Join a Cloud VM into LAN

Your Cloud VM can join to your company LAN with SoftEther VPN. banner2_2.jpg
Anyone on your company can access to the Cloud VM without any settings.

2_cloud2.jpg

Principles

By default, Cloud VMs on Amazon EC2 or Windows Azure are completely isolated from your private network. It means that you can connect to the Cloud VM by using SSH, RDP, HTTP, HTTPS or e-mail protocols through the Internet, however you cannot use LAN-oriented applications and protocols such as File Sharing protocols, File Backup applications, SQL Database protocols, distributed transaction protocols and any remote-management tools which are originally designed for private-network use.

SoftEther VPN can join your Cloud VMs into the corporate private network easily. On the corporate network you can set up SoftEther VPN Server. This has the similar steps to Building Remote Access VPN. After that you install SoftEther VPN Client on Cloud VMs. Then connect VPN Clients on Cloud VMs to the VPN Server on the corporate network. After that all Cloud VMs are now parts of the private corporate network. Any

computers on the corporate can connect to Cloud VMs directly which are physically apart from your office. You can use any LAN-oriented applications and protocols such as File Sharing protocols, File Backup applications, SQL Database protocols, distributed transaction protocols and any remote-management tools which are originally designed for private-network use, despite the physical distance between your office and Cloud VMs.

Step 1. Set up SoftEther VPN Server in Corporate Network

As same as **building Remote Access VPN Server**, set up and configure SoftEther VPN Server on the server PC in your corporate network. Add a user object on the SoftEther VPN Server. Define a Local Bridge between the Virtual Hub and the physical Ethernet segment on your corporate network.

ss5.2.jpg

Step 2. Set up SoftEther VPN Client on each Cloud VM

Set up SoftEther VPN Client on each Cloud VM. You can do it very easily from remote. On Windows-based Cloud VM use RDP (Remote Desktop). On Linux-based Cloud VM use SSH. Note that in a specific case you should assign static private IP address on each

Cloud VM's virtual network adapter for VPN in order to keep a stable VPN communication.

ss1.0_vpnclient.jpg

Step 3. Communicate as if Cloud VMs are on Corporate Network

After Cloud VMs are joined into the corporate network through SoftEther VPN Server, these VMs can communicate with any computers on the corporate network. You can enjoy File Sharing protocols, Remote Printing applications, Remote Desktop applications, SQL Database applications and any other LAN-based applications despite the distances and differences of physical locations.

Notes

Note 1. Local Bridge Requires Promiscuous Mode

Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network adapters by default. If the Promiscuous Mode (MAC Address Spoofing) is

administratively disabled, the Local Bridge function between a Virtual Hub on the VPN Server and a physical network adapter on the physical computer does not work well. You should allow the Promiscuous Mode (MAC Address Spoofing) by using the configuration tool of the VM. For details please refer the documents of your VM. If it is a shared-VM and administrated by other person, please request the administrator to permit the use of the Promiscuous (MAC Address Spoofing) Mode to your VM.

Note 2. Alternative to Promiscuous Mode

If your Cloud VM doesn't permit you enabling promiscuous mode, you cannot use Local Bridge on cloud-side. In that case, as an alternative to promiscuous mode you can use **SecureNAT Virtual DHCP and NAT Server Function** on SoftEther VPN Server. Since this Virtual NAT function works under user-mode, you need no special permission from the administrators of Cloud VMs. However the performance might be reduced from using promiscuous mode.