Remote Management

banner4_1.jpg

Do you have a lot of servers, clients and printers of your client companies which are distributed around the state? SoftEther VPN helps a network administrator as a handy tool. Just from your desk, you can reach to any networks which you have installed SoftEther VPN in advance.

Principles

If you are an IT professional and managing a lot of IP-based devices and computers of customers around the state, it is very troublesome to reach to every devices from your desktop. Most of all devices which are located on the remote location are isolated from your office's network, and are placed behind the firewall of each customer. So you have to make a business trip to each location physically for regular maintenance and irregular troubleshooting.

In order to reduce your costs and gain the comfortable daily business, use SoftEther VPN. You can install SoftEther VPN Client or SoftEther VPN Bridge on each location which you have to support as your business. SoftEther VPN Client and SoftEther VPN Bridge keeps VPN tunnels to your SoftEther VPN Server in your office, even if Clients or Bridges are behind firewalls.

Then you can access to any devices of customer-side networks from your desk. No more need to make business trips for maintenance or troubleshooting.

Method 1. Set up VPN Clients on Customer's Computers

You can **install SoftEther VPN Client** on customer's computer which you are supporting. Before that, you have to **install SoftEther VPN Server** on your company. After that, you can configure the customer-side SoftEther VPN Client to keep a VPN tunnel 24h/365d to your VPN Server. Then you can access to the computer remotely from your desk anytime.

4_remote_m1.jpg

Method 2. Set up VPN Server on Customer's Computer

As an alternative method, you can **set up SoftEther VPN Server** on one of customer's computers as "relay PC" . Even if SoftEther VPN Server is behind the firewall, you can reach to that VPN Server from your office, **because SoftEther VPN Server has built-in Dynamic DNS function and NAT Traversal function.**

You can **set up a Local Bridge** between the Virtual Hub and the physical Ethernet segment on customer's computer. Then you can access to the customer's network remotely from your desk anytime.

4_remote_m2.jpg

Method 3. Set up VPN Bridge on Customer's Computer

Some customer's firewall might block SoftEther VPN Server's NAT Traversal communication. In such a case, as an alternative solution, you can use **SoftEther VPN Bridge** on the customer's side. Before that, you need to set up and prepare a Virtual Hub on SoftEther VPN Server in your office. If you have two or more customers you should make each Virtual Hub for each customer on SoftEther VPN Server to isolate Ethernet segments between customers.

When you visit to customer's network physically, set up SoftEther VPN Bridge on one of customer's computers. **Define a Local Bridge** on the VPN Bridge, and make a Cascade Connection link to a Virtual Hub on your company's SoftEther VPN Server. After that, the Cascade Connection will be kept 24h/365d. If you have two or more customers repeat this step for each customer.

Then your company's SoftEther VPN Server has several Virtual Hubs for each customer. You can connect to a specific Virtual Hub from your PC with SoftEther VPN Client. When you are connected to a specific Virtual Hub, you are now joined to the remote customer's network, and you can communicate with any computers on customer's network.

This method is called as "reverse-connection" , because the direction of VPN connection is "from the customer-side" despite the customer-side network is the destination. This reverse-connection technique is useful especially with customer's troublesome firewall. Usually such firewalls block inbound connection from the Internet so you must obtain special permission from customer's network administrators. However by exploiting the reverse-connection technique you can omit that process, and you can directly connect into customer's network from outside, without network administrator's permission.

4_remote_m3.jpg

Method 4. Use VPN Azure

Method 3 is very useful for penetrating customer's firewall, however it is a bit complicated. So an alternative way to Methods 3 is "**VPN Azure**" .

With VPN Azure, the cloud-based VPN tunneling relay servers which are operated by SoftEther Project can relay VPN tunnels. It can penetrate customer's restricted firewalls without any modifications. VPN Azure is the easiest way to penetrate firewalls, and to reach the SoftEther VPN Server behind the firewall.