enable IP routing
☐ Allow IP-based remote access and demand-dial connections

IP address assignment
This server can assign IP addresses by using:
○ Dynamic Host Configuration Protocol (DHCP)
● Static address pool

Type a starting IP address and either an ending IP address or the number of addresses in the range.

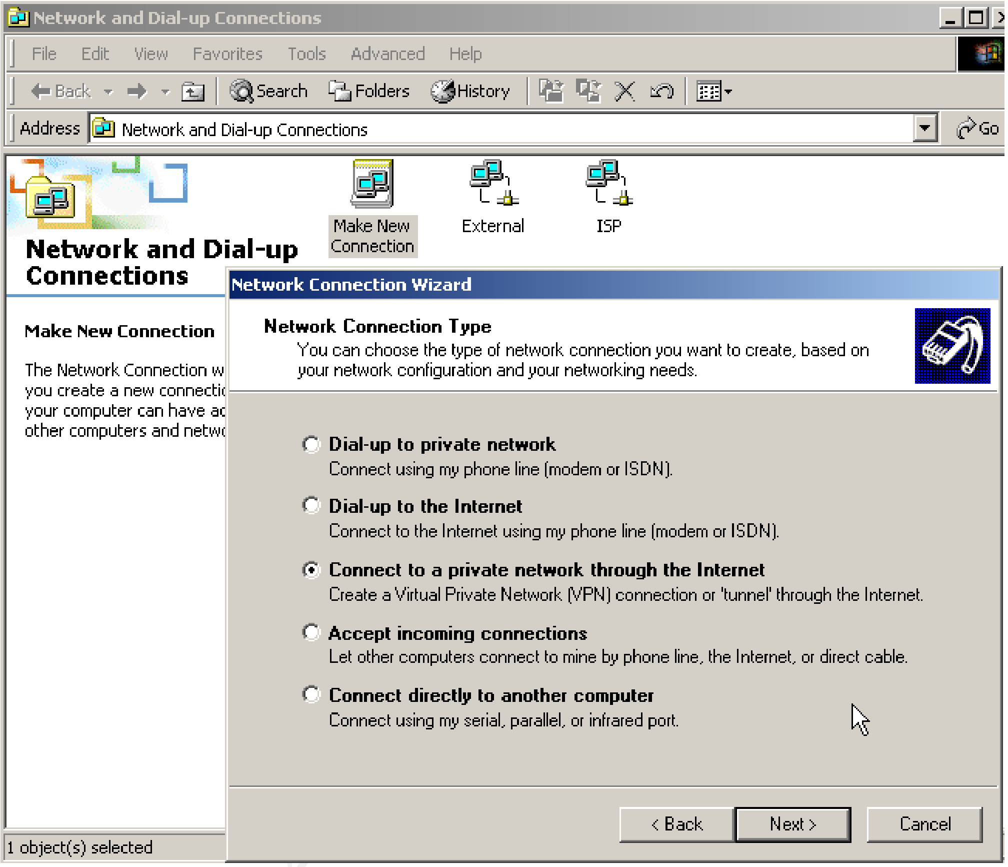
Start IP address: 192 . 168 . 0 . 100
End IP address: 192 . 168 . 0 . 120
Number of addresses: 21

Figure VPN6

- The remaining settings can be left at their default

The VPN clients are best set up using Windows 2000 and the VPN connectivity option located in the Network Connection Wizard. This is the configuration for the VPN connection to the DMZ:

- Select "Connect to a private network through the Internet" <NEXT>


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
External
ISP
Network and Dial-up Connections
Network Connection Wizard
< Back
Next >
Cancel
1 object(s) selected

Make New Connection

The Network Connection w
you create a new connectic
your computer can have ac
other computers and netwc

Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

● **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

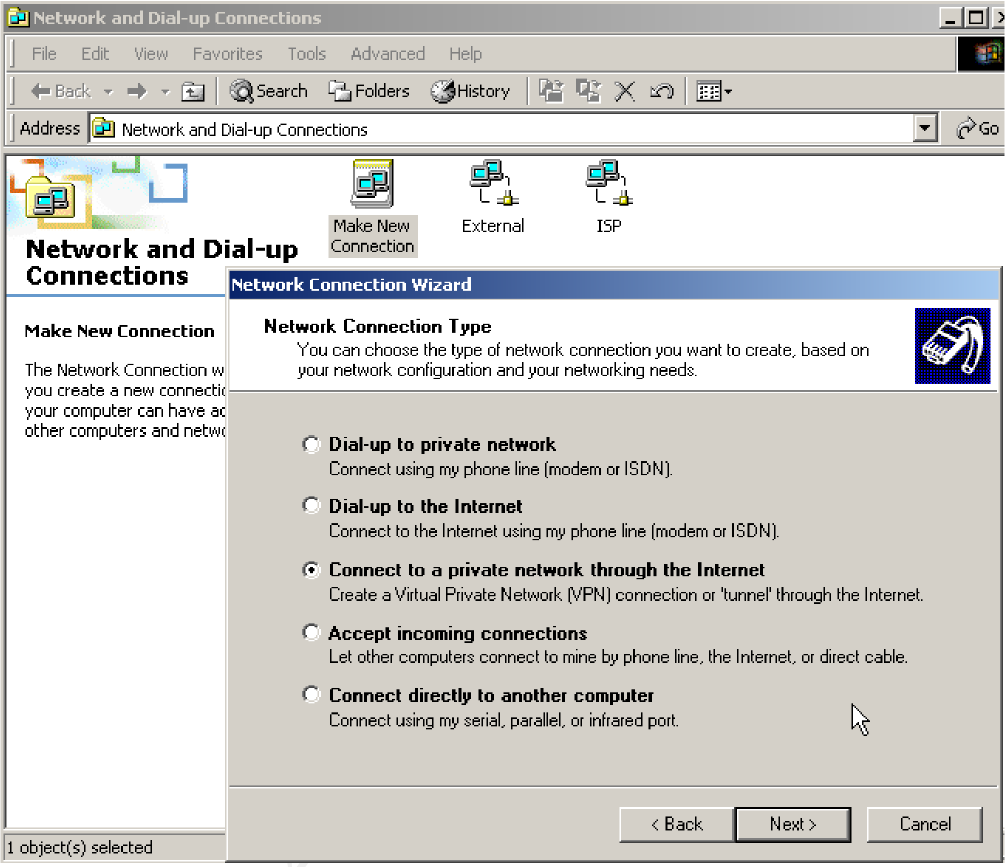
Figure VPN7

Note: The remaining options will not have screen shots due to their self-explanatory nature.

- Choose the connection to be used <NEXT>
- Enter the IP address or Hostname for the other side of the connection <NEXT> (This will be the External Firewall)
- Select the connection to be "Only for myself" <NEXT>
- Name the connection (GIAC DMZ) <FINISH>

The VPN into the Internal Network requires the use of the VPN connection created above. All other configuration options are done in the same manner. This is the configuration information for the VPN into the Internal Network:

- The first step is the same. Again go to the Network Connection Wizard and select "Make New Connection". Select "Connect to a private network through the Internet"


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
External
ISP
1 object(s) selected
< Back
Next >
Cancel

Network and Dial-up Connections

Make New Connection

The Network Connection w
you create a new connectio
your computer can have ac
other computers and netwo

Network Connection Wizard

Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

● **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

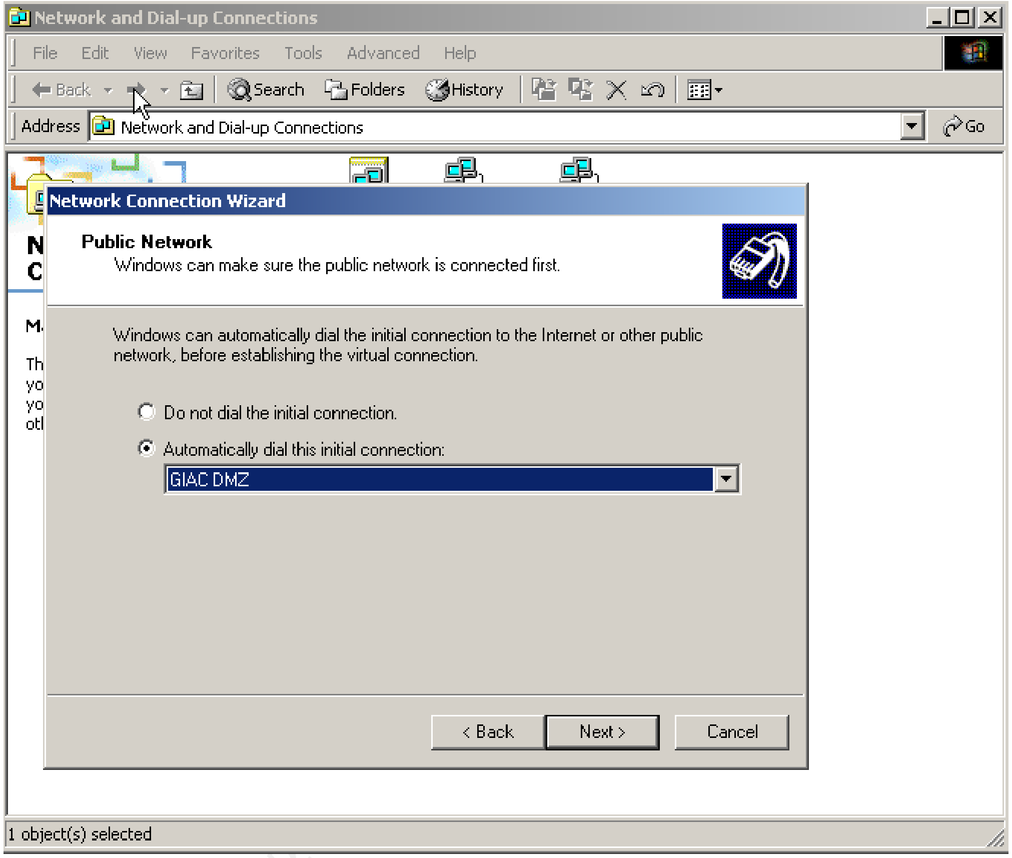
○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

Figure VPN8

- The next step is different. Select the previously created VPN connection as the network connection to be used.

Assignment 2: Security Policy and Tutorial
----
(26)


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Network Connection Wizard
< Back
Next >
Cancel
1 object(s) selected

Public Network
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

○ Do not dial the initial connection.
● Automatically dial this initial connection:
GIAC DMZ

Figure VPN9

The remaining steps are similar to those for the first VPN connection:

- Enter the IP address for the other side of the connection <NEXT> (This will be the Internal Firewall’s external IP address: 192.168.100.10)
- Select the connection to be “Only for myself” <NEXT>
- Name the connection (GIAC INT) <FINISH>

This completes the configuration of the VPN connectivity into GIAC. The employees and partners should be informed to protect their passwords and to only use this method of connectivity when absolutely necessary. The use of PPTP should be replaced with L2TP when feasibly possible.
The tutorial by Thomas Shinder located on the ISAServer.org website is a more detailed description of this procedure..

http://www.isaserver.org/pages/article.asp?id=212

Assignment 2: Security Policy and Tutorial
----
(27)

Tutorial

This explains the configuration of the Border Router. As mentioned earlier, the router is configured for: eliminating Internet "noise", allowing only internal networks to communicate out, and protecting the router itself from compromise.

We will assume the router has already been initialized and basic information such as hostname, IP addresses, password, and interfaces may have been previously configured. This tutorial will deal with resetting these options, the access control lists, telnet access, additional security concerns, and some hints/tips.

1) Connect to the router and log in

a. Connectivity to the router can be through a telnet session, or through the console port by using a terminal program. This demonstration will be through the HyperTerminal program that comes with Microsoft Windows 2000. HyperTerminal can be accessed through the start button in the lower left corner of the screen. (Figure T1)

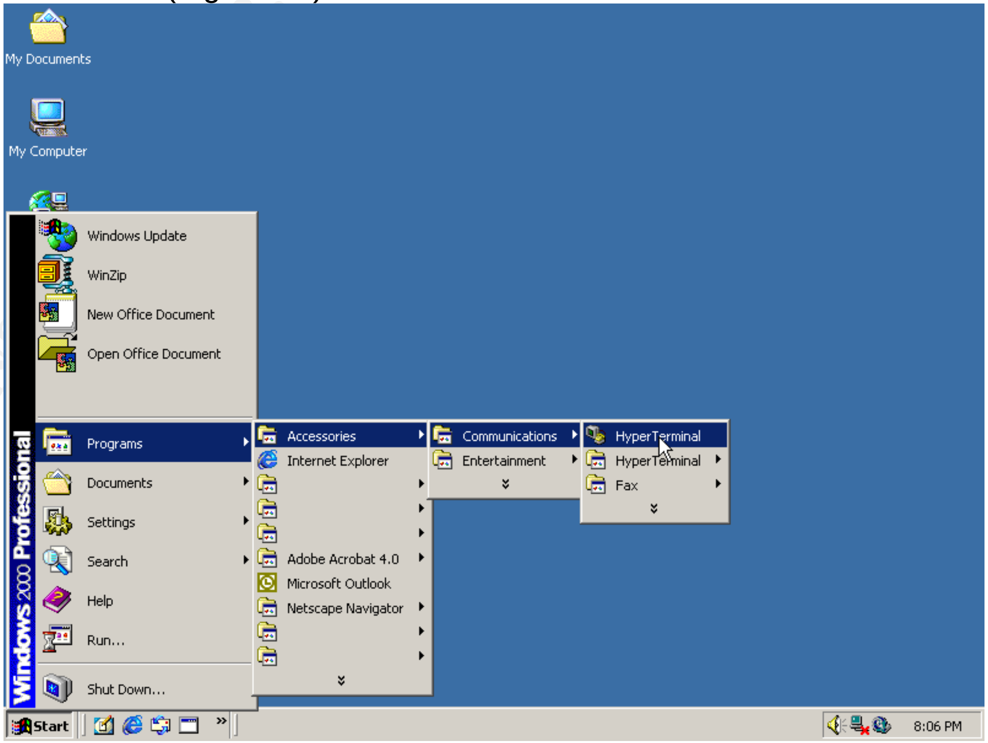
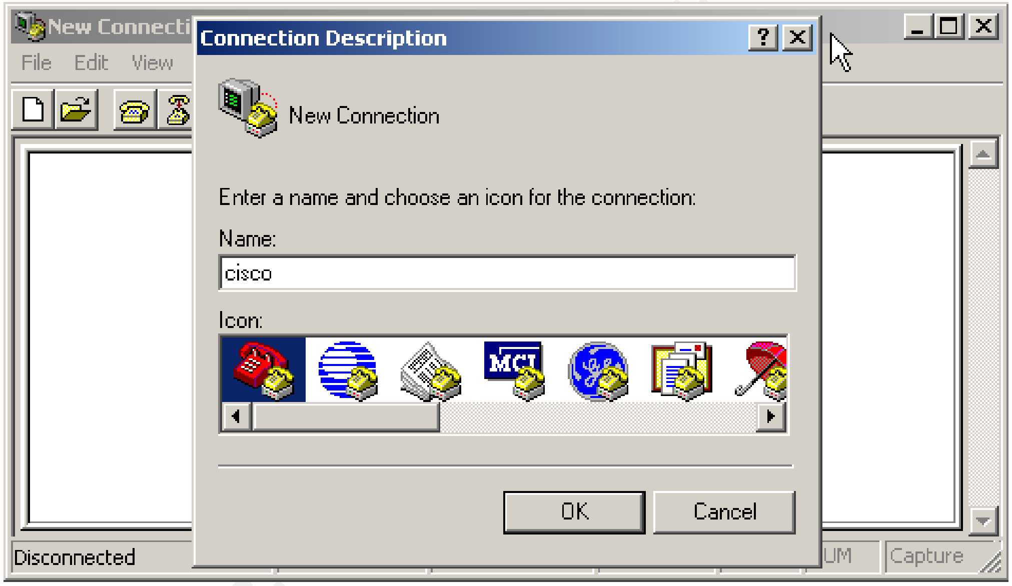


Figure T1 (Accessing HyperTerminal)

b. After starting the HyperTerminal program, you will be presented with the option to create a new connection. Name this connection “cisco” and select “OK”. (Figure T2)



New Connection

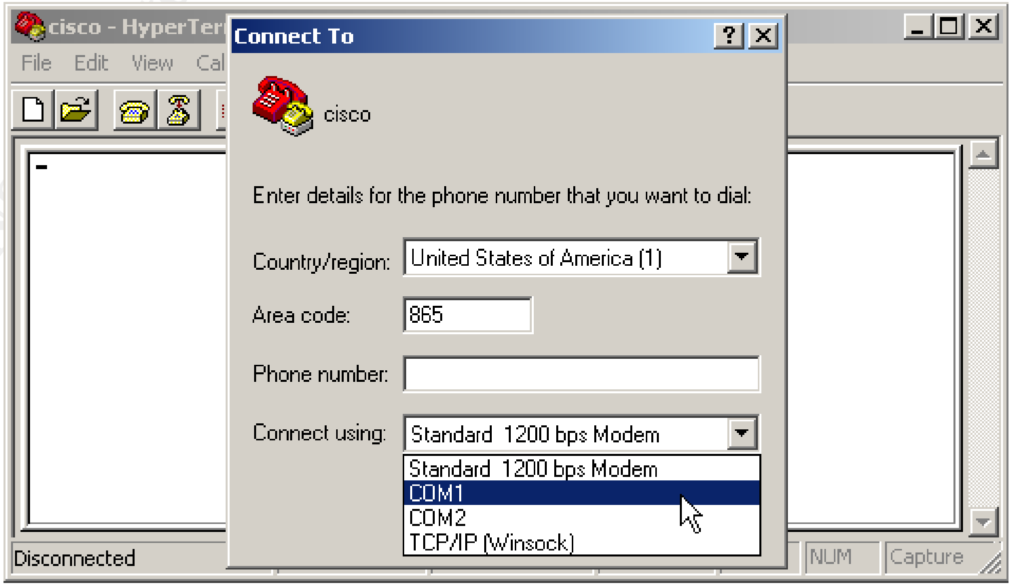
Enter a name and choose an icon for the connection:

Name: cisco

Icon:

Figure T2 (Creating a new connection)

c. Select the communications/COM port you wish to use. (Figure T3)



cisco

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

Area code: 865

Phone number:

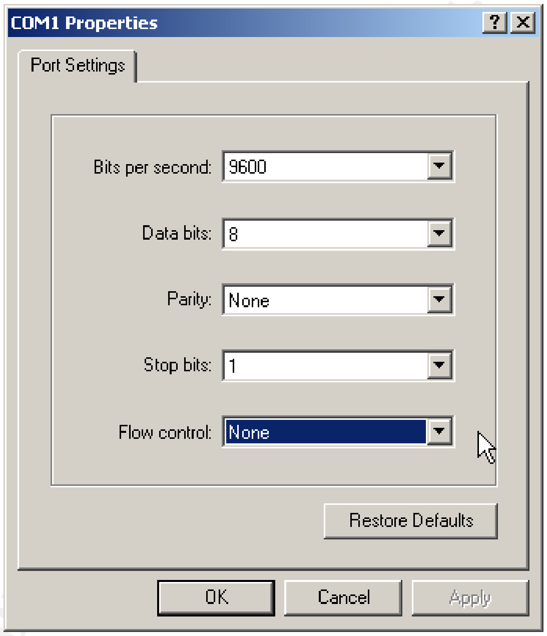
Connect using: Standard 1200 bps Modem

Standard 1200 bps Modem
COM1
COM2
TCP/IP (Winsock)

Figure T3 (selecting a COM Port)

Assignment 2: Security Policy and Tutorial
----
(29)

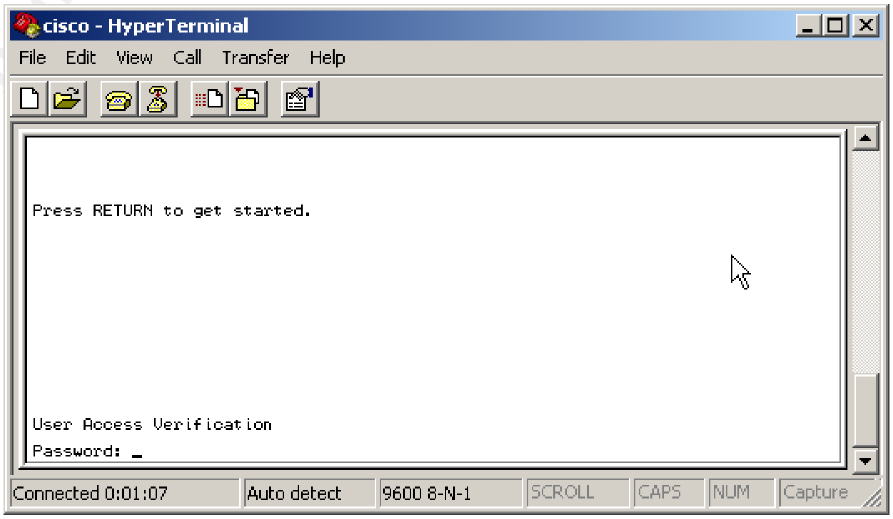
d. Upon selecting a COM port, you will be prompted to set the communication parameters. (Figure T4) These are set to: 9600 bps, 8 data bits, no parity (or None), 1 stop bit, and no flow control.



Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Figure T4 (Communications settings)

e. After “OK” selected, the Hyper Terminal Window will be opened and will be ready for use. Press <ENTER> to begin (Figure T5)



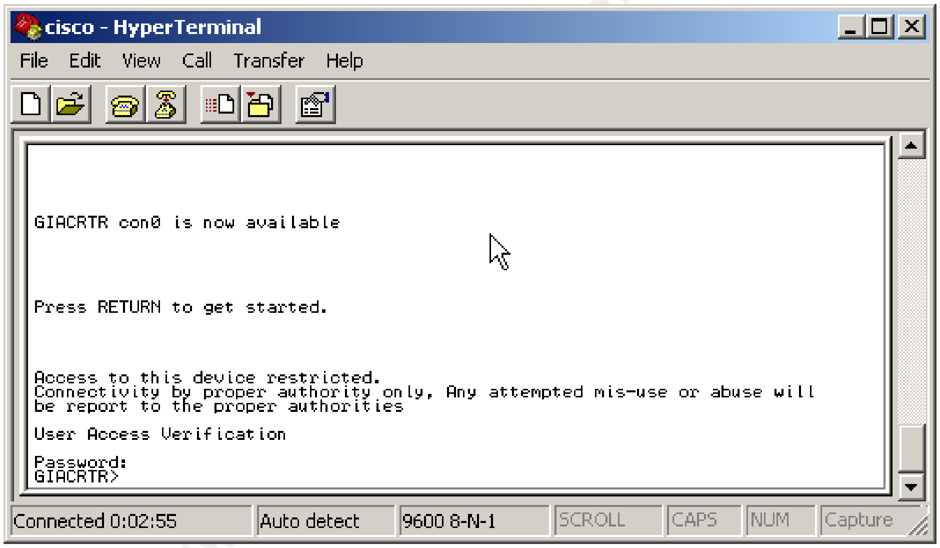
```
Press RETURN to get started.





User Access Verification
Password: _
```

Connected 0:01:07 | Auto detect | 9600 8-N-1 | SCROLL | CAPS | NUM | Capture

Figure T5 (HyperTerminal ready for use)

Assignment 2: Security Policy and Tutorial
----
(30)

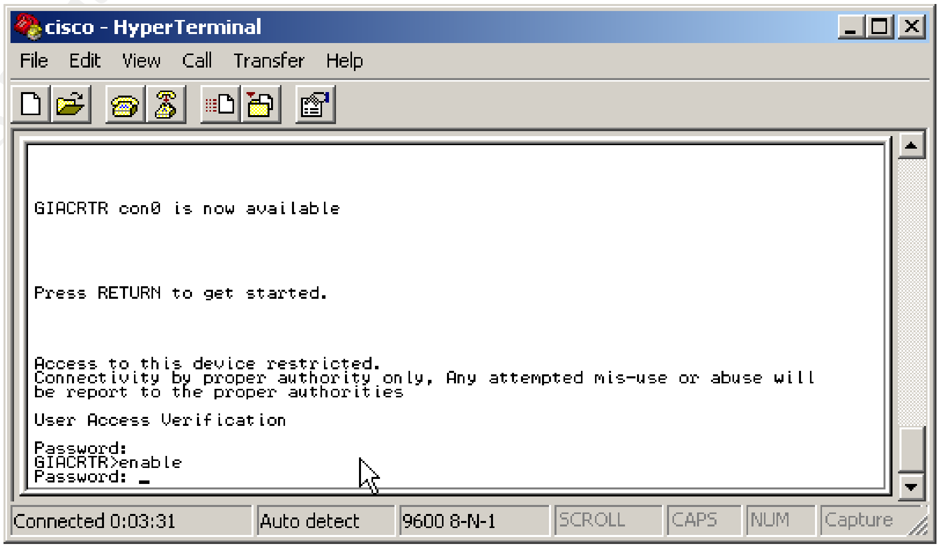
f. Type in the password (if needed) to enter *User EXEC* mode of the router. (Figure T6) This mode has us logged onto the router, but to make changes to the configuration, we must gain administrative access. <hint> Notice that the prompt for this mode is the ">" character. < end hint>



```
GIACRTR con0 is now available



Press RETURN to get started.



Access to this device restricted.
Connectivity by proper authority only. Any attempted mis-use or abuse will
be report to the proper authorities

User Access Verification

Password:
GIACRTR>
```

Figure T6 (Logging into User EXEC mode)

g. Type in **enable** and press <ENTER>. You will be prompted for a password. (Figure T7)



```
GIACRTR con0 is now available



Press RETURN to get started.



Access to this device restricted.
Connectivity by proper authority only. Any attempted mis-use or abuse will
be report to the proper authorities

User Access Verification

Password:
GIACRTR>enable
Password: _
```

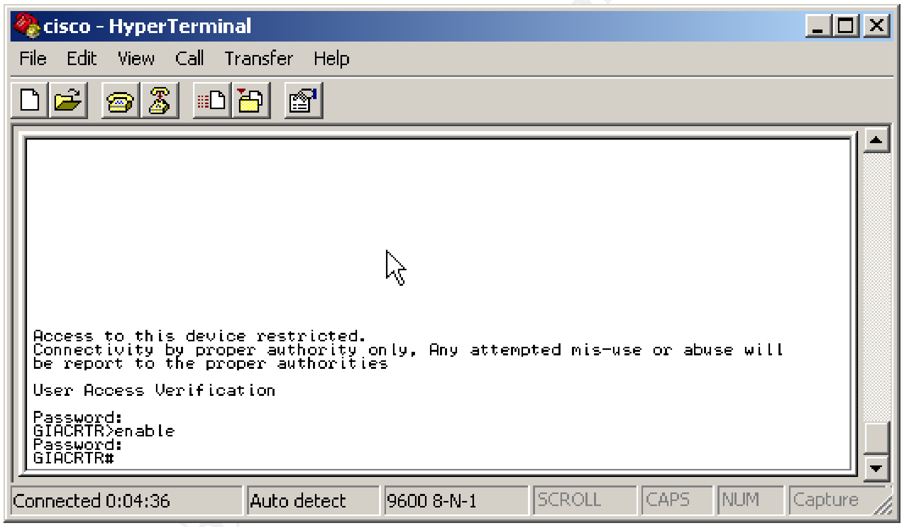
Figure T7 (Entering the Enable Password)

Assignment 2: Security Policy and Tutorial

----

(31)

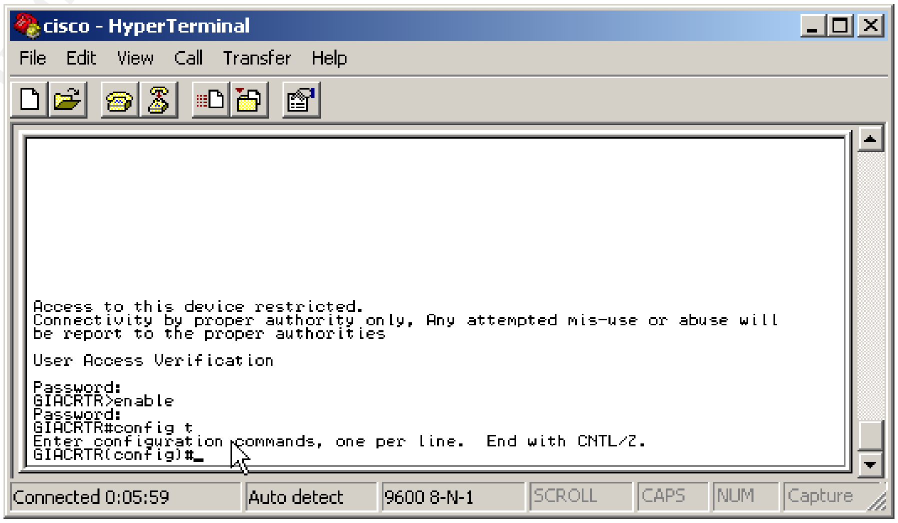
h. Enter the password and press <ENTER>. This will allow access to the *Privileged EXEC* mode of the router. In other words, *the ability make changes to the router configuration.* From here we will begin the configuration process. (Figure T8) <hint> Notice the prompt has change to the "#" character. <end hint>



```
Access to this device restricted.
Connectivity by proper authority only, Any attempted mis-use or abuse will
be report to the proper authorities

User Access Verification

Password:
GIACRTR>enable
Password:
GIACRTR#
```

Figure T8 (Privileged EXEC mode access)

i. Type in **config t** and press <ENTER>. This places the router in *Global Configuration* mode. (Figure T9) <hint> Note that the prompt is now: *GIACRTR(config)#* <end hint>



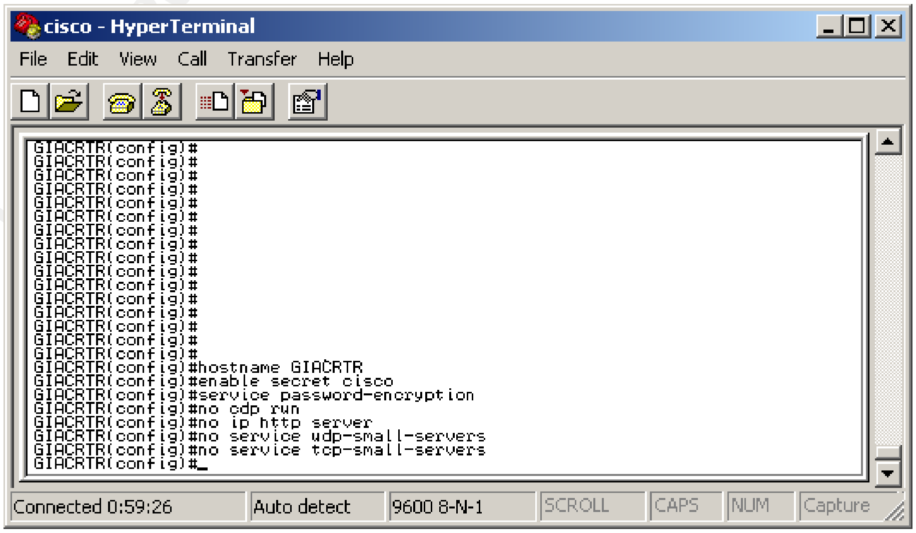
```
Access to this device restricted.
Connectivity by proper authority only, Any attempted mis-use or abuse will
be report to the proper authorities

User Access Verification

Password:
GIACRTR>enable
Password:
GIACRTR#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIACRTR(config)#_
```

Figure T9 (Global configuration mode)

Assignment 2: Security Policy and Tutorial
----
(32)

2) Configure the settings that affect the entire router

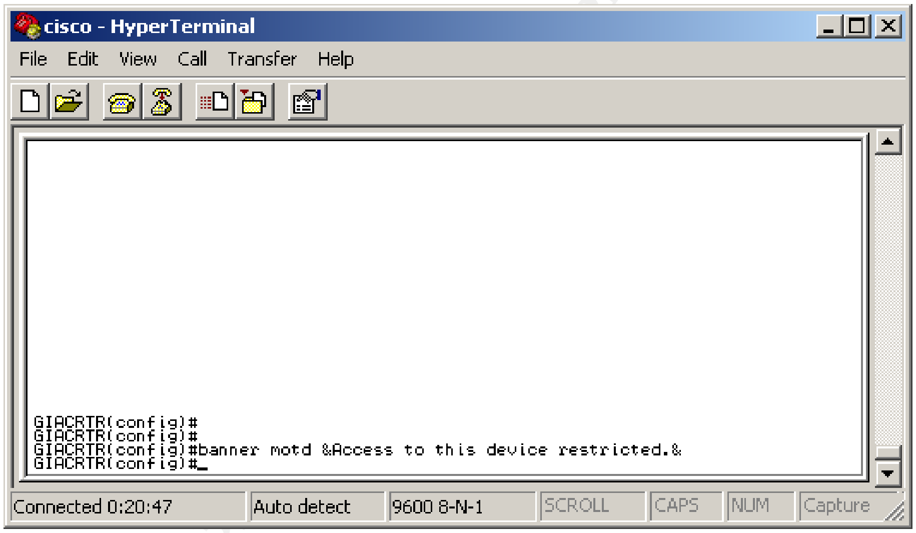
a. Type in **hostname GIACRTR** and press <ENTER>. This will set the host name of the router. (Figure T10)
b. To set the password for the *Privileged Exec* mode the following method is used. **enable secret cisco** <ENTER>, will set the password to "cisco" and the password will be encrypted. Use a password that follows the rules for your organization. (Figure T10)
c. Type in **service password-encryption** <ENTER> so that other passwords used on the router will be encrypted. Note: This encryption is not as complex as that used for the enable secret password shown above. (Figure T10)
d. Type in **no cdp run** <ENTER> to disable the use of the Cisco Discovery Protocol (CDP) on the router. CDP is used to send information such as the router's model number, features, and addresses to neighboring Cisco devices. It should be turned off to keep this information more secure. (Figure T10)
e. Unneeded services such as the web server interface (http), udp-small-servers, and tcp-small-servers (echo, chargen, discard, and daytime), can be turned off since they are not needed and this will reduce the vulnerability of the router.



```
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#hostname GIACRTR
GIACRTR(config)#enable secret cisco
GIACRTR(config)#service password-encryption
GIACRTR(config)#no cdp run
GIACRTR(config)#no ip http server
GIACRTR(config)#no service udp-small-servers
GIACRTR(config)#no service tcp-small-servers
GIACRTR(config)#_
```

Figure T10

f. Set up a warning message that will be displayed whenever any attempts to log into the router. The following will input a *Message of The Day (MOTD)* banner. The use of the "&" character is to *of The Day (MOTD)* banner. The use of the "&" character is to signify the beginning and end of the banner message. Use the appropriate message for your company. **banner motd &Access to this device is restricted. Authorized connections only, Any attempted mis-use or abuse will be reported to the proper authorities&** (Figure T11)



```
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#banner motd &Access to this device restricted.&
GIACRTR(config)#_
```

Figure T11 (Message of the day banner)

3) **Create the Access List that will be used to control traffic entering the network from the Internet. (ingress filter)**

a. From the *global configuration* prompt GIACRTR(config)#,begin entering in the networks or hosts that are allowed or denied access to the network. The format for a standard access list is as follows:

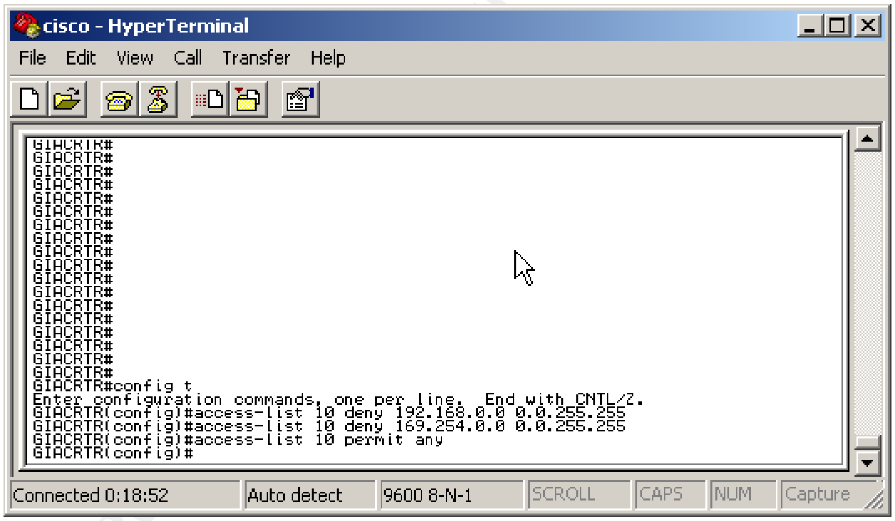
access-list {access list number 1-99}{permit or deny}{ip address}{wildcard mask}

An example would be:

access-list 10 deny 192.168.0.0 0.0.255.255
access-list 10 deny 169.254.0.0 0.0.255.255
access-list 10 permit any

This adds two lines to access list 10 that denies access to anyone on the network starting with 192.168, and anyone on the network starting with 169.254.

The permit line allows everyone else to connect. <hint> Access lists have a built-in "deny all" that is applied after all the other lines are entered. If you forget to put in a "permit" line, then no one will are entered. If you forget to put in a “permit” line, then no one will have access. <end hint> <hint> Standard access lists do not allow editing or rearranging of the lines that are entered. To make configuration easier, use a text editor to create a file with all of the entries, and then upload the file from within the terminal program, or cut and paste from within telnet.<end hint> See the policy for the border router for more examples of entries that can be used in the access list (ingress filter). (Figure T12)



```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIACRTR(config)#access-list 10 deny 192.168.0.0 0.0.255.255
GIACRTR(config)#access-list 10 deny 169.254.0.0 0.0.255.255
GIACRTR(config)#access-list 10 permit any
GIACRTR(config)#
```

Figure T12 (Creating access list 10)

4) **Create the access list to control traffic leaving the network. (egress filter)**

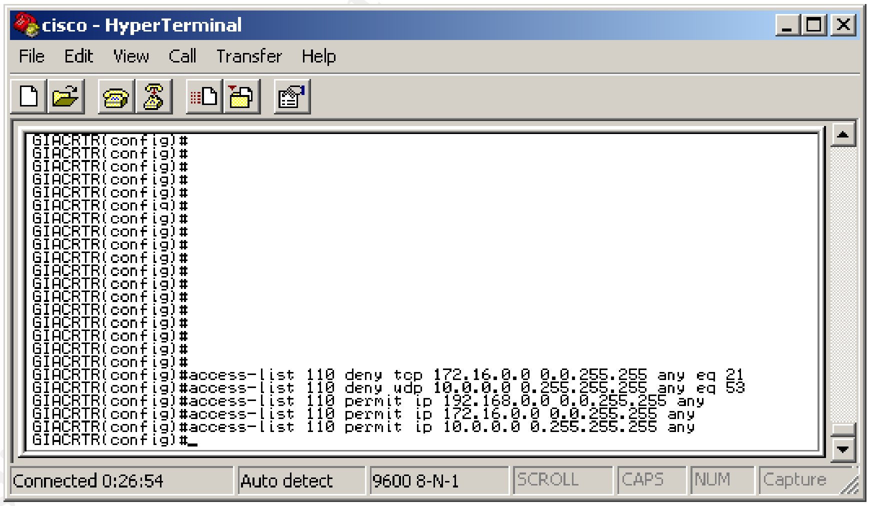
a. From the *global configuration* prompt GIACRTR(config)#,begin entering in the networks or hosts that are allowed or denied access to the network. The format for an extended access list is as follows:

access-list {access list number 100-199}{permit or deny}{protocol}{source ip address}{source wildcard mask} {operator and source port} {destination ip address}{destination wildcard mask}{operator and destination port}

An example would be:

```
access-list 110 deny tcp 172.16.0.0 0.0.255.255 any eq 21
access-list 110 deny udp 10.0.0.0 0.255.255.255 any eq 53
access-list 110 permit ip 192.168.0.0 0.0.255.255 any
access-list 110 permit ip 172.16.0.0 0.0.255.255 any
access-list 110 permit ip 10.0.0.0 0.255.255.255 any
```

Line one of this access list blocks tcp traffic to port 21 (ftp) on all external hosts if the internal host is anywhere on the 172.16 network. The second line blocks port 53 UDP (DNS) access by hosts on the 10.0.0.0 network. The last line allows all hosts on the 192.168 network to access the Internet. The remaining two lines permit any additional traffic for the 172.16 and 10.0.0.0 networks that is not blocked by the first two lines. All other hosts are blocked. (Figure T13) <hint> Remember that there is an explicit deny at the end of the access list and only the hosts we allow with the “permit” statement will be allowed through.<end hint> See the policy for the border router for more examples of entries that can be used in the access list (egress filter).



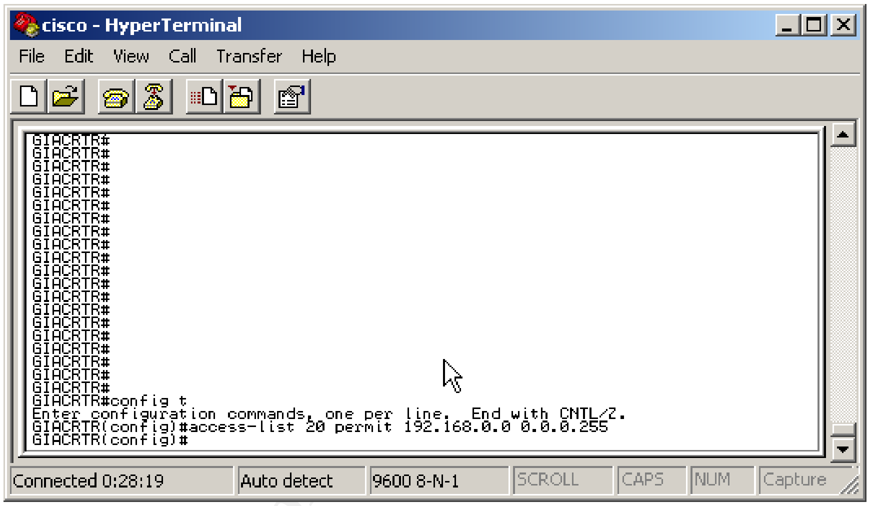
```
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#access-list 110 deny tcp 172.16.0.0 0.0.255.255 any eq 21
GIACRTR(config)#access-list 110 deny udp 10.0.0.0 0.255.255.255 any eq 53
GIACRTR(config)#access-list 110 permit ip 192.168.0.0 0.0.255.255 any
GIACRTR(config)#access-list 110 permit ip 172.16.0.0 0.0.255.255 any
GIACRTR(config)#access-list 110 permit ip 10.0.0.0 0.255.255.255 any
GIACRTR(config)#_
```

Figure T13 (Creating extended access list 110)

5) **Create an access list to control access to the vty (telnet) ports**

a. From the *global configuration* prompt GIACRTR(config)#,begin entering in the networks or hosts that are allowed access to the router. The format for these access lists can follow that of the standard access list:
access-list {access list number 1-99}{permit}{ip address}{wildcard mask}
An example would be:
access-list 20 permit 192.168.0.0 0.0.0.255
This list will allow all hosts on the 192.168.0 network to access the router. Note: they would still need to know the vty password to log in. There is also not a “deny” line in the above access list. It is relying on the built-in or “implicit deny” that is at the end of all

relying on the built-in or “implicit deny” that is at the end of all access lists. (Figure T14)



```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIACRTR(config)#access-list 20 permit 192.168.0.0 0.0.0.255
GIACRTR(config)#
```

Connected 0:28:19 | Auto detect | 9600 8-N-1

Figure T14 (Creating access list 20)

6) Configure the Ethernet Interface

a. From the *global configuration* mode prompt: GIACRTR(config)#, type in **interface fa0/0** <ENTER>. The prompt will change to: GIACRTR(config-if)#. This is the interface level prompt for the FastEthernet interface on the 2600. <hint> One thing to note is that the prompt does not indicate which interface you are on. You will need to look at the previous line you typed in, or scroll back through the session history to see what was typed. To scroll through the history file, of which there are 10 lines by default, press CTRL P to see previous commands, and CTRL N to see the next command typed. <end hint> (Figure T15)

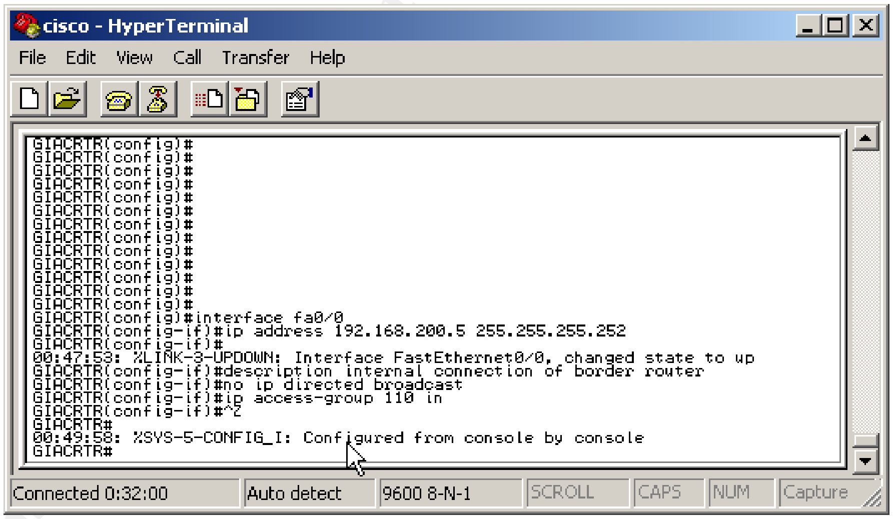
b. To set the IP address of the interface, the address is entered in dotted-decimal format, along with the netmask. For example: **ip address 192.168.100.5 255.255.255.252** <ENTER> (Fig. T15)

c. The description for this interface can now be entered. <hint> Entering a description is useful to remind you of where an interface connects to, or in the case of a serial port it can be used to enter the circuit number assigned to that connection by a WAN service provider. <end hint> The following is a description example: **description internal connection of border router. using classful notation and the 2nd available subnet in 192.168.200.4-7 range** <ENTER> (Figure T15)

d. At this point we need to make sure we block any broadcasts that try to pass through the router and off of our network. The **no ip directed-broadcast** <ENTER> command will do this. (Figure T15)

e. The egress filter created above can now be applied to the interface. **ip access-group 110 in** <ENTER>. This applies the filter to all traffic coming into the FastEthernet interface. <Hint> The advantage to applying this as an incoming filter is that blocking the traffic before it enters the router saves the router from having to process the packets against the routing table to see where they go. So, less processing, equals a more efficient router.

f. This completes the setup of the Fast Ethernet interface and **CTRL Z** can be press to return to the *Privileged EXEC* prompt.



```
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#interface fa0/0
GIACRTR(config-if)#ip address 192.168.200.5 255.255.255.252
GIACRTR(config-if)#
00:47:53: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
GIACRTR(config-if)#description internal connection of border router
GIACRTR(config-if)#no ip directed broadcast
GIACRTR(config-if)#ip access-group 110 in
GIACRTR(config-if)#^Z
GIACRTR#
00:49:58: %SYS-5-CONFIG_I: Configured from console by console
GIACRTR#
```

Figure T15 (Configuring FastEthernet 0/0)

7) Configuration of the DSL port

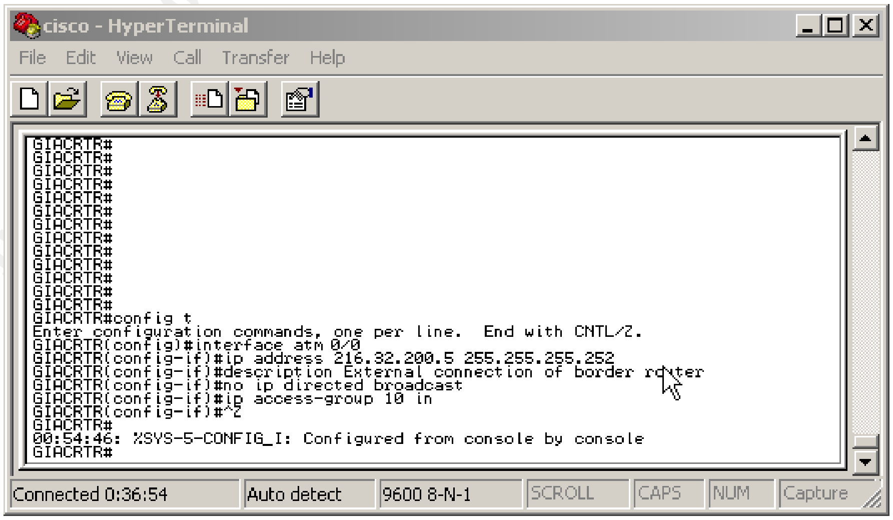
a. From the *global configuration* mode prompt: GIACRTR(config)#, type in **interface dsl0/0** <ENTER>. The prompt will change to: GIACRTR(config-if)#. This is the interface level prompt for the DSL interface on the 2600. <hint> Again, use the session history if you forget which interface you are on. <end hint> Note: The DSL port is not a built in port on the 2600 and must be bought as an add-in module. (Figure T16)

b. To set the IP address of the interface, the address is entered in dotted-decimal format, along with the netmask. The following is an example: **ip address 216.32.200.5 255.255.255.252**

Assignment 2: Security Policy and Tutorial
----
(38)

<ENTER>. Note: This ip address and netmask will be supplied by the internet service provider. (Figure T16)

c. The description for this interface can now be entered. <hint> As mentioned above, useful information, or something that may be otherwise forgotten about the interface can be entered here. <end hint> The following is a description example: **description External connection of the border router. The IP address and netmask were supplied by the isp. This is a synchronous DSL connection.** <ENTER> (Figure T16)
d. At this point we need to make sure that we block any broadcasts that try to enter our network from the Internet. Again, we use the **no ip directed-broadcast** <ENTER> command. (Figure T16)
e. The ingress filter created above can now be applied to the interface. **ip access-group 10 in** <ENTER>. This applies the filter to all traffic coming into the DSL interface. <hint> This filter is used to block "noise" or what can be considered "unwanted traffic from the internet". By doing this at the border router we are taking some of the load off of the firewall. This way the firewall should only have to deal with "real" traffic. <end hint> (Figure T16)
f. This completes the setup of the DSL interface and **CTRL Z** can be press to return to the *Privileged EXEC* prompt. (Figure T16)



```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIACRTR(config)#interface atm 0/0
GIACRTR(config-if)#ip address 216.32.200.5 255.255.255.252
GIACRTR(config-if)#description External connection of border router
GIACRTR(config-if)#no ip directed broadcast
GIACRTR(config-if)#ip access-group 10 in
GIACRTR(config-if)#^Z
GIACRTR#
00:54:46: %SYS-5-CONFIG_I: Configured from console by console
GIACRTR#
```

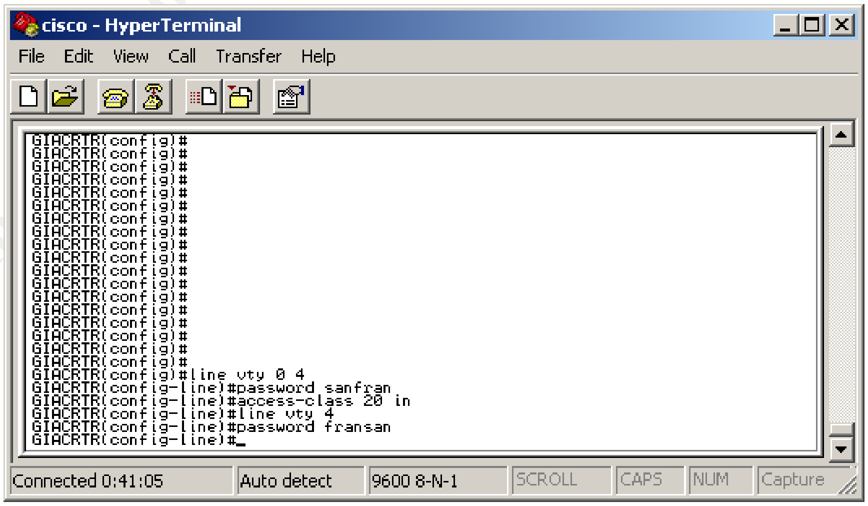
Figure T16 (Configuring the DSL Port)

8) Securing the VTY (or Telnet) ports

a. From the Privileged Exec prompt: GIACRTR(config)#, enter the command **line vty 0 4** . The prompt will change to

GIACRTR(config-line)# indicating that we are now editing the vty ports 0-4. (Figure T17) <hint> Again, use the history to see what line you are editing. <end hint>

b. To set a password for the vty ports the following syntax is used: **password sanfran** <ENTER>. This will set the password for router access via telnet to "sanfran". (Figure T17) <hint> The vty lines are enabled for login by default, but do not have a password set. This in effect prevents anyone from logging in via the network until a password is. To disable telnet access the **no login** command can be entered at the config-line prompt. <end hint>
c. The following command will apply the access list 20 listed above so that only certain hosts or networks can telnet into the router. **access-class 20 in** <ENTER>. In this case we are giving all hosts on the 192.168.0.0 network the ability to telnet into the router. (Figure T17)
d. Type **line vty 4** <ENTER> to change to just editing vty port 4 (the last vty port). Type **password fransan** <ENTER>. This will change the password on vty 4 so that in the event we or someone else locks us out of the first 4 ports, we still have a port with a password that should be unknown to anyone else and therefore a way to gain access. (Figure T17)



```
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#
GIACRTR(config)#line vty 0 4
GIACRTR(config-line)#password sanfran
GIACRTR(config-line)#access-class 20 in
GIACRTR(config-line)#line vty 4
GIACRTR(config-line)#password fransan
GIACRTR(config-line)#_
```

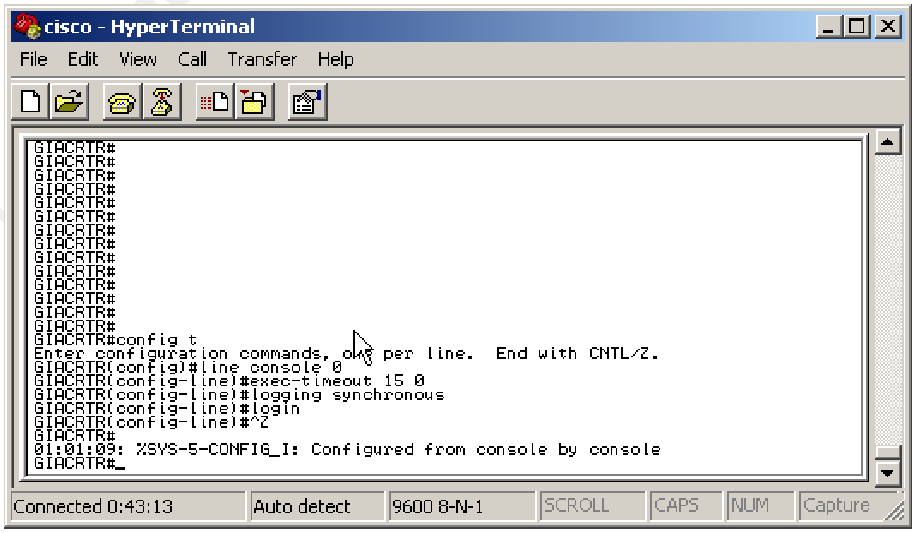
Figure T17 (Configuring the VTY Ports)

9) Securing the Console Port

a. From the Privileged Exec prompt: GIACRTR(config)#, enter the command **line console 0** . The prompt will change to GIACRTR(config-line)# indicating that we are now editing the

GIACRTR(config-line)# indicating that we are now editing the console port. (Figure T18)

b. Type in **exec-timeout 15 0** <ENTER>. This will set the console port to close the connection after 15 minutes and 0 seconds. This will help prevent the console port from being compromised if you forget to logout. If this is not done and the port has been set for exec-timeout 0 0, then anyone could connect to the port at a later time and continue accessing the device from the last command you entered. (Figure T18)
c. Type in **logging synchronous** <ENTER>. This command, while not a security feature, does help while configuring the router. Whenever a message is displayed to the console screen, it will appear at the end of the current text on the screen. If this happens to be when you are typing in a command, it becomes difficult to read what you have inputted. The logging synchronous command will cause the new line to appear and the line you were typing to appear below it, thus preserving your sanity and the ability to read your commands. (Figure T18)
d. Type **login** <ENTER>. This will configure the console port, so that when communications are first initiated, a password will be required to access user mode. (Figure T18)
e. Type in **CTRL Z** to return to the *Privileged Exec* mode. (Fig T18)

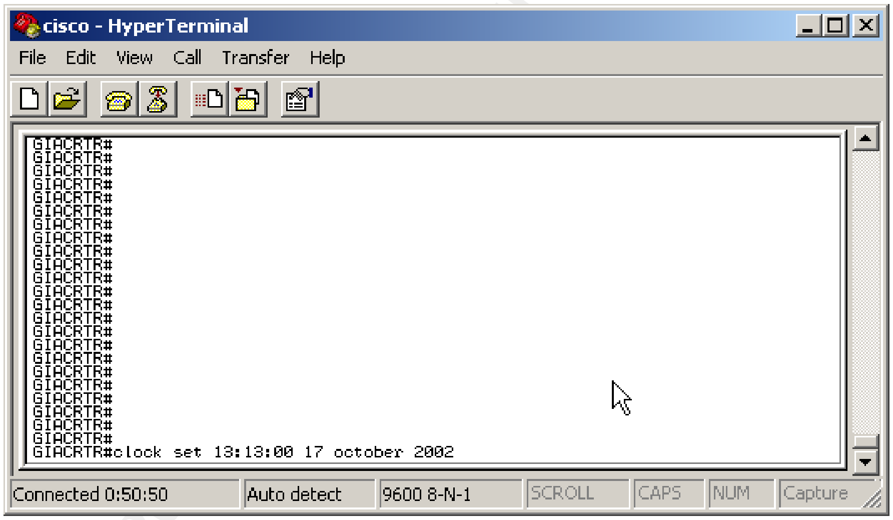


```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIACRTR(config)#line console 0
GIACRTR(config-line)#exec-timeout 15 0
GIACRTR(config-line)#logging synchronous
GIACRTR(config-line)#login
GIACRTR(config-line)#^Z
GIACRTR#
01:01:09: %SYS-5-CONFIG_I: Configured from console by console
GIACRTR#_
```

Figure T18 (Console configuration)

10) Privileged EXEC mode settings

a. Set the time and date on the router. The following is an example of what will need to be type in. Use the appropriate times and dates. Typing in **clock set 13:13:00 17 october 2002** <ENTER>, will set the time to 13:13:00 (24 hour time format for 1:13PM) on October 17th 2002.

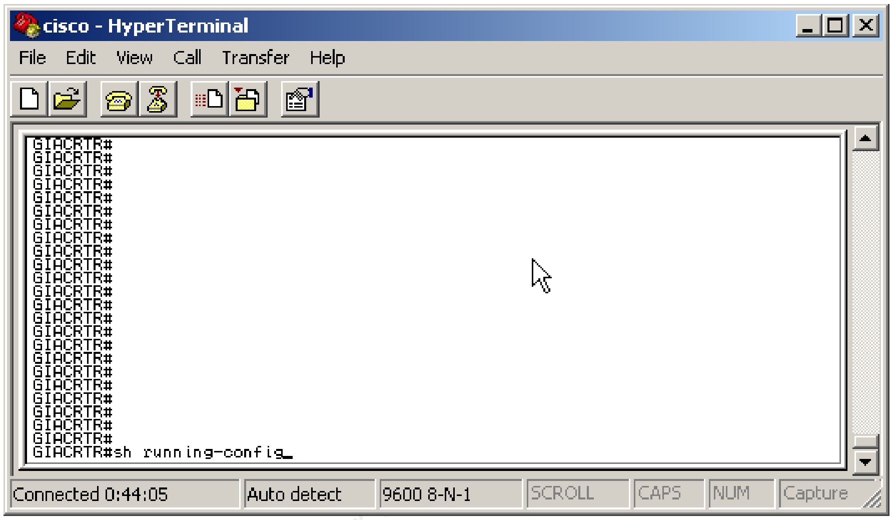


```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#clock set 13:13:00 17 october 2002
```

Figure T19 (Setting the System date and time)

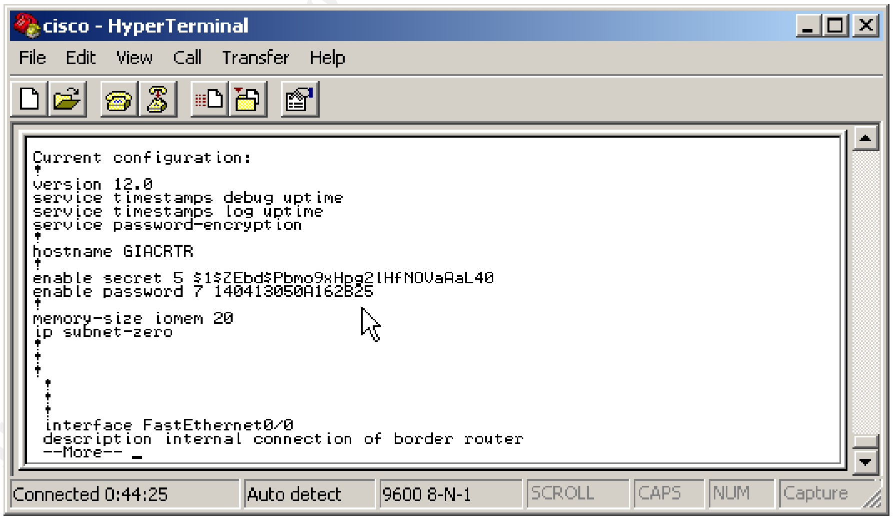
11) Verify the configuration

a. From the Privileged Exec prompt: GIACRTR(config)#, enter the command **show running-config** <ENTER>. This will show all the current configuration settings so they can be reviewed. (Figures T20 and T21)



```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#sh running-config_
```

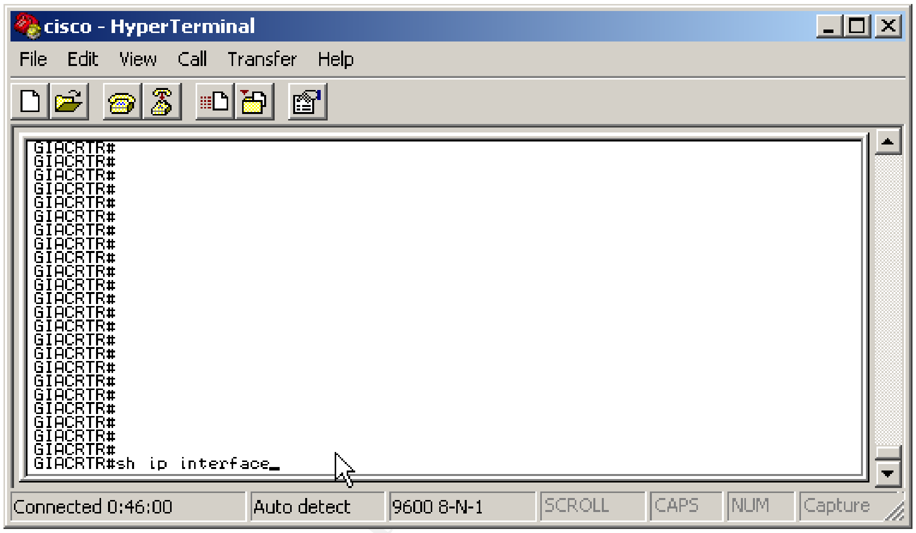
Figure T20 (show running-config)



```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname GIACRTR
!
enable secret 5 $1$ZEbd$Pbmo9xHpg2lHfNOVaAaL40
enable password 7 140413050A162B25
!
memory-size iomem 20
ip subnet-zero
!
!
!
 !
 !
 !
 interface FastEthernet0/0
 description internal connection of border router
 --More-- _
```

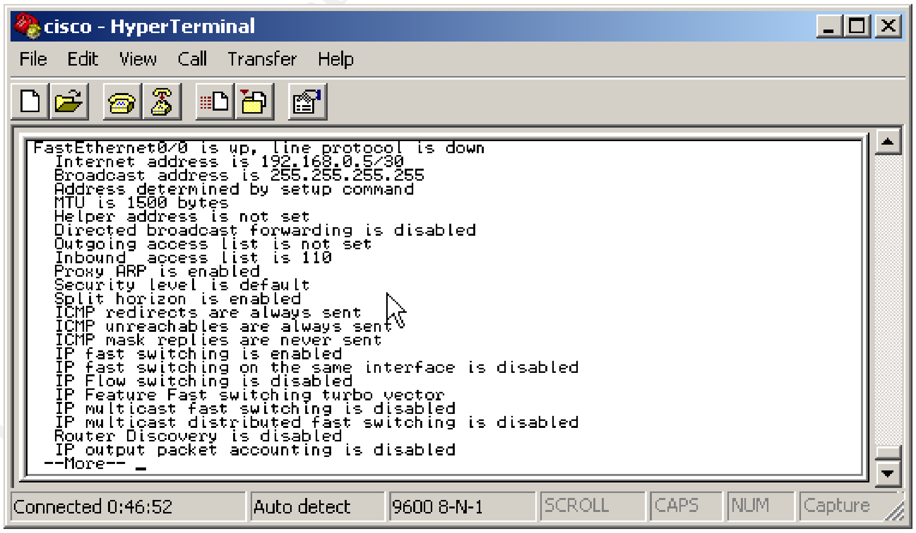
Figure T21 (Some results of “show running-config”)

b. Type **sh ip interface** <ENTER>. This will show the configuration of all the interfaces running the IP protocol. (Figures T22 and T23)



```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#sh ip interface_
```

Figure T22 (The show ip interface command)

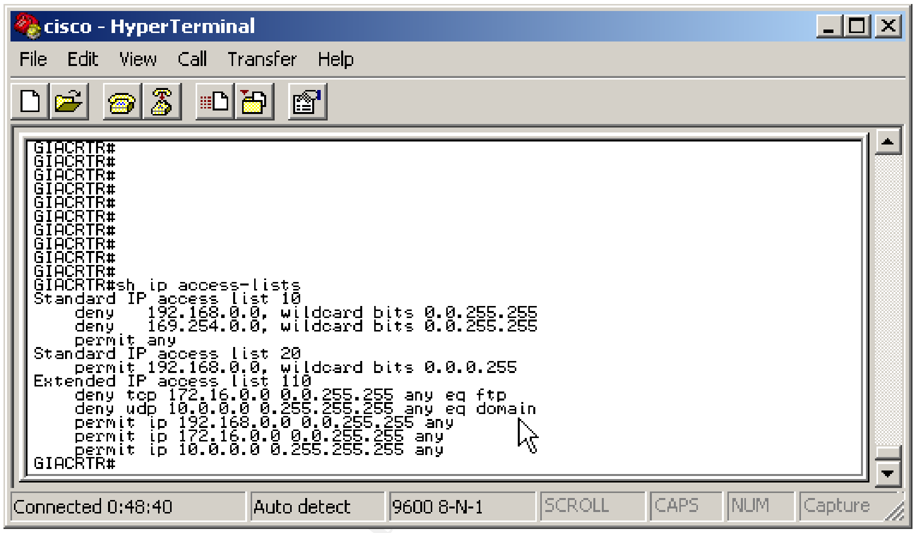


```
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.0.5/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 110
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Feature Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
 --More-- _
```

Figure T23 (Sample output of "sh ip interface" command)

c. Type **sh ip access-lists** <ENTER>. This will show the contents of the IP access lists. (Figure T24)

Assignment 2: Security Policy and Tutorial
----
(44)

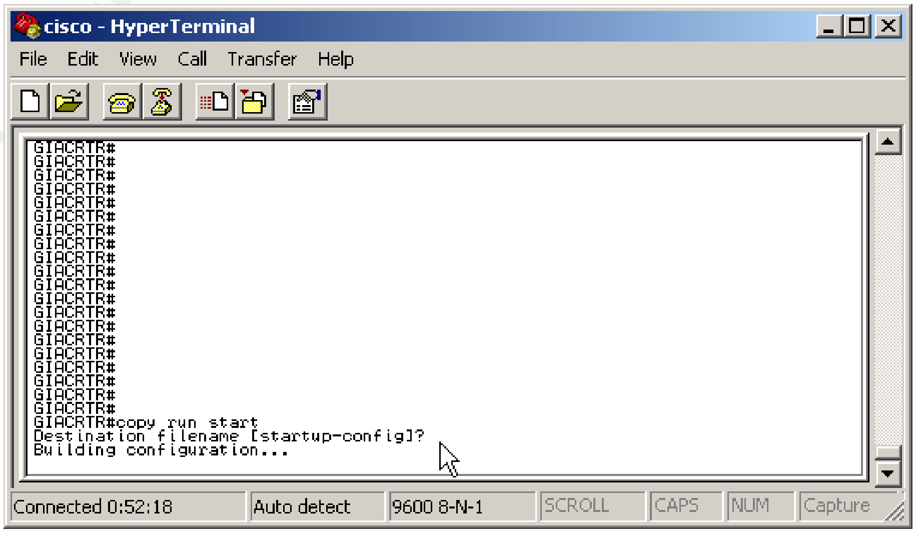


```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#sh ip access-lists
Standard IP access list 10
    deny   192.168.0.0, wildcard bits 0.0.255.255
    deny   169.254.0.0, wildcard bits 0.0.255.255
    permit any
Standard IP access list 20
    permit 192.168.0.0, wildcard bits 0.0.0.255
Extended IP access list 110
    deny tcp 172.16.0.0 0.0.255.255 any eq ftp
    deny udp 10.0.0.0 0.255.255.255 any eq domain
    permit ip 192.168.0.0 0.0.255.255 any
    permit ip 172.16.0.0 0.0.255.255 any
    permit ip 10.0.0.0 0.255.255.255 any
GIACRTR#
```

Figure T23 (The "show ip access-lists" command)

12) Save the configuration

a. At this point, everything that has been entered is stored in system RAM and not NVRAM. To save the configuration so that it will be used the next time the router is restarted, use the command **copy run start**. This will copy the configuration in RAM (running-config) to NVRAM (startup-config). (Figure T24)



```
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#
GIACRTR#copy run start
Destination filename [startup-config]?
Building configuration...
```

Figure T24 (Copying running-config to startup-config)

13) Information

a. No routing protocols are turned on for this device due to the fact there are few routes and they should be configured manually.
b. The Border router is not used to block any of the top 20 known vulnerabilities. If the 2600 router is pressed into too much filtering, it may begin to lose packets.
c. Logging is also turned off for incoming traffic. Logging would consume valuable router memory that can be better used as packet buffers.

<End of Tutorial>

This area left blank for formatting reasons

Assignment 3: Verify the Firewall Policy (25 Points)

Audit Plan

Technical Approach

- The audit will take place on Sunday morning
  - Normal web traffic is at its lowest
  - The employees are not at work
  - If something goes wrong, the remainder of the day can be used to fix the problem
- The individuals involved will be:
  - The person who designed and implemented the new network structure (grandson)
  - A second pair of eyes to also evaluate the results (a friend of the grandson who works in network security)
- The following will be audited:
  - The GIAC border. (the connection from the Internet to the Border Router)
  - Connectivity to, and vulnerabilities of the perimeter network (DMZ). This will be tested from the Internet side of the External Firewall.
  - Connectivity out of the Internal network to the Internet.
  - Direct scanning for ports and vulnerabilities of hosts in the Perimeter network. (from the perimeter network)
  - Direct scanning of hosts on the Internal network. (from the Internal network)
  - Test of External firewall rules (inbound)
  - Test of Internal firewall rules (inbound)
  - Test of Internal firewall rules (outbound)
  - Check firewall and IDS logs for proper logging
  - Capture VPN traffic to verify proper encryption

Considerations

- The following should be done prior to auditing
  - Create a checklist of items to be audited
  - Start a log of activities
  - Back up all servers
  - Back up the ISA Server configurations
  - Copy the startup-config and IOS of the border router to a tftp server.
  - Post a message on the GIAC website that the

        - system will be down for maintenance for that Sunday morning. Post it two weeks in advance.
        - Contact the ISP and notify them of the test day and times. This is to prevent them from seeing the test as an attack on one of their customers.
        - No company authorization will need to be done (no approval to perform testing) since the test is being performed in-house.

<u>Costs</u>

- Cost will be minimal due to the nature of the implementation
    - Bare-bones budget
    - Family run business
    - No outside (paid help) involved

<u>Risks</u>

- The risks involved can be summarized as follows:
    - The system could fail (DoS for customers)
    - The system could stay up, but performance be reduced to the point it is unusable by customers
    - A "real" attack could occur

<u>Tools</u>

- Two Laptops with the following tools will be utilized: (See Appendix F for descriptions and sources)
    - Ethereal Ver. – General Packet analysis
    - SARA ver. 4.1.2 – To scan for vulnerabilities and for fingerprinting.
    - SuperScan ver. 3.00 – Basic Port scanning
    - NMAP for Windows - For port scanning and fingerprinting
    - Snort for Windows – Intrusion detection and alerting
    - Microsoft Internet Explorer
    - Microsoft ftp client (command prompt)

<u>Audit</u>

<u>Validation</u>

The plan behind the audit is:

- Test the connection from the Internet to the Border Router.
- Test ability of the Border Router rules to allow and deny traffic to the external firewall
- Test the External Firewall
- Test the ability of the External Firewall rules to allow and deny traffic to the perimeter network (DMZ)

Assignment 3:
Verify the Firewall Policy
----
(3)

The first item on the checklist is an audit of the Border Router rules.

- Attempting to send allowed and blocked packets to the public interface of the external firewall will do this. A laptop will be connected to this segment of the network.
- SARA will be used to scan the Border Router for open ports and services. The results are as follows:
  - SARA Scan of 216.32.200.5:

```
Data collection in progress...

Adding a primary target
Add-primary: 216.32.200.5
Deleting: 216.32.200.5||a|||||rpcinfo error #256
Deleting: 216.32.200.5|dns.sara|u|||||unknown error #15
Add-target: 216.32.200.5 prox 0
Primaries being rescanned, rebuilding tables.
Reading all hosts info from results/sara-data/all-hosts...
Reading facts from results/sara-data/facts...
Reading old todo list from results/sara-data/todo...
policy: 216.32.200.5 prox 0 level 3
Check-pulse: 216.32.200.5
==> running bin/timeout 240 bin/fping 216.32.200.5
process_targets: probe 216.32.200.5...
Prox: 0
AL  : 3
Add-todo: 216.32.200.5|dns.sara|
Add-todo: 216.32.200.5|rpc.sara|
Add-todo: 216.32.200.5|finger.sara|
Add-todo: 216.32.200.5|backdoor.sara|
Add-todo: 216.32.200.5|hosttype.sara|
Add-todo: 216.32.200.5|tcpscan.sara 1-1522,1522-1525,1527-9999|
Add-todo: 216.32.200.5|tcpscan.sara 10000-19999|
Add-todo: 216.32.200.5|tcpscan.sara 20000-29999|
Add-todo: 216.32.200.5|tcpscan.sara 30000-39999|
Add-todo: 216.32.200.5|tcpscan.sara 40000-49999|
Add-todo: 216.32.200.5|tcpscan.sara 50000-59999|
Add-todo: 216.32.200.5|tcpscan.sara 60000-65535|
Add-todo: 216.32.200.5|udpscan.sara 1-
2050,6500,27444,31335,31337,32767-33500|
==> running bin/timeout 120 bin/backdoor.sara  216.32.200.5
==> running bin/timeout 120 bin/tcpscan.sara 1-1522,1522-
1525,1527-9999  216.32.200.5
==> running bin/timeout 120 bin/tcpscan.sara 20000-29999
216.32.200.5
==> running bin/timeout 120 bin/finger.sara  216.32.200.5
==> running bin/timeout 120 bin/tcpscan.sara 30000-39999
216.32.200.5
==> running bin/timeout 240 bin/udpscan.sara 1-
```

```
2050,6500,27444,31335,31337,32767-33500  216.32.200.5
==> running bin/timeout 120 bin/rpc.sara  216.32.200.5
Add-fact: 216.32.200.5||a|||||rpcinfo error #256
==> running bin/timeout 240 bin/hosttype.sara  216.32.200.5
==> running bin/timeout 120 bin/tcpscan.sara 40000-49999
216.32.200.5
==> running bin/timeout 120 bin/dns.sara  216.32.200.5
==> running bin/timeout 120 bin/tcpscan.sara 50000-59999
216.32.200.5
Waiting for all processes to complete
==> running bin/timeout 120 bin/tcpscan.sara 60000-65535
216.32.200.5
==> running bin/timeout 120 bin/tcpscan.sara 10000-19999
216.32.200.5
Add-fact: 216.32.200.5|udpscan.sara 1-
2050,6500,27444,31335,31337,32767-33500|u|||||unknown error #15
Data collection completed (1 host(s) visited).
```

- NmapWin will be used to scan the Border Router for open Ports and Services.
    - Using the SYN Stealth Scan shows no vulnerable ports:

CMD: nmap -sS -PT -PI -O -v -T 3 216.32.200.5

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (216.32.200.5) appears to be up ... good.
Initiating SYN Stealth Scan against  (216.32.200.5)
The SYN Stealth Scan took 4 seconds to scan 1601 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1601 scanned ports on  (216.32.200.5) are: closed
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=11/26%Time=3DE407B7%O=-
1%C=1)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN
=134%DAT=E)
Nmap run completed -- 1 IP address (1 host up) scanned in 14 seconds
```

- Using the UDP Scan returned no results:

CMD: -sU -PT -PI -O -v -T 3 216.32.200.5

no results

- A FIN Stealth Scan reveals the same results as the SYN Scan:

SYN Scan:

FIN Stealth Scan

```
CMD: nmap -sF -PT -PI -O -v -T 3 216.32.200.5
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (216.32.200.5) appears to be up ... good.
Initiating FIN Scan against  (216.32.200.5)
The FIN Scan took 4 seconds to scan 1601 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 1601 scanned ports on  (216.32.200.5) are: closed
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=11/26%Time=3DE40882%O=-1%C=1)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)
Nmap run completed -- 1 IP address (1 host up) scanned in 13 seconds
```

- The IP Protocol Scan reveals the following:

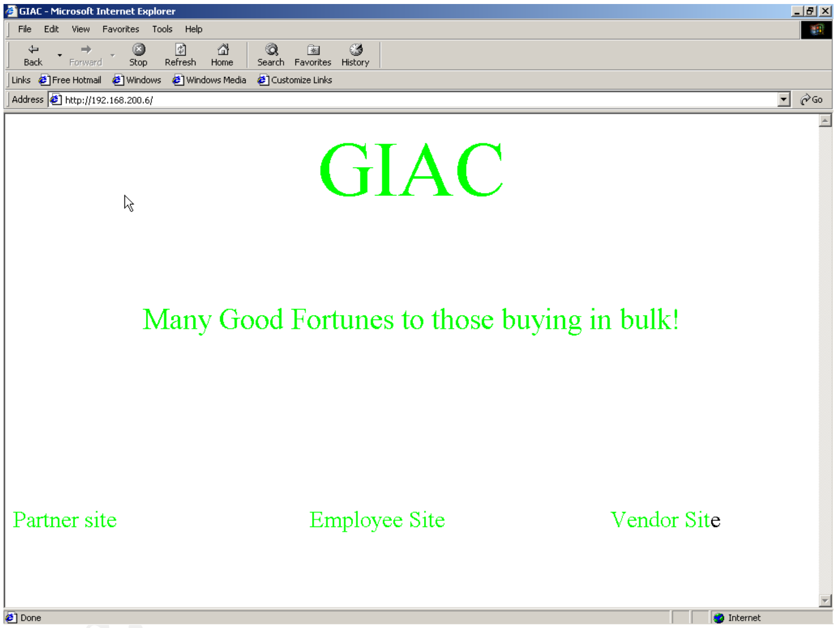
```
CMD: nmap -sO -PT -PI -O -v -T 3 216.32.200.5

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (216.32.200.5) appears to be up ... good.
Initiating IPProto Scan against  (216.32.200.5)
The IPProto Scan took 182 seconds to scan 255 ports.
Adding open port 9/udp
Adding open port 17/udp
Adding open port 6/udp
Adding open port 89/udp
Adding open port 77/udp
Adding open port 54/udp
Adding open port 4/udp
Adding open port 94/udp
Adding open port 47/udp
Adding open port 53/udp
Adding open port 55/udp
Adding open port 88/udp
Adding open port 1/udp
Adding open port 8/udp
Adding open port 103/udp
Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
Interesting protocols on  (216.32.200.5):
(The 240 protocols scanned but not shown below are in state: closed)
Protocol   State       Name
```

```
1          open       icmp
4          open       ip
6          open       tcp
8          open       egp
9          open       igp
17         open       udp
47         open       gre
53         open       swipe
54         open       narp
55         open       mobile
77         open       sun-nd
88         open       eigrp
89         open       ospfigp
94         open       ipip
103        open       pim
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=11/26%Time=3DE409A5%O=-1%C=-
1)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN
=134%DAT=E)
Nmap run completed -- 1 IP address (1 host up) scanned in 191 seconds
```

These results show the border router has been secured well enough to prevent easy fingerprinting. The SARA scan returned inconclusive data back to SARA. In other words, the OS could not be identified and there were no vulnerable ports. NMAPWIn returned basically the same information. It recognized that a host was present, but could not find any vulnerable services.

- The ability of the border router rules to allow and deny traffic to the external firewall.
  - To test the allowed traffic, the connectivity to the Web Server (Ports 80 and 443), the FTP Server (Ports 20/21), and the passing of Email (Ports 25,110, and 143). This will also validate the External Firewall "Allow Rulesets" that were created. <Note> Email (as listed) will not actually be tested for this paper due to the lack of an Exchange Server) <End Note>
  - The following screenshots (Figure Aud1 and Figure Aud2) show connectivity to the Web server and to the FTP server from the Public side of the Border

Router. This was done using Microsoft Internet Explorer and the Command Prompt version of the ftp client.


GIAC - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History
Links Free Hotmail Windows Windows Media Customize Links
Address
Go
Done
Internet

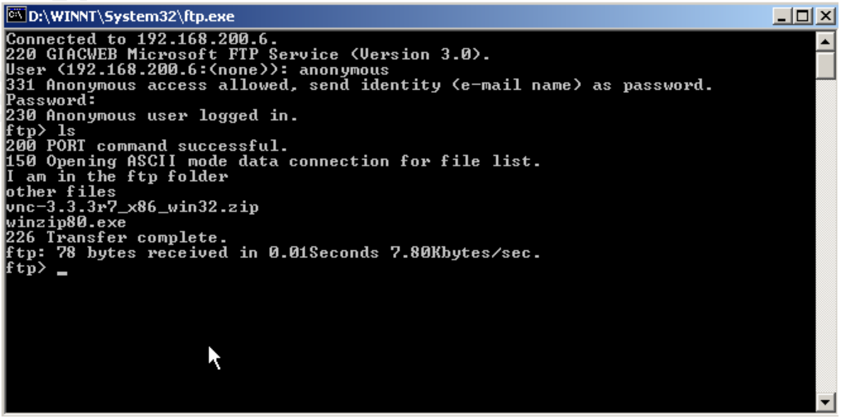
Address: http://192.168.200.6/

GIAC

Many Good Fortunes to those buying in bulk!

Partner site Employee Site Vendor Site

Figure AUD1 (The GIAC Web Site)



```
Connected to 192.168.200.6.
220 GIACWEB Microsoft FTP Service (Version 3.0).
User (192.168.200.6:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
I am in the ftp folder
other files
vnc-3.3.3r7_x86_win32.zip
winzip80.exe
226 Transfer complete.
ftp: 78 bytes received in 0.01Seconds 7.80Kbytes/sec.
ftp> _
```

Figure AUD2 (Connecting to the GIAC FTP Site)

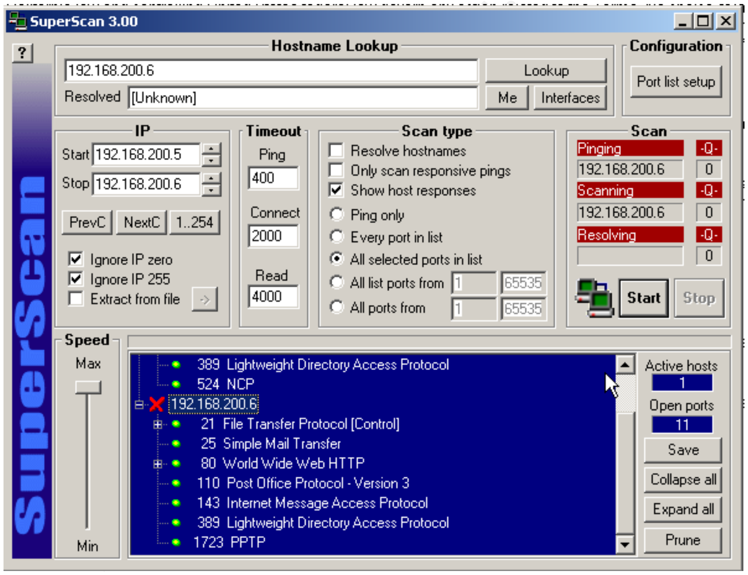
- Connectivity to, and vulnerabilities of the perimeter network (DMZ). This will be tested from the Internet side of the External Firewall.
    - The following are Superscan and NMAPWin scans of the External Firewall. This was done to see what services were being offered and/or passed through

Assignment 3: Verify the Firewall Policy

----

(8)

to the DMZ by the External Firewall. Both show that the services published earlier are available. The LDAP 389 Protocol is open and will need to be investigated.



Hostname: 192.168.200.6
Resolved [Unknown]

IP
Start 192.168.200.5
Stop 192.168.200.6
PrevC NextC 1..254
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

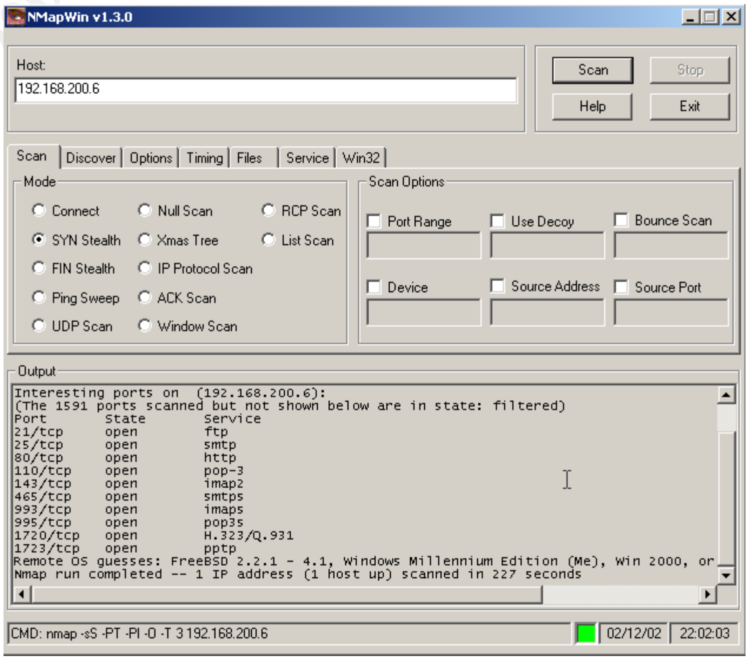
Scan
Pinging -Q-
192.168.200.6 0
Scanning -Q-
192.168.200.6 0
Resolving -Q-
0

Speed

389 Lightweight Directory Access Protocol
524 NCP
192.168.200.6
21 File Transfer Protocol [Control]
25 Simple Mail Transfer
80 World Wide Web HTTP
110 Post Office Protocol - Version 3
143 Internet Message Access Protocol
389 Lightweight Directory Access Protocol
1723 PPTP

Active hosts 1
Open ports 11

Figure AUD3 (Firewall scan to determine services)



Host: 192.168.200.6

Mode
○ Connect ○ Null Scan ○ RCP Scan
● SYN Stealth ○ Xmas Tree ○ List Scan
○ FIN Stealth ○ IP Protocol Scan
○ Ping Sweep ○ ACK Scan
○ UDP Scan ○ Window Scan

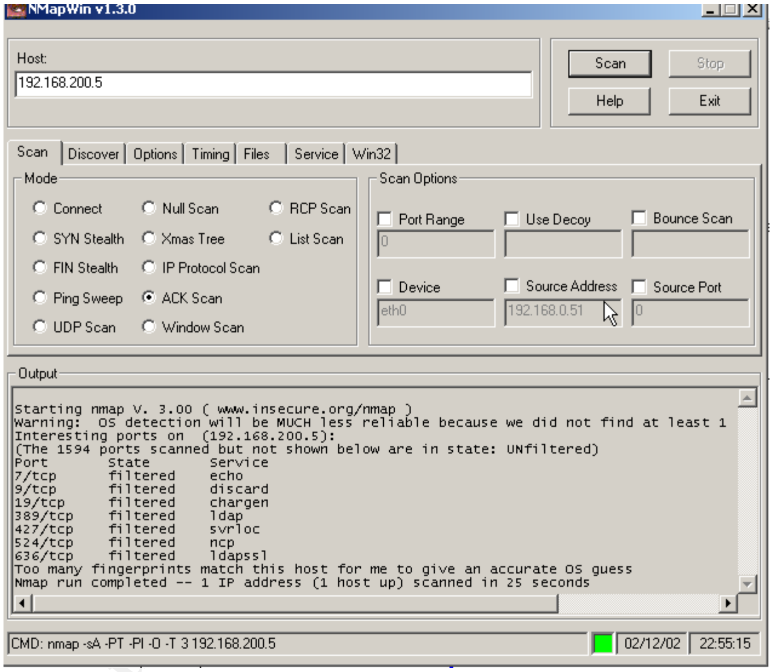
Scan Options
☐ Port Range ☐ Use Decoy ☐ Bounce Scan
☐ Device ☐ Source Address ☐ Source Port

Output

```
Interesting ports on  (192.168.200.6):
(The 1591 ports scanned but not shown below are in state: filtered)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
110/tcp    open        pop-3
143/tcp    open        imap2
465/tcp    open        smtps
993/tcp    open        imaps
995/tcp    open        pop3s
1720/tcp   open        H.323/Q.931
1723/tcp   open        pptp
Remote OS guesses: FreeBSD 2.2.1 - 4.1, Windows Millennium Edition (Me), Win 2000, or
Nmap run completed -- 1 IP address (1 host up) scanned in 227 seconds
```

CMD: nmap -sS -PT -PI -O -T 3 192.168.200.6 02/12/02 22:02:03

Figure AUD4 (Firewall scan to determine service)



Host: 192.168.200.5

● ACK Scan

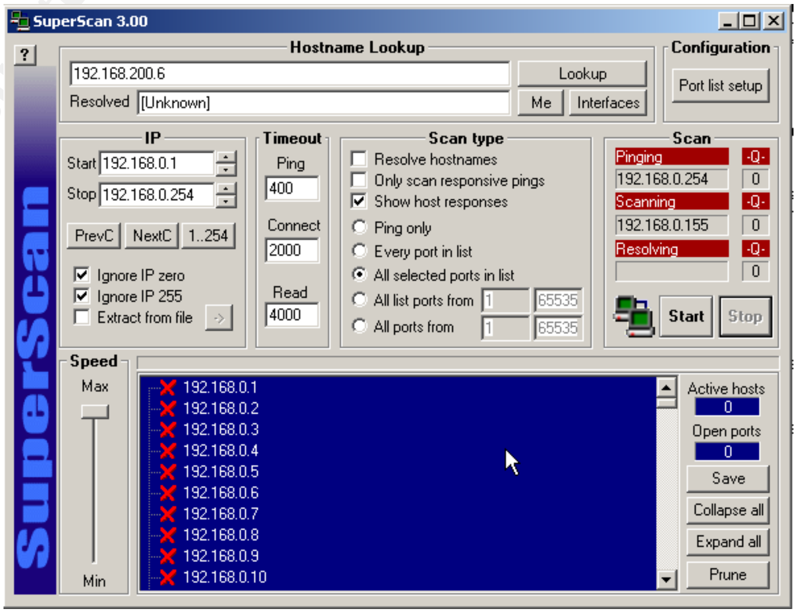
☐ Source Address 192.168.0.51

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
Interesting ports on  (192.168.200.5):
(The 1594 ports scanned but not shown below are in state: UNfiltered)
Port       State       Service
7/tcp      filtered    echo
9/tcp      filtered    discard
19/tcp     filtered    chargen
389/tcp    filtered    ldap
427/tcp    filtered    svrloc
524/tcp    filtered    ncp
636/tcp    filtered    ldapssl
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 25 seconds
```

CMD: nmap -sA -PT -PI -O -T 3 192.168.200.5 | 02/12/02 | 22:55:15

Figure AUD5 (Additional scan attempt)

- Connectivity to, and vulnerabilities of the internal network - This will be tested from the Internet side of the External Firewall. Superscan will be used for this test (Figure AUD6).



192.168.200.6
Resolved [Unknown]

Start 192.168.0.1
Stop 192.168.0.254
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Ping 400
Connect 2000
Read 4000

☐ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Pinging 192.168.0.254 0
Scanning 192.168.0.155 0
Resolving 0

192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
192.168.0.5
192.168.0.6
192.168.0.7
192.168.0.8
192.168.0.9
192.168.0.10

Active hosts 0
Open ports 0

Figure AUD6 (Attempted scan of the internal network)

Assignment 3: Verify the Firewall Policy
----
(10)

The results of the scan showed that no internal addresses were accessible, and an alert was added to the log files. (See Firewall logging below)

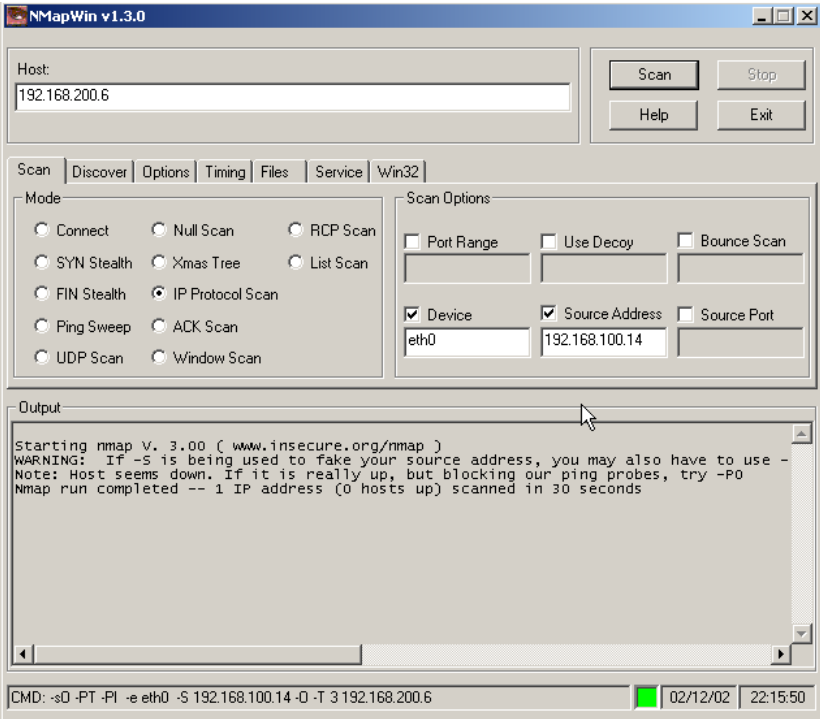
- Connectivity out of the Internal network to the Internet – This was tested using Internet Explorer and a connection to MSN.com was successful.

- Direct scanning for ports and vulnerabilities of hosts in the Perimeter network. (from the perimeter network) – This was done using Superscan. Figure AUD3 gives an example the results of a typical scan attempt. No unexpected services were discovered at this time. This process of scanning will nee ot be done on a periodic basis to catch ports that may have been inadvertently open from software, patch, or super pack updates.

- Direct scanning of hosts on the Internal network. (from the Internal network) – Again, Figure AUD3 gives an example of a typical scan. The internal network is still secure due to the fact that all of the computer configurations were recently set up and audited, with corrections taking place as the setup progressed. In the future, these machines will need to be periodically scanned due to the same reasons listed for the perimeter network, and because individuals may intentionally change their settings or open “shares” not knowing they are creating vulnerabilities.

- Test of External firewall rules (inbound). This was done using NMAPWin and with attempts made to access the IP addresses of hosts on the Perimeter network. Several alerts were generated during the testing. There were also attempts to spoof (Figure AUD7) connectivity by using one of the DMZ addresses and then attempting to access the DMZ from the “Outside” of the firewall (see firewall and IDS logs below).

Assignment 3: Verify the Firewall Policy
----
(11)



Host: 192.168.200.6

● IP Protocol Scan

☑ Device: eth0

☑ Source Address: 192.168.100.14

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
WARNING:  If -S is being used to fake your source address, you may also have to use -
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds
```

CMD: -sO -PT -PI -e eth0 -S 192.168.100.14 -O -T 3 192.168.200.6 | 🟩 | 02/12/02 | 22:15:50

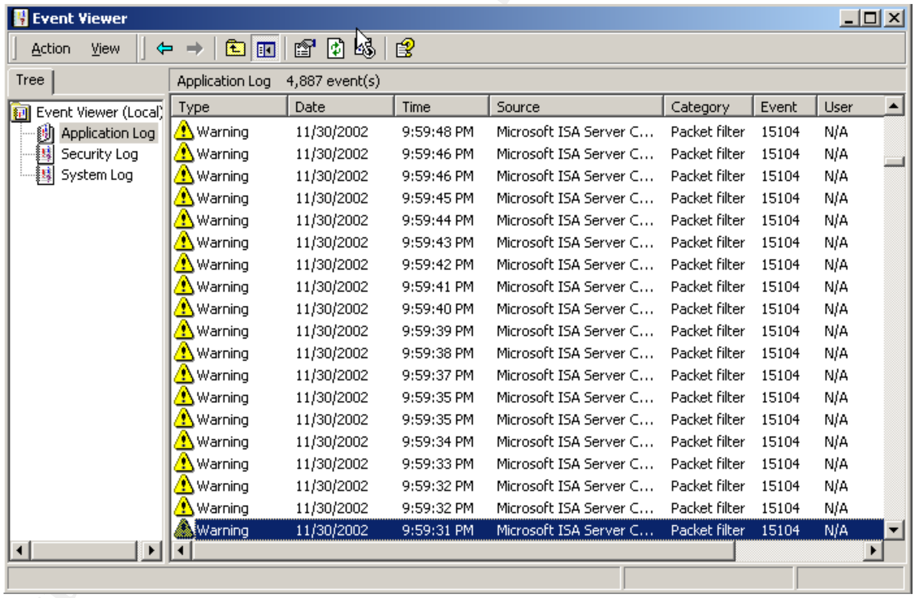
Figure AUD7 (Spoof attempt)

- Test of Internal firewall rules (inbound) – The SQL server part of this could not be real-world tested properly for lack of a SQL Server on the test Internal network. The same publishing rules described above for the other servers was used, but there was not a server internally to receive packets. Nmap could be used to test pass-thorough to the proper port and IP address on the internal network. Terminal Server connectivity was validated by accessing GIACCORP1 and pinging internal resources.

- Test of Internal firewall rules (outbound) – This was tested by accessing Web Sites, Mail Servers, and FTP sites. Yahoo Instant messaging was used to test other outbound protocols and it failed. Packets captured with Ethereal showed the use of Ports 5000, 5001 and 5010 and 5050. These were not allowed by the firewall rule “Inet” and were therefore blocked.

Assignment 3: Verify the Firewall Policy
----
(12)

- Check firewall and IDS logs for proper logging.
    - The following is an example of the firewall log on the ISA Server. One of the options, and the way this system is configured, is that ISA Server sends the firewall alerts to the Windows 2000 application Log (Figure AUD6). Other options for the alerts are run an application, start or stop a service, and send email. Any combination of these options can be selected.



```
Application Log   4,887 event(s)
Type     Date        Time         Source                Category       Event   User
Warning  11/30/2002  9:59:48 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:46 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:46 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:45 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:44 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:43 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:42 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:41 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:40 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:39 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:38 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:37 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:35 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:35 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:34 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:33 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:32 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:32 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
Warning  11/30/2002  9:59:31 PM   Microsoft ISA Server C...  Packet filter  15104  N/A
```

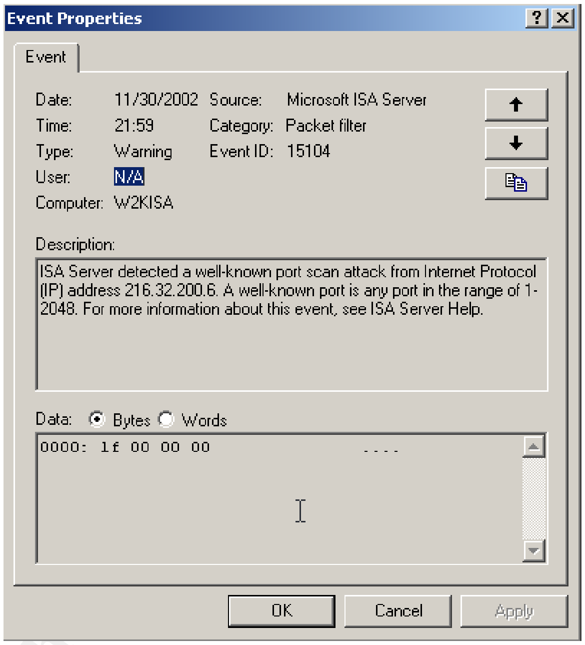
Figure AUD6 (Firewall Log)

- A more detailed look at the Packet Filter alert listed above shows that the port scanning from our fingerprinting attempt showed was recognized as a "port scanning" attack. It also gives a brief explanation of the alert (Figure AUD7).

Assignment 3: Verify the Firewall Policy

----

(13)



Date: 11/30/2002 Source: Microsoft ISA Server
Time: 21:59 Category: Packet filter
Type: Warning Event ID: 15104
User: N/A
Computer: W2KISA

Description:

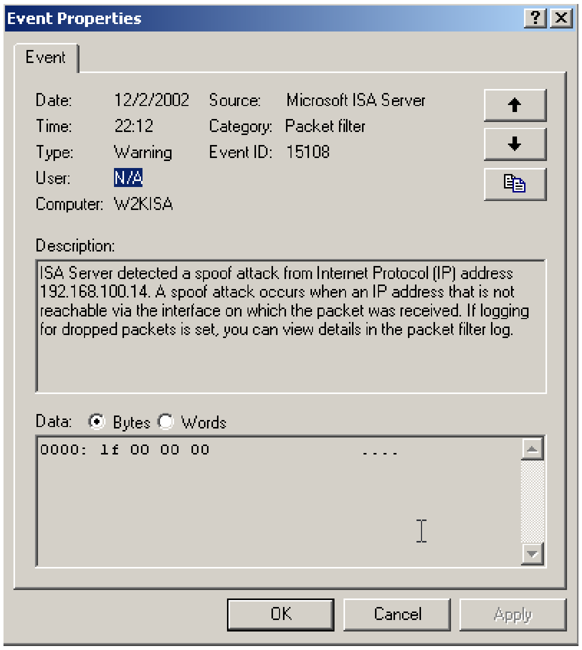
ISA Server detected a well-known port scan attack from Internet Protocol (IP) address 216.32.200.6. A well-known port is any port in the range of 1-2048. For more information about this event, see ISA Server Help.

Data: ● Bytes ○ Words

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

Figure AUD7 (Alert detail)

- The following alert was generated by the attempt to spoof a DMZ address from the outside of the External Firewall (Figure AUD8):



Date: 12/2/2002 Source: Microsoft ISA Server
Time: 22:12 Category: Packet filter
Type: Warning Event ID: 15108
User: N/A
Computer: W2KISA

Description:

ISA Server detected a spoof attack from Internet Protocol (IP) address 192.168.100.14. A spoof attack occurs when an IP address that is not reachable via the interface on which the packet was received. If logging for dropped packets is set, you can view details in the packet filter log.

Data: ● Bytes ○ Words

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

Figure AUD8 (An attempt to spoof an address)

- Capture VPN traffic to verify proper encryption – Packets captured using Ethereal were analyzed and the existence of MPPE and GRE packets was verified. MPPE (Microsoft point-to-Point Encryption) indicates that the packets are indeed using encryption. GRE (Generic Route Encapsulation) protocol indicates that a VPN tunnel has been established and is being used to route packets. A screen shot of this was not available.
  GRE Link: (GRE Port 47 description and use)
  http://support.microsoft.com/default.aspx?scid=kb;en-us;241251

Audit Evaluation

Analysis

The system configuration would pass a casual scan/attack. The Border Router is configured sufficiently to pass initial fingerprinting attempts but a determined attacker could saturate the router with traffic and cause a slow down or complete Denial of Service. At this stage of GIACs existence on the Internet, and considering the amount of funds available, this is an acceptable risk. The Border Router is not configured to address all security issues, but instead, to clean up the inbound traffic that is passed to the firewall. The router may be able to handle the immediate load, but an increase in traffic and the activation of logging could quickly degrade performance. This could manifest itself in lost packets or the passing of "blocked" traffic to the first firewall.
The External Firewall was identified by fingerprinting, and the exploits to be concerned with are geared towards the operating system (Windows 2000.) The ISA Server itself, when raised to the service pack 1 level and with available patches, does not have many vulnerabilities
The External Firewall/ISA Server performed properly for redirecting port 80 and 443 requests to the DMZ Web server. Port 20/21 traffic was properly redirected to the FTP server. The Mail server traffic (ports 25,110, and143) would have been properly redirected.
Direct connectivity from the Public side of the External Router was blocked to all Internal and DMZ hosts. Connectivity from the DMZ to the Internal network worked as designed, and no other hosts on the internal network could be reached from the DMZ
The outbound connectivity from the Internal network to the Internet worked properly and met the design. Trying to run Instant Messenger (IM) programs failed unless they were configurable for a proxy server. The Server logs were updated as required.

Recommendations

The Border router could be upgraded to a more powerful model. A 3700 series would be able to handle a greater load.

Logging could be initiated periodically to provide baseline information and to help tune the rulesets. This would mean moving higher in the access list those rules that are being used the most. This would increase the performance of the router because of shorter search times to find a rule that is effective.

Other Border router changes would be to an extended access list to replace access-list 10 (the ingress filter). This would allow more of the SANS/FBI top 20 items to addressed, such as blocking specific ports. Ports 137 and 138 are examples of what could be blocked by an extended access-list.

A Certificate Server could be set up to supply authentication for VPN connections. This would give a higher level of security than the initial PPTP connection, because L2TP with a form of extended authentication could be performed. (Keycards, Key exchange)

A message screener could be used. ISA Server offers an extension that redirects mail to an SMTP capable computer (usually a windows PC with the Simple SMTP Service running), that would check the emails for content, attachments, and keywords and then pass the acceptable ones on to the Exchange Server.

The Internal Firewall could be replaced with a different brand, such as the Cisco PIX 501. A different firewall would help in that having two different brands would give added protection in that they should not both have the same vulnerabilities at the same time.

Security or Awareness training should be given to all of the employees, and those connecting to GAIC from external locations (partners).

No host based virus protection was mentioned. This should be given a high priority and it should be purchased as soon as funding becomes available.

Periodic scanning of the DMZ and Internal Networks should be performed to look for vulnerabilities due to software installation, configuration changes, or accidental opening of Microsoft shares.

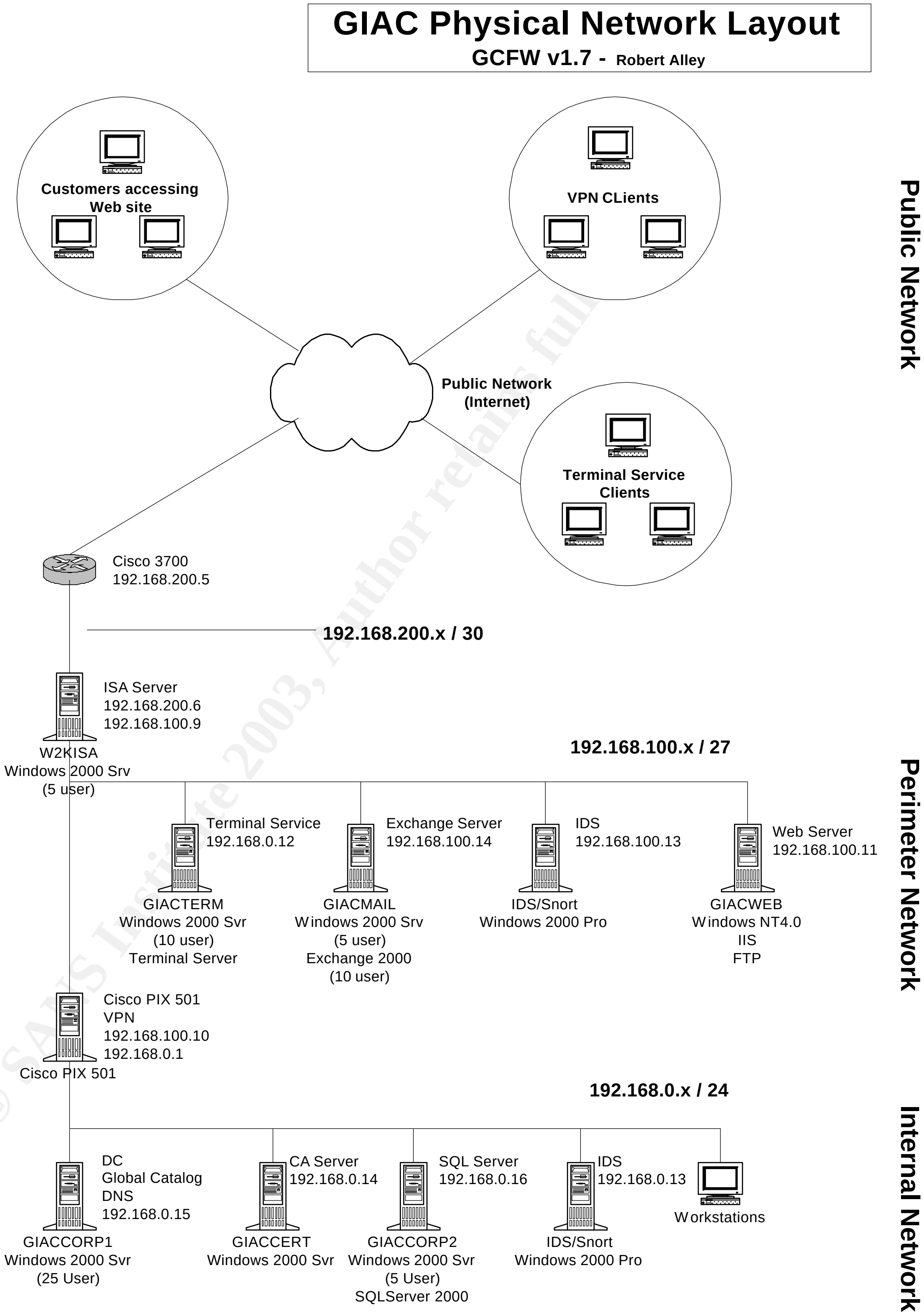
The addressing scheme for the DMZ will need to be changed to include more addresses. It is currently set to support only the DMZ servers, the subnet mask will need to be changed to /27 (30 available addresses).

Diagrams

Assignment 3: Verify the Firewall Policy

----

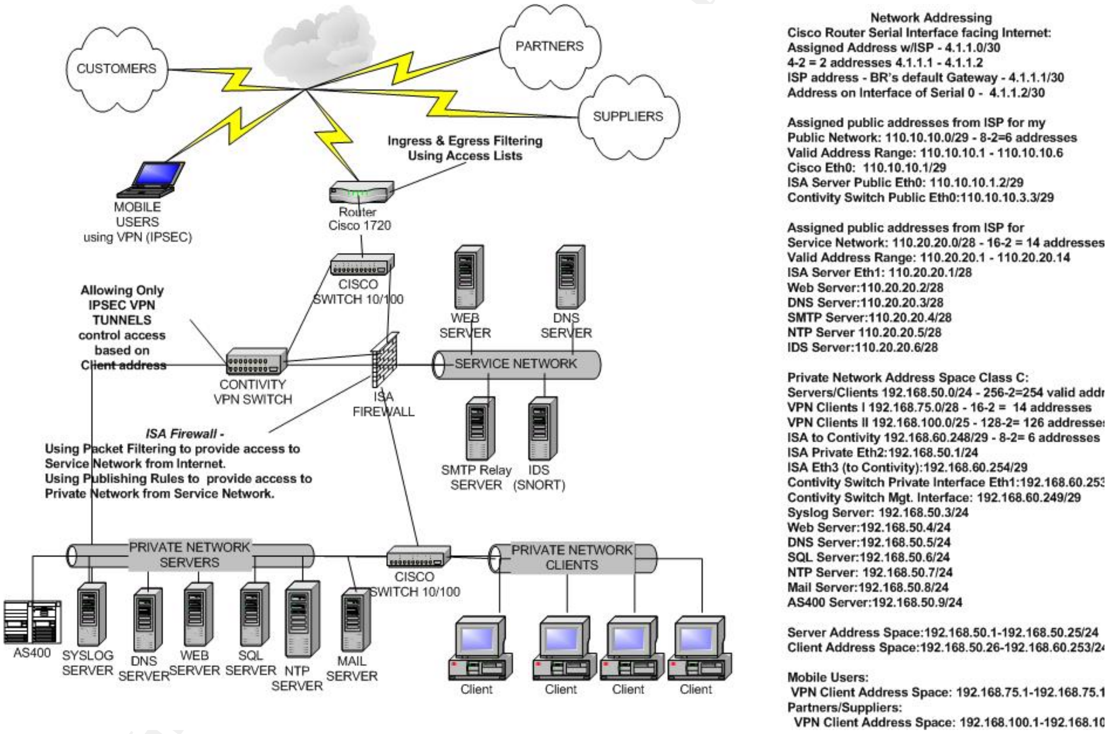
(16)



Assignment 4: Design Under Fire (25 Points)

Chosen Practical

The Practical that will be used is that is that of Lloyd Ardoin: http://www.giac.org/practical/Lloyd_Ardoin_GCFW.zip. This practical was chosen due to the fact that it also includes the Microsoft ISA Server as part of the security design.



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 addr
VPN Clients I 192.168.75.0/28 - 16-2 = 14 addresses
VPN Clients II 192.168.100.0/25 - 128-2= 126 addresse
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 Eth1:192.168.60.25
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:192.168.50.26-192.168.60.253/2

Mobile Users:
VPN Client Address Space: 192.168.75.1-192.168.75.1
Partners/Suppliers:
VPN Client Address Space: 192.168.100.1-192.168.10

The main firewall in the design is the Microsoft ISA Server for Windows 2000 Not many attacks have been identified, so the system will be checked for those listed below that are specific to ISA server and to the Windows 2000 OS.

Firewall Attack

Vulnerability

The initial vulnerability that will be checked for is identified in the following security bulletin from Microsoft: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-021.asp

Microsoft Security Bulletin MS01-021

Print

Web Request Can Cause Access Violation in ISA Server Web Proxy Service

Originally posted: *April 16, 2001*

Summary

Who should read this bulletin: System administrators using Microsoft® ISA Server 2000.

Impact of vulnerability: Denial of service

Recommendation: System administrators who have enabled the ISA Server Web Publishing feature should apply the patch immediately. Administrators who have not enabled the feature should consider applying the patch.

Affected Software:

- Microsoft ISA Server 2000

Patch availability

Download locations for this patch

- Microsoft ISA Server 2000: http://download.microsoft.com/download/ISAServer2000/webproxy/Q295279/NT5/EN-US/isahf63.exe

Note: This patch has been superseded by the one provided in Microsoft Security Bulletin MS01-045.

Other information:

Acknowledgments

Microsoft thanks Dr. Richard Reiner, Graham Wiseman, Matthew Siemens, and

Kent Nicolson of FSC Internet Corp. / SecureXpert Labs (http://www.fscinternet.com / http://www.securexpert.com) for reporting this issue to us and working with us to protect customers.

Support:

- Microsoft Knowledge Base article Q295279 discusses this issue and will be available approximately 24 hours after the release of this bulletin. Knowledge Base articles can be found on the Microsoft Online Support web site.
- Technical support is available from Microsoft Product Support Services. There is no charge for support calls associated with security patches.

Security Resources: The Microsoft TechNet Security Web Site provides additional information about security in Microsoft products.

Disclaimer:

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions:

- V1.0 (April 16, 2001): Bulletin Created.
- V1.1 (April 17, 2001): Bulletin updated to address the possibility that an external attacker could exploit the vulnerability via a web page or HTML e-mail.
- V1.2 (August 21, 2001): Patch Availability section updated to advise that the

patch provided here has been superseded.

Attack Design

- To increase the success of mounting an attack on Lloyd Ardoins GIAC design, some preliminary information can be gathered:
    - The type of Firewall
    - How long have they had it?
    - IP addresses
    - Who maintains the Firewall
    - Are they trained on the product?
- Attempt social engineering to gather information.
- The next thing will be to research available vulnerabilities for the firewall they are using.
- Check with ARIN to find the Addresses assigned to GIAC
- Fingerprint GIAC if needed to gather FW information
- Select a time for the attack
- Launch attack.

The Attack

To initiate the social engineering aspect of the attack, several ideas were tossed around. One method would be to call as a Firewall company and try to sell GIAC the "latest and greatest" in hopes that they would identify their current system. Another was the "polling" technique. In other words, pretending to be from a magazine or periodical and then directly polling or "asking" what equipment and firewall, etc were in use. A third option was to call as a training provider and offer firewall training to see what information could be gathered.
The Firewall company method was chosen, but after repeated attempts it was obvious that the operator was not going to forward the call. After a week, the training company option was tried and was successful. The operator, who also handled travel requests, had noticed the systems department were getting Microsoft training on ISA Server. After being forwarded to voicemail this part of the plan was complete.
A quick check of whois at the ARIN website:
http://www.arin.net/whois/index.html reveals the IP address ranges used by GIAC
Friday night will be the time the attack takes place. This will hopefully catch the staff of GIAC at a time when they aren't able to respond easily. If the system notifies them by pager, they will have to respond in some way

the system notifies them by pager, they will have to respond in some way that will not be a quick as someone on-site. If someone is on-site then we'll hopefully catch them busy with other tasks.
A scan of the machine will probably trigger an alert, so we will have to act quickly.
Keying the IP Address into the Web Browser does show that the GIAC web site comes up. (So far, so good)
At 11:00 NMAP is used, and the IP address is fingerprinted. As expected we are only able to determine that the machine may be a Windows box. (still okay, but we may have alerted them)
The first attempt is against the firewall itself and will cause a denial of service. The vulnerability is documented at the following locations:
NIST ICAT Metabase:
http://icat.nist.gov/icat.cfm?cvename=CVE-2001-0239

The Security Focus Archive and Bugtraq:
http://www.securityfocus.com/archive/1/176912
http://www.securityfocus.com/archive/1/179986

The Microsoft Technet bulletin:
http://www.microsoft.com/technet/security/bulletin/MS01-021.asp

Apparently, the web proxy service can be shutdown on the ISA Server by sending a valid http request that contains an extremely long pathname component.

The method discussed in the Security Focus document uses a "C" program which they supply, and a Linux computer.

For this attack, A Linux computer has been setup, the program has been compiled, and a bogus account has been set up through one of the free internet service providers. The program is launched.

By 11:30 PM, we are no longer receiving responses from the GIAC website. This should mean that the web proxy service W3PROXY has had a heap overflow and terminated. The ISA Server will need to be rebooted, or the Proxy service restarted to bring it back on line.

We try again for the next 15 minutes and find that the service is still not up. By 12:00 AM the service is running again (GIAC must have someone on the late shift that brought the server back up).

We don't want to give away too much, so this vulnerability is tucked away to try again later when it will have a serious affect on customer access to GIAC.

Countermeasures

Hopefully, our foray will simply be consider a glitch and will not be recognized as an attack. Microsoft offers a patch for this vulnerability:
http://download.microsoft.com/download/ISAServer2000/webproxy/Q295279/NT5/EN-US/isahf63.exe
and we don't want it to be applied before we have a chance to do our damage.

Denial of Service Attack

There exists a DOS attack fro Cisco routers running IOS version 12.0 to version 12.2.1 (CAN –2001-1097 http://icat.nist.gov/icat.cfm?cvename=CAN-2001-1097). It makes use of a flood of UDP packets that are sent to the device and they are supposed to consume the CPU cycles. Cisco was not able to duplicate the problem and recommends no corrective action.

The Attack

Prior to the attack, a bogus email was sent to several hundred users of the local cable service stating "…and this is a critical patch that is required for continued service…". It contained instructions on installing the "patch" that was really a trojan. After approximately fifty (50) of the machines were compromised, they proper program was uploaded and triggered to generate numerous UDP packets to GIAC.
The result: Response time slowed at GIAC, but the Cisco router did not fail. Depending on the alert configuration at GIAC, they will see an unusual increase in the load, and possibly detect this as an attack on the chosen port.

Countermeasures

None. This attack does not seem to have an affect.
The recommendation for GIAC would be to make sure the IOS is at the most current release, and to move to a more robust router.

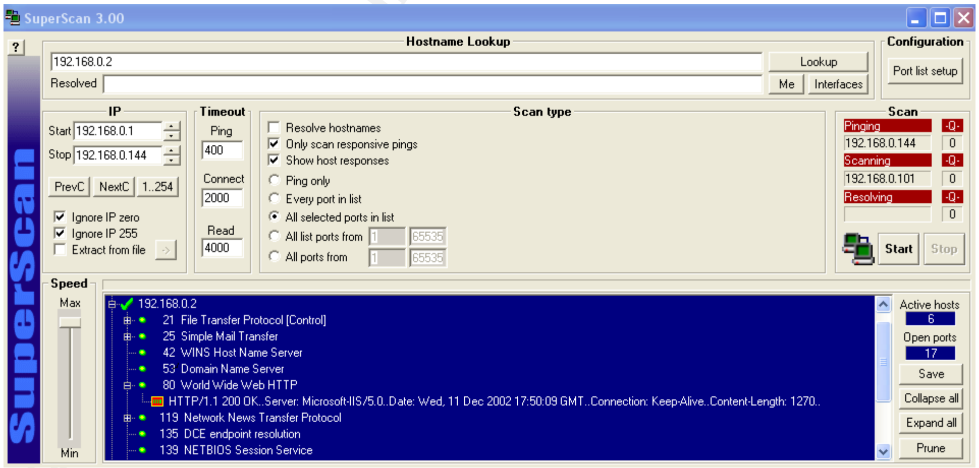
Assignment 4: Design Under Fire
----
(7)

Internal System Attack

The first attempt is to send a Unicode exploit to the Web Server.
The Microsoft ISA Server will redirect the web requests to the internal server. (It does not doing any checking to see if we are making a valid request or trying to exploit a weakness)
With GIAC appearing to be a Microsoft shop, we are going to investigate whether IIS is in use. We suspect this to be the case. If the attack is successful, we will be able to gain access to directories other than the \inetpub directory, and then attempt to transfer those files. (The internet publishing directory of the IIS5.0 web server)

Target Selection

As with a lot of attacks, the web server will be the target. The paper did not indicate the type of Web server in use, so SuperScan will be used to identify the type and version in use. (Figure A1)



192.168.0.2
Resolved
Start 192.168.0.1
Stop 192.168.0.144
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file
Ping 400
Connect 2000
Read 4000
☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535
Pinging -Q-
192.168.0.144 0
Scanning -Q-
192.168.0.101 0
Resolving -Q-
0
Active hosts 6
Open ports 17

```
192.168.0.2
   21  File Transfer Protocol [Control]
   25  Simple Mail Transfer
   42  WINS Host Name Server
   53  Domain Name Server
   80  World Wide Web HTTP
      HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Date: Wed, 11 Dec 2002 17:50:09 GMT..Connection: Keep-Alive..Content-Length: 1270..
   119  Network News Transfer Protocol
   135  DCE endpoint resolution
   139  NETBIOS Session Service
```

Figure A1 (Determining the Web Server Type)

< Note> This is a representative scan of an IIS Server showing the typical response that can be expected. <End Note>

The Attack

As expected this is an IIS 5.0 server, and the attack will be attempted using information gathered from the ICAT Metabase, and the Security Focus Archives for CVE –2000-0884 (A Unicode exploit):

http://icat.nist.gov/icat.cfm?cvename=CVE-2000-0884

http://online.securityfocus.com/bid/1806/info/

IIS 5.0 is vulnerable to what is called a directory transversal exploit if the “\” character is replaced by the equivalent “Unicode” character. This would allow access to all the directories that are accessible by the IUSR_Machine name account (the account used for IIS to perform it’s functions). The IUSR_Machine name account has access equivalent to the Everyone and Users groups by default, and therefore has the ability to read, write and delete files to which these groups have access.

There are several exploits listed on the Security Focus website, and with the compiled code, we attempt to access the Web server.

Our attempt fails, and after trying with server of the other listed exploits we determine that the Web server is probably patched. The Code Blue Worm uses this exploit, and the Microsoft patch has probably been applied.

Microsoft Patch Q269862
http://download.microsoft.com/download/win2000platform/Patch/q269862/NT5/EN-US/Q269862_W2K_SP2_x86_en.EXE

The team at GIAC may have used the Microsoft URLSCAN tool to control IIS settings and lockdown access to the server.

http://download.microsoft.com/download/iis50/Utility/1.0/NT45XP/EN-US/UrlScan.exe

This attempt failed, and looking at the ISA Server and Border Router configurations, we would not have been able to make use of some of the exploit’s features. These included sending commands to make use of tftp to transfer files, or using Samba/NetBIOS to make connections. The firewall blocks the NetBIOS ports (135-139), and the ISA server is not set up to allow tftp traffic from the Web Server.
We would only have been able to make use of transferred accomplished through using HTTP.

Good Job GIAC!

Appendices: (1)

Appendix A
References

ISA Server

Configuring ISA Server for inbound VPN
http://www.isaserver.org/pages/article.asp?id=232

Configuring Intrusion Detection in ISA Server
http://www.isaserver.org/pages/article.asp?id=343

VPN Access in a back to back ISA configuration
http://www.isaserver.org/pages/article.asp?id=212

ISA Server Service Pack 1
http://www.microsoft.com/isaserver/downloads/sp1.asp

ISA Server 2000 Security Patch for Unchecked Buffer in Gopher Protocol Handler
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-027.asp

ISA Server 2000 Hotfix for Rules Engine and Potential Web Proxy Service Crash
http://www.microsoft.com/downloads/Release.asp?ReleaseID=38362

ISA Server 2000 Security Patch for Web Proxy Service and H.323 ASN DLL
http://www.microsoft.com/technet/security/bulletin/MS01-045.asp

ISA Server 2000 Security Patch for Web Proxy Service
http://www.microsoft.com/technet/security/bulletin/MS01-021.asp

ISA Server Security Checklist by Dr. Thomas W. Shinder
http://www.tacteam.net/isaserverorg/isachecklist.htm

Excellent GCFW Practical by Lloyd Ardoin involving the Microsoft ISA Server
http://www.giac.org/practical/Lloyd_Ardoin_GCFW.zip

Appendices (2)

Cisco

Cisco's Web Site
http://www.cisco.com

Cisco's Solution Finder
http://www.cisco.com/pcgi-bin/finder/msbsearch.pl

Cisco notes on configuring DSL modules in a 2600
http://www.cisco.com/en/US/products/hw/routers/ps259/products_module_installation_guide_chapter09186a008007cb65.html

Cisco TCP and UDP Small Servers
http://www.cisco.com/warp/public/66/23.html

Sybex - CCNA Study Guide – Todd Lammle – ISBN 0-7821-4167-6

Cisco Press - ICND – Edited by Steve McQuerry – ISBN 1-57870-111-2

Exchange 2000

Exchange 2000 Service Pack 1
http://search.microsoft.com/gomsuri.asp?n=1&c=rp_BestBets&siteid=us/security&target=http://www.microsoft.com/exchange/downloads/2000/sp2.asp

IP

Internet Protocol Version 4 Address Space
http://www.iana.org/assignments/ipv4-address-space

Ipv4 Address Space Allocations
http://www.mentovai.com/network/ipv4-allocation.html

Microsoft

Microsoft Security Bulletin MS01-021
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-021.asp

Microsoft Security Tools page
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp

Custom Security Template information
http://www.giac.org/practical/Robert_Alley_GCWN.doc

Misc

ICAT Metabase
http://icat.nist.gov/icat.cfm

Appendix B
Border Router Configuration (startup-config)

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no ip http server
no service udp-small-servers
no service tcp-small-servers
!
hostname GIACRTR
!
enable secret 5 $1$n85C$dN1cMKxCytHoTDFCva/Eh/
enable password 7 140413050A162B25
!
memory-size iomem 20
ip subnet-zero
!
!
!
 !
 !
 !
 interface FastEthernet0/0
 ip address 192.168.200.5 255.255.255.252
 no ip directed-broadcast
```

Appendices (4)

```
 no ip mroute-cache
!
interface Serial0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial0/0.1
 no ip directed-broadcast
 no ip mroute-cache
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial0/2
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
interface Serial0/3
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
!
 interface ATM0/0
 ip address 209.165.201.1 255.255.255.224
 dsl operating-mode gshdsl symmetric annex A
 dsl equipment-type cpe
 dsl linerate auto
 load-interval 30
 atm vc-per-vp 256
 no atm ilmi-keepalive
 pvc 10/100
 vbr-rt 672 672 512
 encapsulation aal2
!
```

Appendices (5)

```
 pvc 10/200
 protocol ip 209.165.202.159 broadcast
 encapsulation aal5snap
 !
 no fair-queue
 !
ip classless
no ip http server
!
access-list 10 deny   10.0.0.0 0.255.255.255
access-list 10 deny   172.16.0.0 0.15.255.255
access-list 10 deny   192.168.0.0 0.0.255.255
access-list 10 deny   169.254.0.0 0.0.255.255
access-list 10 deny   224.0.0.0 31.255.255.255
access-list 10 deny   127.0.0.0 0.255.255.255
access-list 10 deny   0.0.0.0 0.255.255.255
access-list 10 deny   1.0.0.0 0.255.255.255
access-list 10 deny   2.0.0.0 0.255.255.255
access-list 10 deny   5.0.0.0 0.255.255.255
access-list 10 deny   7.0.0.0 0.255.255.255
access-list 10 deny   23.0.0.0 0.255.255.255
access-list 10 deny   27.0.0.0 0.255.255.255
access-list 10 deny   31.0.0.0 0.255.255.255
access-list 10 deny   36.0.0.0 0.255.255.255
access-list 10 deny   37.0.0.0 0.255.255.255
access-list 10 deny   39.0.0.0 0.255.255.255
access-list 10 deny   41.0.0.0 0.255.255.255
access-list 10 deny   42.0.0.0 0.255.255.255
access-list 10 deny   49.0.0.0 0.255.255.255
access-list 10 deny   50.0.0.0 0.255.255.255
access-list 10 deny   58.0.0.0 0.255.255.255
access-list 10 deny   59.0.0.0 0.255.255.255
access-list 10 deny   60.0.0.0 0.255.255.255
access-list 10 deny   70.0.0.0 0.255.255.255
access-list 10 deny   71.0.0.0 0.255.255.255
access-list 10 deny   72.0.0.0 7.255.255.255
access-list 10 deny   64.0.0.0 31.255.255.255
access-list 10 deny   197.0.0.0 0.255.255.255
access-list 10 deny   201.0.0.0 0.255.255.255
access-list 10 deny   222.0.0.0 0.255.255.255
access-list 10 deny   223.0.0.0 0.255.255.255
access-list 10 deny   240.0.0.0 15.255.255.255
```

```
access-list 10 permit any
access-list 20 permit 192.168.0.0 0.0.0.255
access-list 110 deny   udp any any log
access-list 110 deny   ip any any log
access-list 110 permit ip 192.168.0.0 0.0.0.255 any
access-list 110 permit ip 192.168.100.0 0.0.0.255 any
access-list 110 permit ip 192.168.200.0 0.0.0.255 any

no cdp run
banner motd _Access to this device restricted.
Connectivity by proper authority only, Any attempted
mis-use or abuse will
be report to the proper authorities_
!
line con 0
 exec-timeout 0 0
 password 7 06150E2F4A5C0817
 logging synchronous
 login
 transport input none
line aux 0
line vty 0 4
 password 7 110A1016141D
 login
!
end
```

Appendix C
Windows 2000/NT Hardening

There are many guides available for hardening of Windows 2000 computers. The SANS Institute, Microsoft, government agencies, and various security organizations publish guidelines and tools.
http://nsa1.www.conxion.com/
http://www.systemexperts.com/win2k/HardenWin2K.html
http://security.microsoft.com

The basic first steps are:
- Disk partitions are formatted with NTFS
- Disable unneeded services
- Disable or rename guest, account
- Rename administrator account

Appendices (7)

- Set NTFS permissions on files and directories
- Install Virus protection
- Install service packs
- Install Hotfixes
- Configure Auditing and increase log file sizes
- Configure password policies for 8 character, complex passwords

Local Policy Settings and Services for Firewalls and W2K Servers on the Perimeter Network

Listed below a checklist, recommended settings, and options for Local policy, Services, and directories:

1. No shared passwords for user or administrator accounts
2. Unique User IDs and passwords are used for all accounts
3. Unique passwords are used for each separate account
 (including Administrator / Guest/ and all user accounts)
4. The Guest account is disabled / Guest password set
5. All default accounts have been removed or passwords changed (guest, Administrator)
6. Privileged/Power Users are kept to a minimum
7. The screen saver has been enabled for 10-minute delay and password protected
8. The pre-logon message is displayed stating company policy on access

9. The Event Log for Security is set to not overwrite log entries, increase size to 2048
 (Control Panel/Administrative Tools/Event Viewer)
10. The following policies are set
 (Control Panel/Administrative Tools/Local Security Settings)

Account Policy:

Password Policy:

Enforce Password History: 10 Passwords remembered
Maximum Password Age: 180 days
Minimum Password Age: 2 days
Minimum Password Length: 8 Characters
Password must meet complexity requirements (disabled)
Store Passwords using Reversible Encryption (disabled)

Account Lockout Policy

Account lockout duration: Must be reset by system admin (0)
Account Lockout Threshold: 5 invalid attempts
Reset Lockout count after: 1440 minutes

Audit Policy:

Account logon events:	Success and Failure
Account management:	Failure
Logon events:	Success and Failure
Policy Change	Failure
Privileged Use	Success and Failure

Appendices (8)

Access this Computer from the Network: Limit to Administrators,
Act as part of the Operating System: None
Add Workstations to Domain: None
Backup Files and Directories: Limit to Administrators
Bypass Transverse Checking: Limit to Administrators
Change System Time: Limit to Administrators
Create a Pagefile: Limit to Administrators
Create a Profile: None

Create Token Objects: None
Create Permanent Share Objects: None
Debug Programs: Limit to Administrators
Deny Access to the Computer from the Network: None
Deny Logon as a Batch Job: None
Deny Logon as a Service: None
Deny Logon Locally: None
Force Shutdown from a Remote System: Limit to Administrator
Generate Security Audits: Limit to Administrators
Increase Scheduling Priority: Limit to Administrators
Load and Unload Device Drivers: Limit to Administrator
Logon as a Batch Job: None
Logon as a Service: None
Log on Locally: Limit to Administrator, Administrator group
Manage Auditing and Security Logs: Limit to Administrators
Modify Firmware Environment Values: Limit to Administrators
Profile system performance: None
Replace Process Level Token: None
Restore Files and Directories: Limit to Administrators
Shut down the system: Limit to Administrators, User
Take Ownership of Files and other objects: Limit to Administrators

SECURITY OPTIONS

Accounts: Administrator account status: Enabled
Accounts: Guest account status: Disabled
Accounts: Limit local account use of blank passwords to console logon only: Enabled
Devices: Restrict CD-ROM access to locally logged-on user only: Enabled
Devices: Restrict floppy access to locally logged-on user only: Enabled
Interactive logon: Number of previous logons to cache (in case domain controller is not available): 0 logons
Microsoft network server: Amount of idle time required before suspending session: 10 minutes
Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication: Disabled
Network security: LAN Manager authentication level: Send LM & NTLM-Use NTLMv2 security if Negotiated
Shutdown: Allow system to be shut down without having to log on: Disabled

Appendices (9)

Shutdown: Clear virtual memory pagefile: Enabled

11. Is the NTFS file system used?
12. Add "System", "Services" and any User IDs that need access to C:\. (Properties Box) Remove "Authenicated Users"
13. Is the Hard Drive set for **Not Shared**
14. Have the OS2 and Posix files/ directories been removed?
    - To remove the OS/2 and Posix subsystems the following files should be removed:
      %System directory%\system32\dllcache
      Os2.exe
      Os2ss.exe
      Os2srv.exe
    - **NOTE:** W2K has a facility called the System File Checker to detect changes to certain system files in the %system directory%. It will automatically replace those files with backup copies from the \dllcache directory.

      %System directory%\system32
      Psxss.exe
      Posix.exe
      Psxdll.dll
    - All files in the \os2 folder, with the exception of the DLL folder and its contents.

15. A security scan has been run Y/N
16. BIOS password is set if available

SERVICES

Alerter Service	Notifies computers and users of administrative alerts	Manual	
Application Management	Provides Software installation services	Manual	
Automatic Updates	Enables the download and installation of critical Windows updates	Manual	
Clipbook	Supports Clipbook viewer	Disable	
COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Started	Manual
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Started	Automatic
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Disable	
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Started	Manual
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.	Manual	
DNS Client	Resolves and caches Domain Name System (DNS) names.	Started	Automatic
Event Log	Logs event messages issued by programs and Windows.	Started	Automatic

Help and Support	Allows Help and Support Center to run on this computer		Disable
Indexing Service	Provides rapid access to files through flexible querying		Disable
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.		Disable
IPSEC Services	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Started	Automatic
Logical Disk Manager	Logical Disk Manager Watchdog Service	Started	Manual
Logical Disk Manager Administrative Service	Administrative service for disk management requests		Manual
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.		Manual
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.	Started	Automatic
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.		Disable
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connection	Started	Manual
Network DDE	Provides network transport and security for dynamic data exchange (DDE).		Manual
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE		Manual
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.		Manual
Performance Logs and Alerts	Configures performance logs and alerts.		Manual
Portable Media Serial Number	Retrieves the serial number of any portable music player connected to your computer		Disable
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Started	Automatic
Print Spooler	Loads files to memory for later printing.	Started	Automatic
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.	Started	Automatic
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.		Disable
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.		Manual
Remote Access Connection Manager	Creates a network connection.	Started	Automatic

Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Started	Automatic
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.	Manual	
Remote Registry Service	Allows remote registry manipulation.	Disable	
Removable Storage	Manages removable media, drives, and libraries.	Started	Automatic
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.	Disabled	
Security Accounts Manager	Stores security information for local user accounts.	Started	Automatic
Server	Provides RPC support and file, print, and named pipe sharing.	Started	Manual
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.	Manual	
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.	Manual	
SSDP Discovery Service	Enables discovery of UPnP devices on your home network	Disable	
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.	Started	Automatic
Task Scheduler	Enables a program to run at a designated time.	Manual	
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Started	Automatic
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN,	Disable	
Telnet (Client Setting)	Allows a remote user to log on to the system and run console programs using the command line.	Disable	
Terminal Services	Allows multiple users to be connected interactively to a machine as well as the display of desktops and applications to remote computers	Disable	
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.	Automatic	
Web Client	Enables Windows-based programs to create, access, and modify Internet-based files	Disable	
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files.	Manual	
Windows Management Instrumentation	Provides system management information.	Started	Manual
Windows Management Instrumentation Driver Extensions	Provides systems management information to		

	and from drivers.	Started	Automatic
Windows Time	Sets the computer clock.	Started	Manual
Wireless Zero Configuration	Provides automatic configuration for the 802.11 adapters	Disable	
Workstation	Provides network connections and communications.	Started	Automatic

HIDDEN SHARES

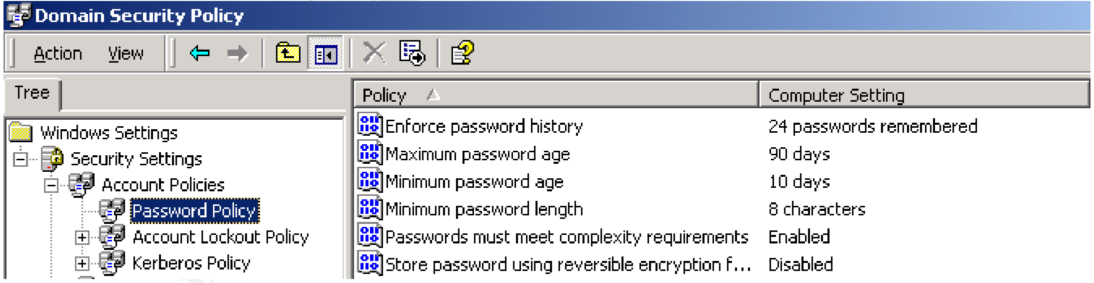
Remove Hidden Administrative Shares (C$, D$, etc.)….Add a value named "AutoShareWks" with REG_DWORD value of 0 to the key.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\

Appendix D
Hardening of the Active Directory Domain (Custom Config)

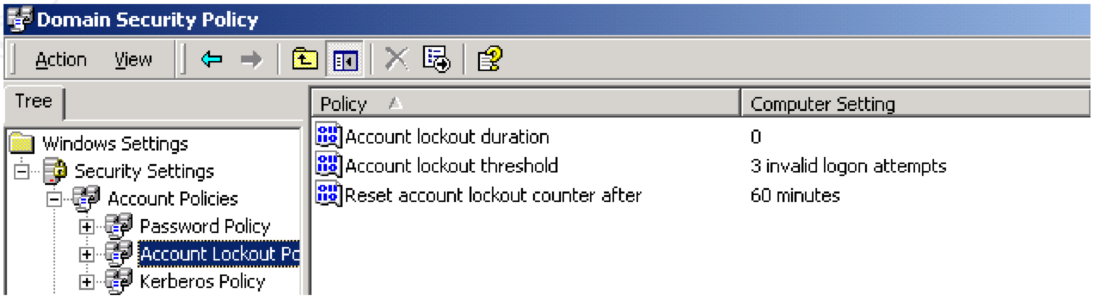
Default Domain Policy on the Internal Network

This appendix covers some of the Active Directory settings that can be used to tighten up security on the Internal Network. By controlling these at the domain level, any settings that get changed from the norm will be set back to the desired values at periodic intervals.



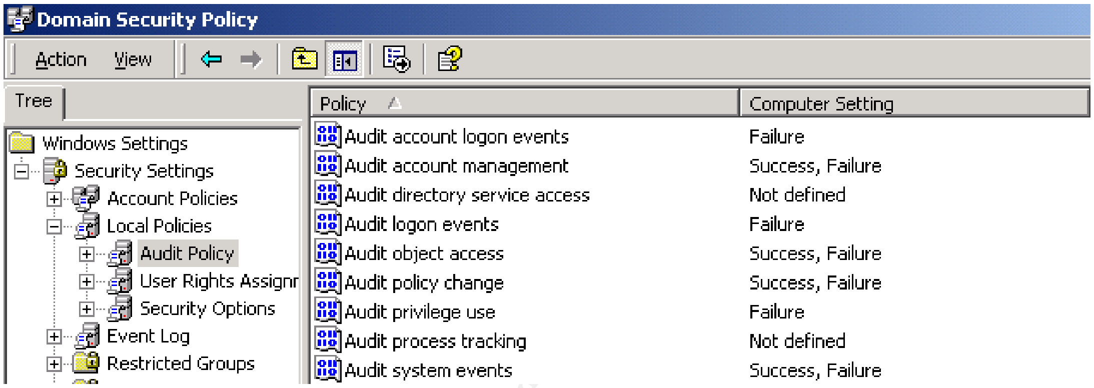
Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	10 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption f…	Disabled

In the Default Domain Policy, the **Password Policy** settings are configured to be strict. A setting of ninety days (90) is used for the Maximum Password Age to help reduce the chance that people would write their password down due to it changing frequently.



Policy	Computer Setting
Account lockout duration	0
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	60 minutes

The **Account Lockout Policy** is set so that the account will have to be reactivated by a member of the systems support staff. Automatic reset of the accounts has effectively been disabled.



Policy	Computer Setting
Audit account logon events	Failure
Audit account management	Success, Failure
Audit directory service access	Not defined
Audit logon events	Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	Not defined
Audit system events	Success, Failure

The **Audit Policy** is set to monitor important events but not overwhelm the staff.

<u>Audit Account Logon Events:</u>

Set to log when there is a failure logging into a user account.

<u>Audit Account Management:</u>

Set to log both successful and failed attempts to change user account info.

<u>Audit Logon Events:</u>

Failure of service accounts and major application accounts is recorded with this setting. It is set for failures.

<u>Audit Object Access:</u>

Used to track access to Active Directory Objects. The object must have auditing turned on for the objects that access it.

<u>Audit Policy Change:</u>

This setting will produce log records when changes are made to policies, and other settings. Most notably to user accounts and security settings.

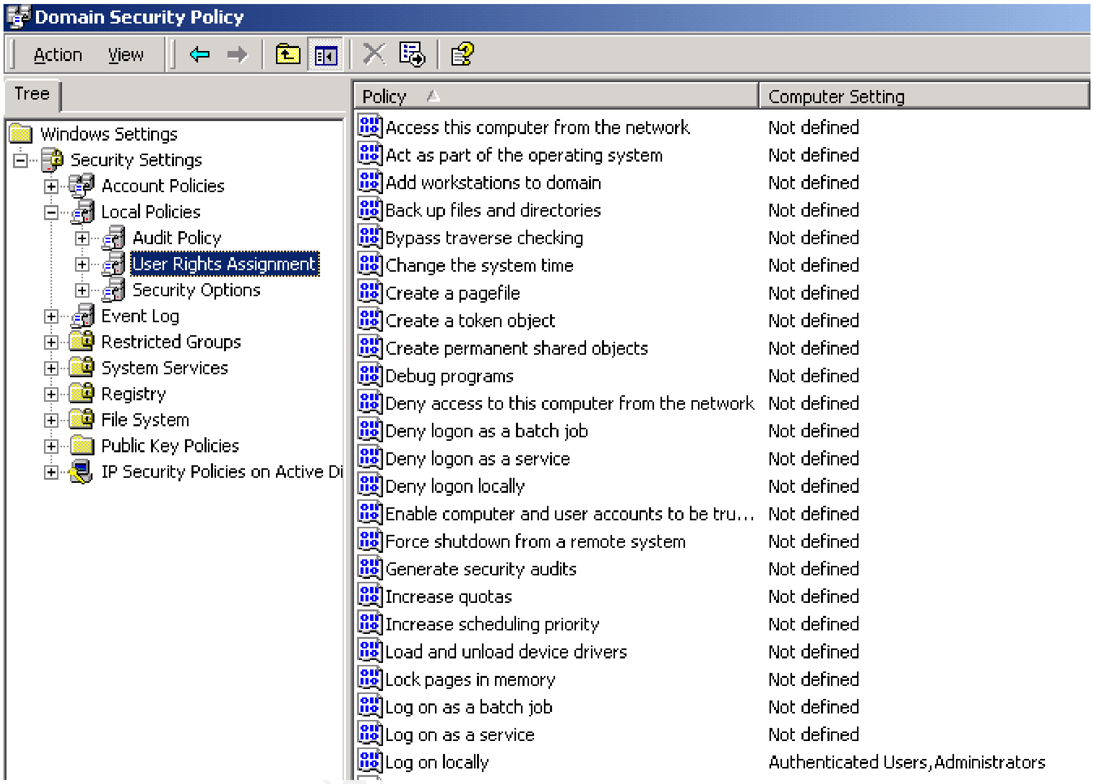
<u>Audit privilege Use:</u>

Will log events such as changes to the system time.

<u>Audit System Events:</u>

Tracks start up and shutdown of the computer, and other events that affect the whole system. Failure of these events will be tracked.

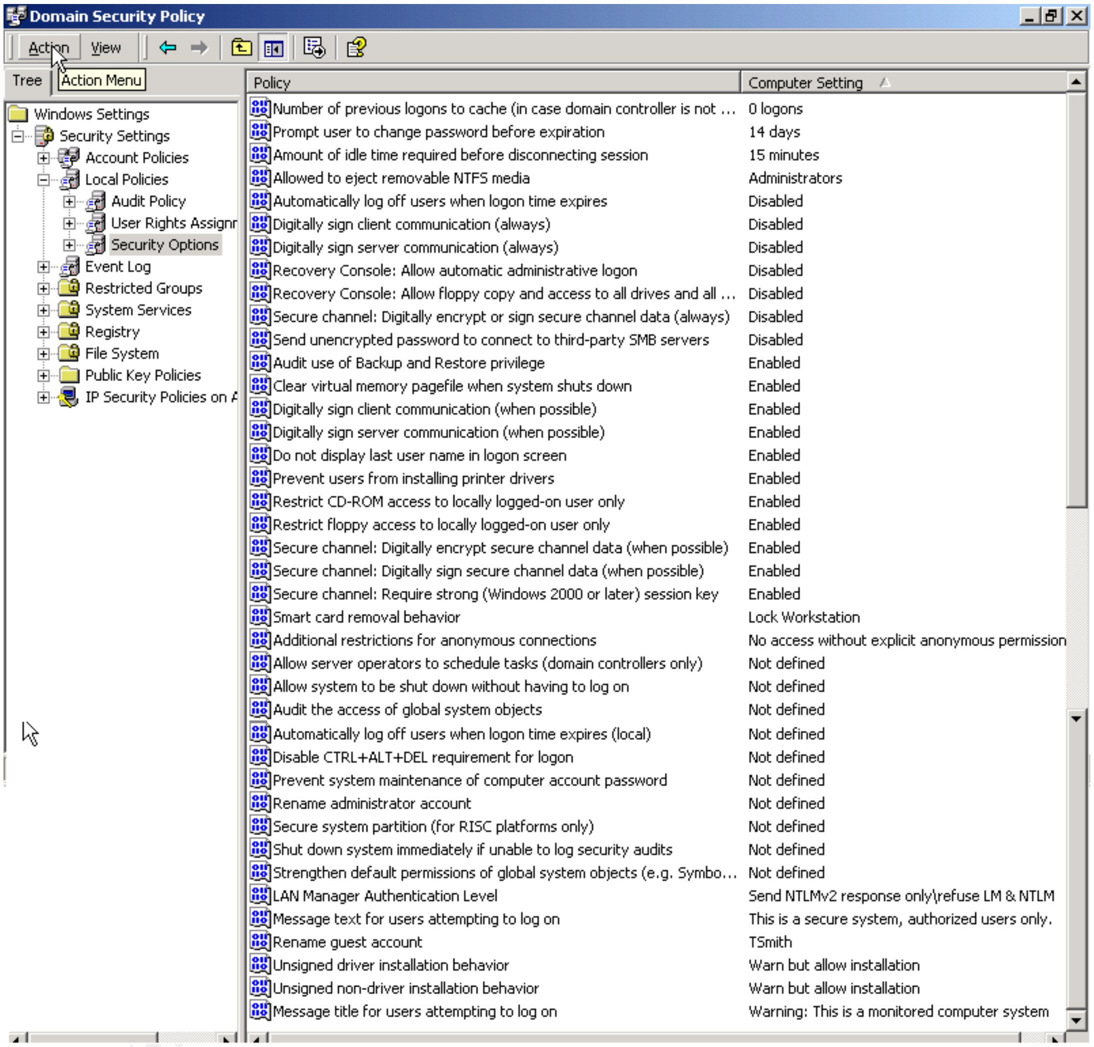
Appendices (14)



Policy	Computer Setting
Access this computer from the network	Not defined
Act as part of the operating system	Not defined
Add workstations to domain	Not defined
Back up files and directories	Not defined
Bypass traverse checking	Not defined
Change the system time	Not defined
Create a pagefile	Not defined
Create a token object	Not defined
Create permanent shared objects	Not defined
Debug programs	Not defined
Deny access to this computer from the network	Not defined
Deny logon as a batch job	Not defined
Deny logon as a service	Not defined
Deny logon locally	Not defined
Enable computer and user accounts to be tru...	Not defined
Force shutdown from a remote system	Not defined
Generate security audits	Not defined
Increase quotas	Not defined
Increase scheduling priority	Not defined
Load and unload device drivers	Not defined
Lock pages in memory	Not defined
Log on as a batch job	Not defined
Log on as a service	Not defined
Log on locally	Authenticated Users,Administrators

The only setting changed in User Rights Assignments is who is allowed to log on locally. It is set to allow only administrators and authenticated users.

This area left blank for formatting reasons



Policy	Computer Setting
Number of previous logons to cache (in case domain controller is not ...	0 logons
Prompt user to change password before expiration	14 days
Amount of idle time required before disconnecting session	15 minutes
Allowed to eject removable NTFS media	Administrators
Automatically log off users when logon time expires	Disabled
Digitally sign client communication (always)	Disabled
Digitally sign server communication (always)	Disabled
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all ...	Disabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Audit use of Backup and Restore privilege	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (when possible)	Enabled
Do not display last user name in logon screen	Enabled
Prevent users from installing printer drivers	Enabled
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Smart card removal behavior	Lock Workstation
Additional restrictions for anonymous connections	No access without explicit anonymous permission
Allow server operators to schedule tasks (domain controllers only)	Not defined
Allow system to be shut down without having to log on	Not defined
Audit the access of global system objects	Not defined
Automatically log off users when logon time expires (local)	Not defined
Disable CTRL+ALT+DEL requirement for logon	Not defined
Prevent system maintenance of computer account password	Not defined
Rename administrator account	Not defined
Secure system partition (for RISC platforms only)	Not defined
Shut down system immediately if unable to log security audits	Not defined
Strengthen default permissions of global system objects (e.g. Symbo...	Not defined
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	This is a secure system, authorized users only.
Rename guest account	TSmith
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation
Message title for users attempting to log on	Warning: This is a monitored computer system

In the area of Security Options, several items are changed from the default.

<u>Number of previous logons to cache:</u>

Set to 0. This forces authentication to a Domain Controller for access. If not set, a computer could be disconnected from the network after a user account has been disabled, and the user will still be able to logon.

<u>Prompt user to change password before expiration:</u>

Set to 14 days as courtesy to the user.

<u>Amount of idle time before disconnecting session:</u>

Set to 15 minutes

<u>Allowed to eject removable NTFS media:</u>

Administrators only

Automatically log off users when logon time expires:

Disabled

Digitally sign client communications (always):

Disabled. This setting may cause communications problems, so it is disabled.

Digitally Sign server communications (always):

Disabled. Same as above.

Recovery Console: allow Automatic administrative logon:

This is set to Disabled to force the use of a password to enter the Recovery Console.

Recovery Console: Allow floppy copy and access to all drives and…:

Disabled. This option would allow someone to copy files from non-W2000 system directories when they are in the Recovery Console.

Secure Channel: Digitally encrypt or sign secure channel data (always):

Disabled. This option would force all computers to connect to Domain Controllers with a secure channel.

Send unencrypted password to third-party SMB servers:

Disabled. This is to prevent non-Microsoft servers from receiving an unencrypted password.

Audit use of Backup and Restore privilege:

Enabled to track which users are backing up data that can be restored elsewhere.

Clear virtual memory pagefile when the system shuts down:

Enabled to prevent information from being retrieved from the pagefile if the harddisk is stolen.

Digitally sign client communication (when possible):

Enabled. This will allow secure communications when both sides support it, but still allow a connection when they don't.

Digitally sign server communications (when possible):

Enabled. Same as above.

Do not display last user name in logon screen:

Enabled. Although a determined individual could get logon names another way, this is less it could be done.

Prevent users from installing print drivers:

Enabled to prevent possible loading of Trojans

Restrict CD-ROM access to locally logged-on user only:

Enabled. Prevents sharing of the CD-ROM drive.

Restrict floppy access to locally logged-on user only:

Enabled. Prevents sharing of the floppy drive.

Secure Channel: Digitally encrypt secure channel data (when possible):

Enabled. To enhance secure communications when possible.

Secure Channel: Digitally sign secure channel data (when possible):

Enabled. Same as above.

Secure Channel: Require strong (Windows 2000 or later) session key:

Enabled. Same as above.

Smart Card removal behavior:

It is set to Lock Workstation, so that the key has to be present and in the reader for the computer to be used.

Additional restrictions for anonymous connections:

"No access without explicit anonymous permissions" is the option chosen. This option is to prevent the "null" user account from gaining access to information.

LAN Manager Authentication level:

This option is set to "Send NTLMv2 response only\refuse LM & NTLM" to ensure the higher level of protection from NTLMv2 is used.

Message text for users attempting to log in:

This is set to a message that informs the users that they are on a secure system, and that it is for authorized access only.

Rename guest account:

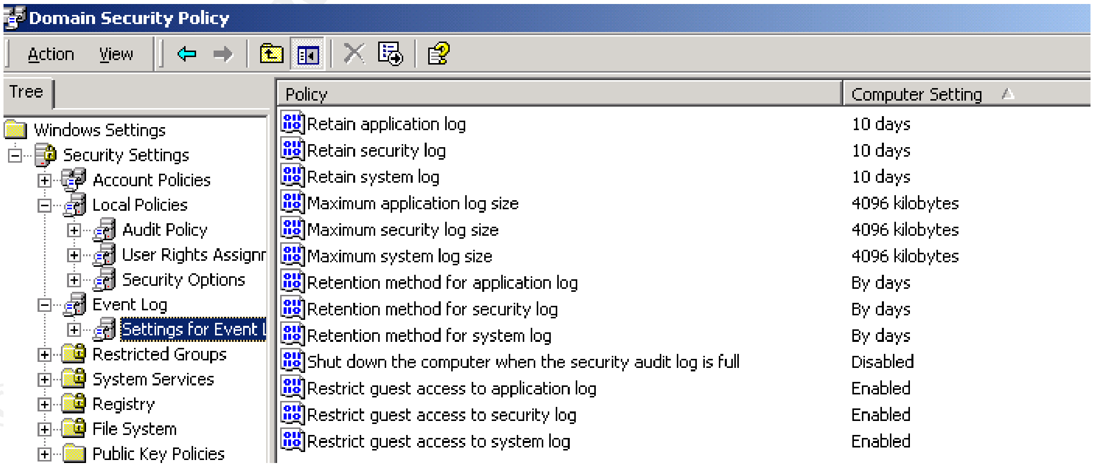
Any generic name that follows the naming rules.

Unsigned driver installation behavior/ Unsigned non-driver installation behavior:

Warn but allow a installation

Message title for users attempting to log on:

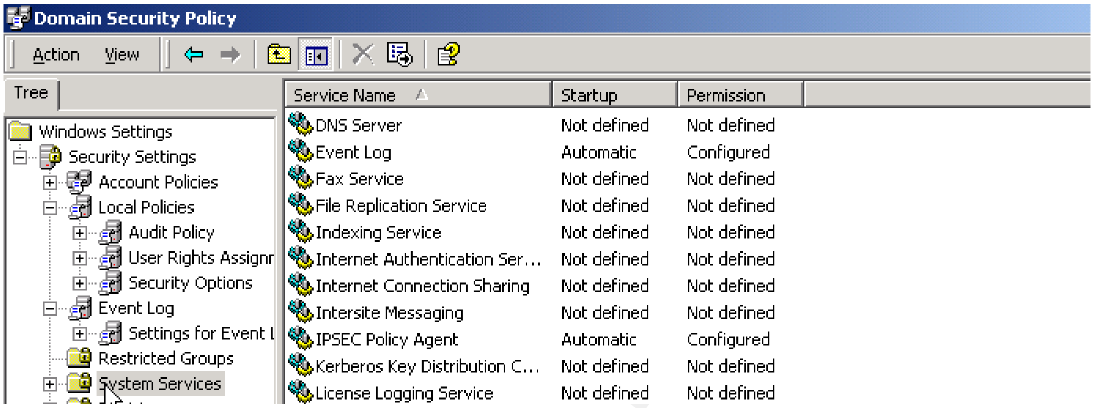
A warning that they are login onto a secured or monitored system.



Policy	Computer Setting
Retain application log	10 days
Retain security log	10 days
Retain system log	10 days
Maximum application log size	4096 kilobytes
Maximum security log size	4096 kilobytes
Maximum system log size	4096 kilobytes
Retention method for application log	By days
Retention method for security log	By days
Retention method for system log	By days
Shut down the computer when the security audit log is full	Disabled
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled

The Event Log settings are configured for each machine to have four (4) Megabytes of disk space and to overwrite on a ten (10) day schedule. The ten (10) day schedule is to allow more than a one (1) week overlap.

Appendices (18)



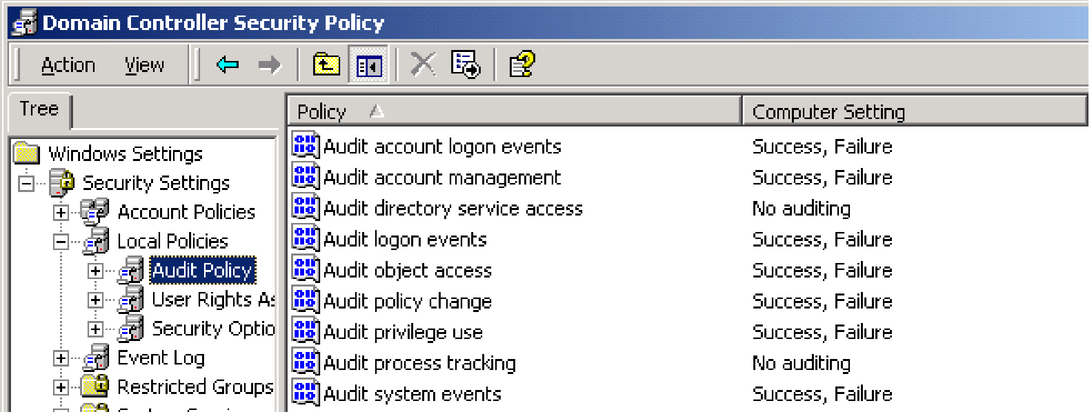
Service Name	Startup	Permission
DNS Server	Not defined	Not defined
Event Log	Automatic	Configured
Fax Service	Not defined	Not defined
File Replication Service	Not defined	Not defined
Indexing Service	Not defined	Not defined
Internet Authentication Ser...	Not defined	Not defined
Internet Connection Sharing	Not defined	Not defined
Intersite Messaging	Not defined	Not defined
IPSEC Policy Agent	Automatic	Configured
Kerberos Key Distribution C...	Not defined	Not defined
License Logging Service	Not defined	Not defined

The only System Services that are configured are the Event Log and the IPSEC Policy Agent. Both are configured to start automatically when the system starts. This is to ensure that logging and IP security cannot be inadvertently turned off.

An additional GPO is assigned to the domain for items not covered in the Default Domain Policy. (see Additional Group Policy below)

Group Policy for Domain Controllers on the Internal Network

Very few changes are made to the Group Policy for Domain Controllers over what is set for the Domain Policy. One thing to note is that by replicating the settings here, it is ensured that changes to the Domain Policy does not affect the security of the Domain Controllers. Listed below are the differences from Domain Policy.



Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

The Audit Policy is different in that Audit Account Logon Events, Audit Logon Events, and Audit Privileged Use are now all set for Success and Failure. The reasoning for this is that these settings:

Appendices (19)

Audit Account Logon Events:

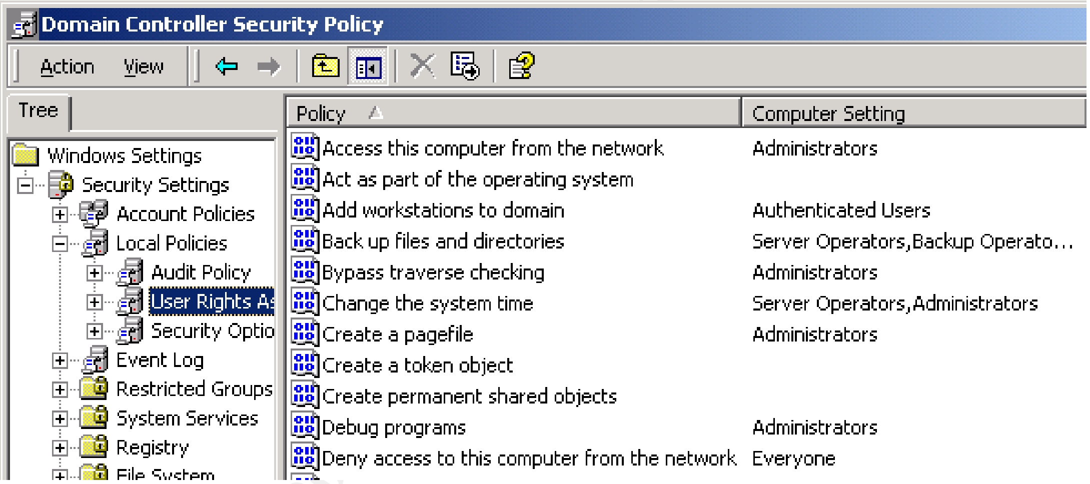
Will allow the tracking of successful logons to the servers.

Audit Logon Events:

The successful logon of services on the system. This may identify services that have accidentally or maliciously been turned on.

Audit Privileged Use:

The successful change of the system time is one example of what will now be tracked on the server.



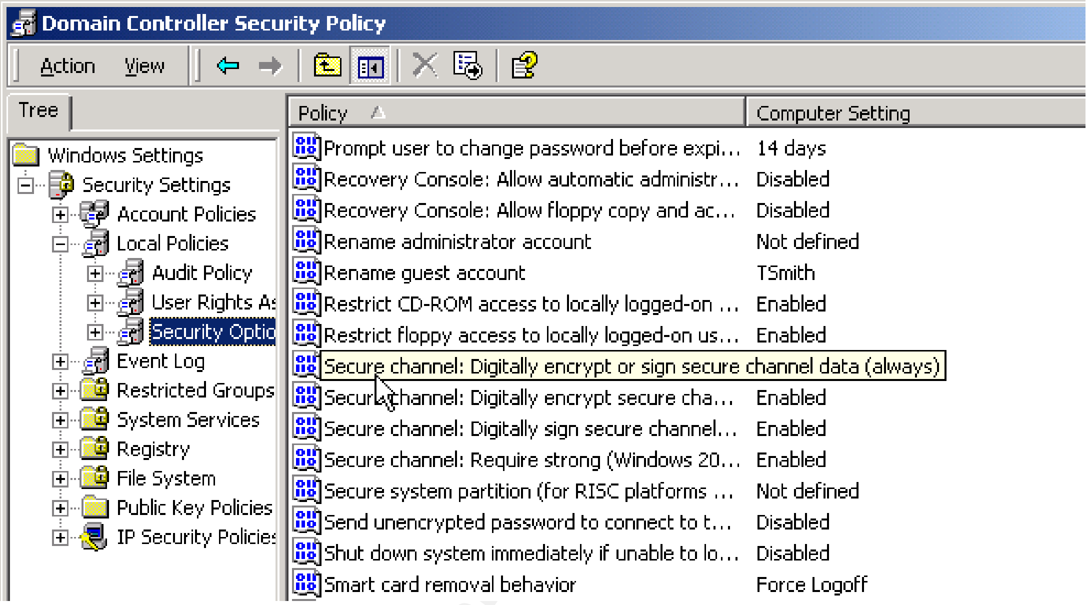
Policy	Computer Setting
Access this computer from the network	Administrators
Act as part of the operating system	
Add workstations to domain	Authenticated Users
Back up files and directories	Server Operators,Backup Operato...
Bypass traverse checking	Administrators
Change the system time	Server Operators,Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	Everyone

Multiple options are set in the User Rights Assignment page. The "basicdc.inf" security template is applied by default to "new" domain controllers and makes these configuration settings at the time of installation. An upgraded NT4 domain controller, on the other hand, does not have this template applied. This template was modified to include GIAC settings and is imported into the Domain Controller GPO so that it will be applied to all Domain Controllers. If a Domain Controller's settings get changed, they will be changed back when the GPO refreshes. There is only one setting changed from the default.

Access this computer from the network:

Set to Administrators. This option is set to allow only administrators to attach to the Domain Controllers.

Appendices (20)



Policy	Computer Setting
Prompt user to change password before expi...	14 days
Recovery Console: Allow automatic administr...	Disabled
Recovery Console: Allow floppy copy and ac...	Disabled
Rename administrator account	Not defined
Rename guest account	TSmith
Restrict CD-ROM access to locally logged-on ...	Enabled
Restrict floppy access to locally logged-on us...	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	
Secure channel: Digitally encrypt secure cha...	Enabled
Secure channel: Digitally sign secure channel...	Enabled
Secure channel: Require strong (Windows 20...	Enabled
Secure system partition (for RISC platforms ...	Not defined
Send unencrypted password to connect to t...	Disabled
Shut down system immediately if unable to lo...	Disabled
Smart card removal behavior	Force Logoff

In the Security Options page the main things of additional concern are: renaming the guest account, and smart card removal behavior. All other setting are set the same as those of the Domain Group Policy.

Rename guest account:

The guest account is renamed to a name that matches the current naming scheme, but is disabled and never used.

Smart card removal behavior:

Is set to "Force Logoff". The domain setting is to lock the computer, but the Domain Controllers are set to log the user off.

Additional Group Policy for the Domain:

There is an additional Group Policy assigned to the domain.
Listed below are the settings that are changed from the standard configuration.

Turn off Autoplay	Yes	This is to prevent CDs with
Delete cached copies of	Yes	
Run logon scripts	No	This option will force the logon

Appendices (21)

		in which they were intended
Run startup scripts visible	No	This is an "out of sight, out of mind" item, the users dos not need to see this happen
Run shutdown scripts visible	No	Same as above.
Don't display the Getting Started welcome screen at logon	Yes	This is a general cleanup item to keep users from being bothered with it.
Turn off background refresh of group policy	No	GPOs should continue to be updated on the default schedule of 90 min. (plus 0 to 30 min)
Scripts policy processing	Yes	To force scripts to be run
Security policy processing	Yes	To ensure security policy
IP Security policy processing	Yes	To ensure that IPSEC policies are enforced
Prohibit use of Internet Connection Sharing on DNS Domain Network	Yes	To prevent PCs from sharing the connection of one PC
Web based printing	No	Precaution to remove unneeded functionality and possible security problems
Prohibit new task creation	Yes	This option is turned off to stop someone from scheduling a malicious program to run
Do not keep history of recently opened documents	Yes	This is to make it harder for someone to visit an unattended machine and locate documents.
Clear history of recently opened documents	Yes	Same as above.
Remove user name from Start menu	Yes	Forces the user to enter a username at logon and reduces the ease at which someone can get user names
Hide "my network places" icon on desktop	No	Not a total deterrent, but it makes it harder for some user to browse the network
Password protect the screen saver	Yes	To secure the workstation when the user is absent
Screen saver timeout	10 min	Same as above
Prevent access to registry editing tools	Yes	Disables use of regedit and regedt32

Run legacy logon scripts hidden	Yes	Out of sight, out of mind
No "Computers near me" in My Network Places	Yes	Makes it harder to see other local computer in same workgroup or Domain
No "Entire network" in My Network Places	Yes	Cuts down on casual browsing of local network objects

Appendix E
Audit Checklist

_____The GIAC border. (the connection from the Internet to the Border Router)

_____Connectivity to, and vulnerabilities of the perimeter network (DMZ). This will be tested from the Internet side of the External Firewall.

_____Connectivity out of the Internal network to the Internet.

_____Direct scanning for ports and vulnerabilities of hosts in the Perimeter network. (from the perimeter network)

_____Direct scanning of hosts on the Internal network. (from the Internal network)
_____Test of External firewall rules (inbound)

_____Test of Internal firewall rules (inbound)

_____Test of Internal firewall rules (outbound)

_____Check firewall and IDS logs for proper logging

_____Capture VPN traffic to verify proper encryption

Appendices (23)

Appendix F:
Software and Sources

- Ethereal Version 0.9.8 – Free - General Packet analysis tool available for Windows and nix platforms. It can be used to examine live captured data or that from a file.
  http://www.ethereal.com
- SARA Version 4.1.2 – Free – Advanced Research Corporation - A nix based tool used to scan for vulnerabilities and for fingerprinting. It has reporting capabilities.
  http://www-arc.com/sara/
- SuperScan Version 3.00 – Free – Foundstone - One of the free tools available from Foundstone. A Windows based fast TCP port scanning utility.
  http://www.foundstone.com/knowledge/proddesc/superscan.html
- NMAP for Windows Version 1.2.3 – Free – SourceForge. A Windows based front end for NMAP. It is used for port scanning and fingerprinting. It also has spoofing capabilities.
  http://nmapwin.sourceforge.net/
- Snort for Windows Version 1.8.7 – Free – Sourcefire – Open source Network Intrusion detection and alerting system for Windows and nix based systems.
  http://www.snort.org
- Microsoft Internet Explorer – Part of the Windows Operating Systems.
- Microsoft ftp client (command prompt) – Part of the Windows Operating Systems