WinGate

V1.3

Users Guide

DISCLAIMER OF WARRANTY.

This Software is provided on an "AS IS" basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement. The entire risk as to the quality and performance of the Software is borne by you. Should the Software prove defective, you and not Adrien de Croy assume the entire cost of any service and repair. You must determine that the Software sufficiently meets your requirements.

LIMITATION OF LIABILITY.

Under no circumstances and under no legal theory, tort, contract, or otherwise, shall Adrien de Croy or his suppliers or Resellers be liable to you or any other person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. In no event will Adrien de Croy be liable for any damages in excess of Adrien de Croy's list price for a license to the software, even if Adrien de Croy shall have been informed of the possibility of such damages, or for any claim by any other party. This limitation of liability shall not apply to liability for death or personal injury to the extent applicable law prohibits such limitation.

1 Welcome to WinGate

Welcome to the new release of WinGate. WinGate is basically a multiple proxy server, Telnet server, FTP Server, SOCKS (V4.0) server and extra bits rolled into one.

Set up correctly, WinGate will allow users on a Local Area Network (LAN) that is not directly connected to the Internet to access the Internet via a single machine on the LAN which is connected, either via a dial-up modem / ISDN connection, or second Ethernet interface. WinGate will allow you to use the following:

- Email
- World Wide Web
- FTP
- News
- Telnet
- WAIS
- and others

WinGate can save you money by removing the need to get a separate dial-up account, with phoneline and modem for each user that wants access to the Internet. Now they can all use the one link, at the same time.

1.1 System Requirements

The following systems are presented as a rough guideline for running WinGate:

Small LAN: 2-5 users

- 486 DX2/66 8Meg RAM or better
- Windows 95 or Windows NT
- 28k8 modem
- TCP/IP installed

Mediun LAN: 5-20 users

- 486 DX2/66 20Meg RAM or better
- Windows NT
- ISDN connection
- TCP/IP installed

Large LAN: 20+ users

- Pentium 90 with 32Meg RAM
- Windows NT
- 28k8 modem
- TCP/IP installed

1.2 Software Licensing

For the time being, WinGate is released on a policy of expiration on a fixed date. After this date a registration key is required to continue operation of the software. These registration keys are purchased from Qbik Software. The software is registered for a maximum number of concurrent users. Keys are available for the following numbers of users:

- 1 User
- 2 Users
- 5 Users
- 10 Users
- unlimited

Prices may vary from time to time. See below for information on how to find out more about WinGate.

1.3 WinGate home page

This document is updated with new releases, however, for the latest documentation, an FAQ, prices, and software updates, you should check the WinGate home page at:

http://nz.com/NZ/Commerce/creative-cgi/special/qbik/wingate.htm

In the event that this page moves, an Internet search-engine query for WinGate, Qbik, or "Adrien de Croy" should quickly locate it.

1.4 Updates

Updates are generally released every 6 weeks or so, when the previous version is set to expire. Version 1.3 is set to expire on 28 February 1996.

2 Features

WinGate provides the following features:

- SOCKS V4 Server
- WWW Proxy Gateway (HTTP only - later releases will support FTP, Gopher, WAIS, and HTTPS)
- FTP Gateway
- Telnet Gateway
- Mapped Links
- Rules based Firewall
- Dial-on-demand

The SOCKS V4 server allows any SOCKS-compatible client application (such as Netscape) to operate fully.

The WWW Proxy Gateway allows the use of WWW browsers such as Netscape or Mosaic to access the World-Wide Web. This release still only supports the use of HTTP protocol, so browsers should use the SOCKS server for other protocols.

The FTP Gateway allows use of FTP client applications that support the username@hostname method of firewall traversal. Examples of this are WS_FTP, and CuteFTP, as well as command-line FTP clients.

The Telnet Gateway allows use of Telnet clients to connect to remote servers.

Mapped links (sometimes called “plugs”) are used to support applications which do not support traversing a firewall, or working through a proxy server. This includes applications such as most email packages and news readers.

The rules based firewall applies to all connections through WinGate. WinGate can very easily be set up to allow or deny connections to or from specified hosts, or URLs (Addresses for Web pages) containing specified words or parts of words.

In addition, the new interface allows you to monitor who is accessing the gateway.

Dial-on-demand allows more convenient use, by obviating the need to physically initiate a connection to an Internet Service Provider.

3 Fundamentals

If you know a few fundamental things, then the concepts of WinGate become a lot easier, and it becomes correspondingly easier to set up for those services listed here, as well as other specific applications you may have.

Gateways

The first main thing to keep in mind is, that (under normal situations) when using the Internet through WinGate, at no time are you directly connected to any machine beyond your LAN (in fact unless you are routing on the gateway machine this would be physically impossible). You may seem to have a connection to the Internet, but this is only because WinGate is connecting out for you, and passing data back to you.

This means that in ALL circumstances, the machine wanting access to the Internet connects to the machine running WinGate (the Gateway machine).

One of the first questions that should spring to mind is "how does WinGate know where to connect to?". The answer to this is simple - you have to tell it. Some applications can tell gateways where to connect to (i.e. Netscape, WS_FTP) but some cannot (i.e. News, email, and many others). When the application cannot tell WinGate where to connect to, the user must do it manually. This is where the Mapped Links feature of WinGate comes in. Mapped Links are a way of telling WinGate where you want it to connect you through to.

Most software that can talk through gateways does not do so by default, so you will have to configure the software to use the gateway machine instead of trying to connect directly to the end destination (which it cannot do).

TCP/IP

There are a couple of basic things you should know about TCP/IP that will make life much easier.

IP Numbers

There are a few good analogies between computers and telephones, this is a very good example of one. You may think of an IP number as a telephone number with all the international dialling codes attached. This means that any machine can contact any other machine using the IP number, as long as there is a path between the machines.

This also means that no two machines on the same network should be allowed to have the same number. I say on the same network, because machine on unconnected networks often do have the same addresses, for a specific reason which applies here. You can think of this in the telephone world as you might know two people who work for different companies but who have the same extension number for the phone on their desks, there is no conflict (except perhaps in your mind).

Ports

A port can be thought of as a channel of communications to a machine. Packets of information coming into a machine are addressed not only to that machine, but to that machine on a specified port. You can think of a port as a radio channel if you like, but the fundamental difference between a radio receiver and a computer, is that the computer can listen to any / all of 65000 possible channels at once!

However, the thing to note here is that typically the computer is not listening on very many ports at all. The computer will not respond to data or connection requests that come in on a port that it is not listening to.

One other thing to note, is that there are a number of important predefined ports which are universally used for various services. The major ones of these are:

Service	**Port#**	**Description**
FTP	21	File Transfer Protocol - for transferring files
Telnet	23	for logging into an account on a Remote Host
SMTP	25	For Sending mail
Gopher	70	Text menu based browser
HTTP	80	WWW protocol - Netscape, Mosaic
POP3	110	Downloading Mail
NNTP	119	Internet Newsgroups
IRC	6667	Internet Relay Chat
Compuserve	4144	Compuserve WinCIM communications

One further thing to note, is that two applications on one computer generally cannot both listen on the same port at the same time. This is relevant in that if you try to set WinGate to listen on a port that some other application is already listening on (i.e. you are already running an FTP server), it will not be able to start listening. This means you should never launch more than on instance of WinGate

DNS

These three letters don't mean much to many people, but they stand for the Domain Name System. Those three words don't mean much to many people either, so enter Adrien's telephone parallel #4. In a world without telephone books, you can think of a DNS server as a telephone directory service. To talk to any machine, unless you have the number already, you are going to have to look it up. You contact the directory services, and give them the name, they give you the number. You cannot contact a machine without a number. In the same way, you can think of the "HOSTS" file in your system directories, as a personal address book. If you want to contact a machine, you first look in your personal address book for the number, if it isn't there, you ring directory services (by the way, if you don't have a number for directory services, you can't look anyone up).

OK, so now you're armed with practically everything you need to get going.

4 Using WinGate

If you keep in mind the concepts of the previous section, using WinGate should be easy. For setting it up, in all cases there are two main steps:

Step 1

you must configure WinGate to gate traffic for a specific service (i.e. tell it to listen on a port)

Step 2

you must configure your client applications to use the gateway machine (i.e. tell them to talk to the gateway on the port WinGate is listening on). If your application does not support this, you must tell WinGate where to pipe connections through to.

4.1 Setting up your LAN

The first thing you must do is set up your LAN to use TCP/IP. This is probably the hardest part of all, however, if you follow the following guidelines it should be manageable.

There are some changes here from the 1.0 release. One of the quirks of the SOCKS protocol, is that a request for a connection is made in the form of a request for connection to / from an IP number. This means that a SOCKS client needs to have DNS in order to supply the number to the SOCKS server.

For this reason, the DNS Patch was developed to relay DNS requests through to a specified DNS server. If you already have DNS on your internal network, and it has sufficient scope to resolve all the names you wish to connect to, then you will not need to run the DNS patch in order to use the SOCKS server.

You WILL need to enable the DNS on your LAN however.

If you are using the DNS patch, you should set the DNS Server settings for your LAN adapters (on all machines EXCEPT the gateway machine) to be the IP number of the gateway machine.

There are a lot of very good resources on the Internet which will help you to set this all up. In particular, the following page will most likely be able to help you if you run into difficulties:

http://www.windows95.com/connect/

Remember back in Section 3 when I said that IP numbers have to be unique for machines on the same network? Well, you can think of the entire Internet as a single network. But your LAN is probably not on the same network, even if one of the machines (i.e. the gateway machine) is on the Internet. You see, it is not so much a computer being on the Internet as a **computer interface**, whether this be a LAN card or a serial port to your modem. The Internet can see the interface that is connected, but no further.

This means that you can choose any number you like for the machines on your LAN. However it isn't a good idea to choose just any old thing, because you have to think of the situation the gateway machine is in.

The gateway machine can see the entire Internet, and your LAN. So, you don't want to confuse it by giving your LAN the same addresses that the gateway machine can see on the Internet.

Fortunately some smart person already thought of this one, and so a whole heap of addresses have been kept aside for just this purpose. These addresses are called "private addresses" and are not meant to be available anywhere on the Internet. Therefore, by using them on your LAN, there won't ever be any confusion for the gateway machine.

Depending on the number of machines on your LAN, you probably will want to use a c-class (256 interfaces) address range. A good one to use is

192.168.0.*

the corresponding subnet mask will be 255.255.255.0

You should set up your LAN using numbers in this range. You should need no other settings in the TCP/IP setup of your LAN machines, except that on the gateway machine, you need an entry for DNS server, which will be the IP number given to you by your service provider. If you have been using the Internet before getting hold of WinGate, then this will have already been set up for you.

Note

For getting started, you may like to put an entry for the gateway machine in the hosts file of each of your LAN machines (or if you are running a DNS server, you should put it in there, and make sure all your LAN machines are pointing to it - except for the gateway machine, which should use the DNS server of your Internet Service Provider).

An example may be (if you are using the 192.168.0.0 private c-class addresses on your LAN, which I recommend)

192.168.0.1 gateway

remember you must put an enter at the end of the last line in your hosts file, else it may not be recognised.

4.2 SOCKS Server

The SOCKS server allows any SOCKS compatible client to access the Internet to both connect out, and listen for connections as if the client was directly connected.

Step 1

The port number for SOCKS servers is normally 1080.

The setting “Allow Unresolved Connects” may be required to access some sites. The explanation for this is as follows. When a client supplies an IP number for the SOCKS server to connect to, the server must check to see if the client is allowed to connect to the remote site. In order to check against the rule-base, the server needs to look up the name of the host from its IP number supplied. There may be some rule which denies connections to a site, and this needs to be checked.

If the server cannot resolve the name from the IP number (i.e because of a bad DNS entry somewhere, or incorrect DNS setup somewhere for the site concerned), then if the “Allow Unresolved Connects” is not set, the request will be denied.

As mentioned above, to use SOCKS, you must have DNS avbailable on your LAN (see below)

Step 2

Configuring clients requires specifying gateway as the socks server on port 1080. In Netscape, you should set the socks host to gateway, and clear all the other proxies. You can continue to use the WWW Proxy server for HTTP if you like, and this will give you the benefits of more meaningful error messages, and filtering of URLs.

There are a number of SOCKS compatible clients, for things such as FTP, Telnet etc.

4.3 DNS Forwarding

The DNS forwarding feature (under the Settings tab) allows you to relay DNS requests through to a remote DNS server on the other network (e.g the Internet). You can think of this as a Mapped link which maps all requests on UDP port 53 through to the specified remote host on UDP port 53.

What it does do is allow you to use DNS on your internal LAN, so SOCKS and utilities like nslookup will work.

Normally the remote host to relay DNS requests through to will be your ISP. If not, it should be the same as the DNS setting in your dial-up adapter on the gateway machine, or you may have to get the name of your ISPs DNS server from your ISP.

On the LAN workstations, add an entry in the DNS servers section of your TCP/IP setup specifying the IP number of the gateway machine. Unless you have nslookup, the only way to test if this is working, is by testing the SOCKS gateway with a SOCKS client (i.e Netscape) or by trying to ping a site (you will get request timed out, however the IP number of the site should be displayed.

4.4 WWW Proxy Gateway

Step 1

The WWW Proxy Gateway currently handles only HTTP requests. If you look back at the table in Section 3, you may note that HTTP figures there, associated with port 80. So unless you are already running a Web server on the gateway machine, then port 80 is as good a port as any to pick for the WWW Proxy.

Step 2

Now if you are using Netscape, you go to Options → Preferences → Proxies, and set up

HTTP Proxy:	gateway	Port:	80
SOCKS Host	gateway	Port:	1080

The HTTP proxy (i.e in WinGate the WWW proxy server) will handle all requests for HTTP URLs, so this will be the majority of your Web browsing. The SOCKS server will be used for any other protocol (i.e FTP, Gopher, WAIS, HTTPS).

If you are using the Microsoft Internet Explorer, you will be restricted to URLs using HTTP, as MIE does not currently support SOCKS. This is why the WWW Proxy gateway is still being developed to support other protocols (such as FTP and gopher - it is a lot harder to do it this way).

Using both proxy servers means you get the benefit of meaningful error messages from WinGate whenever anything goes wrong with an HTTP request. The SOCKS server cannot send back error messages that Netscape can display on your screen, because the SOCKS server can't be sure that what it is talking to will understand HTTP.

4.5 FTP Gateway

Step 1

Set up an FTP Gateway. A good port for this is 21, unless you are already running an FTP server on the gateway machine.

Step 2

Configure your FTP client to use the gateway. To do this in WS_FTP you go to Options → Session Options, and select "Use Firewall". Make sure that the "Use PASV Transfer Mode" is not checked. The FTP gateway will return an error message if you try to use an FTP client in PASV mode. Save as default, and exit options.

Under Connect→Advanced enter

Firewall:	gateway
Port:	21

Select “User with no logon”

Now you’re ready to rock and roll. The only problem you may have with this is if you try to connect to a remote site which does not support PASV mode transfers (very rare). PASV (short for passive) transfers are when the client initiates the data connection to the FTP server, normally the client tells the server which port to connect to it on, and the server initiates the connection.

4.6 Telnet Gateway

Step 1

Set up a Telnet Gateway. Unless you are already running a Telnet server, you may like to use port 23 (this will save you some hassles in your client applications).

Step 2

Well, since Telnet is inherently a command-line based service, there is no special setup for the Telnet client. To use it however you must **always** first Telnet to the gateway machine on the port you set up for the Telnet gateway. You will then be presented with a prompt like this:

WinGate>

now you simply type in the name of the host you wish to connect to, and optionally a port number as well. WinGate will display “Connecting to …”, when the “Connected” message comes back, you are now connected through to the remote machine.

There have been a few changes with the WinGate telnet gateway, which affect telnet clients that issue telnet commands (e.g. EWAN, simpterm, and UNIX clients). You will probably get a double-echo while you are typing in the hostname you want to connect to. Once you are connected however, things should be alright again.

4.7 Mapped Links

You will most likely want to use at the very least 2 of these links (for your email), and probably a couple more as well.

Mapped Links are perhaps the simplest level of gatewaying, however perhaps the most difficult to grasp (still easy though).

If you think of a Mapped Link as a patch cord, then you are effectively patching machines through to remote machines, on specified ports. You can specify a remote host and port number for each individual LAN workstation, or a default remote host and port, which would be used if the machine connecting to the gateway did not have a specific map entry.

EMAIL

You need 2 Mapped Links to get email working. If you cast your eyes back to the table in Section 3, you will see that there is a port (25) for sending mail, and a port (110) for retrieving mail.

Step 1

Set up a Mapped link on port 25. The default remote host should be set to the SMTP server of your Internet Service Provider also on port 25.
Set up a Mapped link on port 110. The default remote host should be set to the POP3 server of your Internet Service Provider also on port 110.

If different users on your LAN need to connect to different mail hosts, then you need to set up a mapping for their machine, else they will use the default (if enabled).

Step 2

In your email software,

Set your SMTP server (sometimes called your mail relay host) to "gateway"
Set your POP3 server (sometimes called mail server) also to "gateway"

if you are using Eudora, set your POP account to username@gateway

NEWS

Step 1

Set up a Mapped link on port 119. The default remote host should be set to the news server of your Internet Service Provider also on port 119.

Step 2

In your newsreader software,

Set your NNTP server (sometimes called your news server) to "gateway"

Notes

If you do not specify a mapping for a machine, and do not have a default remote host, then a connection from that machine will not be accepted.

For specific mappings, the incoming host must be an IP number. In general, all WinGate knows about a machine connecting to it is it's IP number (so this applies for rules for incoming connections as well). So if you want WinGate to do something based on which machine is connecting to it, you must specify an IP number.

The use of the name "gateway" in the previous examples assumes you have set up an entry in the hosts file for each LAN workstation that will be using the gateway. If you have not done this, then in the examples above, you need to substitute the IP address of the LAN adapter of the gateway machine.

4.8 Rules

Rules were incorporated in order to protect your LAN from people connecting back through your gateway. There are three ways you can limit access through the gateway.

- Based on connecting host
- Based on requested remote host
- Based on URL (for WWW Proxy Gateway)

You can set default rules for all of these, as well as specifying specific allow / deny rules for particular circumstances.

One standard example of this would be to set up default rule for inward connections to deny all, and then individually allow inward connections from the machines on your LAN, and any specific machine on the Internet you wanted to allow access.

One thing to remember, with the current WinGate release, all comparisons are done on a text basis. This means you could set up a rule which denied connections to hosts containing ".com". However if a user knew the IP number of a forbidden host, they may try to use the number instead of the hostname, in which case if you hadn't also set up a rule to deny the IP number as well, the request would be granted.

4.9 Dial-on-demand

Dial-on-demand requires that Remote Access Service (RAS - for Windows NT) or Microsoft Dial-up Networking (DUN - for Windows 95) be installed. If the appropriate service is not installed, the Dialler setup page will not be displayed, and no dialler features will be enabled.

The setup for the Dialler page is relatively straightforward. It however assumes that you have had a dial-up profile (phonebook entry) previously configured in RAS / DUN. If you have not used either of these before, it is likely that your phonebook file (from which Wingate gets all it's dial-up settings) will be empty, and you will have to run and configure DUN / RAS until you have a profile which allows a complete login without user intervention (save entering a password and pressing the connect button).

All you need to get going then is to select the phonebook entry you wish to use in WinGate, and specify what you want the dialler to do.

Dialler Options

The Options dialog deserves some more explanation. The Username and Password fields may not be required by all PPP servers / phonebook entries. If you choose Save Password, your password will be encrypted and saved in the registry, otherwise you may need to enter a password here every time you run WinGate.

There are two advanced options you may specify.

- When to dial
- What to do if there is an existing connection

When to Dial

When to dial deals with the circumstances under which the dialler is started. In some cases, you may want to connect through WinGate to machines which are available without the need to invoke a dial-up session. You may not want to simply start the dialler regardless. There are two options for this scenario: The first: ***Try to connect first*** involves WinGate attempting a TCP/IP connection to the desired host first, without dialling up, and only dialling up if that connection fails. This means that whenever there is a site you want to connect to, that is available locally, you will not need to dial up to connect to it. There are however some disadvantages with this scenario, not the least being that a failed connection can take over 1 minute to time out. This is where the second option comes in. If you select Dialling ***For everything except connections to sites containing:*** items that you enter into the listbox, then WinGate will check this list first before invoking the dialler. If the requested host is found in the list, then the dialler will not be started, and WinGate will connect directly. This avoids lengthy time-outs. The reasoning behind the "Sites containing" bit, is that if you have a LAN of 200 machines, you will not want to enter every number or machine name into this list. If you specify enough text to identify the machines of interest, then you can normally get away with only a couple of entries in this list. Normally, if you are using the 192.168.0.x subnet, you will enter only "**192.168.0.**" in here (note the final dot). This will mean that WinGate will not invoke the dialler for connections to any machine on your local network. If you have names for machines on your network, you would include the last part of the names (the part that they should all share in common).

Take over an existing connection on selected profile

This setting covers what to do if you are running DUN or RAS as well as WinGate, and you have a user on the gateway machine as well.

Consider the following scenario:

You have a 2 machine LAN at home, and a 1 user license for WinGate (free). You are on the gateway machine, dialled in using DUN, because you don't have enough licenses for both machines to work through WinGate, so you are set up to connect directly. You are 90% through downloading a 7Meg file, and the other user wants to get access. You start WinGate.

Well, here is where it gets interesting. If you have this little check box checked in the advanced dialler options dialog, then the next thing WinGate is going to do is hang up your connection, because there are no current users connected to Wingate, leaving you with 90% of a large useless file.

WinGate will only hang up connections it owns. This setting is to tell WinGate whether or not it will take ownership of a connection that is existing on its selected profile. You may at some stages wish WinGate to do this (if at any stage the link enters an unstable state, setting this, and hitting the reset button will shut down the port, and make it available for re-use.).