The VPN Gate Academic Experiment Project wants volunteers to provide VPN servers.

If you have a Windows computer, please kindly provide your computer as a Public VPN Relay Server, and join to VPN Gate Experiment.

Setup of Public VPN Relay Server is very easy. After the setup will be completed, your computer will be registered on the Public VPN Relay Servers List page. Anyone on the world can communicate to the Internet via your computer as a relay.

You can install it as a normal user privileges. No Administrators privileges required. Even if you don't have Administrators account in your company, you can run VPN Gate Service on your company's computer. It is very convenient.

After you activate the VPN Gate Service, anyone can connect a VPN connection to your computer, and access to any hosts on the Internet via your computer. VPN Client has also a tiny VPN Gate Service and it is equivalence if you activate it manually.

A guest user can access to hosts on the Internet via your computer, but he cannot access to hosts on your private network nor your computer itself. He cannot browse Windows file sharing or other private materials. It is very secure.

It is safe to install VPN Gate Service on your company's private network. Any access towards the private address blocks (192.168.0.0./255.255.0.0, 172.16.0.0/255.240.0.0 and 10.0.0.0/255.0.0.0) are filtered. It is greatly secure.

The VPN Gate Service provides the mirror site relay service for www.vpngate.net. If your computer will be qualified as a provider of the mirror site, your IP address will be registered on the Mirror Sites List page.

Important Notice

When you are attempting to enable the VPN Gate Relaying Function, you will see the four warning messages. Please read every warning messages very carefully before activating the VPN Gate Relaying Function. Do not enable the VPN Gate Relaying Function unless you fully understood and agreed all the warnings and risks about running the relay.

When you are running the VPN Gate Relaying Function on your company's network, then any person's communication to Internet hosts will be relayed via your company's network. If you company's network has a policy which prohibits to run such a relaying program, you have a risk to violate the policy. Therefore, you have better to take an explicit permission from the network administrator of your company in advance to enabling the VPN Gate Relaying Function.

After you checked "Enable the VPN Gate Relay Service and Join the VPN Gate Research as a Volunteer" manually (which is disabled by default)

and press OK, then the VPN Gate Relaying Function will start to run on your computer as one of the VPN Gate volunteers.

This means that any VPN Gate client users will be able to communicate with Internet servers via your volunteer VPN server.

You must enable the function after fully understanding. If your company or campus doesn't permit users to run such

a relaying program, DO NOT enable the VPN Gate Relaying Function.

Notice: About background services

The notes in this section are not specific to SoftEther VPN or VPN Gate, but apply to general system software.

SoftEther VPN Client, SoftEther VPN Server, SoftEther VPN Bridge, and VPN Gate Relay Service will be installed on your computer as system services. System services always run in the background. System services usually do not appear on the computer display. Then your computer system is booted, system services automatically start in the background even before you or other users log in. To check whether SoftEther-related system service is running, check the process list or the background service list of your OS (called as "Services" in Windows, or "Daemons" in

UNIX.) You can activate, deactivate, start, or stop system services using the functions of the OS anytime. SoftEther-related GUI tools for managing system services communicate with these system services. After you terminate these management GUI tools, SoftEther-related system services will continue to run in the background. System services consume CPU time, computer power, memory and disk space. Because system services consume power, your electricity charges and amount of thermal of your computer increase as result. In addition, there is a possibility that the mechanical parts of the life of your computer is reduced.

1. Download and install SoftEther VPN Server

Click the below link to download SoftEther VPN Server (Windows version).

Download SoftEther VPN Server

After you start the installer, follow the instructions which are displayed on the wizard.

Select "SoftEther VPN Server" in the "Select Software Components to Install" list.

Read the End User License Agreement. SoftEther VPN Sever is currently freeware, and planned to be published as open-source software (GPL).

Read the notice. This is very important.

SoftEther VPN Server installation process will be started.

Installation finished.

2. Activation and initial configuration of VPN Gate Service on SoftEther VPN Server

After you install SoftEther VPN Server, connect to the SoftEther VPN Server instance running on localhost.

At the first time you connect to the VPN Server in Management Mode, the "Easy Setup" will appear. If you want to just only activate VPN Gate Service, click the "Close" button.

The top windows of VPN Server Manager. Click the "VPN Gate Setting" button.

The "VPN Gate Service Control Panel" will appear. Check the "Enable the VPN Gate Relay Service and Join the VPN Gate Research as a Volunteer" checkbox. After that, click the "VPN Gate Service Option Settings" button.

In the VPN Gate Service Options, input the information of the server operator.

Please note that any information inputted here are registered in the Public VPN Relay Servers List page, and published to anyone.

Minimum VPN Gate Service initial configuration finished by above steps.

You can change the assigned DDNS name of the VPN Gate Service computer. The default DDNS name is "vpn**********.opengw.net" . You can change the DDNS hostname. To change it, click the "Dynamic DNS Setting" button and follow the screen instructions.

3. View the list of current active VPN guest sessions

You can browse the list of current active VPN guest session by opening the "VPNGATE" virtual hub.

Double-click a particular session to see the detail information about the session.

4. Pop-up your message to your guests

You can show your message to users who connect to your VPN Server. To set up the message, open the property of the "VPNGATE" virtual hub, and specify the message.

Please enable your L2TP/IPsec VPN for guests to help people behind Government's Firewall

If you enable VPN Gate Service for guests around the world, please also consider to accept L2TP/IPsec connection from guests.

In the current volunteers' list, there are few L2TP/IPsec enabled VPN servers all over the world. We really need more L2TP/IPsec enabled servers.

How to let my PC's L2TP/IPsec server become reachable from Internet?

To enable L2TP/IPsec server function, check the "Enable L2TP/IPsec VPN Server Function" checkbox on the "VPN Gate Service Options" dialog.

After you enabled L2TP/IPsec server function on the software, you have to open both UDP 500 and 4500 ports to the Internet. How to open UDP 500 / 4500 is depended on each router or NAT. Please read your router, firewall or NAT's documents to make your VPN server computer become reachable from the Internet.

Note: Both UDP 500 and 4500 are required.

How to confirm that my PC's L2TP/IPsec server (UDP 500 / 4500) is certainly reachable from the Internet?

Reload the Public VPN Relay Servers List a few minutes later after you enabled the function and opened the UDP 500 / 4500 ports toward the Internet. If your server is listed and marked as L2TP/IPsec is enabled, your PC is reachable from the Internet. Otherwise please verity the setting again.

Please note that some private networks (e.g. behind the NAT which is managed by other person) unfortunately you cannot activate L2TP/IPsec server function toward the Internet because such a NAT doesn't pass L2TP/IPsec packets to your server.