SYGATE® Home Network

VERSION 4.0

USER GUIDE

SyGate Technologies, Inc.
6591 Dumbarton Circle, Suite 102
Fremont, CA 94555
http://www.sygate.com

SYGATE® Home Network 4.0 User's Guide

08/28/2000

OVERVIEW

SYGATE® Home Network 4.0

SYGATE® Home Network 4.0 is a software product that enables multiple users on a local network to share a connection to the Internet through a single machine that acts as the server. SYGATE® Home Network 4.0 allows users on a small network (including laptops) to conveniently and inexpensively share simultaneous Internet access. SYGATE runs on Windows 95, Windows 98, Windows NT, Windows 2000, and Millennium systems and supports many kinds of Internet connections, including analog modems, ISDN, cable modems, DSL, and DirecPC.

SYGATE® Home Network 4.0 server software is installed on a workstation that has access to the Internet via analog modem, ISDN, cable modem, DSL, or DirecPC. SYGATE® Home Network 4.0 client software is installed on the remaining computers in the network. SYGATE manages all aspects of connecting the server and client computers in the local network to the Internet. SYGATE operation is transparent to users.

Key Benefits

SYGATE® Home Network 4.0 provides the following benefits:

Easy to Install SYGATE installs in minutes and requires no additional configuration. You are only required to install the SYGATE server component. If users would like the SYGATE client computers to have additional control, SYGATE client software can also be installed.

Easy to Use SYGATE has an intuitive graphical user interface that any Windows user can navigate. SYGATE starts up and runs in the background without manual intervention. SYGATE connects to the Internet automatically, on demand, as a background task whenever it detects Internet traffic on the local network. Rather than needing to manually dial the Internet each time, users can continue working uninterrupted, transparently sharing the connection with other users while they browse the World Wide Web, send and receive e-mails, chat, use ftp, and conduct other activities. Network users on non-Windows client machines (Macintosh, Solaris, and Linux) can also access the gateway via TCP/IP.

Easy to Administer The SYGATE Client enables users to remotely monitor and manage the SYGATE Server from any workstation on the TCP/IP network. SYGATE can automatically verify your system components during installation and operation to help identify configuration or connection problems. SYGATE maintains logs of usage and configuration settings that can be easily inspected as needed. Although usually not necessary, SYGATE is highly configurable and can be adapted to the needs of most any small network.

Cost-Effective SYGATE enables multiple network users to simultaneously share a single Internet connection, which eliminates the cost of additional phone lines, wiring, modems or adapters, and ISP accounts. SYGATE does not require a dedicated server. SYGATE delivers all the capabilities of similar products at an attractive price point.

Web Site Access Control SYGATE can be configured to *prevent access* to certain undesirable web sites ("black list" sites), as well as *restrict access* to only certain desirable web sites ("white list" sites). This *Permissions* feature is password-protected and allows parents to limit access to specific web sites.

Firewall Protection SYGATE can be configured, via its port blocking technology, to prevent outside intrusion of your local network from the Internet, ensuring that your network remains private even while connected to the Internet. SYGATE users can use a simple firewall embedded in SYGATE or download Sybergen Secure Desktop - an enterprise-quality personal firewall from http://www.sygate.com.

Extensive Online Help Responsive product support is provided via the web site at http://www.sygate.com, email, and an online help guide.

Comparison with Proxy and Hardware Solutions

SYGATE® Home Network 4.0 compares favorably with proxy and hardware solutions that are more costly to purchase, set up, and maintain:

	SYGATE® Home Network 4.0	Proxy	Hardware
Configuration	Automatic	Reconfigure every application running on the client, then reconfigure the server to resolve any conflicts that might arise.	Automatic
Adding Applications	No changes needed	Determine whether the application supports proxies and which port it uses. Configure the port on the server and configure the application to use the port. After learning that the port is already in use, create a gateway to another port, reconfigure the application, and hope it works.	No changes needed
Changing Servers	Automatic	Manually reconfigure the proxy server and start over.	Automatic
Transparency	Simply "telnet DomainName.com"	Configure the telnet server and client, telnet to the proxy server, and open DomainName.com.	Simply "telnet DomainName.com"
Feedback	Displays detailed messages that describe connecting events, such as finding the site, connecting to the site, and opening pages.	Displays only "connected" and, after a long time, you are informed that a proxy error occurred.	Depends on the manufacturer
Compatibility	HTTP,HTTPS, POP3, NNTP, SMTP, TELNET, FTP(PASV mode), IRC,ICQ, MS CHAT, RealAudio (TCP mode) and many other networking applications, including Quake III, StarCraft, and Diablo.	Reliant upon third-party software with individual manual configuration.	Very limited support.
Purchase & Replacement	Download trial version before purchase. Downloadable patches and upgrades.	Download trial version before purchase. Downloadable patches and upgrades.	Purchase and install the device, see if it works, and return it if it fails to obtain a refund or replacement.

SYGATE® Home Network 4.0 Licensing

To get a fully-licensed version or to upgrade from a previous version, you need to purchase a SYGATE license and obtain a serial number and registration code that allow you to "unlock" the trial version.

A variety of licensing options (3-user, 6-user, 10-user, 25-user, and unlimited- user) are now available to customers. A license includes one SYGATE Server and as many client licenses as you purchased. For example, the 3-user license includes one SYGATE Server and up to three concurrent client users. For pricing information, see the web site at http://www.sygate.com.

About Sygate Technologies, Inc.

Sygate Technologies, Inc. (formerly Sybergen Networks, Inc.) is a leading provider of secure Internet access management solutions for small- to medium-sized businesses, enterprise satellite offices, telecommuters and mobile users. Sygate.com, the online delivery and service portal, offers rapid deployment of secure access management products. Sygate Technologies, Inc. products are widely adopted with over one million users worldwide.

The first software product developed by Sygate Technologies, Inc., SYGATE 1.0, quickly became a "stealth" favorite among Internet aficionados when it was introduced in early 1998. Sygate Technologies, Inc. is now shipping SYGATE® Home Network 4.0 as well as Sybergen Secure Desktop and Sybergen Management Server, our distributed firewall solution, to protect and manage your Internet connection. SYGATE also partners with leading hardware companies for bundled solutions and offers partnership programs for VARs, ISPs, and systems integrators.

For the latest information about our products, see the Sygate Technologies, Inc. web site at http://www.sygate.com.

Contacting Sygate Technologies, Inc.

Sygate Technologies, Inc. sells its products directly through its web site at http://www.sygate.com. The web site provides downloadable trial versions of its software as well as product literature, documentation, and a FAQ for this product.

To contact Sygate Technologies, Inc.:

Sygate Technologies, Inc. Web Site	http://www.sygate.com
Sygate Technologies, Inc. Email	sgsupport@sygate.com
Product Support for SYGATE ® Home Network 4.0	http://www.sygate.com/support.htm
Mailing Address	Sygate Technologies, Inc. 6591 Dumbarton Circle Suite 102 Fremont, CA 94555 USA

INSTALLATION

Verifying System Requirements

The system on which you will install the SYGATE® Home Network 4.0 software must meet the following minimum requirements.

Server System

SYGATE software runs on a workstation that connects to the Internet via an analog modem, ISDN, DSL, cable modem, or DirecPC. The computer running SYGATE is referred to as the gateway.

Component	Requirement
Supported Platforms	One of the following operating systems: Windows 95 (MS DUN 1.3 upgrade required for Dial-up connections) Windows 98 Windows NT 4.0 (Service Pack 4 or higher) Windows 2000 Millennium
Processor	486 or higher for analog or ISDN modem sharing Intel Pentium® class or higher for DSL or cable modem sharing
Disk Space	10MB or more available disk space
Memory	32MB or more 16MB in Windows 95
Network Connection	Ethernet Network Interface Card (NIC) and software
Internet Connection	Internal or external analog, ISDN, DSL, or cable modem, or DirecPC
Network Protocol	TCP/IP (with Winsock 2.0 or higher)
ISP Account	An ISP account with Microsoft DUN 1.3 (or higher) or America Online 4.0 (or higher), a cable modem ISP, an DSL ISP, or a DirecPC account.

Client System

SYGATE client software runs on any workstation that connects to the SYGATE server system. Installation of the client software is optional. SYGATE will automatically detect clients and set-up a network for all computers with TCP/IP that support DHCP. If additional network information and control are desired, installing the client software will provide these features. The information and control are provided through a user interface located in the system tray.

Component	Requirement
Supported Platforms for optional SYGATE client software	One of the following operating systems: Windows 95 Windows 98 Windows NT 4.0 (Service Pack 4 or higher) Windows 2000 Millennium

	Users on the following platforms can also share, over the local TCP/IP network, the Internet connection managed by the SYGATE server: Apple Macintosh, Sun SparcStation, or Linux. To access the shared internet connection, users must manually assign the default gateway to address to the IP address of the SYGATE server.
Processor	486 or higher
Disk Space	10MB or more available disk space
Memory	32MB or more
Network Connection	Ethernet Network Interface Card (NIC) and software
Network Protocol	TCP/IP (with Winsock 2.0 or higher)

Network Configuration

SYGATE® Home Network 4.0 runs on workstations connected by Ethernet networks (but *not* ATM or token ring networks). Components of an Ethernet network include cables, network interface cards (NICs) in each workstation, and possibly hubs. This section briefly describes Ethernet network configuration requirements.

Cables

Ethernet networks use two types of cables: UTP or COAX, depending on throughput requirements:

Cables	Unshielded-Twisted Pair (UTP) (10 MBPS and 100 MBPS networks)	Thin Coaxial Cable (COAX) (< 10 MBPS networks)
Connector Type	RJ-45	BNC
Standards	10Base-T	10Base-2

For network cabling, follow these guidelines:

1 For UTP cable, you need a *hub* or a *cross-over cable* (which can connect two computers without a hub).
2 For COAX cable, you need two *terminators* instead of a hub.
3 For other types of network cards, see your network card vendor's documentation.
4 Other types of connections, such as normal telephone wire, power lines and some wireless network cards, are also supported in SYGATE® Home Network 4.0.

Network Interface Cards (NICs) & SYGATE Single NIC Technology

Every networked workstation needs to have a NIC (also known as a *network adapter*) installed and connected to the network cables. The NIC enables each networked PC to communicate with other computers or devices on the network.

As the leading Internet sharing software provider, Sygate Technologies, Inc. is proud to announce its next generation Internet sharing solution – Single NIC (Network Interface Card) Technology. While SYGATE is itself simple enough for small group of networked computers to share the Internet connection, it is very challenging for SOHO users to install a second network adapter into one of their computers. SYGATE Single NIC Technology solves the problem by making use of virtual NIC. The virtual NIC makes installing a second NIC unnecessary. We believe this solution will significantly simplify the process of sharing of cable modem and DSL connection for SOHO users.

1 Traditional LAN to share Internet connection with two Network Interface Cards:

Current Internet connection sharing (ICS) software requires a second network adapter to be used, see figure-1 below.

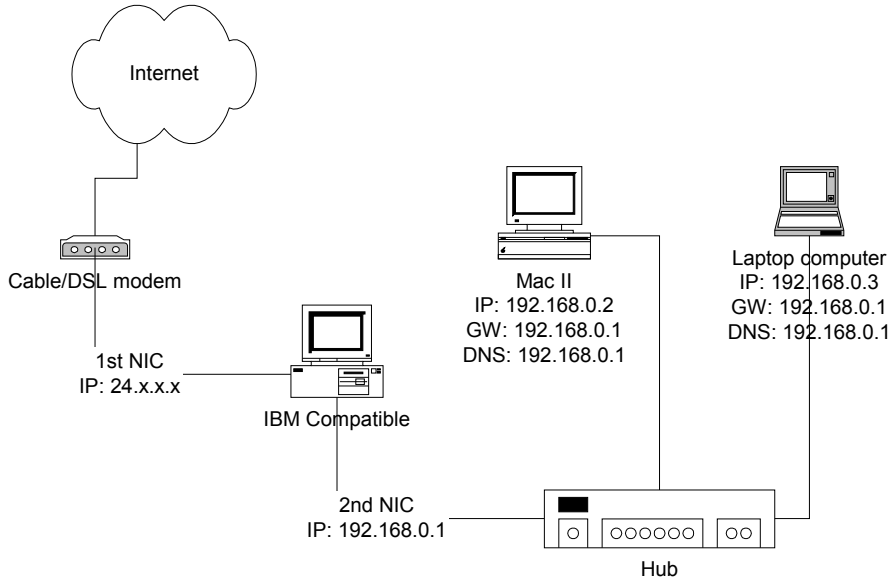


Figure – 1 **Two-NIC Internet sharing**

While the cost of a second NIC is not prohibitive, the installation of a second NIC in one computer is very complex. Users are required to open the computer case, find an empty slot, plug in the adapter, install a driver for the adapter, bind TCP/IP protocol to the adapter, and set the correct network parameters for that binding. These steps are not within the scope for 90% of our end users. As a result, the bulk of our technical support effort is focused on helping users set up their LAN. Although there are benefits for using two NICs in a server PC, there are significant reasons for SOHO users to implement a single NIC solution. Namely, professional IT support is costly. As an Internet security solution provider, our Single NIC Technology solution has also been designed with security in mind.

2 How Single NIC Technology is made possible:

Sygate Technologies, Inc. Single NIC is made possible by creating a virtual NIC. The real/installed NIC is used to connect to the cable/DSL modem. The virtual NIC is used to communicate with the other computers in the LAN.

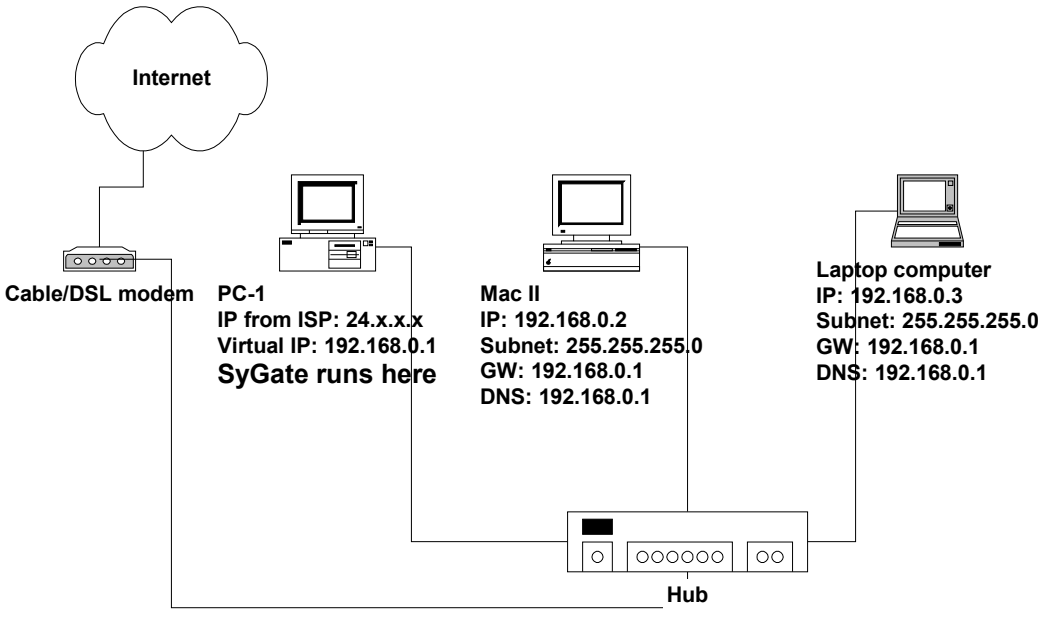


Figure 2 Single NIC Internet sharing

The server PC (PC-1) has one real IP assigned by the ISP. SYGATE uses 24.x.x.x as sample in the above figure. SYGATE runs on PC-1 and creates a virtual NIC with a virtual IP 192.168.0.1

3 Single NIC Technology installation:

The steps to connect the Ethernet cable:

1 Remove the PC-1 side of Ethernet cable between Cable/DSL and PC-1
2 Connect that end to a HUB (In most of the cases, no need to use Uplink port)
3 Connect the rest of the computers to the HUB

The steps to run SYGATE installation:

1 Access Internet from PC-1. It should work as it does before the re-cabling
2 Run the self-extracting SYGATE distribution file
3 SYGATE setup wizard will uncompress the files and copy them into the corresponding folders.
4 SYGATE will detect the active Internet connection, create a virtual NIC to have IP address of 192.168.0.1 (This value can be modified later using SYGATE Manager)

Hubs

A hub is a centralized connection device that concentrates cables for efficient connection and easy maintenance. Hubs are used whenever 10Base-T or UTP cabling is used.

Preparing to Install

Before you install the SYGATE® Home Network 4.0 software, be sure to complete the following steps:

Checking your TCP/IP Settings

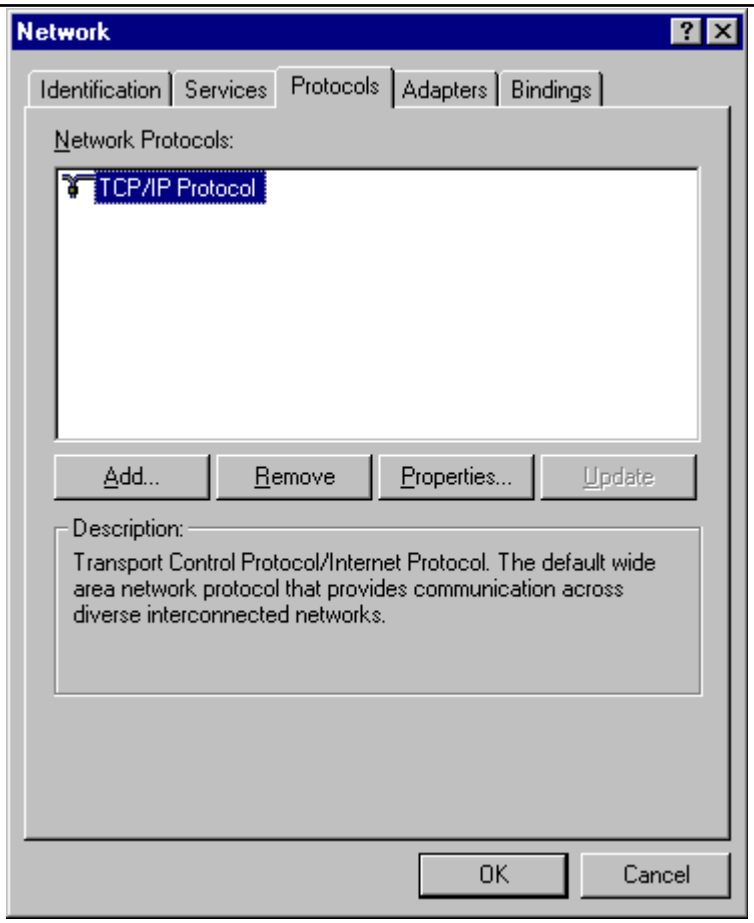
The SYGATE installation procedure determines whether the target workstation is properly configured with TCP/IP before installing the software. Installation succeeds only if the TCP/IP stack exists and the network adapter is properly bound to the TCP/IP protocol.

In Windows 98, Windows NT 4.0, Windows 2000, the TCP/IP stack is usually installed by default when you install the network adapter. However, on Windows 95, the TCP/IP stack is not automatically installed by default. Instead, you must install TCP/IP manually according to the instructions in Microsoft's and your NIC vendor's documentation. Note that TCP/IP installation may require you to insert your original Windows 95 installation CD.

Note: In Windows 95, you might need to explicitly bind your network adapter to the TCP/IP protocol.

To view the TCP/IP settings for a system: Choose Settings > Control Panel. Double-click the Network icon.

On the Configuration tab, scroll the list of network adapters and select an adapter that is configured for TCP/IP. Click the Properties button to display the properties for this network adapter.



Checking Your Internet Connection Settings

To share an analog modem or ISDN via a serial port, you need to properly configure the Dial-Up Networking Profile for your ISP (Start > Programs > Settings > Networking). You need to be able to successfully connect to your ISP and save your password (which is required to support SYGATE's Dial-on-Demand feature). For configuration instructions, see your ISP's documentation.

Note: For ISDN via Ethernet, DSL, cable modem, and DirecPC, you need to verify that these devices can connect to your computer through Ethernet.

Setting Up America Online

SYGATE® HOME NETWORK 4.0 requires America Online 4.0 or 5.0 to use the Dial-on-Demand feature. You must configure America Online to save your password. In addition, sharing AOL has the following requirements:

Share Connection to AOL: If you dial to AOL on the computer running the SYGATE Server, the other computers can access the Internet but *cannot* log into the same AOL accounts using other screen names. Using AOL 5.0 with the TCP/IP feature, multiple AOL accounts can be accessed simultaneously.

Setting Up Cable Modems, DSL, and DirecPC

For SYGATE servers that are connected via a cable or DSL modem, you need only one NIC for the Internet connection. Using SYGATE, you may use two NICs: one for the Internet connection and one for the local network connection. SYGATE will support both configurations. Using two NICs creates a secure separation between your local network and the Internet and also ensures that local network traffic won't create extra load on the backbone. SYGATE also works with DirecPC 2.0 and certain brands of one way cable modems (such as the SurfBoard 1200).

Installing the Software

This section describes how to install SYGATE software on network server and client computers. It is required that users install SYGATE on the server computer. Users may install the client software on the client computers if the server administrator would like to give client computers additional control and functionality. The server and client software are bundled in the same download file. During installation of SYGATE, select Server or Client installation.

Downloading the Software

You download the SYGATE® Home Network 4.0 software from http://www.sygate.com. The software comes in a single, self-extracting installation file that you run to install either the SYGATE Server or the SYGATE Client component.

To download the SYGATE software:

1 Connect to the Internet, if you have not already done so.

2 Using your web browser, go to http://www.sygate.com.

Follow the instructions on the web site to download the SYGATE software.
You normally download the software to a temporary installation directory (such as c:\temp) on the workstation on which you want to install the SYGATE software (usually the SYGATE Server machine). If you are installing on other workstations, you can simply copy the download file to those workstations. Alternatively, put the download file in a shared directory to which those workstations have access so that you do not need to copy the installation file.

Proceed to the installation instructions for the SYGATE Server.

Server Installation

To install the SYGATE Server component on a computer:

1 Determine the computer on which you will install the SYGATE Server software. This system *must* have an Internet connection and must meet the minimum system requirements described in Server System earlier in this document.

2 Verify that your network adapter card and software is properly installed and running according to the vendor's instructions.

3 Verify the ISP connection on this computer, following the procedure you normally use to connect to your ISP.

4 Close any extra open applications or windows.

5 Do one of the following:

1 If you are installing from a downloaded installation file, complete the procedure in Downloading the Software earlier in this section to obtain the download file and store it in a temporary installation directory.

2 If you are installing from a SYGATE install CD, insert the CD into the CD-ROM drive on your workstation.

6 In the Windows Explorer or NT Explorer, double-click the self-extracting installation file to run the SYGATE Setup program. After decompressing, the Welcome window appears.

7 Click Next. The Software License Agreement window appears. Review the license agreement, scrolling as needed, and then click Yes. The Choose Destination Location window appears.

8 If you want to change the destination location for the SYGATE software, click the Browse button. In the Choose Folder dialog box, type the target path or select a target folder from the Directories list, and then click OK. If the specified path does not exist, Setup prompts you to click Yes to create a new folder.

9 Click Next. The Select Program Folder window appears. Edit the Program Folder name, if you want.

10 Click Next. Setup copies the software files to the destination location and Setup starts testing your system configuration, including:

1 System settings
2 Network adapters
3 TCP/IP protocol and settings

Note: If any of these tests fail, Setup displays a message describing the problem and suggests possible actions. Click OK, and then click Exit to exit Setup. You need to correct the problem first. See *Troubleshooting Your Installation* in this document for more information.

If you are not currently connected to the Internet, follow the procedure you normally use to connect to your ISP, and then return to this window.

11 Click Continue. SYGATE® Home Network 4.0 verifies the ISP connection as well as TCP/IP settings. If your configuration is correct, Setup displays a message indicating that the test was successful.

Note: If any of these tests fails, Setup displays a message describing the problem and suggests possible actions. Click OK, and then click Exit to exit Setup. You need to correct the problem first. See *Troubleshooting Your Installation* in this document for more information.

12 Click OK. Then click Finish. For a first-time installation, the Register dialog box appears. Do one of the following:

1 If you have purchased your SYGATE license and obtained your serial number and registration code, complete the Register dialog box. Enter your user name, company name (optional), e-mail address (optional), serial number, and registration code, and then click OK.

2 If you have not yet purchased your SYGATE license, click the I Am a Trial User button.

13 Setup then prompts you to reboot your system. Click Yes. Your system reboots.

14 After your system starts up, launch the SYGATE Manager. From the Start menu, choose Programs > SYGATE > SYGATE Manager. The SYGATE Manager starts running.

Note: You will need to register your SYGATE software. For instructions, see To *Register SYGATE.*

Proceed to Client Installation

Client Installation

SYGATE client installation is optional. You would install the client software to perform specialized tasks, such as diagnose the status of your connection, hang-up or dial-up the Internet connection, or provide help information to the client. The SYGATE client software is most useful on the computer of an administrator or power user that would enable them to remotely manage the SYGATE server from their workstation, rather than the inconvenience physically going to the server machine.

To install the SYGATE client on a workstation:

1 Determine the workstation(s) on which you will install the SYGATE client software. This system must meet the minimum system requirements described in Client System earlier in this document.
2 Verify that your network adapter card and software are properly installed and running according to the vendor specifications.
3 For each workstation on which you install SYGATE server or client software, verify that the network connection exists between the client workstation and the server workstation.
4 Close any open applications or windows.
5 Do one of the following:
    1 If you are installing from a download installation file, complete the procedure in *Downloading the Software* earlier in this section to obtain the download file and store it in a temporary directory.
    2 If you are installing from a SYGATE install CD, insert the CD into the CD-ROM drive on your workstation.
6 In the Windows Explorer or NT Explorer, double-click the self-extracting installation file to run the SYGATE Setup program. After decompressing, the Welcome window appears.
7 Select “Client” to launch the installation of the SYGATE client software.
8 Client installation requires that an IP address be assigned to the client computer. A default IP address will be assigned to the computer. If the default IP address is acceptable, click Yes. If a customized IP address is desired, click NO and manually set the IP address in the Windows Network Settings Control Panel.
9 The SYGATE Network Diagnostic service will then evaluate the network system configuration, including: system settings, network adaptors, TCP/IP protocol, TCP/IP settings, Assigned IP addresses, and connection with the SYGATE Manager. Once the Diagnostic reads, *SYGATE Network Diagnostic Finished Successfully*, click Finish.

    NOTE: If any of these tests fails, Setup displays a message describing the problem and a possible solution. Click OK, and then click Exit to complete the setup. You need to correct the problem first, and then run the SYGATE Diagnostics again. If your configuration is correct, Setup displays a message indicating that the test was successful.

10 The Welcome message appears next. Please read carefully.

11 Click next. The Software License Agreement window appears. Review the license agreement, scrolling as needed, and click Yes. The Choose Destination Location window appears.

12 If you want to change the destination location for the SYGATE software, click the Browse button. In the Choose Folder dialog box, type the target path or select a target folder from the Directories list, and then click OK. If the specified path does not exist, Setup prompts you to click Yes to create a new folder.

13 Click Next. The Select Program Folder window appears.

14 Click Next. Setup then copies the software files to the destination location. The installation is then complete.

Configuring your Installation

During installation, the Setup program assigns TCP/IP settings automatically for each SYGATE Server or Client installation. In most cases, you do *not* need to change your configuration. For the SYGATE Server, the IP address is assigned by your ISP. For the SYGATE Client, the IP address is assigned dynamically by the built-in SYGATE DHCP server.

Note: The IP address is assigned to the Server or Client software, *not* to the physical workstation on which the software is installed.

Setup uses IP addresses from the Private IP Address class, which is a special class of IP addresses that is reserved for private, local networks (not to be confused with Virtual Private Networks, or VPNs). All computers on which SYGATE is installed will have the following default TCP/IP parameters:

Setting	Server Machine	Client Machine
IP Address	192.168. 0 . x	automatic (set by the floppy)
Subnet Mask	255.255.255.0	255.255.255.0
DNS	(*Do not change*.)	Automatic(same address as the local IP address of the SYGATE server, default I s192.168.0.1)
Gateway IP Address	None	Automatic (same address as the local IP address of the SYGATE Server. Default is 192.168.0.1.)

You do not need to manually change TCP/IP settings *unless* automatic configuration failed during installation or if you have client systems running on other platforms (such as Macintosh, Solaris, or Linux). To manually reconfigure TCP/IP settings, use the settings in the table above. For more information on SYGATE configuration, see *Configuring the SYGATE Manager.*

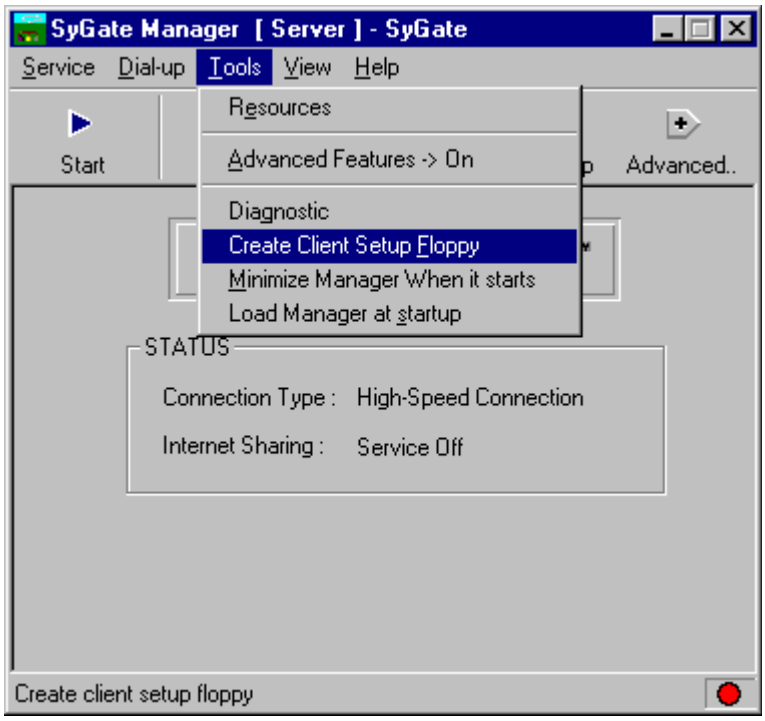
Note: We do *not* recommend using different TCP/IP settings unless you have experience with configuring TCP/IP networks.

Configuring SYGATE® Home Network 4.0 Client Computers

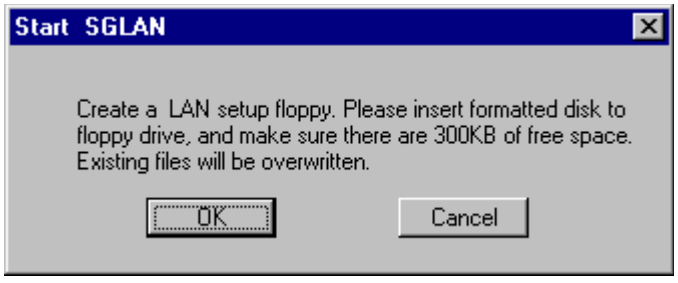
After you have installed and configured SYGATE® Home Network 4.0 server and clients properly, you can use the SYGATE SGLan utility to configure client computers if you decide not to use the SYGATE built-in DHCP service feature. **This occurs when SYGATE is set up in single NIC**

configuration. In this case, the SGLan utility will replace the function of the DHCP service and assign a static IP, Gateway IP and DNS IP to your network card on your client PC. If you have successfully set up your internal network with proper settings, you don't need to perform this step. If you change your server settings later, you may be required to run this utility on each client again. SGLan installation instructions are presented below.

The first step in installing SGLan on individual computers involves installing configuration files on a floppy disk. The disk is used to transfer configuration files to each computer. To create the floppy disk, select TOOLS and CREATE CLIENT SETUP FLOPPY from the menu bar.

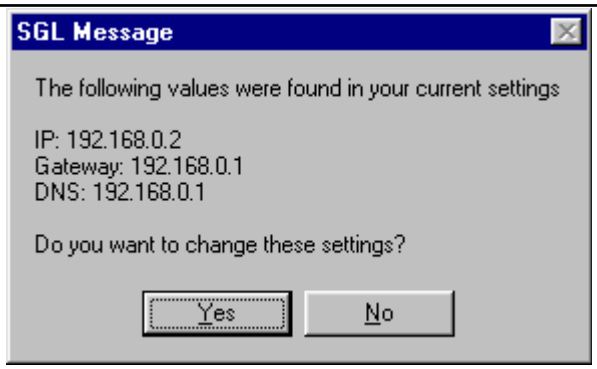


Second, insert a blank floppy compatible with each computer and press OK.

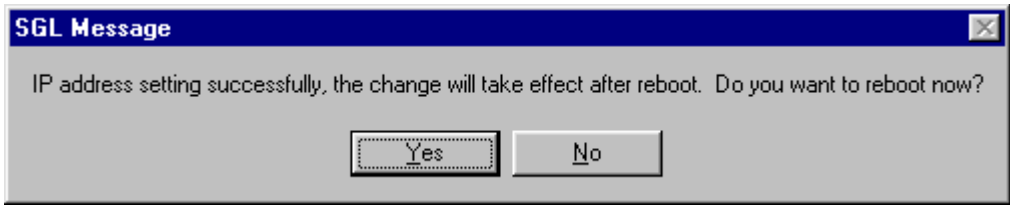


Third, remove the floppy form the SYGATE server machine and insert the floppy into the floppy drive of the computer. From the Start Menu, select RUN and type A:\SGLan.exe.

SGLan will automatically detect and install the appropriate configuration for SYGATE® Home Network 4.0 server computer and client computer communication. Based on the installation and configuration detected, SGLan will either report the current settings on the client computer and offer to change them, or SGLan will automatically configure the networked computers. If SGLan does report the current settings and offer to change your network configuration, press Yes. You will be required to reboot the client machine after SGLan has re-configured the client machine.



If SGLan automatically detects and re-configures the client machine, press Yes to conduct the required reboot.



Following the client reboot on each machine in the network, installation of SGLan and SYGATE® Home Network 4.0 should be complete.

Verifying Your Installation

After you have installed and configured SYGATE on the server computer and on at least one other networked computer, you must verify that your installation works correctly. To verify your installation…

1 Verify that the SYGATE Manager is running on the server machine and all other networked machines.

2 Launch the SYGATE Manager. From the Start menu, choose Programs > SYGATE > SYGATE Manager. The SYGATE Manager starts.

3 On each client workstation, open a browser and attempt to access the following URLs:
   1 http://216.167.96.118
   2 http://www.sygate.com

   If you encounter any problems, see *Troubleshooting Your Installation* for more information.

Troubleshooting Your Installation

If you encounter problems during installation:

4 Verify that the server and client workstations conform to the system requirements.

1 Verify that you successfully completed all installation steps on the server and any other networked machines.

1 If you manually configured TCP/IP, verify that you successfully completed all configuration steps on the server and any other networked machines.

1 Test the connection from the client computers to the server computer by going to the command prompt on the client workstation and typing the following command:

ping <*ServerIPAddress*> where <*ServerIPAddress*> is the IP address of the SYGATE Server (such as 192.168.0.1). You should receive a reply (not a timeout).

1 Test the connection from the server to the networked computers by going to the command prompt on the server workstation and typing the following command:

ping <*ClientIPAddress*> where <*ClientIPAddress*> is the IP address of the SYGATE Client (such as 192.168.0.2). You should receive a reply (not a timeout).

5 Test the ISP connection to the Internet by going to the command prompt on the client workstation and typing the following command:

Ping 216.167.96.118 where 216.167.96.118 is the IP address of the SYGATE web site http://www.sygate.com. You should hear the modem dialing or you should receive a reply (not a timeout).

1 Test the DNS by going to the command prompt on the client workstation and typing the following command:

Ping www.sygate.com. You should see a reply and the host name should be resolved to 216.167.96.118.

1 Test the DNS by opening your web browser and going to the following URL:

www.sygate.com. You should see the web site appear.

1 Review the following list for common problems and possible solutions:

Problem	Possible Cause	Suggested Action(s)
Network Adapter Test Failed	Network Interface Card (NIC) is not properly installed & configured.	Install and configure the NIC according to your vendor's documentation.
Cannot access http://216.167.96.118	Problem with ISP connection to the Internet.	Check your dial-up connections and configure your system according to your ISP's documentation.
Can access http://216.167.96.118 but not www.sygate.com	Problem with domain name services (DNS) configuration.	On the SYGATE Client system, set the DNS to be the same as for the SYGATE Server.
SYGATE Client cannot access the SYGATE Server	Problem with network connection or TCP/IP configuration.	Ping the server machine's IP address from the command prompt on the client machine. Ping the client machine's IP address from the command prompt on the server machine. If either of these tests fail (you see a timeout instead of a reply, then check your internal network configuration.

Look through the FAQ for information about the problem you encountered. The FAQ provides immediate answers to most common problems.

If you cannot resolve the problem, see *Getting Product Support.*

Getting Product Support

Sygate Technologies, Inc. provides product support for this product via its web site and e-mail. To get product support, go to http://www.sygate.com/support.htm, and look for information about any issues you may have encountered.

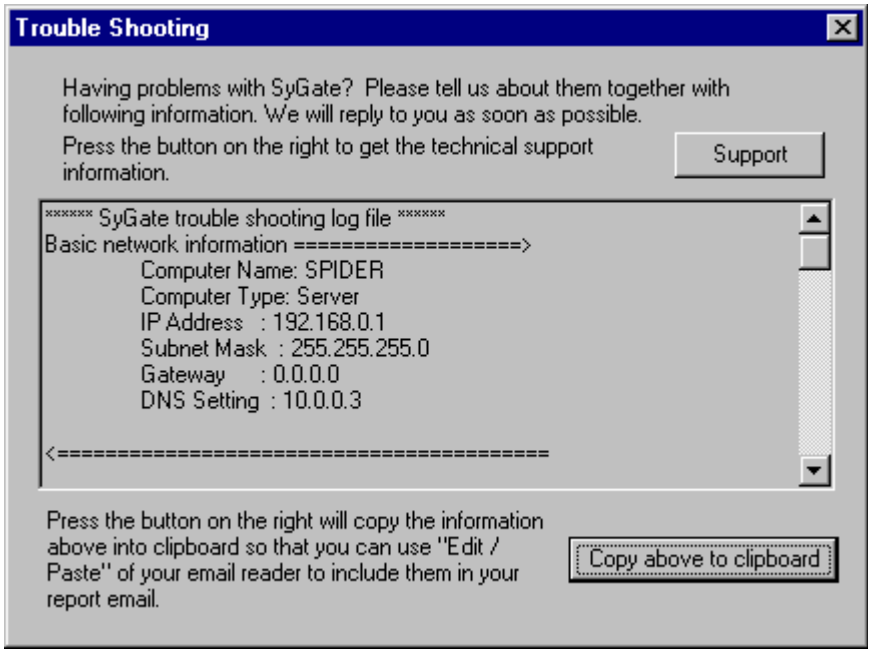
Be sure to check our FAQ if you don't see a solution published on this page. If our online support material does not help you resolve your particular issue, you can send an email to sgsupport@sygate.com too obtain additional assistance.

1 The following steps will provide us with more information that may result in faster resolution of any issues you are experiencing.

2 Compose an e-mail on the workstation on which the SYGATE Server is installed.

3 Provide a detailed description of the issue you are having.

4 Open the SYGATE Manager (Server) window - on the toolbar, click the Troubleshooting tool. The Troubleshooting dialog box appears.



5 Click the Copy Above to Clipboard button and then choose "paste" under the Edit menu in your email application.

6 Go to the command prompt (Start > Programs > Command Prompt) and type ROUTE PRINT and press ENTER. The command displays the workstation's network address, mask, server address, interface, and metric.

7 Mark the output text (Edit > Mark), highlight the section with your curser, and copy it to the Clipboard (Edit > Copy).

8 Open the e-mail window, paste this text into the window, and then send the e-mail message to sgsupport@sygate.com.

PURCHASING YOUR SOFTWARE

To get a fully-licensed version or to upgrade from a previous version, you need to purchase a SYGATE license and obtain a serial number and registration code that allow you to "unlock" the trial version. Sygate Technologies, Inc. offers a variety of licensing options (3-user, 6-user, 10-user, 25-user, or unlimited-user). For pricing information, see http://www.sygate.com. You can securely purchase the software in either of two ways:

1 From within the SYGATE Manager on the server machine, dial your ISP, if needed. On the toolbar, click the Order/Upgrade tool and follow the on-screen instructions.

1 From your browser, open http://www.sygate.com and go to the purchase section of our website.

Upon receiving your order, Sygate Technologies, Inc. will process your purchase request and e-mail a serial number and registration code that you will then use to register the software.
Registering Your Software

Once you have purchased the SYGATE software and obtained a registration code, you need to register your copy in order to "unlock" the trial version to support the number of licenses you bought. You can also re-register if you purchased an upgrade or increased the user count.

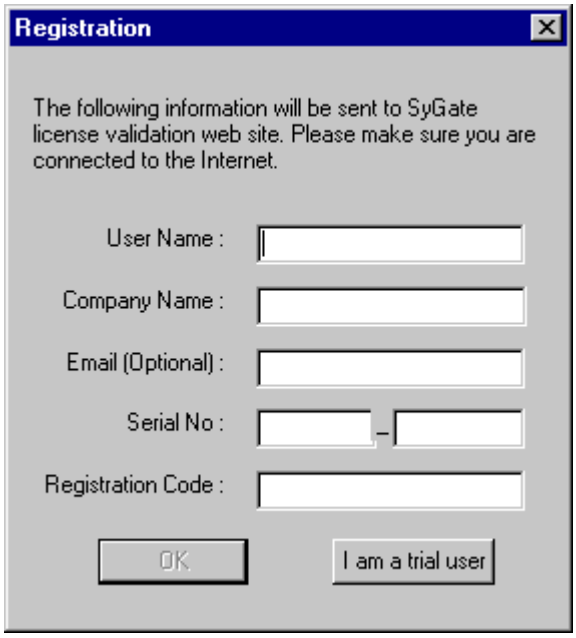
To register SYGATE

1 Connect to your ISP, if you are not currently connected.

2 On the toolbar, click the Registration tool. The SYGATE End User License dialog box appears.

3 Review the license agreement, scrolling as needed, and click Accept. The Registration dialog box appears.

4 Enter your user name, company name (optional), e-mail address (optional), serial number, and registration code. Click OK.



ADMINISTRATION

Running SYGATE® Home Network 4.0

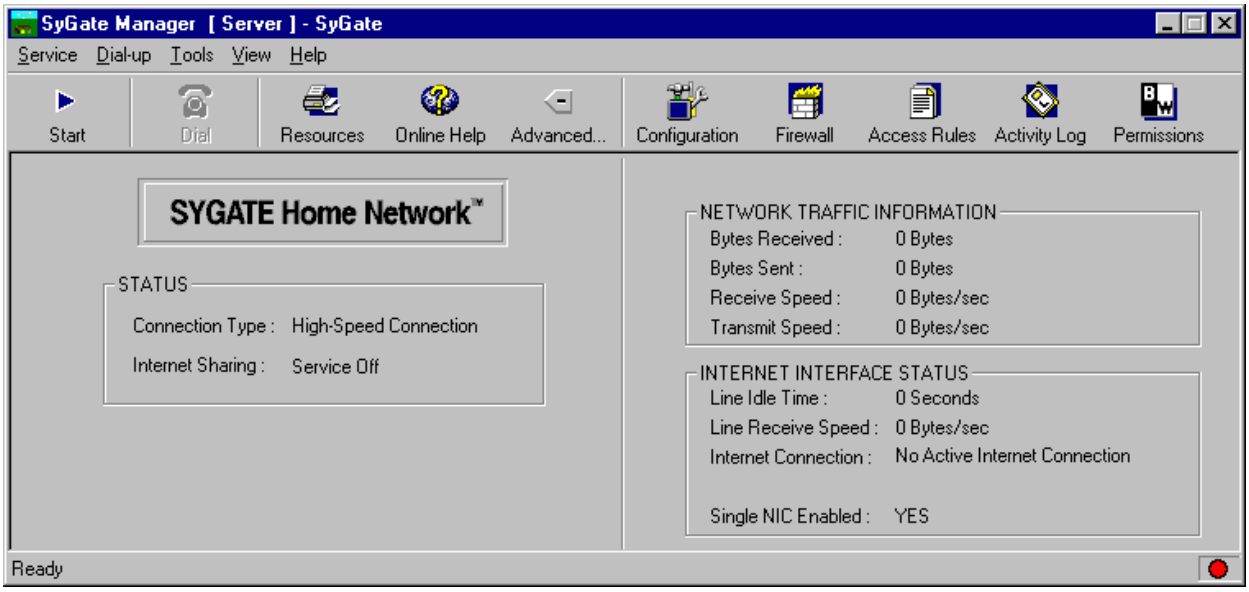
If Auto-Start SYGATE Server is enabled in the Configuration dialog box, SYGATE starts when the system reboots. To manually start SYGATE® Home Network 4.0:
Choose Start > Programs > SYGATE > SYGATE Manager.

Once opened, the SYGATE Manager presents several options to configure and control your network. The icons shown on the SYGATE Manager include:

Start/Stop – Initiates and Cancels the SYGATE Internet connection sharing functionality
Dial/Hang-up – Initiates and disconnects a dial-up networking connection
Resources – Provides Printer and File sharing capabilities amongst the network computers
Online Help – Provides clear direction and troubleshooting advise for users
Advanced – Enables users to configure their SYGATE network, control network security, and manage Internet Content. Press Advanced and start to use these dynamic features to configure your network environment.

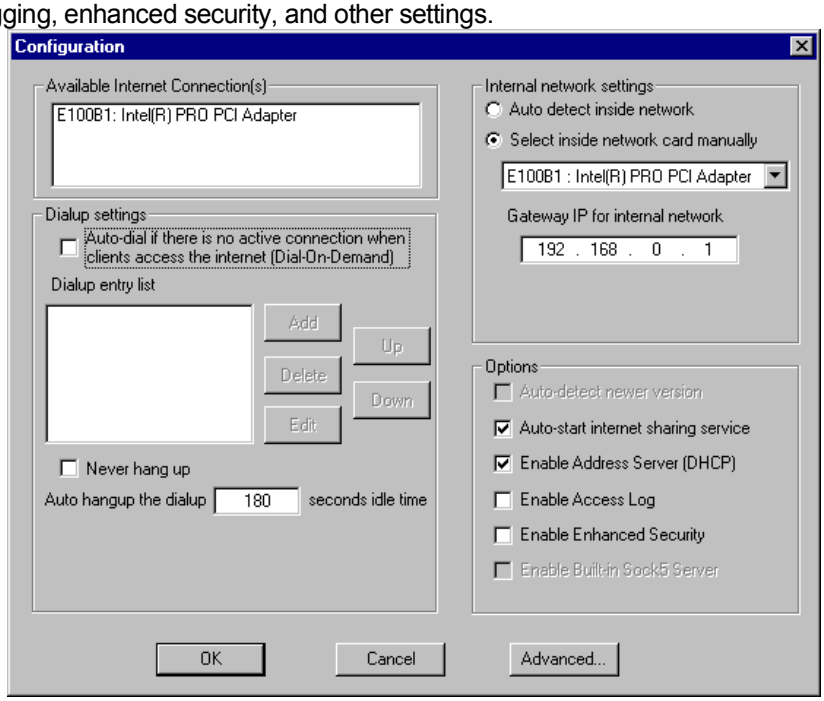
The Advanced features available to SYGATE users include:
Configuration – Optimize the SYGATE technology by configuring the network connection settings
Firewall – Protect your personal data with SYGATE Secure Desktop personal firewall
Access Rules – Create rules that allow new Internet applications to work with your dynamic firewall
Activity Log - Evaluate the Internet traffic on your network
Permissions – Control undesirable content and surfing on the Internet.

Detailed user instructions for these features are presented below.



Configuration

You can configure the SYGATE Manager to manage Internet connection settings, dial-on-demand, logging, enhanced security, and other settings.



On the toolbar, click on the Advanced button and then the Configuration tool. The Configuration window appears (as displayed above). Change configuration settings as needed.

Select Network Adapter for LAN Manually. If the workstation has two network adapters, this option is automatically selected when the Internet adapter is selected. If this workstation has three or more network adapters, select the network adapter that connects to the local network.
Options:

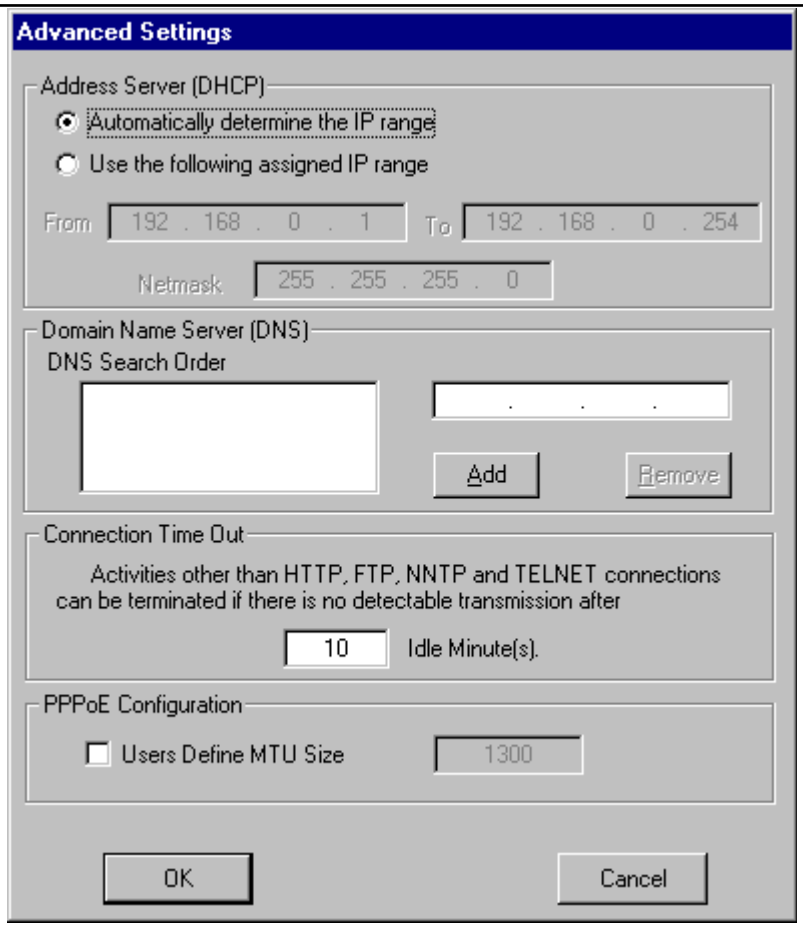
Auto-Start SYGATE Service. Select this setting to have SYGATE automatically start and run in the background when the server machine boots up (you do not need to add SYGATE Manager to the Startup folder). Clear this setting if you want to start the SYGATE service manually by choosing Start > Programs > SYGATE > SYGATE Manager (other network users will not be able to share the modem until the SYGATE service is running).

Enable SYGATE Built-In DHCP Server. Select this option to enable SYGATE's Dynamic Host Configuration Protocol (DHCP) server, which can assign a temporary IP address to a host automatically when the host connects to the network. Clear this option if you want to use the server machine's Windows DHCP server instead.

Enable Access Log. Select this option to enable the SYGATE Client Access Log, which tracks all Internet access and DNS requests from the client machines on your network. The log file resides on the server machine in the SYGATE directory. To view the log, open this file with a text editor, such as Microsoft Notepad or WordPad (Start > Programs > Accessories).

Enable Enhanced Security. Select this option to enable SYGATE's enhanced security feature, a circuit level firewall that prevents users outside your network from accessing the computers within your network. With Enable Enhanced Security activated, SYGATE blocks incoming Internet traffic to ports 1 through 1000 and ports 5000 through 65536. Note that, with this setting enabled, the server machine as well as any web servers on your network will not be accessible from the Internet through the shared connection managed by the SYGATE Server.

If you want to configure *advanced settings*, click Advanced.



Change configuration settings as needed.

DHCP. These settings control SYGATE's built-in DHCP Server. To change these settings, the Enable Built-In DHCP Server option must be selected in the Configuration dialog box.

The range of IP Address. If you want to restrict the range of IP addresses that SYGATE's built-in DHCP server assigns to SYGATE Clients, specify the starting and ending IP address and the Netmask. You would do this to prevent conflicts with other IP addresses on your local network.

DNS Server Search Order. If you want to specify back-up DNS servers in case your primary DNS server fails, specify the search order according to your ISP's instructions. Click Add, enter the IP address of the DNS Server, and click OK. The new entry appears in the list, in the order in which the roll-over will occur.

Timeout: If you want to *override* the default timeout of a special application, specify an default idle time (in minutes). For example, if you specify 10 minutes and you run a game program that normally disconnects if it's idle longer than a 5-minute timeout period, the timeout will be extended to 10 minutes.

Set MTU size. SYGATE should automatically diagnose the server computers correct MTU size. Under certain circumstances users may wish to manually configure the MTU size. Enter the MTU size into the space provided.

When finished, click OK to save your changes. Your configuration settings take effect immediately.

Starting and Stopping the SYGATE Service

You can dynamically start and stop the SYGATE service. When the server computer attempts to hang-up, the administrator will be notified if client computers are currently accessing the Internet. At that point, the server administrator can elect to hang-up or continue to share the Internet connection with the client computers.

To start the SYGATE service from within the SYGATE Manager: From the toolbar, click the Start Service button. The Start Service button (green arrow) becomes inactive, and the Stop Service button (red square) becomes active, indicating that service has started.

To stop the SYGATE service from within the SYGATE Manager: From the toolbar, click the Stop Service button. The Stop Service button (red square) becomes inactive, and the Start Service button (green arrow) becomes active, indicating that service has stopped.

Configuring TCP/IP Parameters Manually for Two NIC or Dial-up Configuration

Every computer on your network must have TCP/IP protocol installed. The operating systems for Windows 95/98/2000/NT and Macintosh OS (7.5.5 or later) include TCP/IP software. Although TCP/IP is not installed by default on Windows 95, you can install TCP/IP from the Windows 95 CD.

On client machines, SYGATE is compatible with operating systems other than Windows, such as Macintosh and UNIX. However, the SYGATE Server must run on Windows 95/98/NT/2000/Millenium. In the Windows environment, TCP/IP is compatible with IPX and NETBEUI protocols.

During a typical installation, SYGATE automatically assigns the TCP/IP parameters for the network according to the following example:

Server machine	
IP Address:	192.168.0.1
Subnet mask:	255.255.255.0
DNS:	Leave unchanged
Gateway IP Address:	None
Client machine #1	
IP Address:	192.168.0.2
Subnet mask:	255.255.255.0
DNS:	192.168.0.1
Gateway IP Address:	192.168.0.1
Client machine #2	
IP Address:	192.168.0.3
Subnet mask:	255.255.255.0
DNS:	192.168.0.1
Gateway IP Address:	192.168.0.1
Client machine #3	
IP Address:	192.168.0.4
Subnet mask:	255.255.255.0
DNS:	192.168.0.1
Gateway IP Address:	192.168.0.1

On the client machines, notice the pattern of the IP Addresses—the last value increases by one on every subsequent client machine. Notice also that the values for the DNS and Gateway IP Address for every client machine are the same as the IP Address of the server machine.

If the SYGATE installation fails to set the TCP/IP parameters according to the above specifications, you can set them manually.

To manually set the TCP/IP parameters

1 From the Taskbar, choose Start > Settings > Control Panel.

2 Double-click the Network icon.

3 From the Network window, then select the TCP/IP protocol for your internal network card, then choose properties. *For Windows NT, select the protocols tab, choose TCP/IP, then select properties.*

4 Enter the correct IP Address, Subnet Mask, and Gateway IP address for the workstation from which you are working. Click OK.

Configuring TCP/IP Parameters Manually for One NIC Configuration

Every computer on your network must have TCP/IP protocol installed. The operating systems for Windows 95/98/2000/NT and Macintosh OS (7.5.5 or later) include TCP/IP software. Although TCP/IP is not installed by default on Windows 95, you can install TCP/IP from the Windows 95 CD.

On client machines, SYGATE is compatible with operating systems other than Windows, such as Macintosh and UNIX. However, the SYGATE Server must run on Windows 95/98/NT/2000/Millenium. In the Windows environment, TCP/IP is compatible with IPX and NETBEUI protocols.

NOTE: Do not adjust the current settings of the one (Internet) NIC.

During a typical installation, SYGATE automatically assigns the TCP/IP parameters for the network according to the following example:

Server machine	
External IP Address:	Do not change
Virtual IP	192.168.0.1
Client machine #1	
IP Address:	192.168.0.2
Subnet mask:	255.255.255.0
DNS:	192.168.0.1
Gateway IP Address:	192.168.0.1
Client machine #2	
IP Address:	192.168.0.3
Subnet mask:	255.255.255.0
DNS:	192.168.0.1
Gateway IP Address:	192.168.0.1
Client machine #3	
IP Address:	192.168.0.4
Subnet mask:	255.255.255.0
DNS:	192.168.0.1
Gateway IP Address:	192.168.0.1

On the client machines, notice the pattern of the IP Addresses—the last value increases by one on every subsequent client machine. Notice also that the values for the DNS and Gateway IP Address for every client machine are the same as the IP Address of the server machine.

If the SYGATE installation fails to set the TCP/IP parameters according to the above specifications, you can set them manually.

To manually set the TCP/IP parameters

1 From the Taskbar, choose Start > Settings > Control Panel.

2 Double-click the Network icon.

3 From the Network window, then select the TCP/IP protocol for your internal network card, then choose properties. *For Windows NT, select the protocols tab, choose TCP/IP, and then select properties.*

4 Enter the correct IP Address, Subnet Mask, and Gateway IP address for the workstation from which you are working. Click OK.

Sharing Internet Connections

To connect to the Internet from a client machine, launch an Internet application such as a web browser. This will cause the server machine to dial out to its ISP to make an Internet connection. This is the dial-on-demand setting.

To enable dial-on-demand

1 On the toolbar, click the Configuration tool.
2 Select Enable Dial-on-Demand.

To disable dial-on-demand

1 On the toolbar, click the Configuration tool.
2 Clear Enable Dial-on-Demand.

To connect to the Internet from a server machine, use standard methods, such as launching a web browser or using your ISP's dialer program.

To share Internet connections, the server and client machines must be connected in a local network using Ethernet and running TCP/IP protocol to communicate with each other. The only computer that must have a Internet connection is the one acting as the server. The Internet connection may be analog, cable, ISDN, DSL, or DirecPC. The machine acting as the server must also have an Internet access account.

Although client machines may have Internet connections as well, only the SYGATE Server system is required to have Internet access in order for all workstations on the network to share Internet access.

You can also share your Internet connection with an outside computer that dials into your network. The computer accessed by the outside computer directs the connection to the IP address of the server.

Resource Sharing

SYGATE allows you to share drives (hard drives, floppy drives, and CD-ROM drives) and printers on your local workstation with other users on the local network.

To share resources:

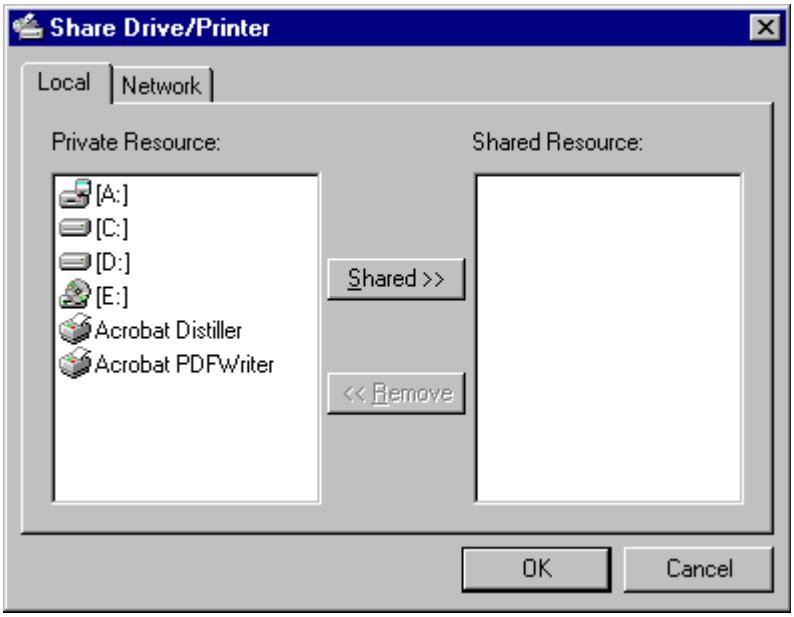
1 On the toolbar, click the Resources tool. The Resources dialog box appears.

2 In the Private Resource list, select a resource that you want to share.

3 Click the Share button. The selected resource appears in the Shared Resource list.

4 Click OK. Users on other workstations are now able to use this drive or printer from their workstation.

NOTE: Share Drive/Print operates in read *only* mode.



To unshare a shared resource

1 On the toolbar, click the Share Drives/Printers tool. The Share Drives / Printers dialog box appears.
2 In the Shared Resource list, select a resource that you no longer want to share.
3 Click the Remove button. The selected resource appears in the Private Resource list.
4 Click OK.

Users on other workstations are no longer able to use this drive or printer from their machines.

Managing Web Site Access

SYGATE's Permissions Editor allows you to control access to specific web sites. You can use SYGATE to prevent users (such as children) from accessing undesirable sites, and you can restrict access to authorized sites only. The Permissions Editor maintains two lists:

1 Black List prevents users from accessing the IP addresses specified therein.
2 White List restricts users to accessing only the IP addresses specified therein.

The Permissions feature uses IP (Internet Protocol) addresses, rather than domain name website addresses, to identify and authenticate web sites. Acquiring the IP address of a web site is easily accomplished. The steps required are presented below.

Determining the IP Address of a Web Site

The Permissions feature uses IP addresses (such as 216.167.96.118), not domain names (such as http://www.sygate.com) to control web site access.

If you do not know the IP address of a specific web site…

Go to the Command Prompt (which is located in Program section of the Start Menu).

Type the following command, and then press ENTER

ping <*domain name*>

Where <*domain name*> is the fully qualified domain name (such as http://www.sygate.com).

Example: ping www.sygate.com

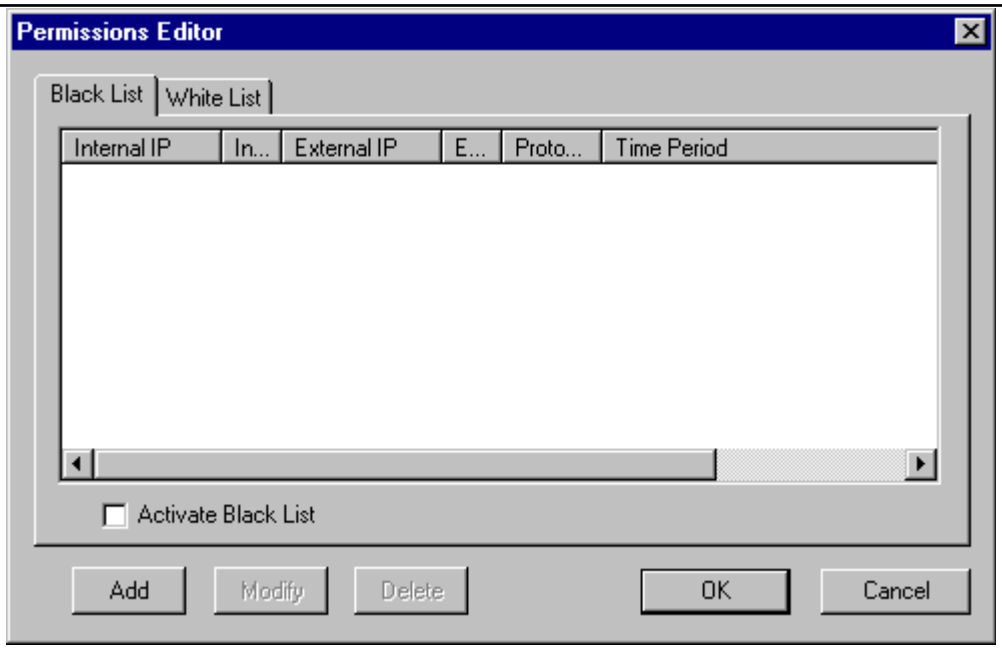
You should see a reply similar to the following example (after pinging http://www.sygate.com):

Pinging www.sygate.com [216.167.96.118] with 32 bytes of data:
Reply from 216.167.96.118: bytes=32 time=141ms TTL=252
Reply from 216.167.96.118: bytes=32 time=130ms TTL=252
Reply from 216.167.96.118: bytes=32 time=121ms TTL=252
Reply from 216.167.96.118: bytes=32 time=120ms TTL=252

The IP address (216.167.96.118) appears next to the domain name. This is the IP address you would specify for the External IP address that is required by the Permissions Editor.

Starting the Permissions Editor

To start the Permissions Editor: From the Toolbar, click the Advanced button and the Permissions Editor button. A password window appears. Enter a valid password (the default is no password). Click OK. The Permissions Editor window appears.



Managing the Black List

The Black List prohibits your network users from accessing certain sites *as long as* they are connecting to the Internet through a shared Internet connection that is managed by SYGATE.

Note: Make sure that you select the Enable Black List checkbox.

To add a web site's IP address to the Black List: In the Permissions Editor, select the Black List tab.

1 Click the Add button. The Add Record window appears.

2 Select the Protocol Type from the drop-down list (TCP or UDP).

3 Leave blank to have this entry apply to all internal IP addresses, or enter the Internal IP Address of the workstation you want to prevent from accessing this web site.

4 Select a Port Number for the Internal IP Address.

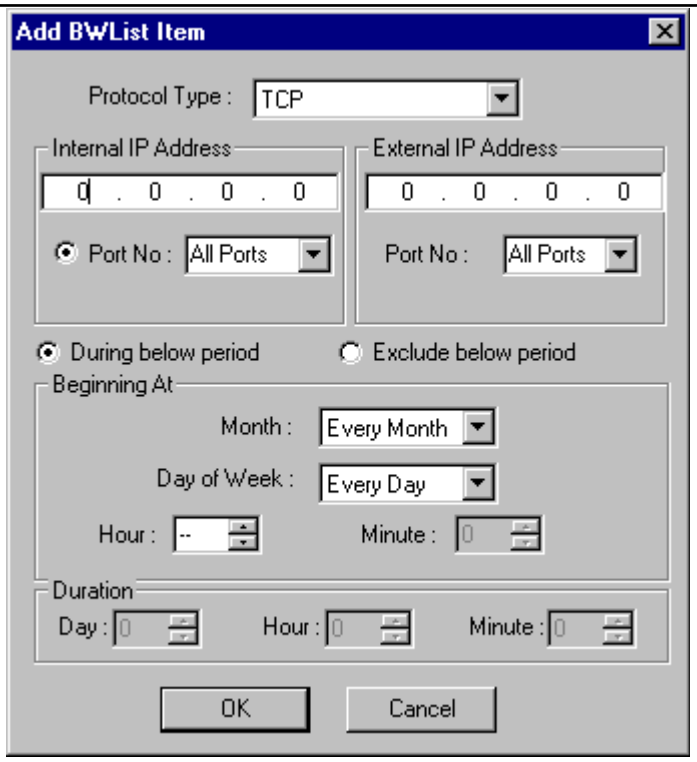
5 Enter the External IP Address.

6 Select a Port Number for the External IP Address.

7 Select one of the following:
   1 Include below period
   2 Exclude below period

8 Select Beginning Time settings, including Month, Day of Week and Hour. The default settings are Every Month and Everyday.

9 Select Duration settings to specify the duration of time you want the entry on the Black List to be in effect (Day, Hour and Minute). Click OK.

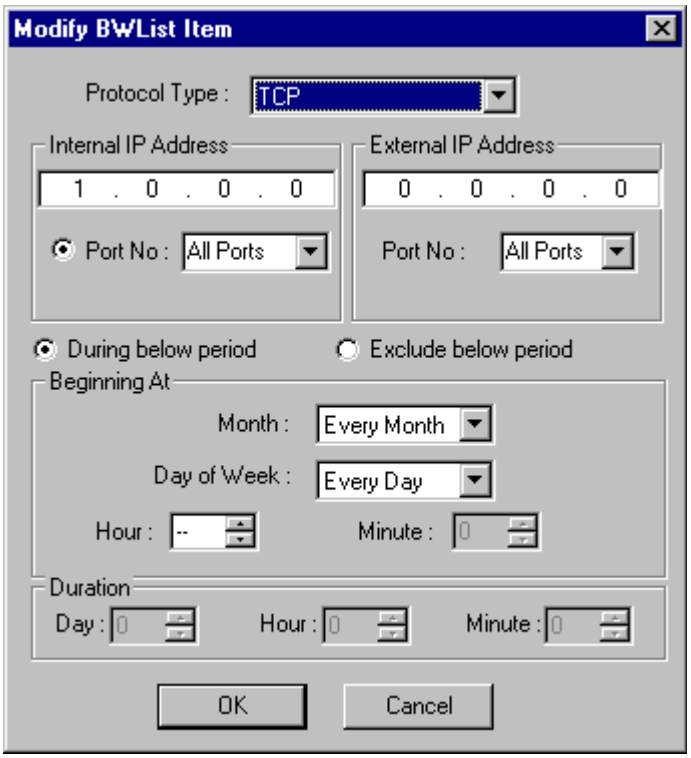

Add BWList Item
Protocol Type :
TCP
Internal IP Address
0 . 0 . 0 . 0
Port No :
All Ports
External IP Address
0 . 0 . 0 . 0
Port No :
All Ports
During below period
Exclude below period
Beginning At
Month :
Every Month
Day of Week :
Every Day
Hour :
--
Minute :
0
Duration
Day :
0
Hour :
0
Minute :
0
OK
Cancel

To modify an entry in the Black List

1 In the Permissions Editor, select the record you want to modify by clicking the item shown under the Internal IP column.

2 Click the Modify button. The Modify Record window appears.

3 Make any desired modifications. Click OK.



To delete an entry from the Black List:

1 In the Permissions Editor, select the record you want to delete by clicking the item shown under the Internal IP column.

2 Click the Delete button. The SYGATE Manager prompts you to confirm deletion. Click Yes.

Managing the White List

The White List restricts your network users to accessing only certain sites *as long as* they are connecting to the Internet through a shared Internet connection that is managed by SYGATE.

Note: Make sure that you select the Enable White List checkbox.

To add a web site's IP address to the White List:

1 In the Permissions Editor, select the White List tab. Click the Add button. The Add Record window appears.

2 Select the Protocol Type from the drop-down list (TCP or UDP).

3 Leave blank to have this entry apply to all internal IP addresses, or enter the Internal IP Address of the workstation that you want to restrict to this web site.

4 Select a Port Number for the Internal IP Address.

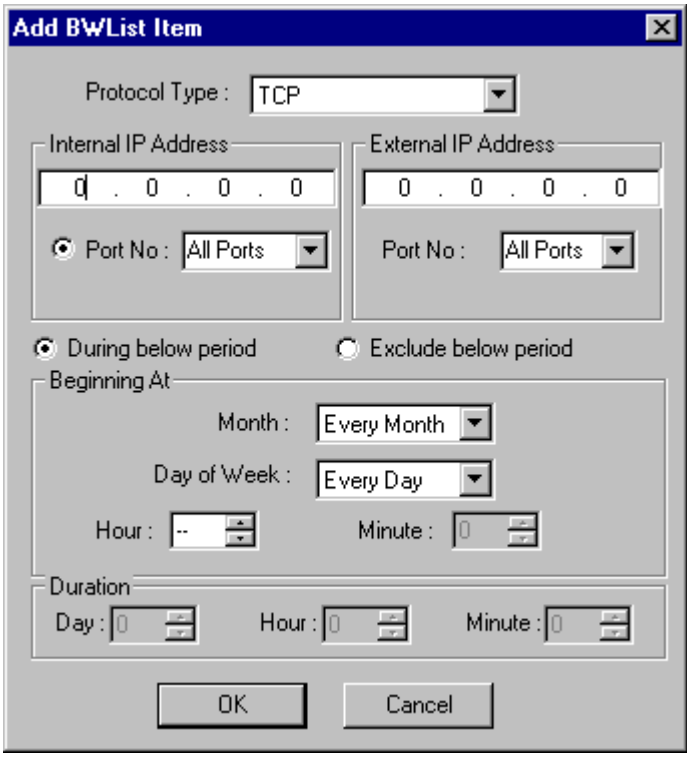
5 Enter the External IP Address.

6 Select a Port Number for the External IP Address.

7 Select one of the following:
   1 Include below period
   2 Exclude below period

8 Select Beginning Time settings, including Month, Day of Week and Hour. By default, Every Month and Everyday are selected.

9 Select Duration settings to specify the duration of time you want the entry on the White List to be in effect (Day, Hour and Minute). Click OK.

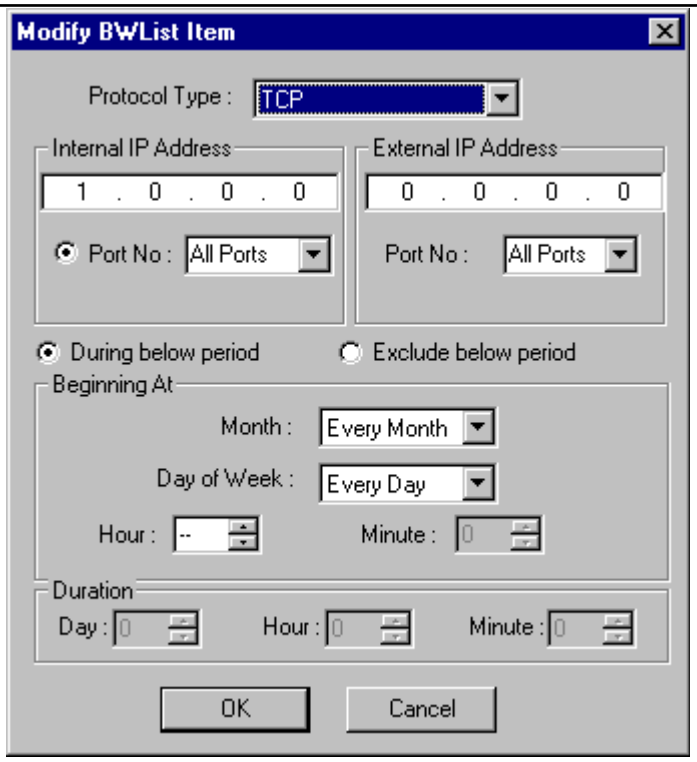


To modify an entry in the White List:

1 Select the record you want to modify by clicking the item shown under the Internal IP column.

2 Click the Modify button. The Modify Record window appears.

3 Make any desired modifications. Click OK.



To delete an entry from the White List:

1 Select the record you want to delete by clicking the item shown under the Internal IP column.

2 Click the Delete button. The SYGATE Manager prompts you to confirm deletion. Click Yes.

Access Rules

Introduction

The features and functions of SYGATE are based on Network Address Translation (NAT). The benefits of this technology include robust Internet sharing and personal firewall protection. In addition, SYGATE offers the ability to customize your use with new Internet applications. Access Rules allow you to specify to the SYGATE server a set of parameters that determine the specific ports applications should use. The Access Rules feature gives users the opportunity to configure new applications far beyond the capabilities of other products on the market today. A special user interface has been designed to allow users to generate these rules.

Internet applications communicate when a client machine makes a request that opens a channel (port) on the server machine and a response is returned from the intended party on the Internet through that same channel - communication is established. For some Internet applications, a client machine makes a request that opens one port and the intended party then responds through a different port (which is closed). SYGATE then protects your network by not allowing information to come into your network on ports that are closed. Therefore, the returning information is dropped - and communication is broken. Access Rules allow such applications to function properly and communicate over the Internet.

Two ways to acquire Access Rules

Download Sygate Technologies, Inc. has developed an extensive list of Access Rules that permit new Internet applications to work with SYGATE. The list of applications can be viewed at http://www.sygate.com/support/applications.htm. To obtain an Access Rule for a specific application, follow these steps.

1 Open the SYGATE Manager and *Press* **Advanced** and **Access Rules.**

2 To view existing rules, *click* on **Add** and *click* on **Import a rule from System rule**. The available list of system Access Rules will appear. Using the drop-down box select the desired rule and *click* **OK**. If an Access Rule for an application is not available, press cancel and proceed to step 3.

3 Open your browser, connect to the Internet and proceed to http://www.sygate.com/support/applications.htm. A list of applications for which rules have been established is listed on the page.

4 **Right**-click on the application you would like to obtain. Select **Save Target As** and determine where the Access Rule should be saved.

5 Open the SYGATE Manager and *Press* **Advanced** and **Access Rules**.

6 *Press* **Import** to upload the Access Rule from the location where it has been saved. The new Access Rule will automatically saved in the SYGATE Folder within the Program Files directory.

7 *Click* on the new Access Rule to view the rule in the Access Rule Configuration format.

Develop your own Access Rules The Access Rules Editor has been designed to encourage development of customized Access Rules. These rules will enable users to run new Internet applications in their unique environments. The following sections have been prepared to provide Access Rule development information.

NOTE: Users cannot use the Access Rule to bypass “enhanced security mode” if you are hosting a server (FTP, Web) on the SYGATE server. The Access Rule is only used

in communication with the SYGATE clients - the SYGATE server does not utilize the Access Rules. If users attempt to host an application server on the SYGATE server the enhanced security must be disabled and the Access Rule file must be left unchanged.

Creating Your Own Access Rules

Developing Access Rules is accomplished by opening the Access Rules user interface, which is located in the Advanced section of the SYGATE Manager. The Access Rules user interface provides existing Access Rules and permits users to develop new rules. Before developing new access rules, please be aware of the following considerations.

Access Rule Considerations

In using the Access Rule feature there are issues to consider:

1 When you enable an application through an Access Rule, you're essentially opening ports for the Internet to get into your network - which can be a potential security risk. Access Rules can be specified to open certain ports only for a specified period of time after a client computer has initiated an application that is defined within an Access Rule - and then to close the specified port so that it can't be access from the Internet.

2 If you wish to setup an application such as a web page server, file server or email server, we've defined several sets of Access Rules that you can enable to make these applications work. If additional information is required, please contact Sygate Technologies, Inc. at sgsupport@sygate.com.

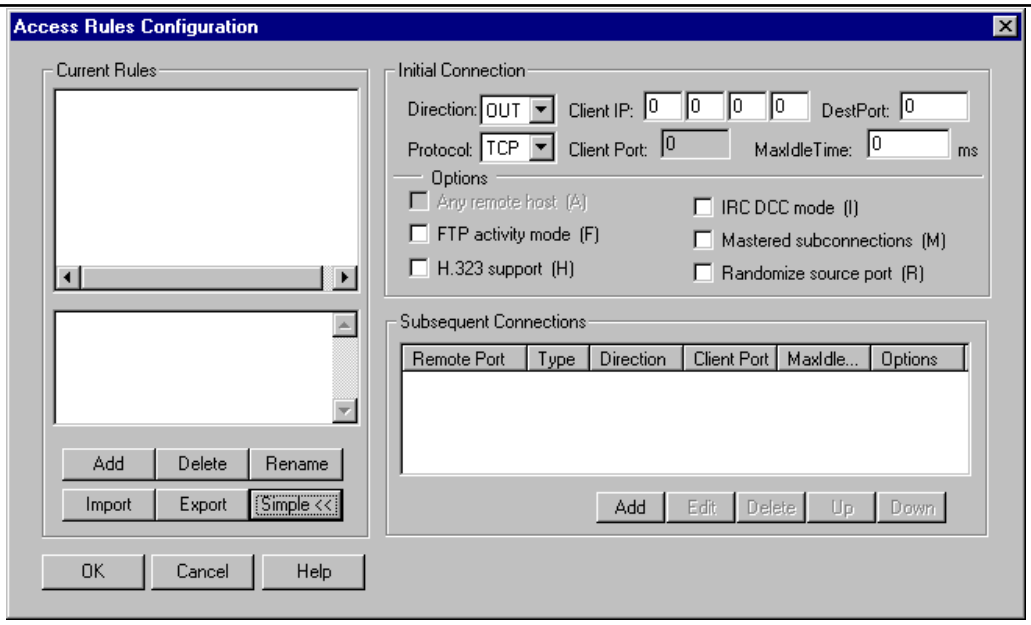
3 See the complete list of applications currently supported at http://www.sygate.com/support/applications.htm. If, during the process developing a new access rule, technical support is required, please contact Sygate Technologies, Inc. at sgsupport@sygate.com.

Access Rule Tutorial

Steps to create an Access Rule in the Access Rule Configuration editor are presented below. The example presented below illustrates the development of the **Net 2 Phone** Access Rule. The syntax for other rules is identical. Please use this rule (and other imported rules) as a reference when necessary. Users are required to develop an understanding of the operating environment required to use the new Internet application.

1 Open the SYGATE manager and *Click* on **Advanced** and **Access Rules**.

2. *Click* on **Detail** to open the Access Rules Editor and view the Access Rule development area.

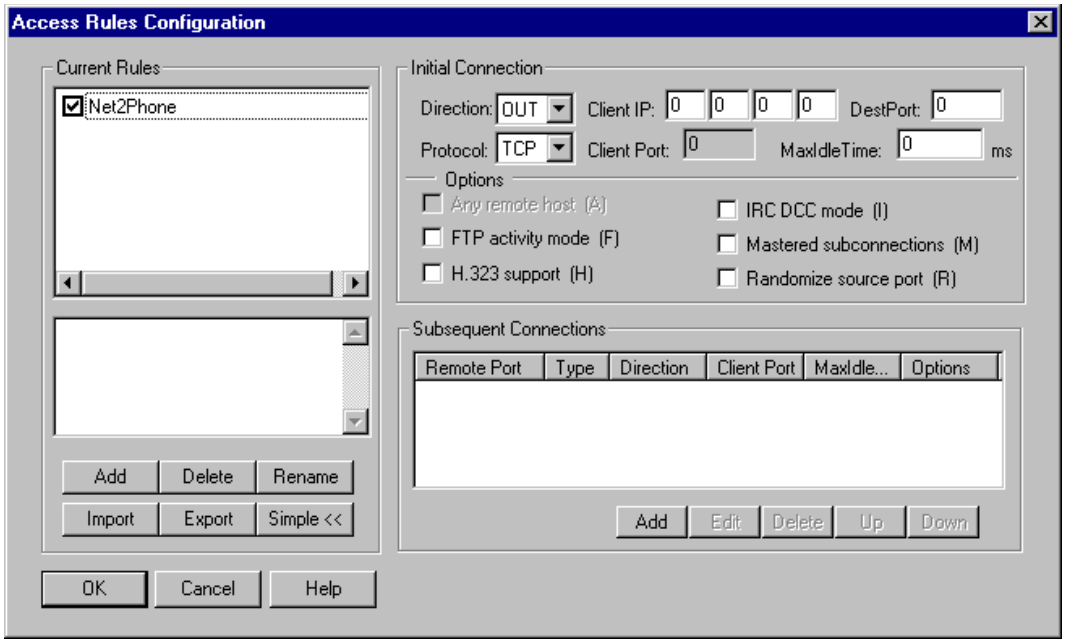


3. *Click* on **Add** to create a new Access Rule.

4. *Click* on **Rename** and name the Access Rule after the new Internet application.

5. *Select* the Access Rule to develop and begin creating the Access Rule code.

6. The first Access Rule development step is to dictate the computer settings on the initial communication between the new application and the Internet. These settings are addressed in the Initial Connection area. This rule will be effective when a client sends OUT a UDP packet with the destination port as 6801. The Client IP address of 0.0.0.0 means it can be any networked client on the network. A description of the input options is presented below.



INITIAL CONNECTION FIELDS

Direction: IN or OUT. This states that the connection coming IN to your network from a remote source or it is going OUT of your network to a remote source.

Protocol: TCP or UDP

Client IP: This field tells the server where to pass the incoming packets with the destination port defined by DestPort. This field has to be set to 0.0.0.0 for Sub-trans-x. For the Initial Communication, this field must be set to the IP of one of the clients.

Client Port: This field only applies to IN connections and tells the server which port of the Client IP to send the incoming packet with the destination port defined by DestPort. If this value is 0, the packet will be sent to the same port as the destination port of the incoming packet. If this value is not zero, the packet will be sent to the defined port instead of the original destination port.

DestPort: The port required by the application to ensure proper communication.

MaxIdleTime: This field tells the server to close the tunnel after certain idle miniseconds. Set to 0 for the server to use the default idle timeout value.

Options:

M This value tells the server to close all Sub-tunnels if the triggering connection no longer exists due to either timeout or user application disconnect, etc. This option is only valid in Triggering Transaction.

R This option tells the server to use a different source port to send the packet. It is general best to use the R option if the application supports it.

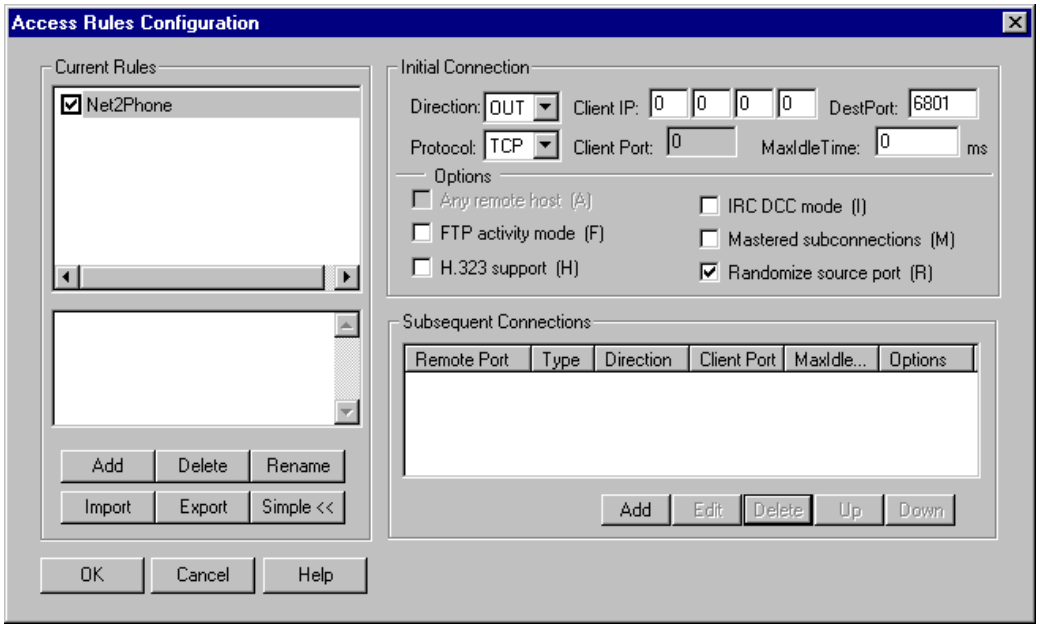
H H.323 specific rule. The server will process the packets according to H.323 protocol. Users should not use this option to define new rules.

A This option permits communication with Any Remote Host. Used only for IN connections

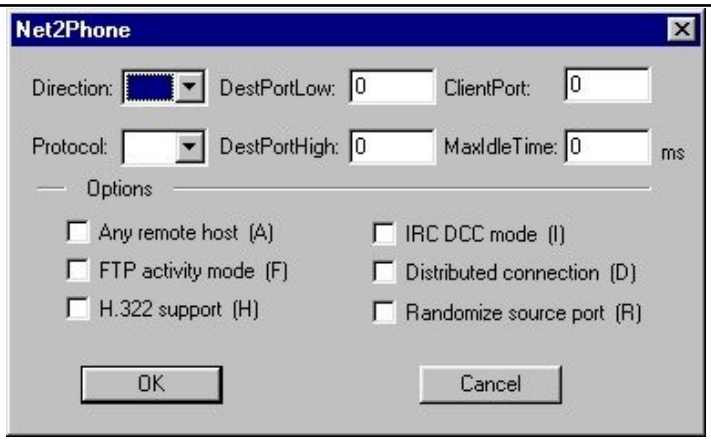
F FTP activity mode specific. Users should not use this option to define new rules.

I IRC DCC mode specific. Users should not use this option to define new rules.

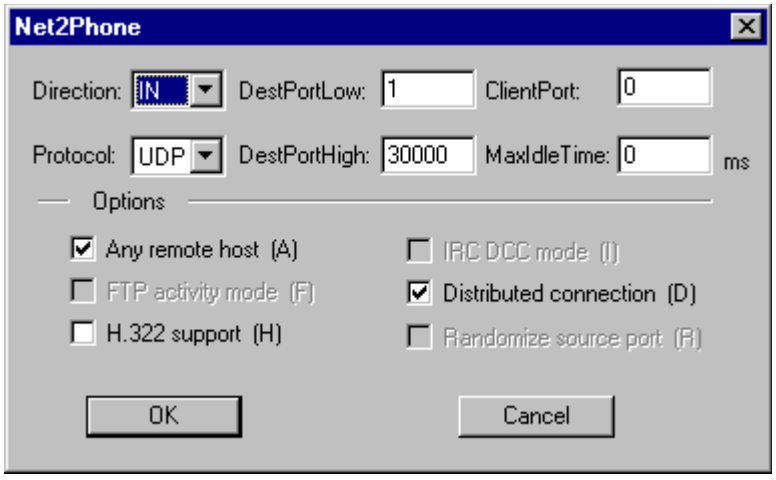
7. *Select* the desired options. Net2Phone requires that Randomize source port (R) is selected. Additional options that can be selected are described above.



8. On going communication with the new Internet application is supported by inputting information into Subsequent Connections. *Select* **Add** in the Subsequent Communication area.



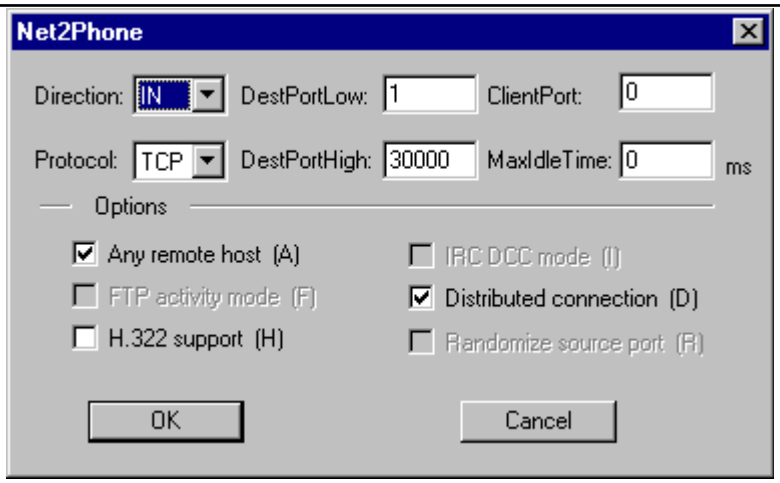
9. In this Access Rule, the server software will create a dynamic tunnel for IN-coming (Direction) UDP (Protocol) packets at port 6801. This is reflected in the Access Rule as shown below. Once completed, *select* **OK.**



SUBSEQUENT COMMUNICATION FIELDS

Direction:	IN or OUT
ProtcolType:	TCP or UDP
DestPortHigh:	The upper bound of the destination port range
DestPortLow:	The lower bound of the destination port range
Client Port:	The client port generally remains zero, except in cases where client port translation is required. Client port translation is required when packets enter one port on the server computer from the Internet and are required to be redirected to another port on the client computer. In such cases, enter the required client port.
MaxIdleTime:	This field tells the server to close the tunnel after certain idle miniseconds. Set to 0 for the server to use the default idle timeout value.

10. In this Access Rule, IN-coming UDP packets must also be specified. From the Access Rule Configuration editor, Subsequent Connection Area, *select* **OK** again. The rule must specify that the server software will create a dynamic tunnel for IN-coming (Direction) TCP (Protocol) packets at port 6801. Options A and D were also selected. Once complete, *select* **OK.**



11. The Access Rule is then complete and can be edited as necessary using the Access Rules Configuration user interface.

Access Rule Tools

Packet Listener

Packet Listener is a utility you can use to identify IN coming and OUT going packets that can help you to create a custom Access Rule. To use this utility, you MUST run BOTH the Packet Listener and your special application on the machine running the server software. It will monitor the ports while your special application is running and grab the first 500 packets. With this information, users are able to see what the special application is trying to do - and then build your own Access Rule to allow that application to be run from the client computers on your network. It is important to determine which packets are sent by your application and which packets are associated with normal LAN traffic. Packet listener should be run at least three times without using your application to evaluate the normal traffic on the LAN.

NOTE: When you run the Packet Listener, it will automatically stop the server software's service. After using this utility, you should manually start the server software's service using the start button in the Manager program.

Use Packet Listener in the following fashion to determine which ports are used:

1 Download SyPkt.exe (or another Internet application) to the desktop of the computer running the server software.
2 Double click on SyPkt.exe on your desktop.
3 Click on the Start button within Packet Listener.
4 Open your special application and start your connection.
5 Watch the Packet Listener and make sure that the buffer is grabbing packets. Keep using your special application until either the buffer is full or you've achieved the results you need from your application.
6 If the buffer isn't full in Packet Listener, click the stop button.
7 On the Packet Listener, click on the details button. This should drop down a window to show you all of the transactions that have taken place. The transactions should appear as follows:

UDP: 192.168.0.1:4319 --> 200.202.298.160:53
UDP: 200.202.298.160:53 --> 192.168.0.1:4319
TCP: 192.168.0.1:4320 --> 200.202.298.160:80
TCP: 200.202.298.160:80 --> 192.168.0.1:4320

Packet Listener Analysis In the example above, the computer running the server software initiated a transaction, assigned a random port (4319), and attempted an OUT going UDP connection at port 53 to 200.202.298.160. IP address 200.202.298.160 then returned to SYGATE IN on the same port 53. The next transaction assigned a random port (4320) and attempted an OUT going TCP connection at port 80 to 200.202.298.160. IP address 200.202.298.160 then returned to the server IN on the same port 80. This example is a DNS connection followed by an HTTP connection. This is only an example. Some applications do send out a DNS request when they start-up. The connection does not initiate the transaction.

Packet Listener can be downloaded from http://www.sygate.com/support/applications.htm. Additional information relating to Access Rules can be obtained at http://www.sygate.com/support.

Running the SYGATE Diagnostics

You can run the SYGATE Diagnostics whenever you encounter a problem running the SYGATE server or client computers. To run the SYGATE Diagnostics:

From the SYGATE Server – Open the SYGATE Manager and select Diagnostics from the Tools menu.

From the SYGATE Client – Right click on the SYGATE client icon located in the System Tray. Click on the Diagnostics option. NOTE: If the SYGATE icon is not located in the System Tray, open SYGATE from the Start menu by clicking on Start > Programs > SYGATE > SYGATE Manager.

The SYGATE Diagnostics loads and begins testing your system configuration, including:

1 System Settings
2 Network Adapters
3 TCP/IP protocol and settings
4 Assigned IP addresses
5 Connection with Management Server

NOTE: If any of these tests fail, an error message will be displayed with potential troubleshooting options. It is recommended that you correct the error and re-run Diagnostics before proceeding. See Troubleshooting Your Installation or visit http://www.sygate.com/support for more information.

FREQUENTLY ASKED QUESTIONS

This is a brief list of frequently asked questions about SYGATE. We have a much larger FAQ available on our website at http://www.sygate.com/faq.htm if the information below doesn't answer your question.

Does SYGATE support VPN?

SYGATE works with AltaVista Tunnel, Bay VPN, Shiva VPN and PPTP (Microsoft VPN) and supports one VPN client on the SYGATE network. This allows your SYGATE network client to communicate with your companies LAN through a secured connection. If you wish to have a VPN server, the SYGATE server can be used in conjunction with Microsoft's PPTP service on Windows NT - allowing remote VPN clients to reach your SYGATE network. SYGATE's enhanced security benefits VPN as it blocks non-VPN connections from coming into your LAN from the ISP.

How secure is SYGATE?

SYGATE offers a one-way wall between your public network (the Internet) and your private network (your LAN). The only connections that will be allowed to your LAN are those that you specify in SYGATE's configuration file (apprule.cfg) or those that are initiated by the LAN itself. Incoming connections are refused unless they are requested by your network or are specified in the apprule.cfg file.

Can I dial into my SYGATE network?

The dial-in service must be on a computer behind SYGATE and not on the computer running SYGATE. The remote dial-in computer must also be using the same subnet and gateway as the computers on your local network.

What if I have more computers than my SYGATE license is for?

If you have a three-user license you can have three simultaneous connections to the Internet. If an additional computer tries to use the Internet and all the connections are taken - it will simply not work. If one of these three users closes their Internet applications, the additional user on your network will then have access. If you run into this issue frequently, we recommend buying an upgrade from us to allow more connections.

How do I setup my non-Windows computers to work with SYGATE?

For Macintosh computers, the easiest way is to make sure that the SYGATE's built-in DHCP server is running on the SYGATE server and configure your Macintosh TCP/IP Control Panel for Ethernet and to obtain it’s settings from a DHCP server. Then restart your Macintosh. SYGATE® Home Network 4.0 DHCP server does support Linux (tested on RedHat 6.0).

How come I cannot receive NetMeeting calls on my SYGATE clients?

SYGATE® Home Network 4.0 cannot route incoming NetMeeting calls to client’s computers because NetMeeting dynamically assigns the ports used from the caller. The SYGATE server computer can both send and receive NetMeeting calls. SYGATE networked clients can only initiate NetMeeting calls.

How come my SYGATE clients cannot send or receive email?

If using a cable modem, we’ve seen this with customers where the "domain suffix" defined by the ISP needs to be set for each computer on the network. If you experience this issue and have a

cable modem, enter the same domain suffix on the client computers as defined on the SYGATE server in the TCP/IP settings. If you are unable to obtain these settings, we have a automated page to provide this information with instructions on setting it up at http://www.sygate.com/support.htm.

How do I set my SYGATE server to automatically dial when it's used?

If the SYGATE server computer does not automatically dial the Internet when it's used on it's own, there may be a problem with the connection settings. Verify that the connection settings in the Internet options Control Panel is set to dial automatically.

How come my SYGATE clients cannot browse the Internet?

Make sure that your browser preferences (Netscape) or Internet options control panel (Internet Explorer) are not setup to use a proxy server for your Internet connection. Continue with the following troubleshooting steps after you have verified you are not setup to use a proxy server.

Make sure that the SYGATE server can browse the Internet. If it cannot, you must fix this problem as it's most likely a problem with the Internet connection.

Check the DNS settings in the TCP/IP settings on the SYGATE server and go to a command prompt and type "ping xxxx" and replace xxxx with the IP's of the DNS servers listed. If you fail to get a reply from the first one listed, the ISP's primary DNS server is down. Switching the order listed in the TCP/IP settings will usually correct the problem and the clients should be able to use the Internet.

If you can ping and browse okay from the server but you are still unable to browse the Internet from the client computers - try pinging the client's IP address from the SYGATE server. If you fail to get a reply, we recommend checking if the two network computers cannot communicate via TCP/IP with one another are cables, hubs, network drivers. and the TCP/IP software installation.