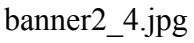# Cloud to Cloud Bridge VPN

Using Amazon EC2 and Windows Azure, or using two or more remote   banner2_4.jpg datacenters of a Cloud service? SoftEther VPN can make a single united network between all Cloud VMs despite differences of physical locations.

Principles

If you are using two or more Cloud Services, you might have a demand to bind all cloud VMs into a single network. SoftEther VPN can realize the single Ethernet segment between different Cloud Provides and different data-center locations.

After you build the single virtual network between Cloud VMs which are geologically isolated, each Cloud VMs can now communicate to each other. Therefore you can design and implement flexible private networks across several Clouds by using SoftEther VPN.

Method 1. Single VPN Server for All Cloud VMs

Easiest method to bind all Cloud VMs is to build-up a VPN which are joined from all Cloud VMs. This method is similar to **Ad-hoc VPN at On-premise environment**. You can **set up a VPN Server** on a Cloud VM. After that, you can install VPN Client on all Cloud VMs and configure them to connect to the VPN Server. Then all Cloud VMs can communicate to each other.

Of course you can add on-premise PC, laptop PC or smartphones as VPN Client to the Cloud VPN. You can add users on VPN Server to accept these additional remote-access VPN client devices.

2_cloud4_m1.jpg

Method 2. Multiple VPN Servers for Every Cloud Groups

The method 1 is easy, but it might cause an overhead problem if there are a lot of Cloud VMs on many Cloud groups. For example, when you have 20 Cloud VMs on U.S. datacenter and other 20 Cloud VMs on Hong Kong datacenter, if you set up SoftEther VPN Server on U.S. datacenter and join all 40 Cloud VMs to the VPN Server, then all communications will be relayed through the U.S. datacenter. It is ineffective.

The solution is to build two VPN Servers on both datacenters. You can set up U.S. VPN Server and Hong Kong VPN Server. The U.S. VPN Server accepts from U.S. located Cloud VMs. The Hong Kong VPN Server accepts from Hong Kong located Cloud VMs. And the U.S. VPN Server and the Hong Kong VPN Server are connected by Cascade Connection link 24h/365d. Then any computers on any side can communicate to not only same-location's Cloud VMs but also different location's Cloud VMs.

When two Cloud VMs on the same location communicates, the traffics are flown only inside the datacenter. It is efficient for throughput and latency. When two Cloud VMs on the different locations communicates, the traffics are flown across the Internet.

2_cloud4_m2.jpg

Method 3. LAN to LAN Bridge VPN for Cloud

You can use the LAN to LAN Bridge VPN method for also Cloud VPN. It is very easy to understand if you consider that the Cloud-side private network is similar to a physical Ethernet segment on the on-premise corporate network. There are no essential difference between the Cloud-based private network and on-premise-based traditional Ethernet network.

2_cloud4_m3.jpg

You can also combine above three methods appropriately. SoftEther VPN has a flexibility solutions to work with both on-premise networks and cloud-based networks.

By using SoftEther VPN, you can design and implement your corporate infrastructures and business systems with flexibility. You can mixture several different Cloud Service Providers and On-premise server facilities by utilizing SoftEther VPN's dependable virtual networking functions. If you are corporate system architects, you can reduce the costs around the network-based problems and gain the comfortable daily network managing life by using SoftEther VPN.

See Also

- 7.2 Install on Windows and Initial Configurations