

WinRoute

A Product Backgrounder

As an award winning ICSA certified Internet router and firewall software solution, WinRoute Pro provides secure Internet sharing solutions for connections to the Internet through dial-up line, DSL, ISDN or Cable, leased line or DirecPC. WinRoute Pro has proven to be an ideal router/firewall software solution for small to medium size networks. It is designed to be a fully capable router that passes traffic from the two industry standard VPN protocols of IP Security proposed by the Internet Engineering Task Force (IETF) and the Point-to-Point Tunneling protocol made popular in recent years due to its inclusion with Microsoft Windows® client Operating System (OS) software.

Network Address Translation (NAT)

NAT is a process that modifies packets sent from/to the Local Area Network (LAN) to/from the Internet or other IP based networks. WinRoute performs NAT on the interfaces chosen by the user. It also performs any preset security rules on the specific interfaces. This gives the user a wide range of freedom when designing and configuring security options.

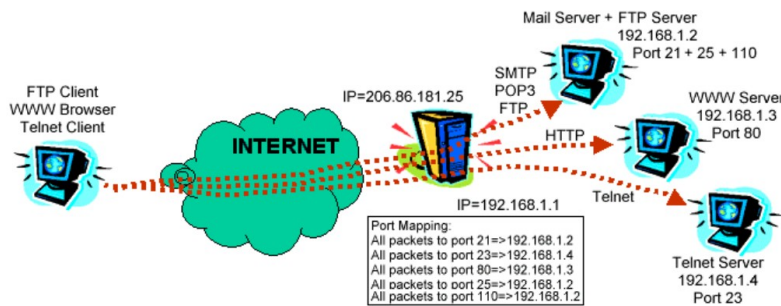
Using NAT technology, WinRoute allows for users to expand a single IP address to a small to medium side network for home and business.

WinRoute Firewall

The basic firewall functionality is provided by NAT. When using NAT, all packets are modified and checked before they reach your computer. As a result, there is almost no opportunity for undesired traffic. Periodically, there is the need to open particular ports or range of ports to allow access to local resources. An example of this is when using the application PC Anywhere for remote management. For this type of access, the user will want to control access rights to that network. WinRoute can easily limit the amount of internal users accessing the Internet. Also, included in WinRoute is a powerful, easy-to-configure packet filter based firewall. The WinRoute firewall allows for very sophisticated security ruling.

Total Protocol Support

Unlike Proxy software servers (i.e. WinGate or WinProxy), WinRoute allows almost any Internet protocol to pass through. At the same time, WinRoute checks each packet utilizing the advanced security and firewall features inherent in the software design. On systems running Windows NT, the NT OS performs the routing and WinRoute manages the Network Address Translation functionality and other data.



Port Mapping (PAT)

Because WinRoute uses NAT, the protected network becomes inaccessible from outside the network. By using the PAT feature,

public services like a web-server, FTP server or others running on the private network may become accessible from the Internet. WinRoute checks each packet received from outside the network whether its attributes (i.e. the protocol, destination port and destination IP address) comply with an entry in the port-mapping table (i.e. protocol, listen port and listen IP). If the arriving packet meets the desired criteria, the packet is modified and sent to the IP address of the protected network defined as the Destination IP in the table's entry and to the port defined as Destination Port.

WinRoute Domain Name Server (DNS) Forwarder

Each computer connected to the Internet is identified by a unique numeric IP address. In order to connect to a computer on the Internet, its address must be known to the computer that is creating the connection. The DNS is a database of descriptive names that are supposed to be easy to remember. Thus the user does not have to know the IP address of the server she/he wants to communicate with. It suffices to enter the appropriate name (e.g. www.tinysoftware.com) and the DNS will find the actual IP address.

WinRoute is equipped with a DNS module that is able to forward DNS queries to a chosen DNS server on the Internet. The DNS module stores the results of the queries in its internal cache where they are kept for a certain time. Subsequent repeated queries are then answered using the cached data without the need to wait until an answer from the Internet arrives.

The DNS forwarder in WinRoute is able to answer DNS queries according to the user-defined HOSTS file. After DNS query arrives WinRoute looks at the HOSTS file prior to forwarding the DNS query to the Internet. If the corresponding record is found the query is answered by its value, if not it is forwarded to the Internet DNS server.

Added Services – WinRoute Pro

Unique to WinRoute Pro is the integration of a Mail Server, enabling Web Browser Access, POP3/SMTP Access and an Aliases feature for additional user addressing and email substitution. WinRoute Pro supports all standard Internet protocols, including: IPSEC, H.323, NetMeeting, WebPhone, RealAudio, RealVideo, ICA Winframe, ICQ and more.

WinRoute Lite

WinRoute Lite is a rock-solid, easy-to-use network router and firewall software application based on award winning, ICSA certified WinRoute Pro technology. The WinRoute Lite version offers a lower level of functionality when compared to WinRoute Pro; however, maintains several popular and well-needed features for a network solution.

WinRoute Lite is an ideal solution for connecting small to medium size networks with secure Internet sharing.

When compared to its superior, WinRoute Pro, the Lite version does not include a configurable router, mail or proxy server. Its DHCP server and router are set for auto-configuration opposed to the configurable DHCP server and router of WinRoute Pro. VPN support with WinRoute Lite is limited to PPTP out only and IPSEC is not supported.

Users on a LAN running WinRoute Lite v4.1 can gain access to local servers and services such as email, FTP and web-use while securing the network from unwanted external intrusion. A limited DNS forwarder is included in WinRoute Lite opposed to the more advanced version in WinRoute Pro.

The low-level network driver of WinRoute Lite can support plug and play adapters making it easy to switch network cards, versus having to uninstall WinRoute before swapping the cards. It also performs packet de-fragmentation by organizing data to improve network security and simplifying system administration. With the configuration of an improved DNS module, network administrators can work on local networking problems directly without having to enter the public Internet domain.

#