VPNFAQ002. How to make VPN Server redundant and fault tolerance

Question

My company provides remote access VPN to employees using SoftEther VPN Server. If the computer on which VPN Server is running fails and no longer works, I want to quickly switch to a spare server computer. However, if two VPN Servers with the same settings are prepared, it is inconvenient because the same settings must be applied to the secondary server each time after adding a user on the primary VPN Server. How can I easily make a spare server configuration with SoftEther VPN?

Answer

There are several ways.

The simplest method is to copy the configuration file from the primary VPN server to the secondary VPN server periodically. Configuration replication can be automated using the vpncmd command line utility.
A secondary VPN server configuration file that is not in operation can be rewritten at any time, but it must be noted that it cannot be overwritten when it is in operation.

A more advanced approach is to use enterprise VM products. Examples include VMware's vSphere and Microsoft's Hyper-V. These VM products have mirroring and failover capabilities. Prepare two or more physical host servers, create a VM on the primary side, and install an OS such as Windows or Linux on it. Install SoftEther VPN Server on the VM and start operation. Then mirror the VM to the secondary server.
The advantage of this method of using a VM is that the VM is responsible for redundancy and failover. In other words, VPN servers can be made redundant in the same way that web servers and database servers are made redundant.

When using VM, it is necessary to confirm in advance beforehand that the promiscuous mode is set to be allowed in the NIC to be locally bridged and that it operates correctly when a failover to the backup system is performed. Is required. These are issues that depend on your VM product, so if you have any questions, please contact VM product technical support.