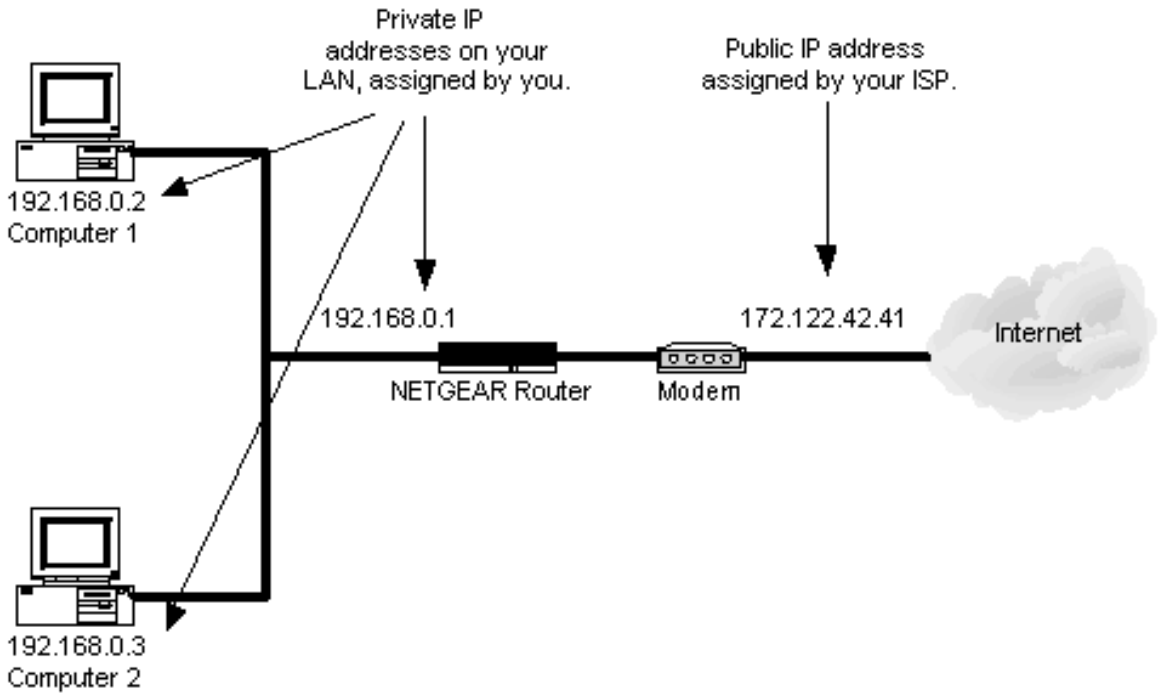
What is NAT (Network Address Translation)?

Using **NAT** with NETGEAR products, accessing the Internet, the addresses on your LAN are substituted for a single WAN IP address. This lets your computers share one IP address from your ISP. It also makes your network more secure, since traffic to and from the Internet now goes through your router's address substitution process, blocking direct access to your local IP addresses. Unless you use port forwarding, port triggering, or a DMZ, your computers are not reachable from the Internet (unless one of your computers requests it, of course!)



This illustrates a network with two computers using NAT.

For instructions on how to do NAT, read your router's Reference Manual.

NAT is implemented in NETGEAR hardware, so that there is almost no performance degradation. (NAT can be implemented in third party software, using one of your computers to substitute the IP addresses. Since it slows that computer down, and requires that it always be on if anyone is accessing the Internet, using NETGEAR equipment is a much better solution.)

For an explanation of how **NAT** relates to other NETGEAR security features, see Security: Comparing NAT, Content Filtering, SPI, and Firewalls.

Since NAT alters the incoming packets, it is not compatible with the security feature called Authentication Header Passthrough. Also NAT is not compatible with multicasting (sending traffic to many hosts).

Multi-NAT is the term used by NETGEAR to describe creating more than one public IP address for your network. This new feature is described in Using Multi-NAT with the FVX538 or FVS338 Firewall. Multi-NAT is used in the situation when your ISP provides you with a number of public IP addresses, and you want to use them to provide access from Internet to multiple internal servers. (Regular NAT translates one public IP address — on a single port to a private IP on a single port — if you have multiple private servers listening on the same port, one-to-one NAT won't accomodate all of them). Multi NAT assigns one of the public IPs to the WAN interface of the router; then Multi-NAT is used for the other public IPs, and with them NATed to multiple internal IP addresses.

Double NAT (as the phrase is used by NETGEAR) means connecting one router directly behind another for the purpose of having multiple LANs. **Double NAT** may cause problems with VPN and visiting secure sites with SSL.

Reverse NAT, not supported by NETGEAR, and not a common process for a typical home user, converts all requests for Internet IPs into different addresses. NETGEAR equipment does not hide public IP addresses, and therefore cannot do Reverse NAT. The term Double NAT is used for non-NETGEAR equipment when both NAT and Reverse NAT are used.

ProSafe VPN Summary
All other configuration details should follow the ProSafe Owner's Manual or the ProSafe VPN Client Owner's Manual.

Additional Resources
Here are some additional resources you find useful.

Netgear
The network products manufacturer (http://www.netgear.com/)has some tech support notes and White Papers on their VPN/Firewall devices and some tips for achieving basic interoperability. They also host auser support forum (http://forum1.netgear.com/)ontheir various products where users can post questions and get answers from their peers.

SafeNet
SafeNet (http://www.safenet-inc.com/)is one of the largest OEM providers of VPN client software to VPN/firewall manufacturers. SafeNet has a tech support area (http://support.safenet-inc.com/)listing tech notes on their products with various VPN gateways including some individual interoperability examples. SafeNet is the OEM supplier of the Netgear ProSafe VPN Client software.

VPNC
The VPN Consortium (http://www.vpnc.org/). VPNC has various writings and White Papers on many manufacturers VPN devices and tips for achieving interoperability.

Practically Networked
Practically Networked (http://www.practicallynetworked.com/)has various writings on many manufacturers VPN devices and tips for achieving interoperability. They also have a section dedicated to VPN issues (http://www.practicallynetworked.com/support/VPN_help.htm).

HomeNetHelp
HomeNetHelp (http://www.homenethelp.com/)has various writings and White Papers on many manufacturers VPN devices and tips for achieving interoperability. They also host a user support forum on VPN Routers where users can post questions and get answers from their peers.

Disclaimer

Both ProSafe VPN/Firewall Routers and ProSafe VPN Client have several ways of setting up and configuring VPN tunnels. The settings may not be the best for your situation and some settings are situation specific.

This case study is published to guides you to setup your VPN Tunnel and VPNCASESTUDY.COM do not held any responsiblity of any mistakes or errors.

Please contact us at info@vpncasestudy.com or visit our site at http://www.vpncasestudy.com