3.9 Clustering

SoftEther VPN Server supports the clustering function. This section explains the clustering function.

3.9.1 What is Clustering?

Clustering Necessity

In general terms, clustering is a processing method which enables the distribution of a large processing load which would be difficult for a single computer to handle among multiple computers, and which appears to the user as a single system such that there is no need to be aware of the fact that it is coordinated processing performed in the background by multiple computers.

SoftEther VPN Server features the clustering function, which gathers the VPN Server computers into one cluster to enable the handling of a large amount of processing as a whole where a single computer would normally not be capable.

Aims of the SoftEther VPN Server Clustering Function

The SoftEther VPN Server clustering function is designed and implemented to create the following two types of networks or a single network combining both. It is not designed or implemented for any other purposes (for example, for separating a cluster node to a remote location and running said mode autonomously etc.).

- Creating a large-scale remote access VPN Service where it would be difficult for a single VPN Server to process all simultaneous connections (please refer to 10.8 Build a Large Scale Remote Access VPN Service for details).
- Creating a large-scale Virtual Hub hosting service where it would be difficult for a single VPN Server to process all Virtual Hubs and simultaneous connections (please refer to 10.9 Build a Large Scale Virtual Hub Hosting Service for details).

Clustering Function Overview

When configuring a cluster with multiple VPN Server computers, one of the computers is run in cluster controller mode, while the other computers are cluster connected to the cluster controller and operated as cluster member servers. The VPN Server operates in stand alone mode by default after installation and no clusters are configured.

Clustering enables the following.

- In environments where a large amount of VPN connections need to be processed, clustering enables their skilful integrated processing on multiple VPN Servers through load sharing where one computer attempting the same task would be incapable or have a serious impact on performance.
- Where a cluster member server running within the cluster stops temporarily due to a hardware problem or software update, the processing to be carried out by that server is automatically taken over by another cluster member server. Therefore, while long-term operation of individual servers may result in a malfunction, as a whole the servers can continue to run almost without disruption.
- When operating a Virtual Hub within the cluster, it is possible to select either a static Virtual Hub or dynamic Virtual Hub as the operating mode depending on the objective.
- The entire VPN Server Administrator and the Virtual Hub Administrators can connect only to the cluster controller and perform cluster member server administration simply without having to be aware of their individual existence.

Prerequisites

It is recommended to connect the all of VPN Servers to a network with minimal delays and high throughput. Typically when joining a cluster, each server is set up in the same location. In this case, it is probably most desirable for all cluster member servers to be directly connected to the cluster controller on the same segment without traveling via a router. Although performance declines, it is technically possible to set up the cluster controller and cluster member servers in separate locations via a router. In either case, the cluster controller must be set up in a location which allows TCP/IP protocol communication from all other cluster member servers.

Connecting the cluster controller & cluster member servers.

3.9.2 Cluster Controllers

What is a Cluster Controller?

The cluster controller is the computer forming the core of the entire cluster. The computer representing the cluster when it is created is known as the cluster controller, and a VPN Client of VPN Server / VPN Bridge attempting to connect to the cluster designates the cluster controller's IP address or host name as the destination IP address or host name.

Overview of Cluster Controller Load Sharing

When the cluster controller receives a VPN connection from a VPN source computer it performs user authentication in the same manner as a regular VPN connection. After successful user authentication, the cluster controller decides automatically which cluster member server is to perform the processing and realizes load sharing by redirecting the connection to that cluster member server. The VPN Server which is the cluster controller is itself also a load sharing destination. The load sharing algorithm compares the load of each VPN Server and automatically determined the assignment destination of a newly-connected VPN session. At this time it uses integers referred to as points in the cluster member list. By presetting the [Function Standard Ratio in Cluster] settings entry for the cluster controller and cluster member servers, it is also possible to manually adjust the parameters for load sharing.

The load sharing discussed here is an overview, and more detailed control is performed depending on the type of Virtual Hub to which the actual VPN connection is made. For details, please refer to 3.9.7 and 3.9.8.

Setting a VPN Server as a Cluster Controller

The VPN Server operates as a stand alone server in the default operating mode. Changing this operating mode to a cluster controller allows the VPN Server to run in cluster controller mode. This and all other settings related to clustering can only be performed by the entire VPN Server Administrator.

To set the VPN Server to cluster controller mode, click on the [Clustering Configuration] button in the VPN Server Manager. Next select [Cluster controller] in the dialog box which appears and click [OK]. In the vpncmd utility, use the **[ClusterSettingController]** command.

3-9-2.png

Configure Clustering settings window.

Using the SoftEther VPN Server in cluster mode makes some functions unavailable. Of the functions used in stand alone server mode, please note that the configuration data relating to functions described in 3.9.12 are all deleted when changing the server operating mode to cluster controller mode or cluster member server mode. It is therefore recommended to make a back up before changing the server's operating mode.

Creating & Administering Virtual Hubs

Virtual Hubs are created for the cluster controller in the VPN Server clustering environment. Where necessary, the cluster member servers create temporary Virtual Hub

instances upon instructions from the cluster controller, but it is not necessary to directly create Virtual Hubs for the cluster member servers. As explained in 3.9.10, Virtual Hub creation and the setting & administration of all Virtual Hubs can only be carried out for the cluster controller in a clustering environment.

3.9.3 Cluster Member Servers

What is a Cluster Member Server?

The term "cluster member server" refers to any computer which forms a part of the cluster configuration other than the cluster controller. By cluster connecting to the cluster controller, the cluster member server is placed under the control of the said cluster controller and shares the processing within the cluster.

When adding a cluster member server to an existing server, the cluster controller's host name or IP address, port number (one of the listener ports made available by the cluster controller) and administration password are required.

Setting a VPN Server as a Cluster Member Server

The VPN Server operates as a stand alone server in the default operating mode. Changing this operating mode to a cluster member server allows the VPN Server to run in cluster member server mode.

To set the VPN Server to cluster member server mode, click on the [Clustering Configuration] button in the VPN Server Manager. Next select [Cluster Member Server] in the dialog box which appears and click [OK]. In the vpncmd utility, use the **[ClusterSettingMember]** command.

The entries required at this time are as follows.

Entry	Description
Controller Host Name or IP Address	Designates the host name or IP address of the cluster controller computer representing the cluster. The VPN Server must be operating in cluster controller mode on the host designated here.
Port Number of Controller	Designates the TCP/IP port of the destination cluster controller.
Administration Password	Designates the administration password of the destination cluster controller. Participation as a member in the cluster is either allowed or denied depending on whether the hash value of the inserted administration password is matched by challenge-response authentication. It is also necessary to change the cluster connection settings' administration

	password of the cluster member servers when the cluster controller administration password is changed. This password is not associated with the VPN Server administration password of the cluster member server itself.
Public IP Address	The public IP address of this cluster member filed with the cluster controller. The IP address designated here is used as the redirect address when this cluster member server is selected by the cluster controller as a VPN connection session load sharing destination from a new VPN source. When no address is entered, the network interface IP address used when cluster connecting to the cluster controller is automatically used. If wishing to use a different public IP address to that of the network interface when cluster connecting to the cluster controller, that address should be designated.
Public Port List	The public port number of this cluster member filed with the cluster controller. Typically, the list of the listener port made public by the cluster member server is designated. More than one public port number must to be designated, and multiple port numbers can be designated by separating them with a comma.

Cluster Connecting to a Cluster Controller with a Cluster Member Mode VPN Server

VPN Servers running in cluster member mode are constantly connected to the cluster controller by a special control TCP/IP connection known as a "cluster connection". The cluster member server attempts to maintain the control cluster connection between the designated cluster controller as far as possible. In addition, if the cluster connection is disconnected or fails to connect, ongoing repeated attempts are made at an interval of a few seconds until the connection is successful.

When seeking to confirm whether the cluster member server is properly connected to the cluster controller, connect to the cluster member server with the VPN Server Manager and click [Clustering Status] to display the following information. In the vpncmd utility, use the **[ClusterConnectionStatusGet]** command.

Entry	Description
Connection Status	Displays [Online] when the cluster connection is in normal status. If the cluster connection is not properly connected, the cause of the error is displayed.
Connection Start Time	The time & date at which the cluster connection commenced.

Time of First Successful Connection	Time & date of first successful connection to cluster controller.
Time of Current Successful Connection	Time & date of currently-connected cluster connection.
Connection Attempts	Displays the number of attempts to connect to the cluster controller to date.
Successful Connections	Displays the number of connection attempts to date which were successful.
Failed Connections	Displays the number of connection attempts to date which failed.

3-9-3.png

Cluster controller connection status display window.

Obtaining List of VPN Servers connected to Cluster Controller & Displaying Details

Connect to the cluster controller with the VPN Server Manager and click the [Clustering Status] button to display a list of all cluster controllers and cluster member servers connected to that cluster controller. In the vpncmd utility, use the **[ClusterMemberList]** command.

3-9-4.png

Intra-cluster VPN Server list administration window.

The entries listed here are as follows.

Entry	Description
Type	Either [Controller] or [Member].
Connection Time	Time & date that member started operating as a member of the cluster after cluster connection to the cluster controller.
Host	Host name of cluster controller or cluster member server.
Points	Value indicating the load status of the cluster member server. The higher this value, the lower the load and the higher the likelihood that the member will be designated as the load share destination for a new VPN session.
Sessions	Displays the number of VPN sessions being processed by the VPN Server.
TCP Connections	Displays the number of TCP/IP connections being processed by the VPN Server.
Dynamic Virtual Hubs	Displays the number of instances of Virtual Hubs operating on the VPN Server.

Note that the information for the cluster controller and each of the cluster member servers displayed in the table of the [Cluster Member List] dialog box is not the latest information, but is instead a few seconds old because it is the result of a query made by the cluster controller to each member server every few seconds.

Also, selecting the desired cluster member server shown in the VPN Server Manager and clicking on [Cluster Member Server Information] enables detailed information on that cluster member server to be viewed. In the vpncmd utility, use the **[ClusterMemberInfoGet]** command.

3-9-5.png

Intra-cluster member server status display window.

While cluster connection communication between a cluster controller and cluster member servers is TCP/IP protocol-based, it differs from the SoftEther VPN protocol in that it is implemented by a proprietary dedicated synchronous and asynchronous RPC (remote proxy call). The System Administrator does not require an in-depth knowledge this protocol. Additionally SSL encryption is used on the protocol contents and a hashed password is used for authentication. However, it does not feature functions such as the sophisticated server certificate authentication of the SoftEther VPN protocol. It is therefore recommended to perform the cluster connection between the cluster controller and cluster members using a physically secure range such as the same LAN. In most cases, there is no problem because all computers used in the cluster are set up in the same room but caution is required where the computers are required to be geographically separated.

3.9.4 Load Balancing

When making a normal VPN connection from the VPN Client and a cascade connection from the VPN Client / VPN Bridge to a cluster, designate the cluster controller's IP address and port number and the name of the destination Virtual Hub.

The cluster controller VPN Server receiving the connection from the VPN source carries out authentication of that connection then selects the cluster member to which to assign that VPN session. The following algorithms are used in this case.

When the Virtual Hub Designated as the VPN Destination is Static:

The cluster controller redirects the connection to the VPN Server with the highest point value among all of those currently available.

Please refer to 3.9.7 for details on static Virtual Hubs.

When the Virtual Hub Designated as the VPN Destination is Dynamic:

The redirect VPN Server is selected according to the following procedure.

1. When the VPN session connected to that Virtual Hub does not yet exist on one of the VPN Servers in the cluster, the connection is redirected to the VPN Server with the highest point value.
2. When the VPN session connected to that Virtual Hub already exists on one of the VPN Servers in the cluster, the connection is redirected to that VPN Server.

Please refer to 3.9.8 for details on dynamic Virtual Hubs.

3.9.5 Load Balancing using Performance Standard Ratio

Weighting by Performance Standard Ratio

As previously mentioned, when the cluster controller selects the server with the lowest load from among the VPN Servers in the cluster, it selects the VPN Server with the highest point value.

The points used here are approximately determined by the following formula.

Points = (4096 - Number of Concurrent VPN Sessions * 100 / weight) ?* 100000 ?/ 4096

The above formula enables a definition of the performance standard ratio of each VPN Server by setting "weighting" parameters for each server. By setting the values of the

[Function Standard Ratio in Cluster] settings entry in the VPN Server's [Configure Clustering], it is possible to change the weight parameter freely. The default setting of the weight parameter is 100.

The [Function Standard Ratio in Cluster] value sets how the subject VPN Server performs against a value of 100 for a normally performing VPN Server. For example, where two servers have respective [Function Standard Ratio in Cluster] values of 100 and 200, this means that the latter server is capable of processing twice the amount of VPN sessions as the former server. The VPN cluster controller determines how many VPN sessions the entire VPN Server should be able to process based largely on the value set here and distributes load accordingly.

Settings to Prevent the Cluster Controller Itself from Processing VPN Communication

The cluster controller may select itself as the VPN Server to process a VPN connection from a VPN source. When the cluster controller decides the VPN Server to which to allocate a new VPN session, the decision is based on the cluster's VPN Server point values determined by the algorithms described in 3.9.4, so both the cluster controller and the cluster members are judged according to an equal standard.

However, when a large volume of VPN connection sessions representing a significantly large load for the entire server have to be processed, it is possible to reduce the load on the cluster controller itself by having it only assume the role of processing the redirection of VPN sessions to each of the cluster members. To enable this setting, open the [Configure Clustering] settings entry and enable the [Controller functions only (It does not process VPN communication itself)] checkbox. This prevents the cluster controller from selecting itself when deciding which VPN Server to assign a new VPN session to.

3.9.6 Fault Tolerance

The SoftEther VPN Server cluster system not only offers load balancing but also realizes fault tolerance at the same time.

When a cluster member server within the cluster terminates suddenly due to hardware trouble or a software / device driver malfunction, or when a situation arises whereby it has to temporarily terminate its VPN Server process in order to update its VPN Server software program and OS, that cluster member server loses connection with the cluster controller, such that the cluster controller automatically deems it as having disengaged from the cluster and excludes it from the load balancing.

In addition, all VPN session which were connected to the cluster member server which has ceased to function are automatically taken over by other cluster member servers. This processing is carried out automatically without the need for any special handling by the

VPN client computer of the VPN source. Therefore, even when a part of the multiple VPN Server computers used by an ISP or a large company terminate due to a malfunction or have to shut down for maintenance, this mechanism enables the entire network to continue operating without stopping as long as other computers remain in the cluster.

3-9-6.png

Realizing fault tolerance with the SoftEther VPN Cluster.

3.9.7 Static Virtual Hubs

Virtual Hubs not using clustering are not particularly classified, but in a clustering environment they are classified into two types: static Virtual Hubs and dynamic Virtual Hubs. While the Virtual Hub's type has to be designated upon creation, it is also possible to change the type at a later date.

First is an explanation of static hubs.

A static Virtual Hub is used to conveniently create a Virtual Hub for remote access VPN. Creating a static Virtual Hub within a cluster generates that hub's instance (entity) in all VPN Servers within the cluster, which continues to run on all VPN Servers as long as the cluster is operating.

When connection source VPN software (usually an end user VPN Client) wishing to make a remote access connection is connected to the cluster controller, the cluster controller uses the aforementioned algorithms to select one of the VPN Servers and redirects the connection to the static Virtual Hub instance within that VPN Server.

By configuring a local bridge connection between the physical Network Adapters connected to each of the VPN Servers for each static Virtual Hub instance created in each VPN Server in the cluster, and by connecting all of the local bridging destination physical LANs to the in-house LAN destination to which the remote access is desired (either a direct layer 2 connection or a layer 3 connection using a router and NAT is acceptable), the VPN Client user can remotely access this in-house LAN regardless of which VPN Server the connection is assigned to.

This mechanism enables the creation of a large-scale remote access VPN service required to process a large volume of simultaneous connections. Please refer to 10.8 Build a Large Scale Remote Access VPN Service for specific configurations.

3.9.8 Dynamic Virtual Hubs

The dynamic Virtual Hub is a type of Virtual Hub convenient for providing VPN Server services such as creating a large number of Virtual Hubs within a cluster and enabling users connected to the same Virtual Hub to communicate freely. Dynamic Virtual Hubs are suitable, for instance, as a way for systems divisions of large companies to make Virtual Hubs for each department, or for ISPs creating Virtual Hubs as a service to their customers, wherein those departments and customers have the administration authority for that Virtual Hub and are free to operate it as they please. Such uses only require the entire VPN Server Administrator to take note of whether the VPN cluster is running properly, and all of the responsibility for setting and administering each Virtual Hub can be delegated to the Virtual Hub Administrators.

When a dynamic Virtual Hub has been created within a cluster but does not have any one connected to it, that Virtual Hub's instance (entity) does not exist on any of the VPN Servers in the cluster. When the first session designating that Virtual Hub makes a VPN connection, the controller selects the VPN Server which should launch that Virtual Hub's instance for the first time, then creates the Virtual Hub instance for that VPN Server and redirects the VPN session to that server. For the second and subsequent sessions to that Virtual Hub, they are automatically redirected to the VPN Server running that Virtual Hub instance such that regardless of how many VPN Servers there are, VPN sessions connected to the same Virtual Hub are always connected to the same VPN Server. When no one is connected to a dynamic Virtual Hub, its instance automatically stops running and releases the CPU and memory reserved for it.

This system makes it possible to create a large-scale Virtual Hub hosting service capable of hosting a large number of Virtual Hubs. Please refer to 10.9 Build a Large Scale Virtual Hub Hosting Service for specific configurations.

3.9.9 Connecting to Arbitrary Servers in Static Virtual Hubs

As mentioned above, a VPN connection to a static mode Virtual Hub is automatically load shared, so it is not possible to know which VPN Server the connection is to until it has been established.

Virtual Hub Administrators may, however, need to connect to the static Virtual Hub instance of an arbitrary VPN Server in a cluster for administration purposes. In this event, when creating the connection settings in the VPN Client or the like, designate the address of the VPN Server and the name of the Virtual Hub to which direct connection is sought instead of designating the cluster controller as the connection destination VPN Server. In addition, designate the password required to connect as an Administrator user (see 3.4 Virtual Hub Functions for details). This exception makes it possible for a VPN connection to be made directly to the desired VPN Server's static Virtual Hub without going via the cluster controller router.

3.9.10 Collectively Administering the Entire Cluster

Collectively Administering the Entire Cluster

Once the cluster is created, the entire VPN Server Administrator and Virtual Hub Administrators need only make an administration connection to the controller to be able to collectively administer the status and VPN sessions of all of the Virtual Hubs operating in the cluster. The administration of the VPN Server and Virtual Hubs is carried out using the VPN Server Manager or vpncmd utility in the same manner as when not using the clustering function.

Simply by connecting to the cluster controller, VPN Server Administrators can administer all of the Virtual Hubs in the cluster. Each Virtual Hub Administrator can administer the Virtual Hub for which they have authority.

The only situations in which it is necessary for VPN Server Administrators to make a direct administration connection to cluster member servers other than the cluster controller are the following.

- When disengaging a cluster member server from a cluster and returning its operating mode to a stand alone server.
- When confirming which Virtual Hub instances (entities) are actually operating within the cluster member servers.
- When editing the cluster member server's [Encryption and Communication Setting] entries, obtaining the contents of the Configuration file or acquiring the server's status.

Virtual Hub Administrators can only perform administration connections to the cluster controller, and not to the cluster member servers.

Local Bridge & Virtual Layer 3 Switch Settings

Local bridge and virtual layer 3 switch settings are carried out for each VPN Server. However, entire VPN Server Administrator authority is required for these settings. Please refer to 3.9.12 for further details.

Changing Virtual Hub Types

After creating the Virtual Hub, the type (dynamic Virtual Hub or static Virtual Hub) cannot be changed. As such, be sure to select a suitable type when creating the Virtual Hub.

3.9.11 Functions not Available Simultaneously with Clustering

When the clustering function is enabled, the following functions cannot be used at the same time.

- **Cascade Connections**
  (it is possible to receive a cascade connection from a separate computer)
- **Virtual NAT**
  (virtual DHCP Server function work)

The local bridging and virtual layer 3 switch functions can be used normally. However, local bridging and virtual layer 3 switching of Virtual Hub instances (entities) designated as local bridge definitions or virtual layer 3 switch virtual interface definitions can only operate between that VPN Server on which they actually exist. In the case of static mode Virtual Hubs, a defined static Virtual Hub instance normally exists, in principle, on all VPN Servers. However, in the case of dynamic hubs, there can only be one VPN Server in the cluster on which an instance can exist at the same time so the local bridging and virtual layer 3 switching functions are typically not available for dynamic Virtual Hubs.