Global Information Assurance Certification Paper

Your assignment is to use resources on the Internet to research an important security issue. The security field changes rapidly, and often the most up-to-date information can only be found on the Internet. As such, it is critical that we as security professionals are able to use the Internet to find the information we need.

You MUST use at least FIVE cited sources, and at least THREE of them must be from the Internet. You may use additional sources, such as books, magazine articles, etc., if necessary.

Your research may cover an exploit or vulnerability, a particular technology, a tutorial or "how to", a legal or regulatory issue, and so on. In writing your paper, you should do more than just write a "book report" that repeats back what you have read in your sources. See below for the specific criteria by which your paper will be evaluated.

Author:Jack Green

Submitted to partially fulfill the requirements for the GSEC certification

Installing Microsoft's Internet Security and Acceleration Server (ISAS): Getting Started and Testing.

Thursday, November 01, 2001

Introduction:

Installing a test firewall environment is challenging and time consuming. It is also necessary for gaining a practical understanding of firewall concepts and practices. The purpose of this discussion is to mitigate some of these challenges by describing the process for setting up a simple, scalable and affordable firewall lab. Since Microsoft offers free trial versions of the software, the lab will use their products.

Additionally, I will briefly review resources that discuss security issues, resources for obtaining patches, and news/support groups for ISAS.

What is ISAS?

A Microsoft product new on the market, ISAS is one of the products included in the .NET family. In the interest of brevity, I won't list all the services. That being said, among its offerings are the following services:

- VPN
- Intrusion Detection
- NAT
- Bandwidth Allocation
- Email Content screen
- Firewall services

A complete discussion of ISAS' capabilities is well beyond the scope of this paper. The references listed at the end provide a detailed discussion of ISAS features.

Test Environment Hardware.

Figure 1 shows our basic lab.

Windows firewall client – any windows compatible PC. The firewall client is not compatible with other OS'es

Firewall - Pentium 300 MHz or higher. 256 RAM, at least 1GB and 20mb+ for SIAS installation, 2 Ethernet cards.

External Client – any PC running any OS

Network Cables or hubs – either two hubs and four standard (straight through) cables or two crossover cables. Appendix A shows the configuration for crossover cables

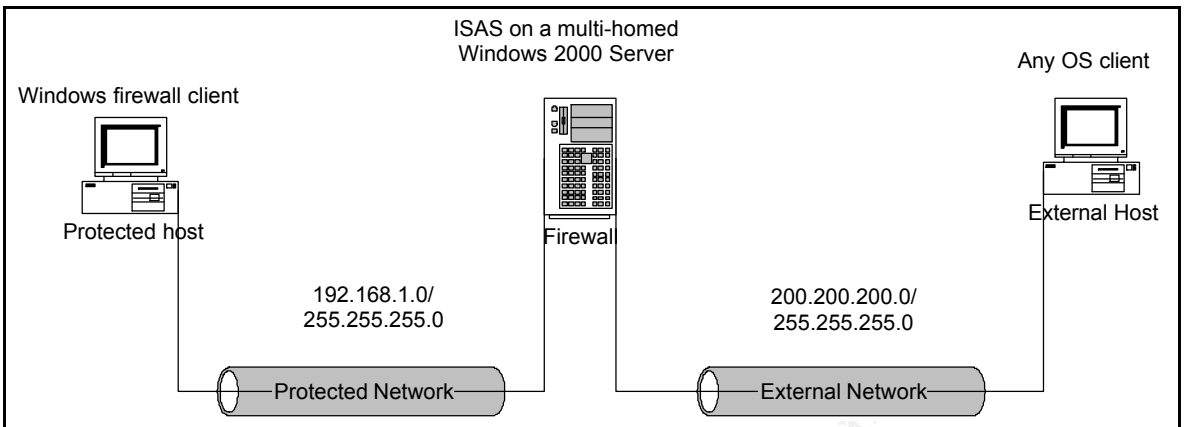


Fig. 1

Test Environment Software

Windows 200 Server Evaluation Edition - available through TechNet, many Microsoft based conferences or through the mail. If nothing else, it may be obtained at

http://www.microsoft.com/windows2000/edk/default.asp

for the price of shipping and handling.

Internet Security and Acceleration Server – is available for download at

http://support.microsoft.com/directory/content.asp?ID=FH;EN-US;ISAS&SD=gn&FR=0&LN=EN-US

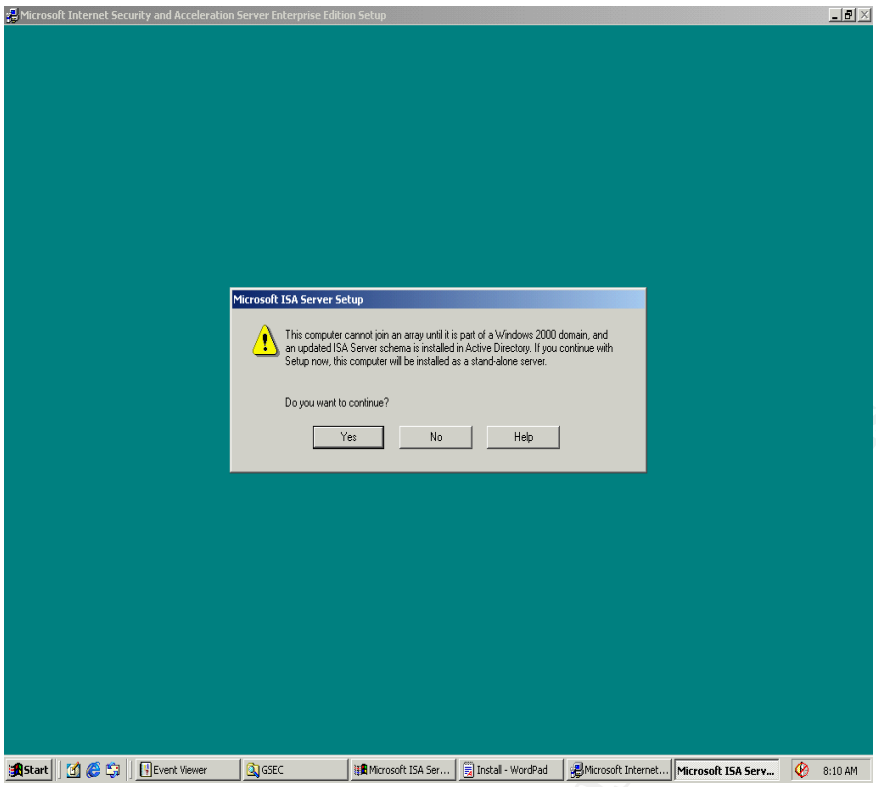
Installing ISAS

As mentioned previously, ISAS runs on a multi-homed Windows 2000 server (or better). You must have routing between the external and internal (protected) networks. If you're unfamiliar with setting up routing on a Windows 2000 server, Appendix B will guide you through installing RIP v2 on the firewall.

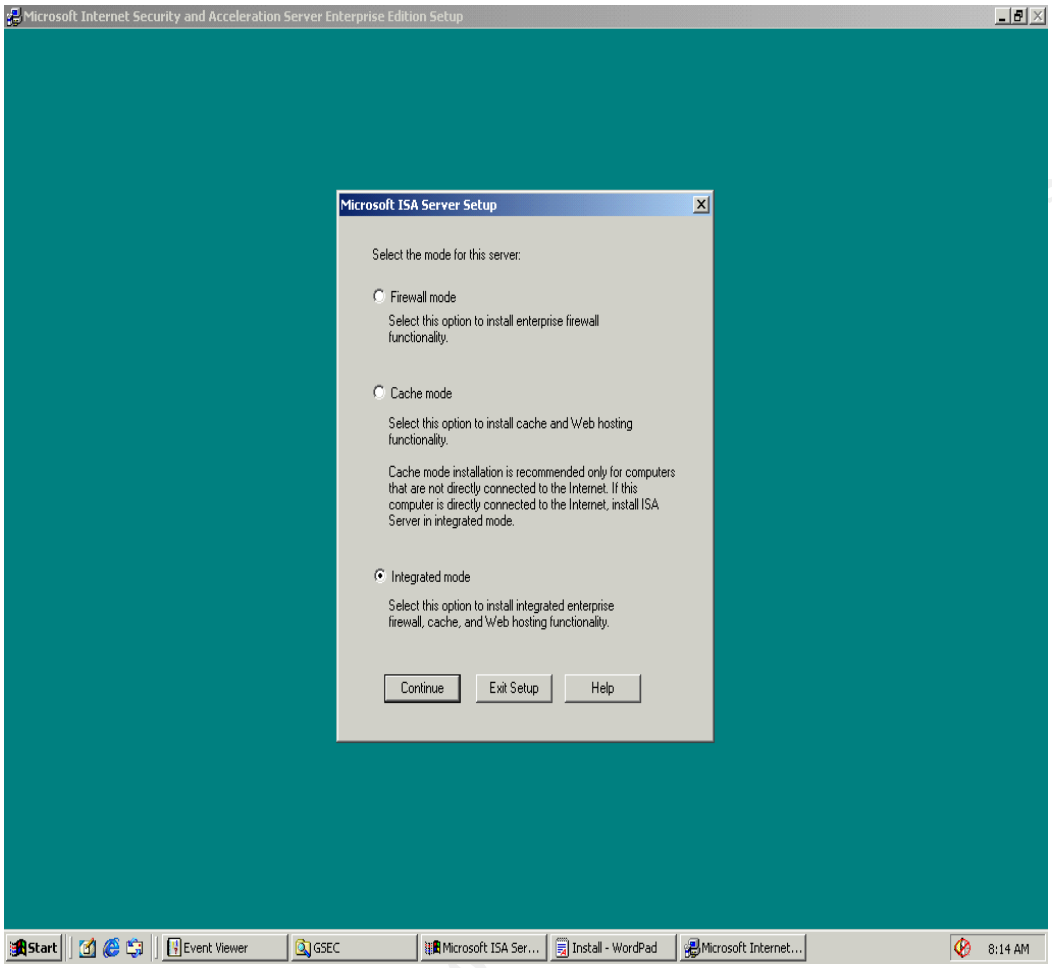
Once routing is enabled, we are ready to install ISAS. Inset the disk in the CD and let autorun take over. After reading any release notes/ readme files, we'll choose I*nstall ISA Server*.

The install routine eventually challenges you for a CD Key. The evaluation key is **880-2897414**[1] **.** During the installation process, you may choose from a number of installation options. Any of them will serve since we're focusing on the firewall services. As shown below, since our installation is on a standalone server we must install a stand-alone ISA server.

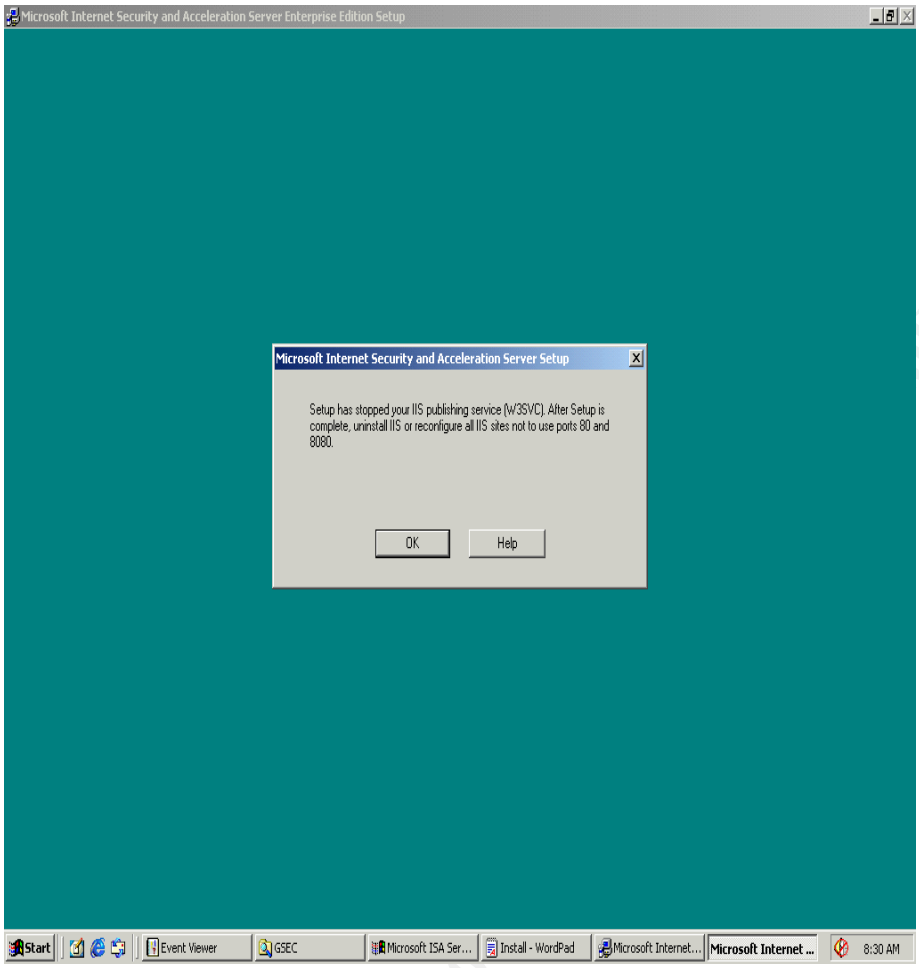
[1] This is an evaluation key available at http://www.microsoft.com/ISASERVER/downloads/evalDL.asp



Choosing server mode gives us three options; firewall only, cache only or integrated. I'll choose *Integrated Mode* because I may want to play with the caching features later.

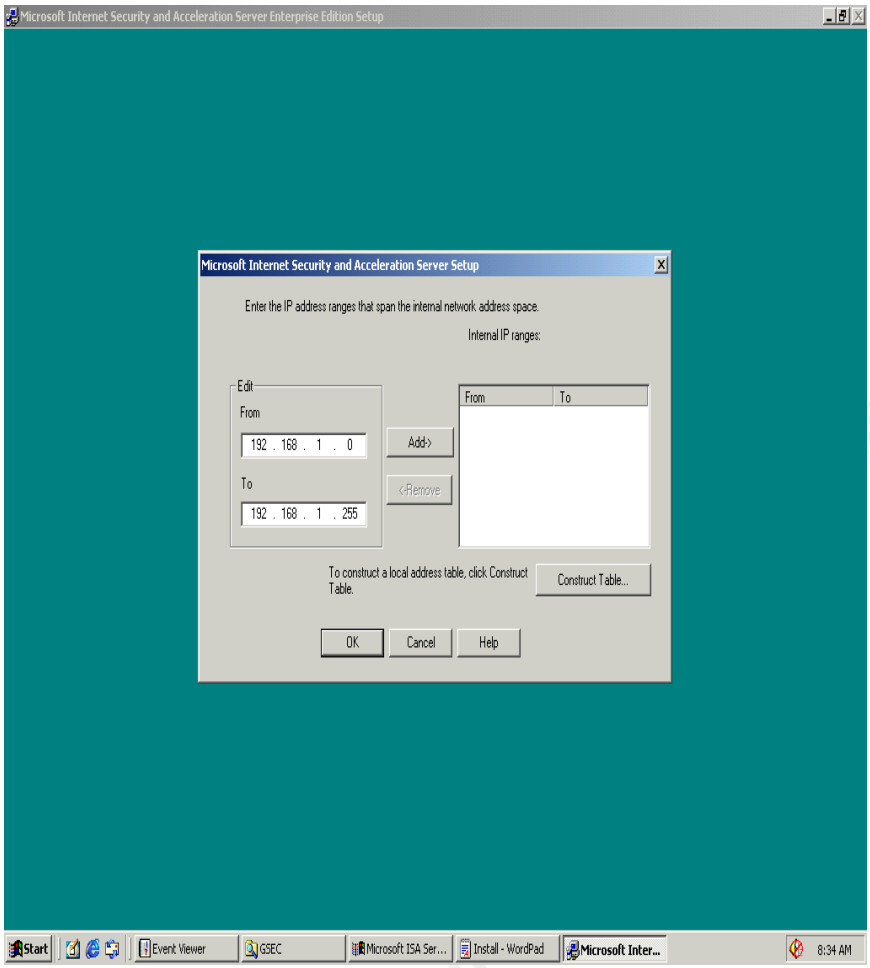


The ISA install routine will stop the WWW service. We are alerted to the fact that, should we choose to run IIS on this machine, we must reconfigure the IIS listening port. ISA server uses port 80 on the external interface.



The next screen is for configuring the web cache settings. I'll choose the default and move on to more interesting things.

The *Local Address Table* (LAT) contains the IP ranges of you trusted network. You may choose to let ISAS construct the LAT for you but check it carefully as it will interpolate ranges for you. I'll elect to enter the ranges manually. The ranges include the network number and the broadcast address.



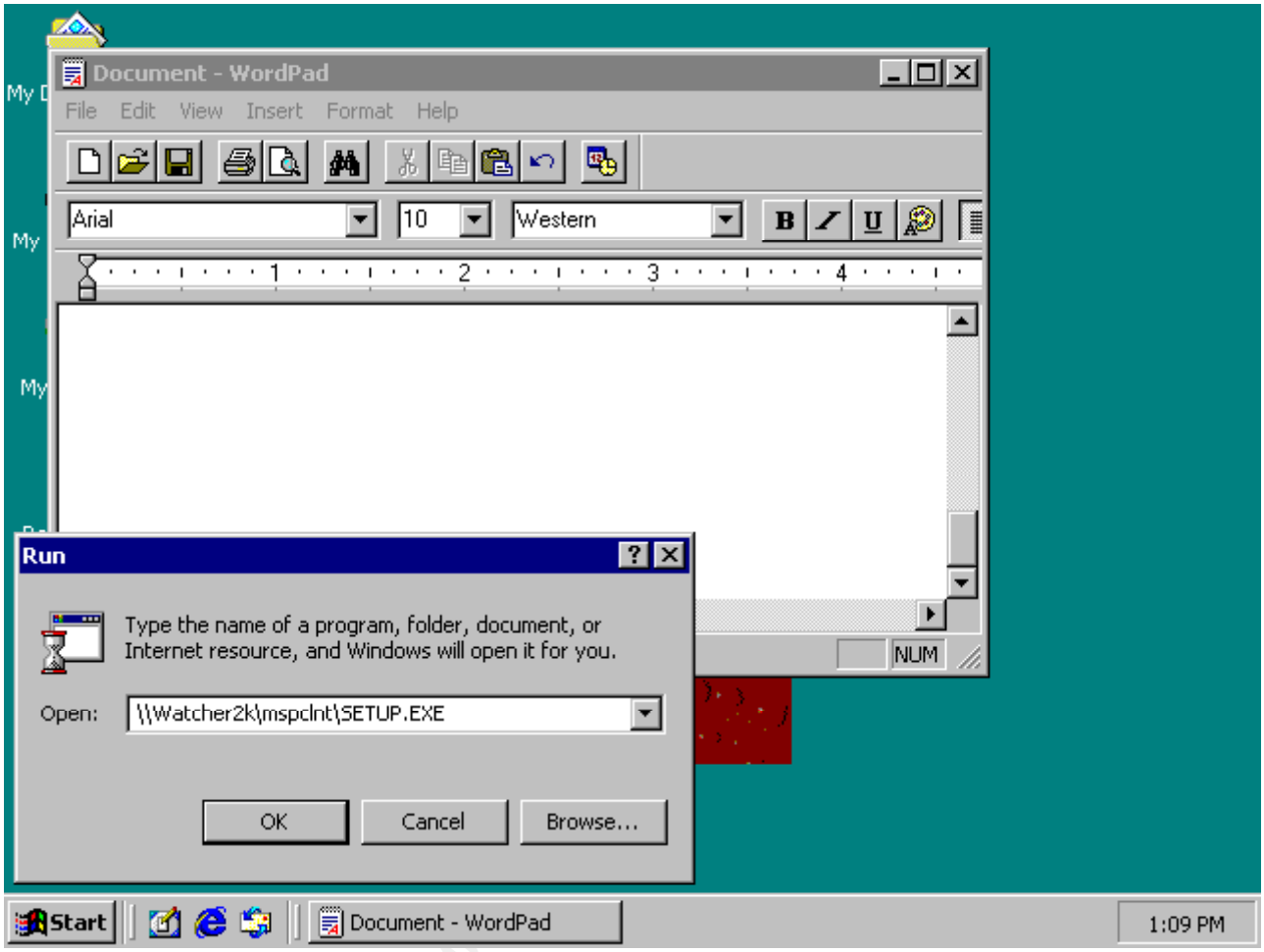
The installation routine continues to install files the gives us the opportunity to launch the getting started wizard. Let's forgo the wizard and let the installer finish up. We'll look at the ISAS MMC a little later. Let's install the firewall client next.

Installing the Firewall Client

The Firewall client is a WinSock proxy client that runs on the protected Windows (only) PC's. Basically the firewall intercepts WinSock calls from each client and redirects those requests to the client chosen internet host.

The client install is installed on a share in the path "\\ISAServerName\mspclnt\"

In our case, the ISAS is named Watcher2K.



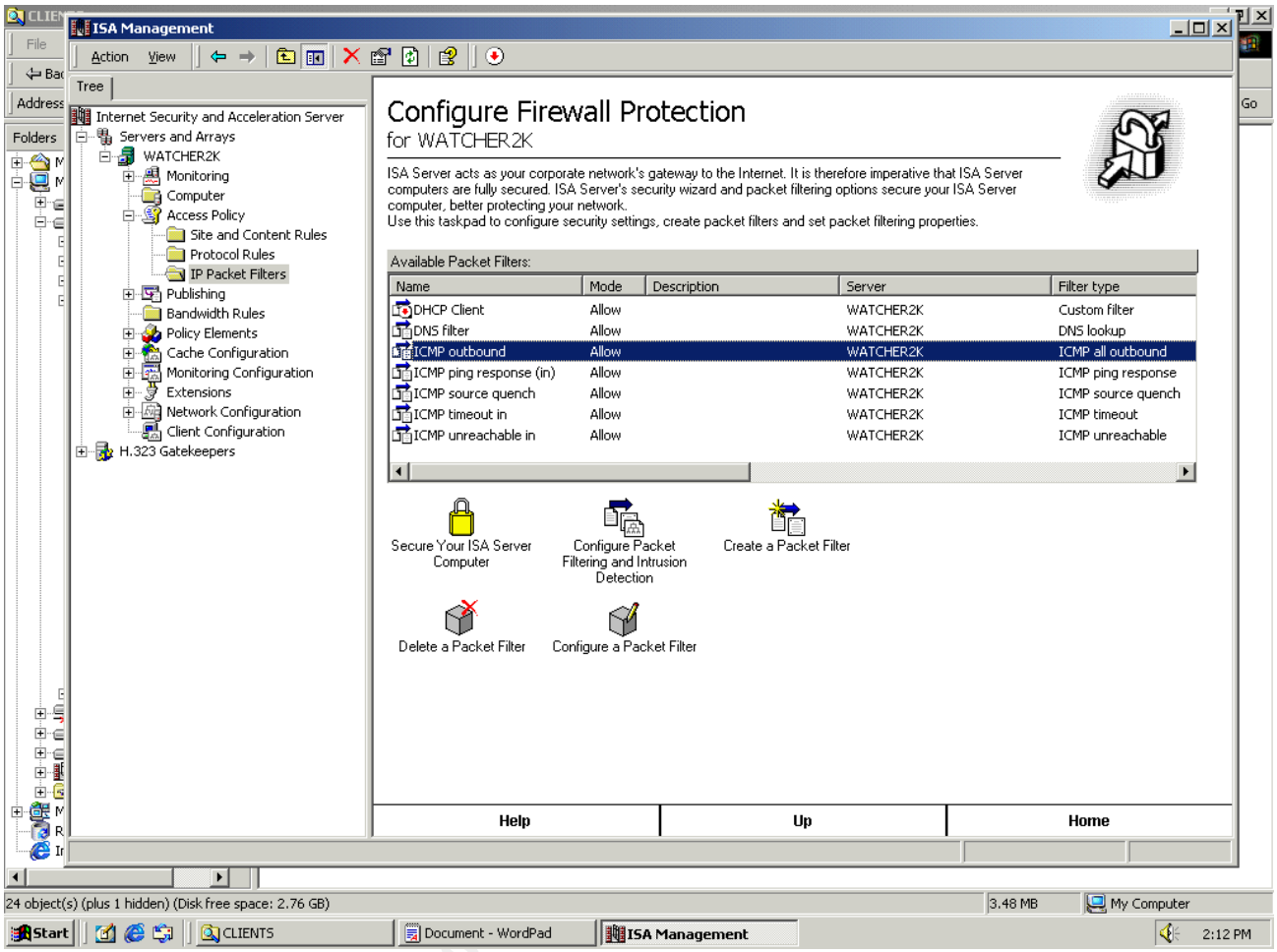
For our introduction, the client installs as easily as that. There are several relatively painless ways to deploy it, including web-based installs and policy based installs. Those topics are well beyond this paper's purview.

Configuring ISAS

IP Packet Filters - Block ICMP

By default we can use ICMP to ping hosts outside the firewall. By allowing outbound ICMP we run the risk of participating in an internally launched DDOS smurf attack against an external host. We can block all outgoing ICMP and prevent our internal clients from launching an echo reply to the victim.

Launching the *ISA Management Monitor*, expand *Access Policy*, the click *IP Packet Filters.* As we see below, ICMP outbound is set to allow.



A test on our firewall client shows that ICMP outbound is allowed:

C:\>ping 159.105.165.17

Pinging 159.105.165.17 with 32 bytes of data:

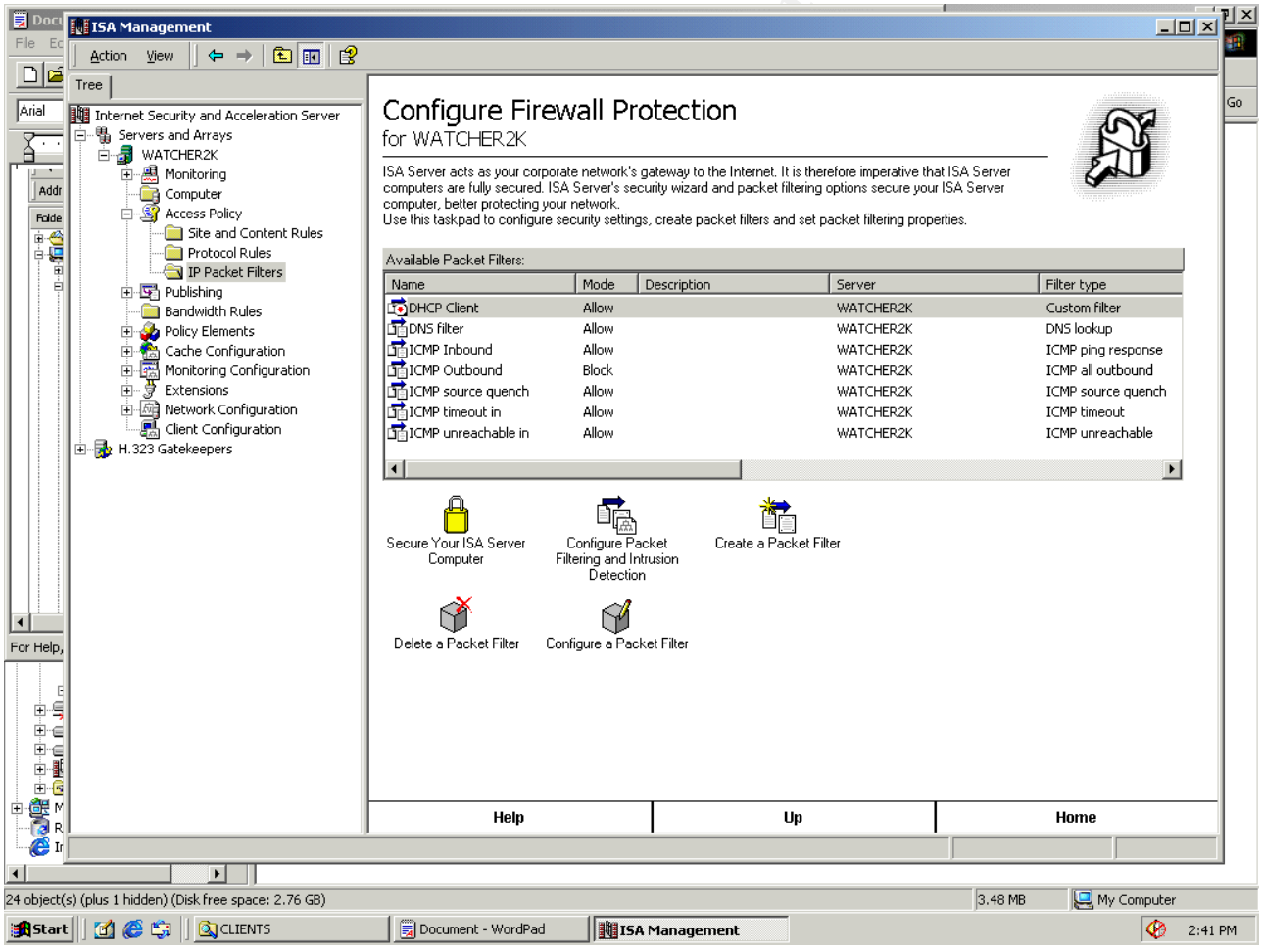
Reply from 159.105.165.17: bytes=32 time<10ms TTL=127
Reply from 159.105.165.17: bytes=32 time<10ms TTL=127
Reply from 159.105.165.17: bytes=32 time<10ms TTL=127
Reply from 159.105.165.17: bytes=32 time<10ms TTL=127

Ping statistics for 159.105.165.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Let's delete the allow ICMP outbound filter by selecting it and clicking *Delete a Packet Filter*. Next we *Create a Packet Filter* using the wizard's prompts:

1) Name the filter **ICMP Outbound** is fine.
2) Click **Block**
3) On the dropdown box choose **ICMP all Outbound**
4) Leave the **Default IP addresses for each external interface…** selected
5) Leave the **All remote Computers** selected
6) Click **Finish**

Your screen should look like this.



Now back to our test we see that our pings are timing out.

C:\>ping 159.105.165.17

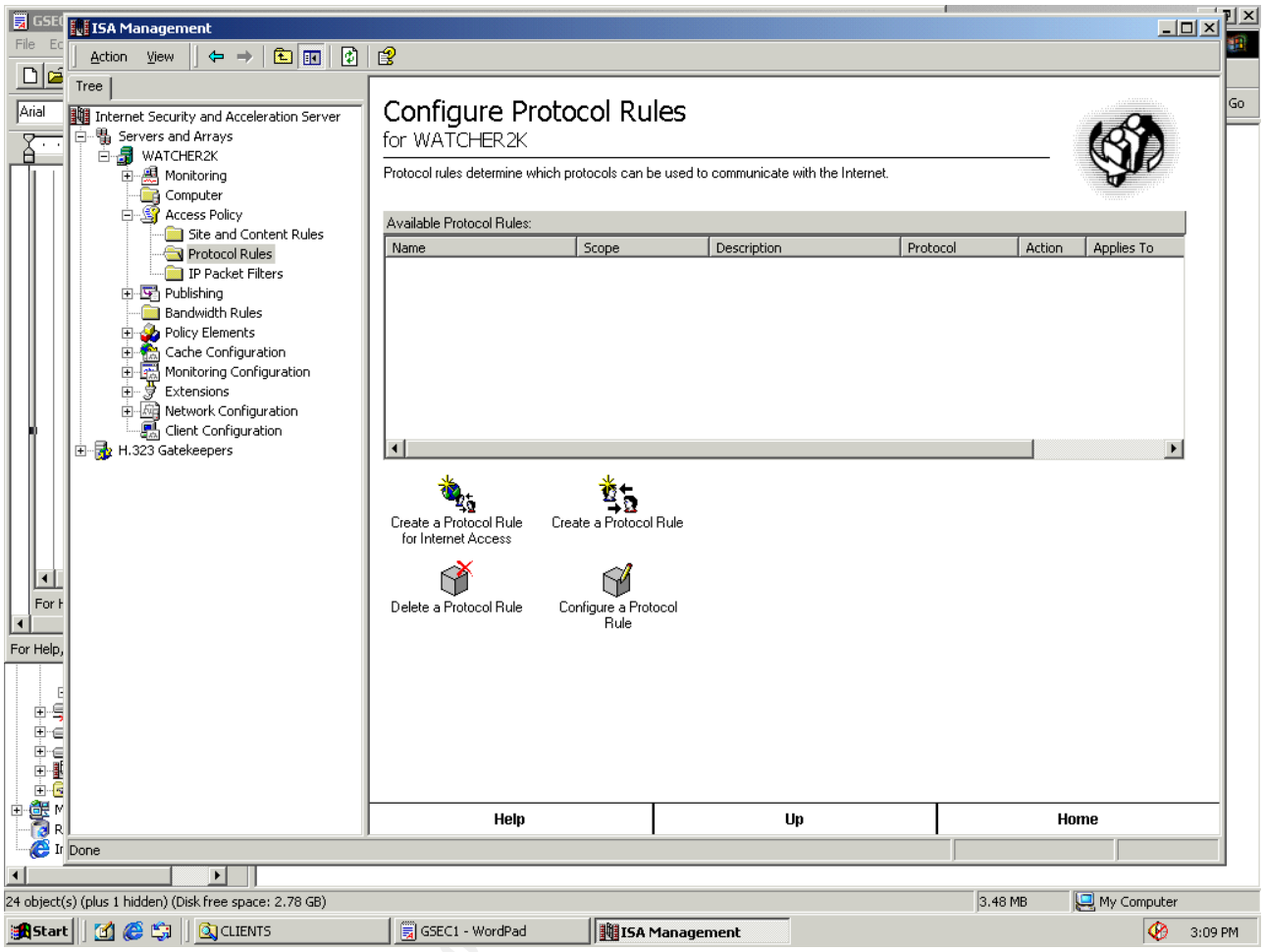
Pinging 159.105.165.17 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

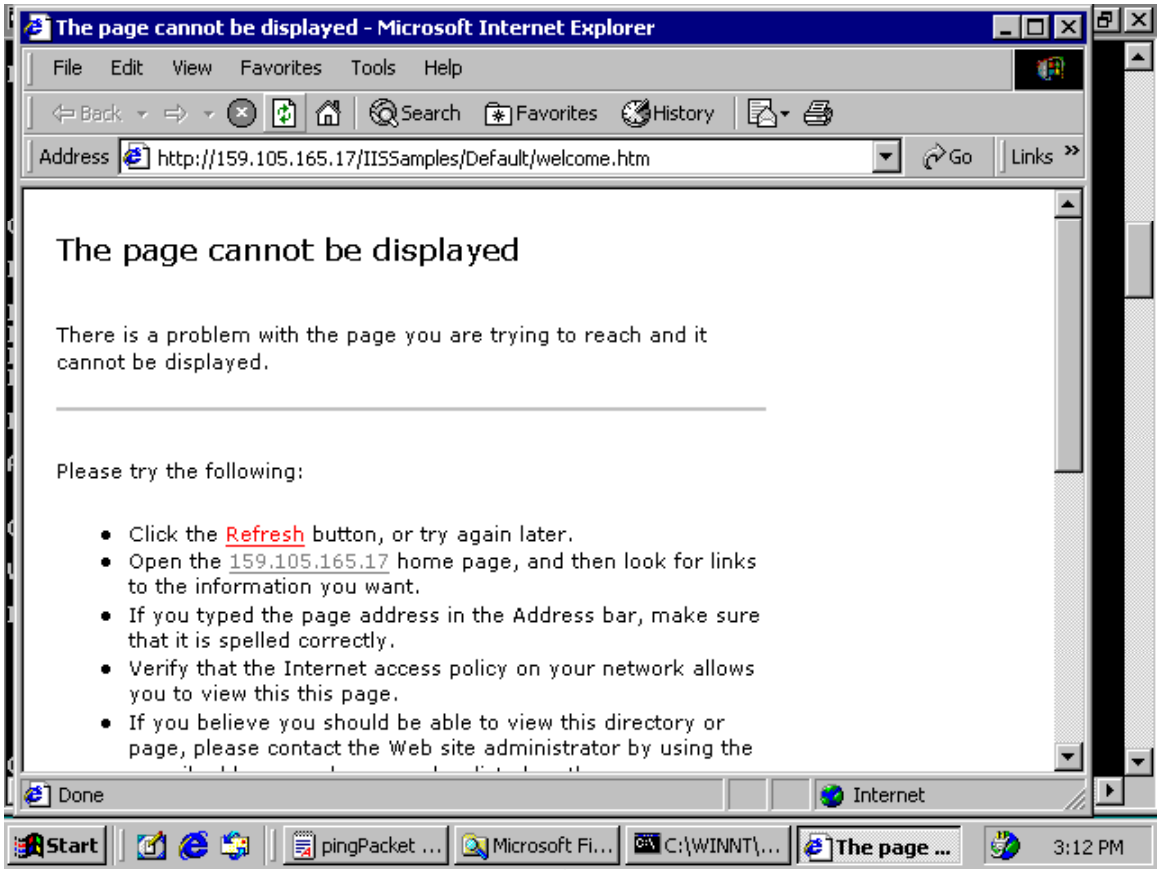
Ping statistics for 159.105.165.17:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Protocol Rule – Allow Web Services

A protocol rule determines which which TCP/UDP protocols the firewall clients may access. Launching the *ISA Management Monitor*, expand *Access Policy*, then click *Configure Protocol Rules.* As we see below, no rules exist to allow Internet services hence services are denied.



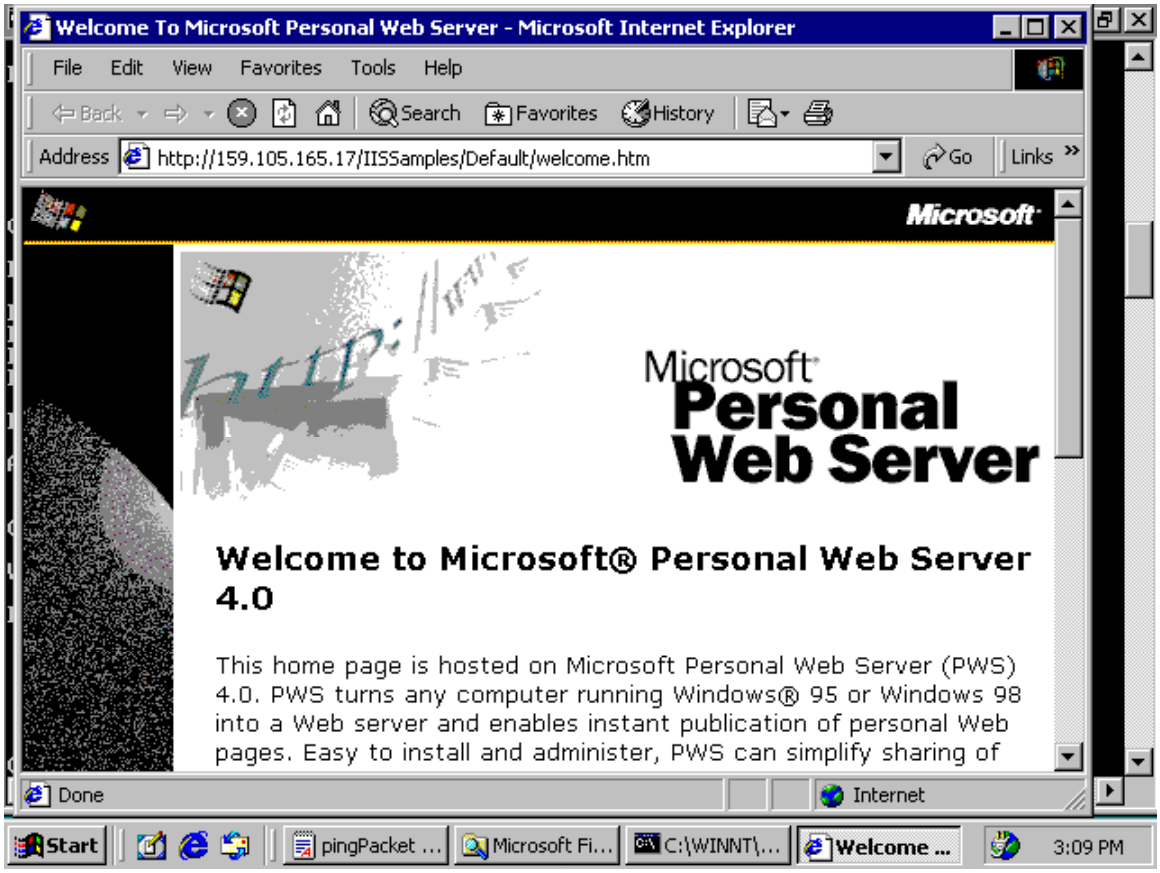
To confirm this we'll try to request http services from our external network host(159.105.165.17). As seen below, services are rejected.



Let's create a Protocol rule to allow for web services"

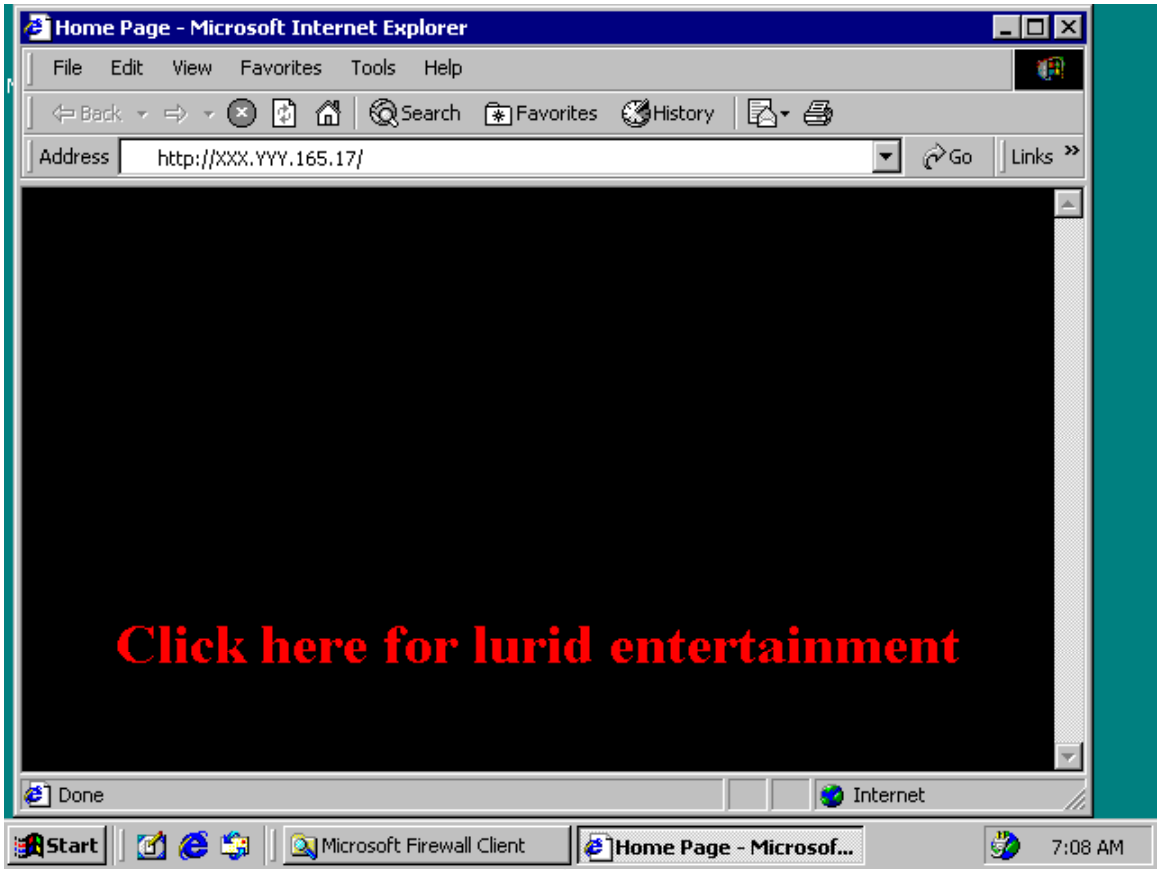
1) Click *Create a Protocol Rule for Internet Access*
2) Name the rule, in my case, **Allow Web** then click *Next*
3) Choose *Selected Protocols.* HTTP, FTP, and etc. should be selected.
4) You may choose a schedule, I'll select *Always*
5) The *Client Type* is *Any Request*
6) You are shown a summary screen, select *Finish* once you are satisfied

Now back to our browser on the internal client, we see that we are able to connect.

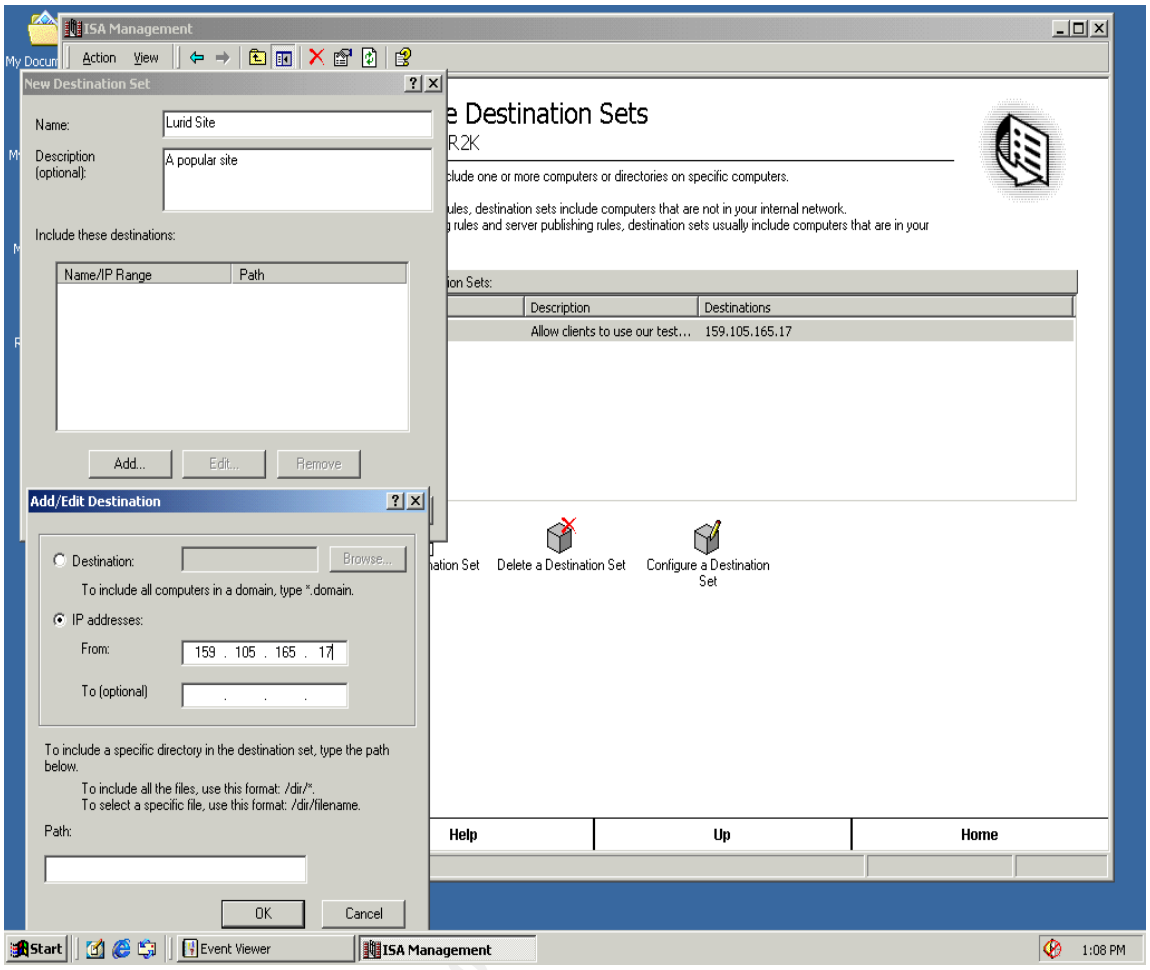


Site and Content Rule – Block Lurid Site

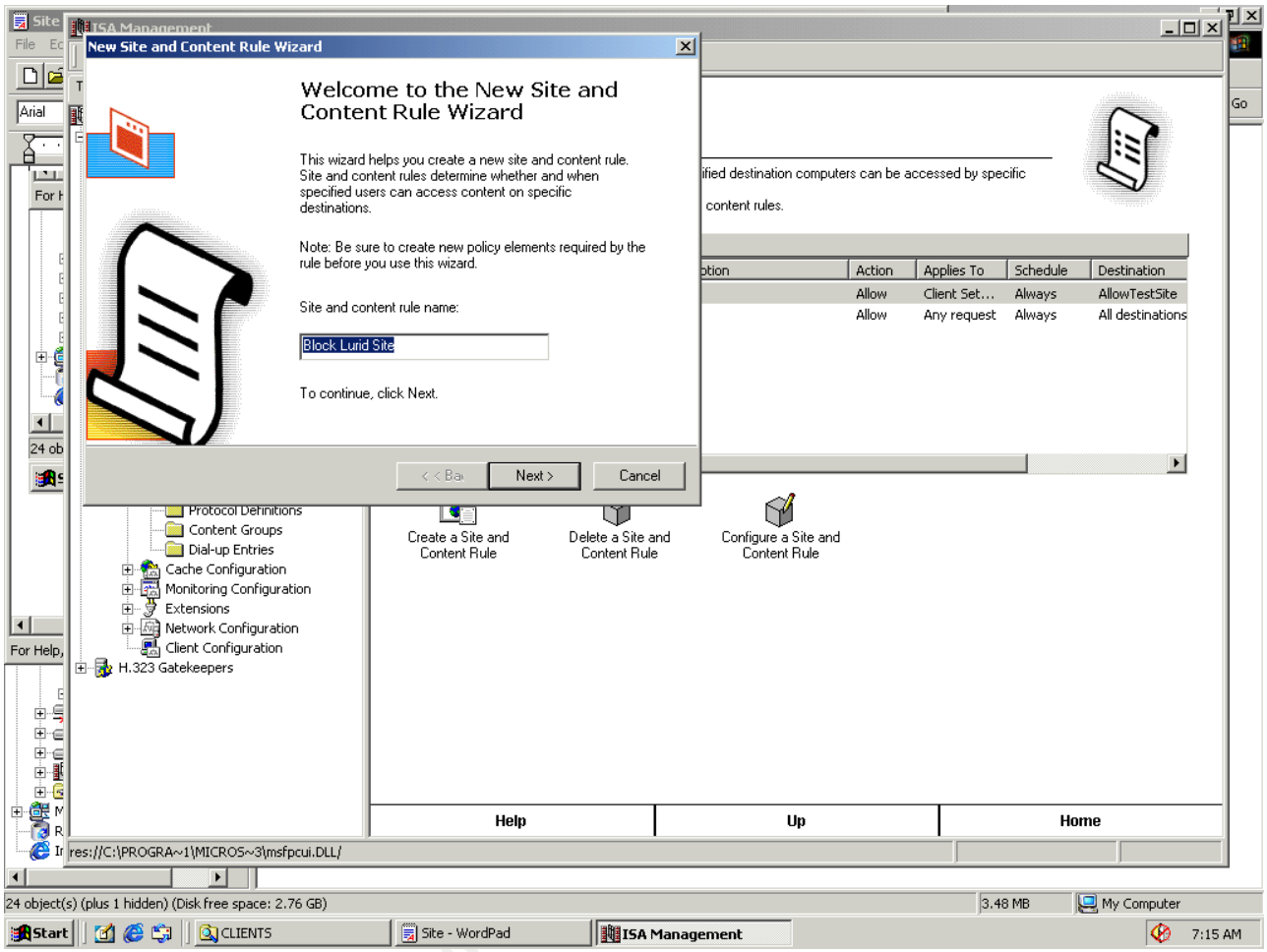
Site and Content Rules allows us a measure of control over which sites our users may visit at any given time. Perhaps a site, a *Lurid Site*, has become popular. By surfing over to this site we have become convinced this site is not work related.



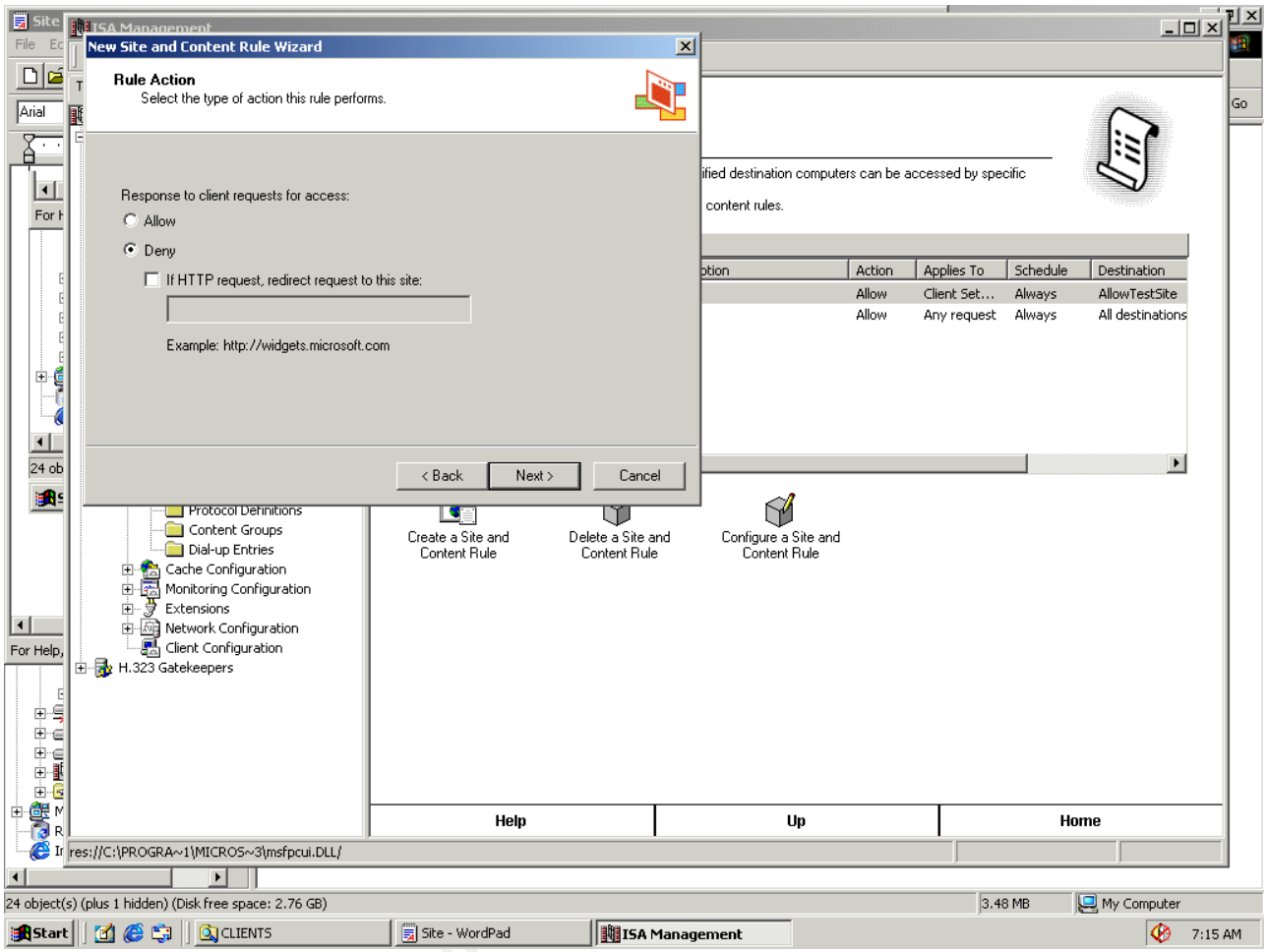
In order to block our site we must first define it as a destination. Launching the *ISA Management Monitor*, expand *Destination Set*, then click *Create a Destination Set.* As we see below, you may name a destination and provide a brief descriptor (top left). Once you click on *Add*, a screen pops up allowing us to enter a domain name or, in our case, an IP to be blocked. The domain name would be preferable in a production environment, I have not set up DNS or a host file to resolve in our test environment. Enter the IP and click *OK*.



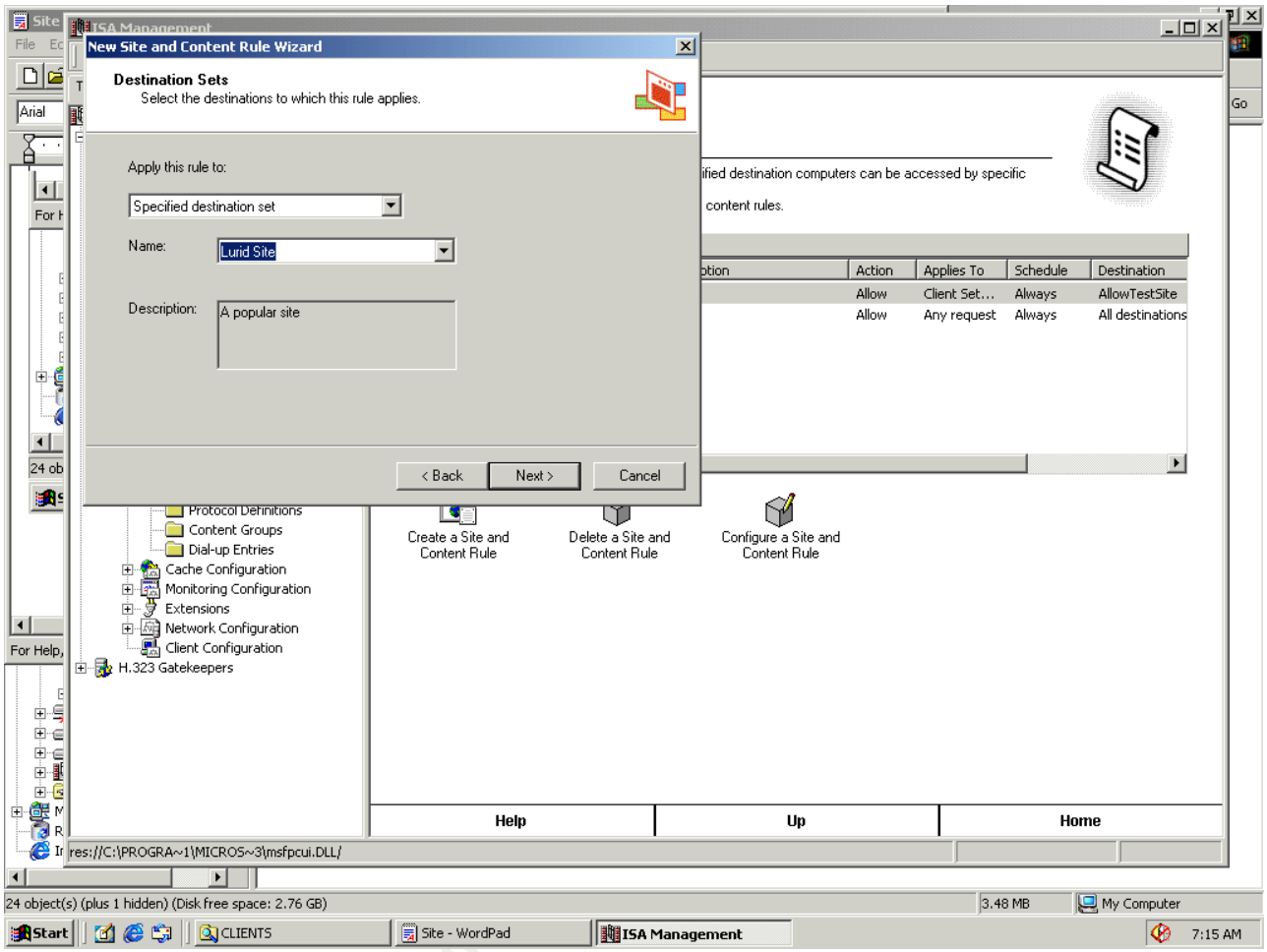
Right click *Site and Content Rules* from the *Access Policy* window. Clicking *Create a Site and Content Rule* will launch the wizard. I'll name this rule **Block Lurid Site**.



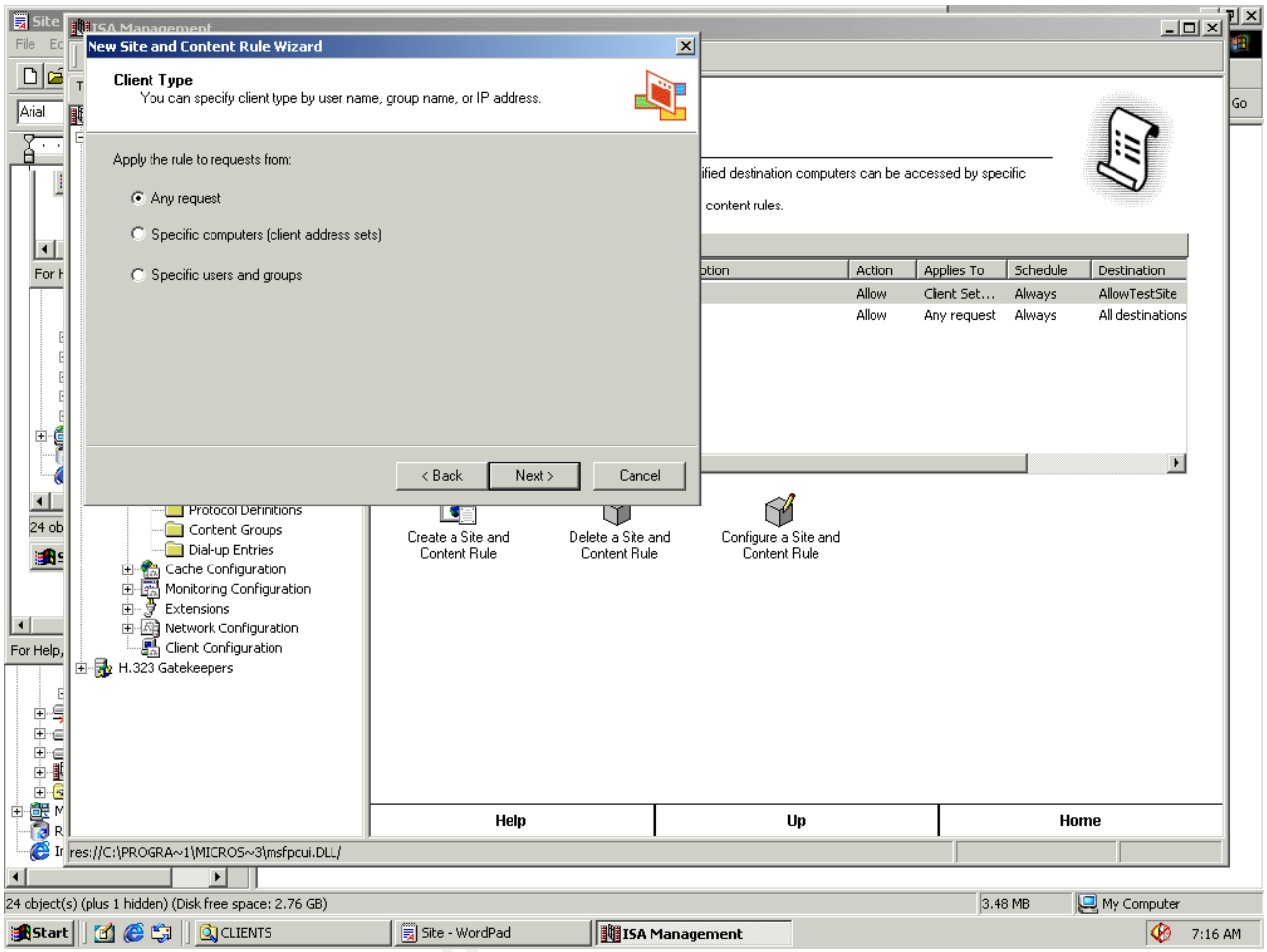
On the next screen we choose deny. I could also choose to redirect the request to a warning page on another server.



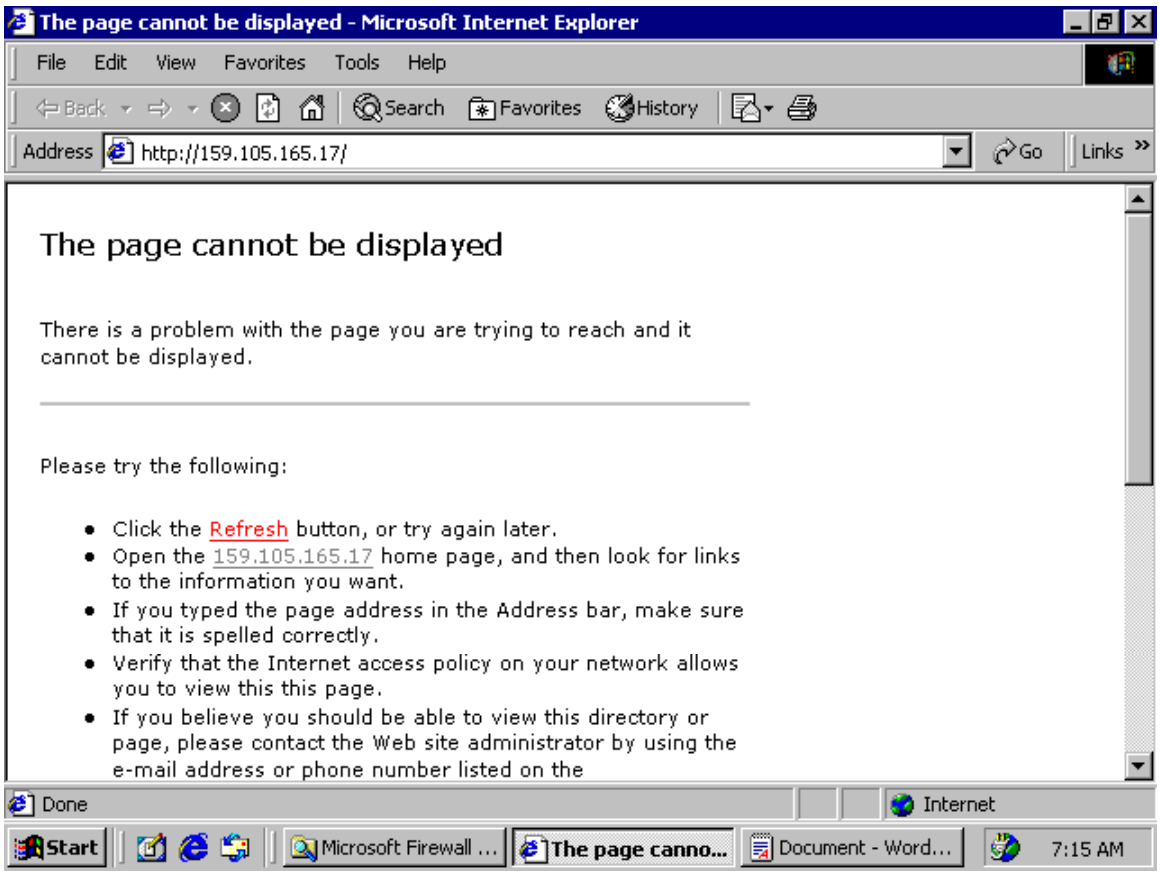
The wizard asks to which destination set the rule will apply. We want our *Specified destination set* from the dropdown box. Choose the destination we just created, **Lurid Site**.



The next screen lets us apply the rule to a schedule. Lastly, we can choose to specify a user name, a group, an IP address or any request to which the rule will be applied. I'll let it apply to everyone.



Now to test our rule, I launch the browser and try to request our blocked site. The results are shown below. Had we redirected to a page that said, “This site not allowed” we would’ve given more information to our users.



Discussion

Resources for ISA Users

The newsgroup - Comp.security.firewalls

Microsoft ISA Home - http://www.microsoft.com/isaserver/default.asp

ISA server organization – http://www.isaserver.org

Bug reports:

As of September 20, 2001 there are only a handful of reported bugs and patches including:

- a potential memory leak in the H323 ASN DLL.
- scripting can be executed in the error return pages from the ISA server.
- many open sockets when the client reaches a high open-and-close connection rate (600/sec.)

- ISA was returning incorrect checksums to Ethernet adapters using hardware checksum
- ISA does not filter and flow traffic routed by a 2000 server using the QOS Packet Scheduler Service.
- a registry patch to block and log all outbound ICMP traffic that is sent from the internal network to the external network
- the logging module prevents the logging of the "Rule#1" and "Rule#2" fields for certain UDP traffic

These reports and their corresponding patches may be found at Microsoft as well as http://www.isaserver.org/pages/bugs/patches.htm .

Summary

This paper presented a procedure for establishing a test environment in which to prove ISA firewall rules. For a minimal investment, a student/professional can develop policies *in vitro* before deploying to the production environment. The sample rules are not presented as exhaustive.

Future topics of research into the use of Microsoft's ISA server might include:

- writing the rules for sans.org's top twenty
- exploring the caching functions
- testing and evaluating the *Secure Nat* functions of ISA
- testing and evaluating the intrusion detection functions
- reviewing 3rd party add-ons to ISA

References

"Microsoft Download Center."
http://www.microsoft.com/downloads/search.asp (26 Oct. 2001)

"Windows 2000 Advanced Server Trial Offer."
http://www.microsoft.com/windows2000/edk/default.asp (26 Oct. 2001)

"Microsoft Internet Security and Acceleration Server – Home."
http://www.microsoft.com/isaserver/default.asp (26 Oct. 2001)

"Microsoft ISA Server Firewall and Cache resource site."
http://www.isaserver.org. (30 Oct. 2001)

Huegen, Craig. "CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. " http://www.cert.org/advisories/CA-1998-01.html. (13 March 2000)

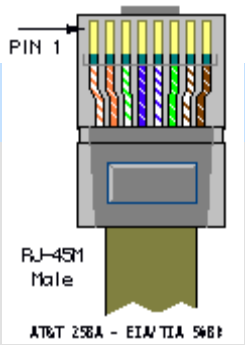
Mingus, Larry. Ethernet Crossover Cable - DIY How-to Guide.
http://www.makeitsimple.com/how-to/dyi_crossover.htm . (10, July 1998)

Shinder, Thomas Dr., Shinder, Debra Littlejohn, Grasdal, Martin. Configuring ISA Server 2000**.** Rockland, MA: Syngress Media Inc. 2001

Simmons, Curt. Microsoft ISA Configuration & Administration.
San Francisco: Hungry Minds, Inc. 2001

Appendix A

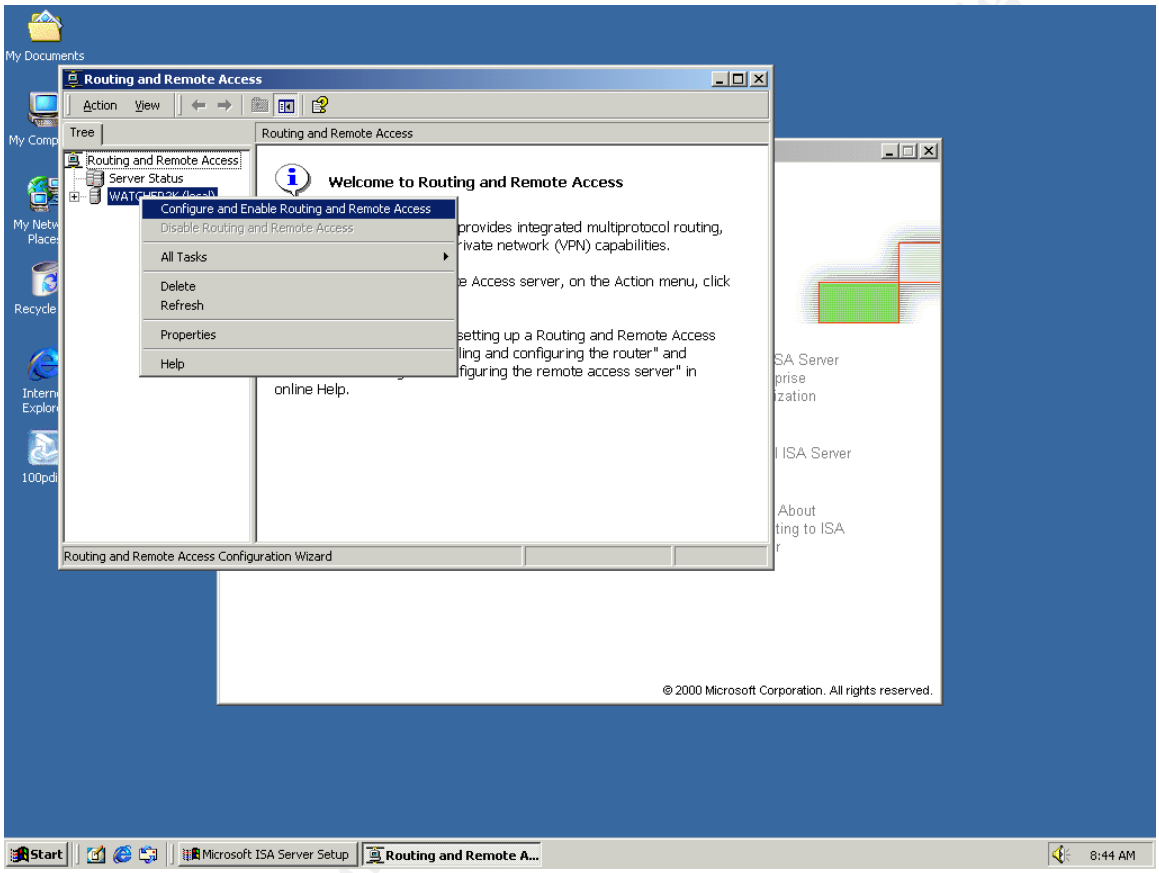
Crossover Cable	
RJ-45 PIN	**RJ-45 PIN**
1 Rx+	3 Tx+
2 Rc-	6 Tx-
3 Tx+	1 Rc+
6 Tx-	2 Rc-



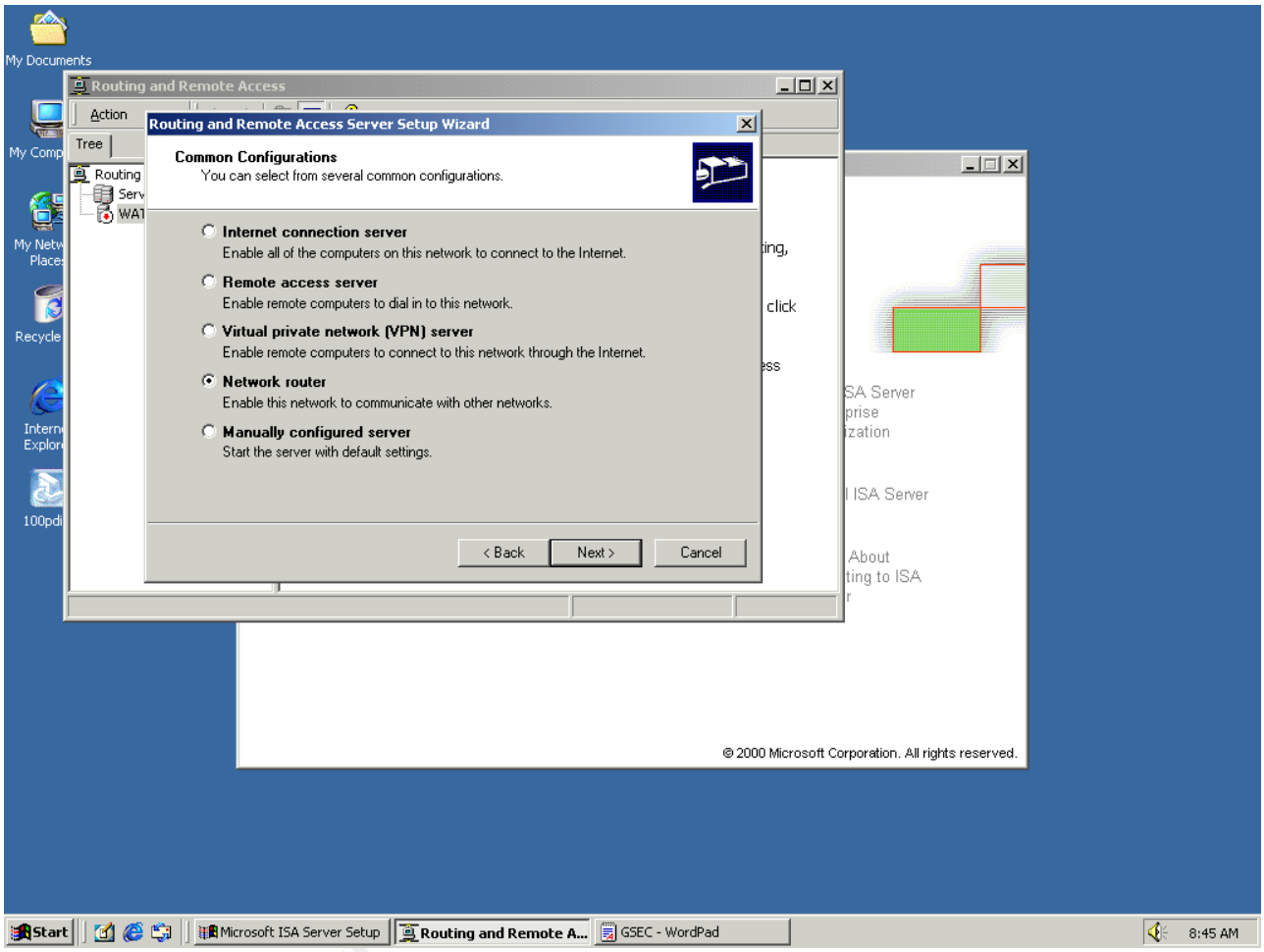
Straight Through Cable	
RJ-45 PIN	**RJ-45 PIN**
1 Tx+	1 Rc+
2 Tx-	2 Rc-
3 Rc+	3 Tx+
6 Rc-	6 Tx-

Appendix B – Routing and Remote Access (RRAS)

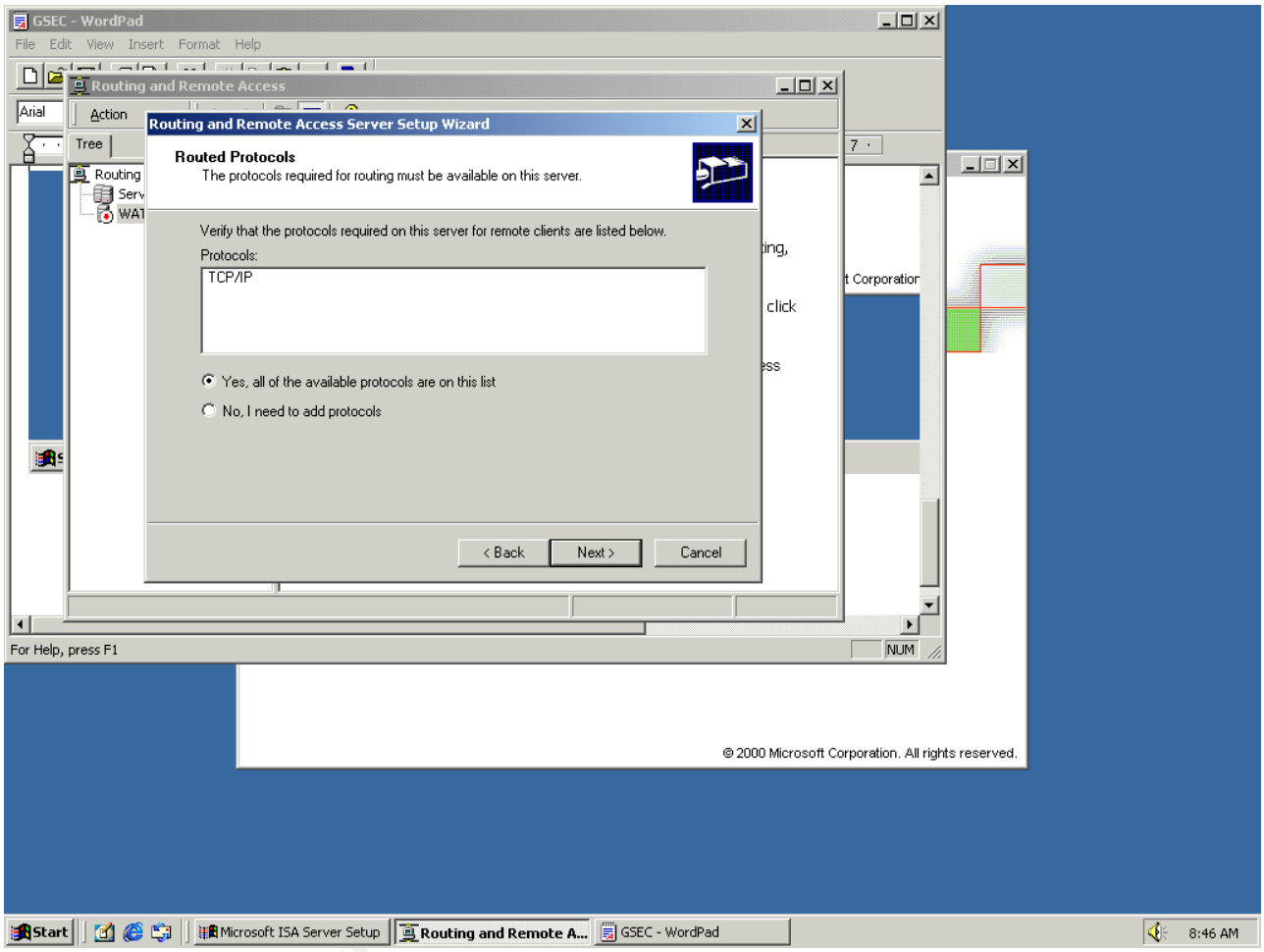
Enabling routing on a multi-homed Windows 2000 system is straightforward.
Start RRAS from
Start => programs => Administrative tools => Routing and Remote Access.
A right-click on the server (Watcher2K here) will display the screen below:



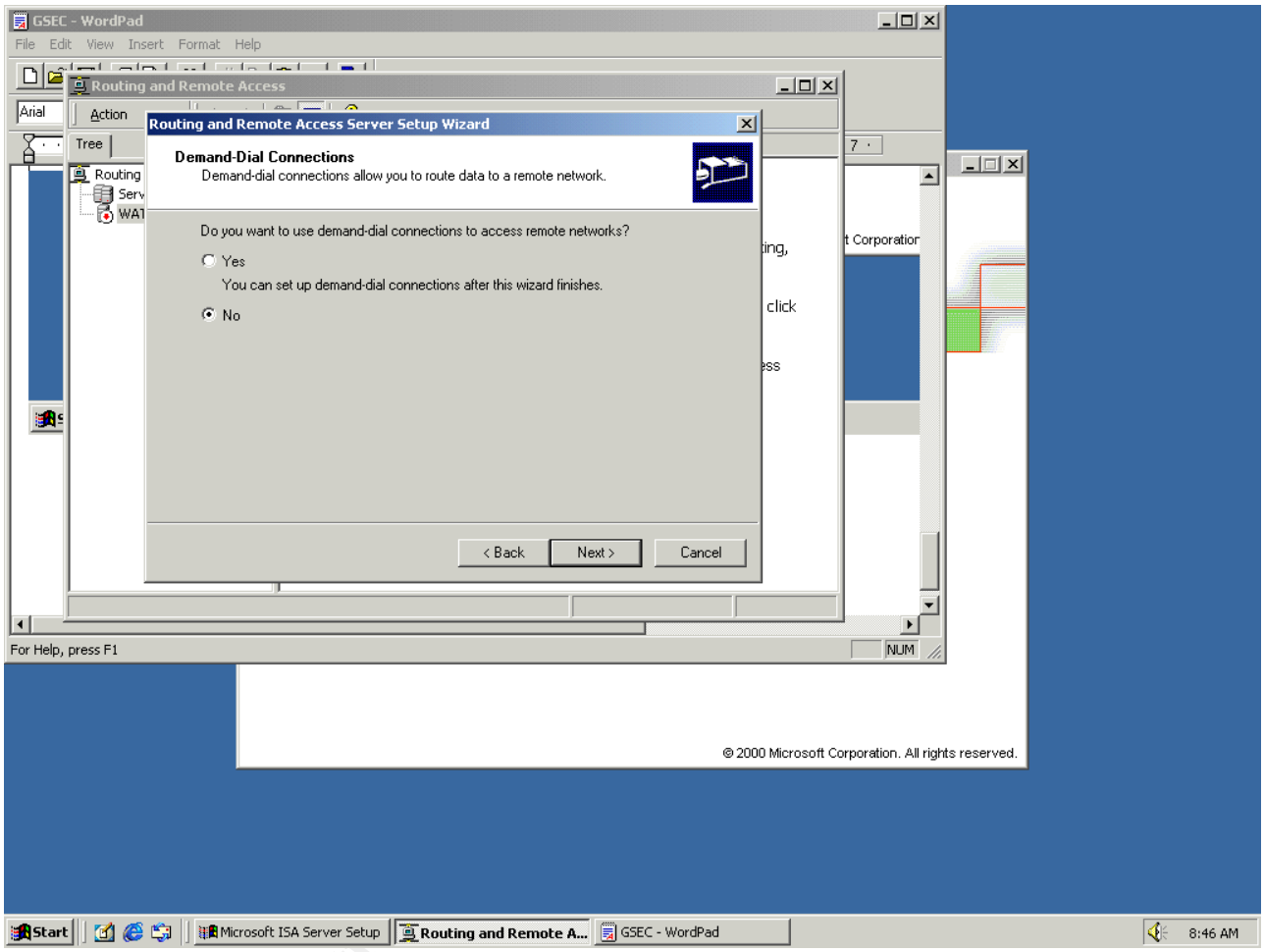
We are setting up a Network router



Routing only IP

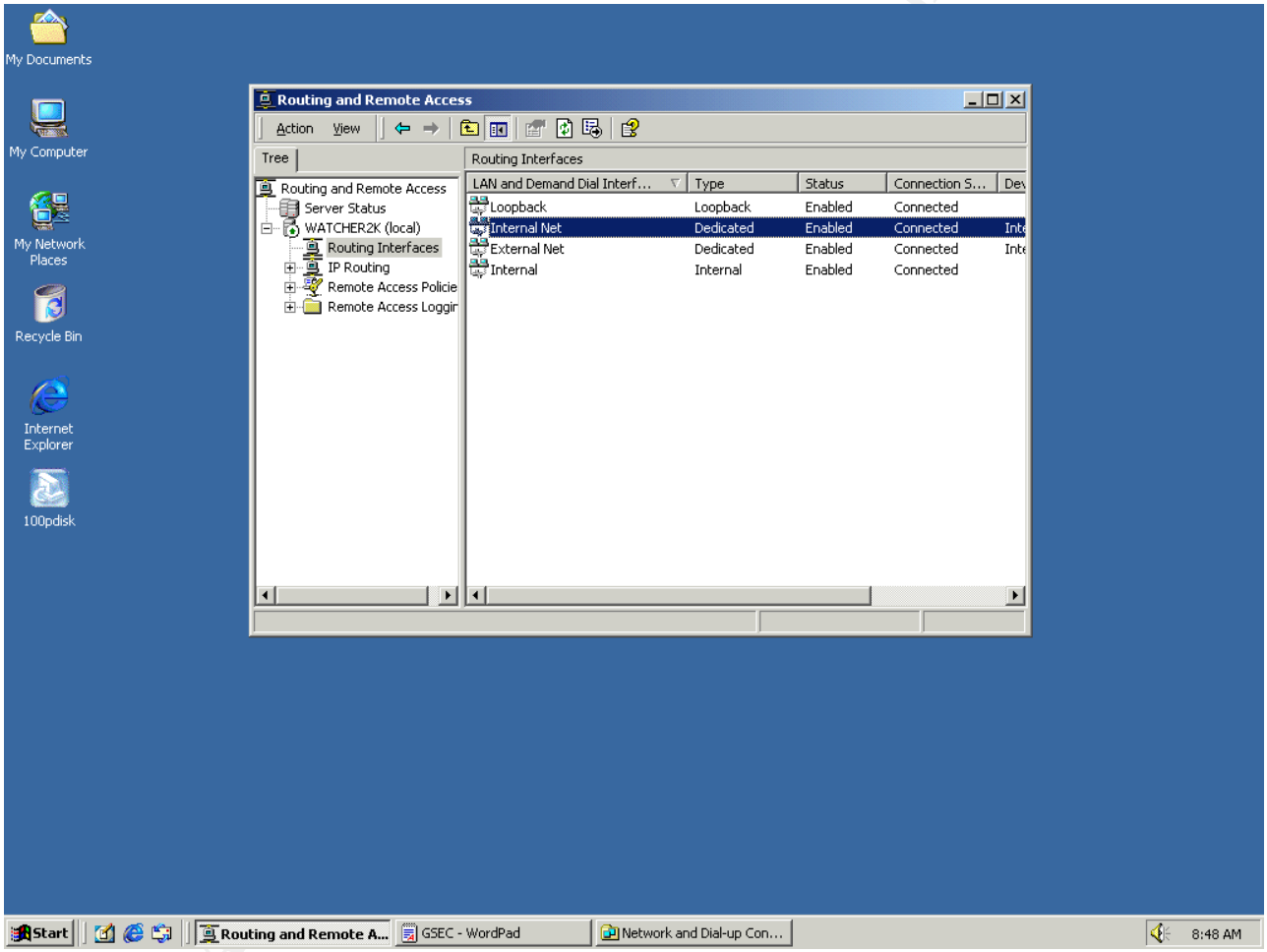


No dial out for us

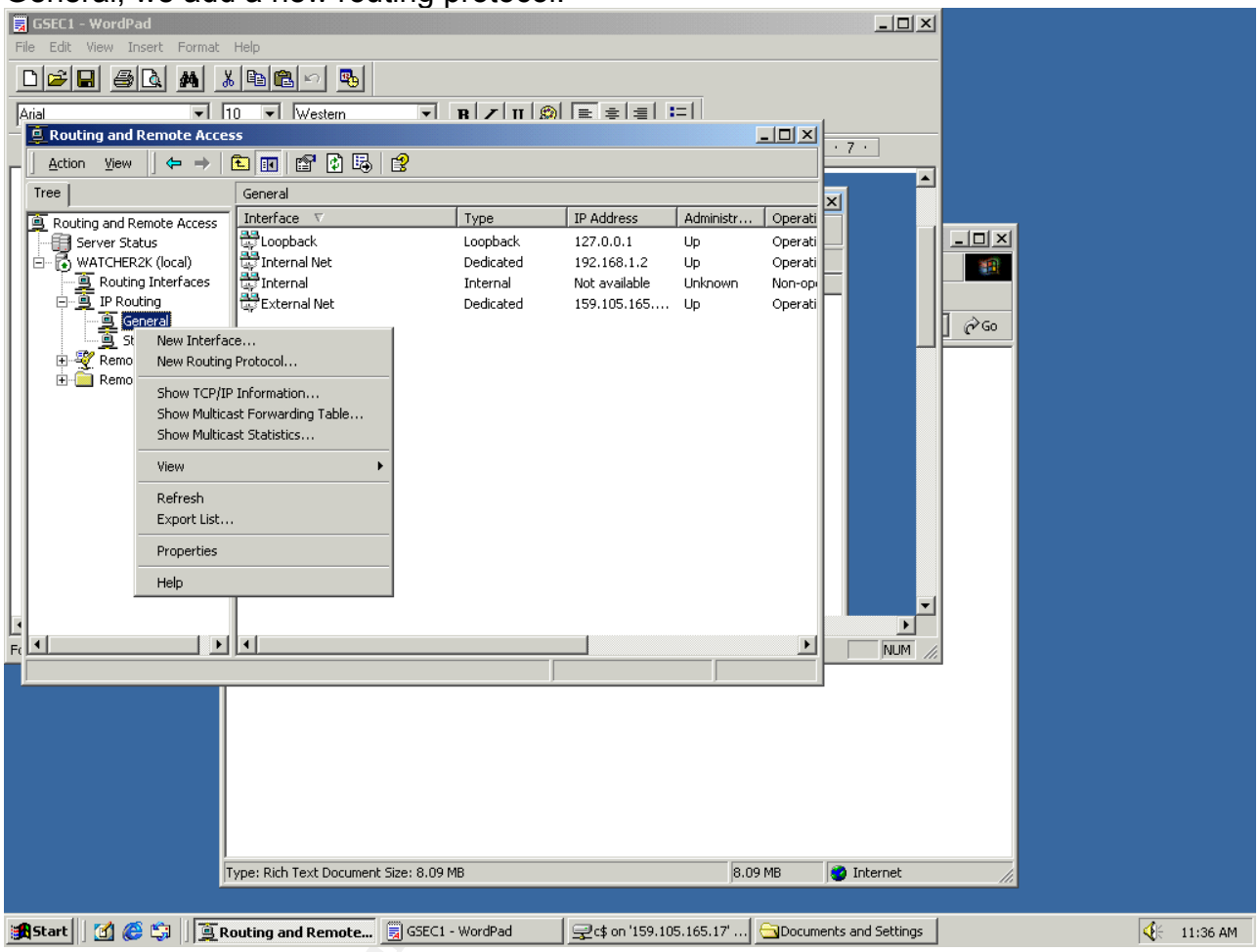


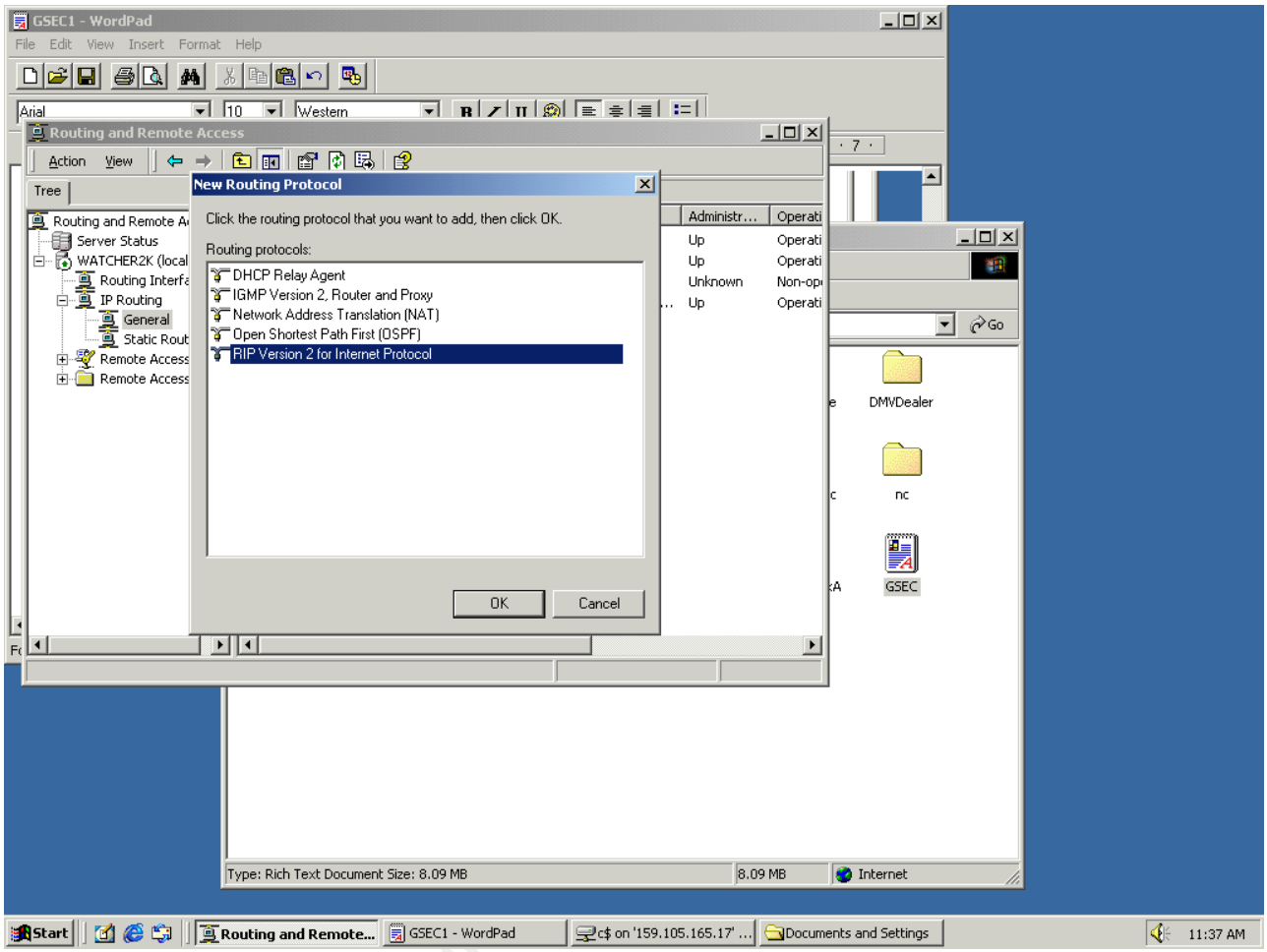
The service starts up and you are presented with a screen much like this. You'll notice that I've named my interfaces internal net and external net. I renamed my interfaces at the *Network and Dial Up Connections* page (Right-click *My Network Places*).

You'll notice that the interfaces are enabled. You may also see that you've had Ethernet traffic (not shown here) in the *Incoming/Outgoing Bytes* column. The process is complete!

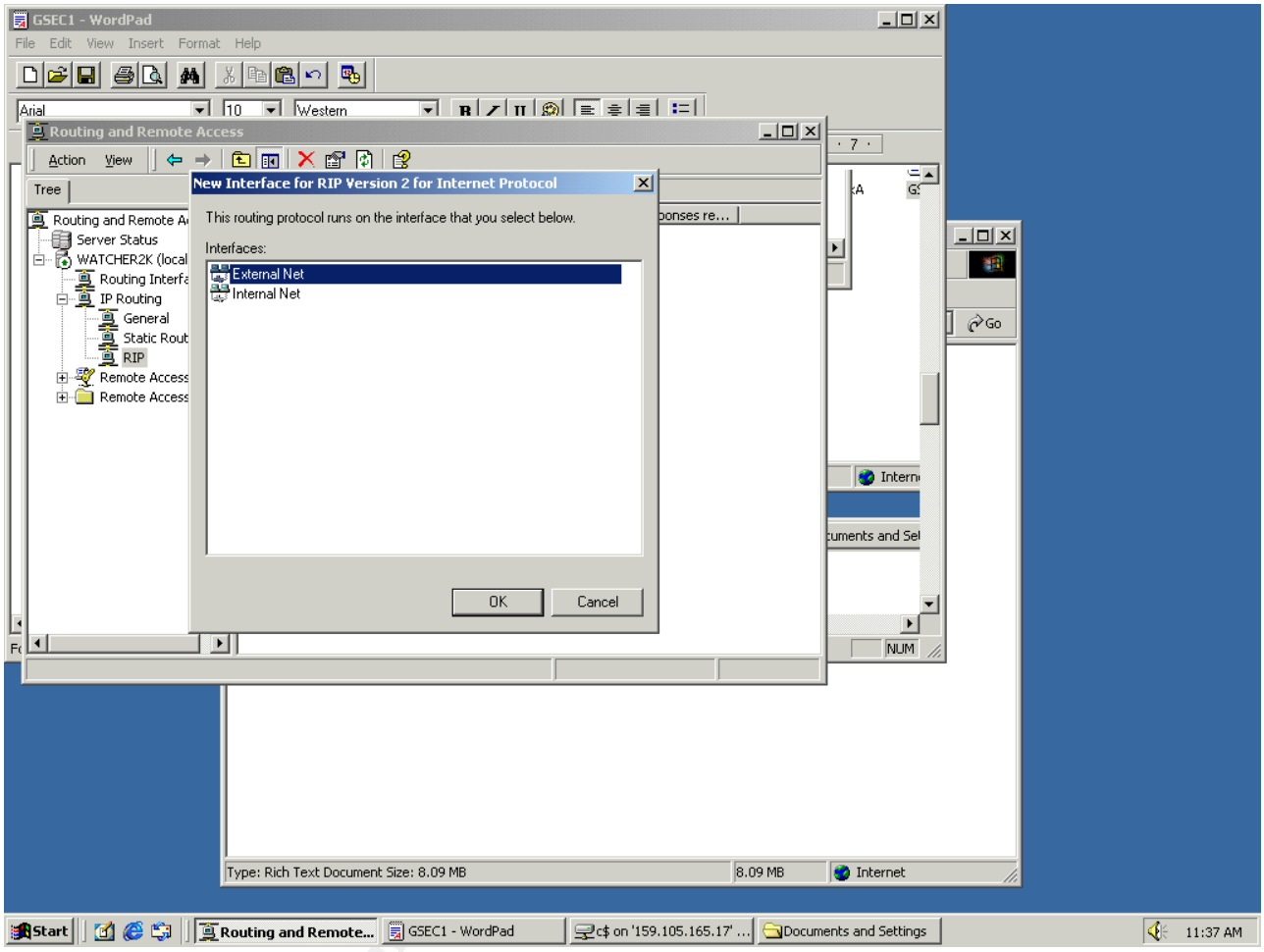


Since this is our private network, let's use the RIP protocol. Right-clicking on General, we add a new routing protocol.





Cycle through choosing both interfaces.



RIP is enabled when both interfaces appear as shown.