Dynamic DNS and NAT Traversal

Unlike legacy IPsec-based VPN, even if your corporate network doesn't banner6_1.jpg have any static global IP address you can set up your stable SoftEther VPN Server on your corporate network.

Principles

Traditional legacy VPNs require static and global IP address for the VPN Server. The IP address must be reachable from the Internet. However, a static and global IP address is very expensive. It costs monthly. It has also a security risk because your VPN Server must be exposed to public Internet.

SoftEther VPN has a solution. SoftEther VPN Server has the built-in Dynamic DNS and NAT Traversal functions. Static IP addresses are no longer required to set up VPN Server. Even global IP addresses are no longer required. SoftEther VPN Server can be set up on the private IP address behind the NAT.

Dynamic DNS

The Dynamic DNS function assigns a world-wide unique identifier on your SoftEther VPN Server. Your global IP address of SoftEther VPN Server will follow dynamic IP address changes. If the IP address of SoftEther VPN Server suddenly changed, the IP address record which is registered to the Dynamic DNS hostname changes automatically and immediately. A VPN client user can specify the Dynamic DNS hostname as the destination VPN Server's hostname instead of the IP address. VPN Clients and VPN Bridges can keep stable connections to your SoftEther VPN Server even if the server-side Internet connection is not a static IP address contracts.

6_ddns.jpg

NAT Traversal

The NAT Traversal function penetrates firewalls or NATs. This technology is almost same to Skype's NAT Traversal, but SoftEther VPN's NAT Traversal is more optimized for the VPN-use.

Legacy IPsec-based or OpenVPN-based VPN Server cannot placed on behind the NAT, because VPN Clients must reach to the VPN Server through the Internet. Some NATs can be configured to define a "DMZ" or "Port-mapping" to relay any packets toward the outside IP address of NAT to the internal VPN Server. However it has a compatible problems. Moreover it requires a special permission by the administrator of the NAT. If your network administrator of the corporate are not cooperative to you, he hesitates to set up the NAT device to open a hole from the Internet.

Unlike legacy VPNs, SoftEther VPN Server can be set up on a private network behind the NAT. No special configuration on the NAT device is required. You need no permission by your network administrator of the NAT. The built-in NAT Traversal Function opens a "Punched Hole" on the NAT or firewall. When the VPN Client or VPN Bridge attempts to connect to your VPN Server behind the NAT, the connection packets will be lead through the hole. The hole is created by the SoftEther VPN Server automatically, so you need nothing special on the NAT.

6_natt.jpg