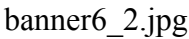# VPN Azure

If the corporate firewall is more restricted and the NAT Traversal of   banner6_2.jpg
SoftEther VPN doesn't work correctly, instead use VPN Azure to penetrate such a
firewall.

6_azure.jpg

VPN Azure Relay Service

NAT Traversal works with most of NATs and Firewalls, however, some restricted
firewalls cannot pass NAT Traversal packets. In such a case do not give up. **You can
activate VPN Azure Relay Service** on SoftEther VPN. After that, all VPN connecting
requests from VPN Client or VPN Bridge will be relayed through the VPN Azure Cloud
Servers operated by SoftEther VPN Project for free of charge. VPN Azure is the ultimate
methods to penetrate any kinds of firewalls.

The principle of VPN Azure is very simple. SoftEther VPN Server behind the firewall
always keep a TCP-based connection toward a VPN Azure relay server. It is permitted
automatically by the firewall because the direction of the initial connection is "from
inside to outside" . The firewall treats such packets as trusted. VPN Client or VPN Bridge
requests the appropriate VPN Azure relay server to connect to the VPN Server. The VPN
Azure relay server will relay the connection request to the SoftEther VPN Server. Then
SoftEther VPN Server will establish the UDP-based VPN tunnel between the VPN Server
and the VPN Client (or VPN Bridge). After the UDP-based link has been established the
VPN relay server doesn't relay the payloads of VPN tunnel.