10.8 Build a Large Scale Remote Access VPN Service

If you expect a large number of simultaneous connections to your VPN Server based remote access VPN system like the one described in section 10.4 Build a Generic Remote Access VPN, you can use the clustering capability to perform load balancing across multiple VPN Servers. This allows you to decrease the load on each VPN Server and increase overall throughput. It also allows you to automatically introduce fault-tolerance into your network design.

10.8.1 VPN Server's Processing Limit

A single VPN Server can theoretically handle up to 4,096 sessions at once. So, a VPN Server being used for a remote access VPN could handle approximately 4,000 VPN Client connections simultaneously.

However, the problem in reality is not software limitations but hardware limitations such as limited memory capacity or CPU processing speed. That being said, if 4,000 VPN sessions were handled by a single VPN Server there would be issues such as significant transmission speed loss or insufficient memory on the VPN Server resulting in memory swap access that would drastically limit the usability of the VPN as a whole.

In the future it is predicted that hardware will advance to a point where it will be able to handle such a load. Unfortunately, that technology is not yet available to us. So, in order to handle these high number of connections we have to design software in such a way so that it can decrease the load on the hardware.

When a large corporation's IT department wants to provide a remote access VPN service to all of its employees, they have to try and predict how many connections might possibly be made to the server at the same time. For example, if your VPN server machine is a Pentium 4 2.8 GHz with 1 GB of RAM we recommend having one server for every 200 to 500 sessions. (Keep in mind that the actual number of VPN Servers required can vary greatly according to network traffic and other factors.)

10.8.2 Increase Network Scalability By Using Clustering

By using the clustering capability built in to SoftEther VPN Server, you create a cluster of servers to handle a large number of remote access VPN connections.

By increasing the number of computers in the cluster you can achieve a system that can handle even more than 4,096 simultaneous sessions at once.

This section will give an example layout of this type of remote access VPN service and inform you of important points to keep in mind when designing a cluster network. Please refer to section 3.9 Clustering for more detailed information about the clustering capability.

10.8.3 Using Static Virtual Hubs

You can create one or more Virtual Hubs within the cluster. When dealing with clusters, there are two types of Virtual Hubs: static Virtual Hubs and dynamic Virtual Hubs.

The best one to use for a remote access VPN is the static Virtual Hub. (See section 3.9 Clustering.)

10.8.4 Network Layout

This section will explain the following type of network layout as an example.

10-8-1.png

Network Layout.

The network example above assumes that there is an existing company LAN to which the VPN Clients make a remote VPN connection to.

In this case there are many VPN Clients that need to connect to the VPN Server. To handle the load, you can install multiple VPN Servers and initiate clustering between them.

In the example above, three VPN Servers are being operated as a cluster. When VPN Clients connect to the cluster they will be re-directed to the VPN Server with the lowest load as calculated by the cluster controller. VPN Clients will not know which static Virtual Hub instance they are connected to. However, all Virtual Hubs are connected via

a local bridge to the remote access VPN's destination network segment, so the user will be able to communicate over the remote network without having to know which VPN Server they were assigned to via the load balancing algorithm.

In this example there are three VPN Servers installed for a predicted total of 300 VPN Clients. However, determining how many VPN Servers to install is not only based on the number of VPN Clients, but can change dramatically based on the VPN Server computer's hardware, or the bandwidth available from the backbone it is connected to. The method we recommend of finding the optimal number of VPN Servers is to first set up a small test VPN of two VPN Servers using clustering. Test to see how many sessions can be active at once before performance starts being affected. From there you can tell about how many sessions a single VPN Server can handle in your network environment, and you can add more VPN Servers as needed. By using this method you can eliminate any wasted costs and build the smallest, most efficient VPN to suit your needs.

This network example assumes that the remote LAN is made up of a single layer 2 segment. However, in most situations where clustering is needed such as in a large corporation, the internal network is most likely separated into multiple segments with IP routing taking place between them. Therefore, when setting up a remote access VPN for this type of network you will need to install a static Virtual Hub on each of the remote networks. Then, you must also connect each VPN Server with each Ethernet segment containing a Virtual Hub with a local bridge connection.

10.8.5 Installing and Configuring the Cluster Controller

When installing multiple VPN Servers as a cluster you must first install the first VPN Server as the cluster controller. If the VPN Server machines you have prepared have different hardware specifications, you should pick the one with the most memory and the most powerful hardware to be the cluster controller.

Please refer to section 3.9 Clustering for more information on setting up a VPN Server as a cluster controller.

10.8.6 Installing and Configuring the Cluster Member Servers

Each VPN Server installed after the first will connect to the cluster controller as a cluster member server. Please refer to section 3.9 Clustering for more information on setting up a VPN Server as a cluster member server.

10.8.7 Creating Static Virtual Hubs

Once you have all your VPN Servers installed connect to the cluster controller and create a single Virtual Hub. Set the type of the Virtual Hub to static. As explained previously, if the network you wish to connect to remotely has multiple segments, create a Virtual Hub for each segment.

Note that the Virtual Hub that exists on a fresh install of VPN Server named "DEFAULT" is a dynamic Virtual Hub. (You can change it to a static Virtual Hub and use it if you would like.)

10.8.8 Making a Local Bridge between the Existing LAN and the Virtual Hubs

When a static Virtual Hub is created on the cluster controller an instance of that static Virtual Hub will automatically be made on all VPN Servers in the cluster. (See section 3.9 Clustering.)

Next, make a direct administrative connection to each VPN Server and set up a local bridge connection between that Virtual Hub and the physical LAN you wish to connect to remotely. (For more information on creating local bridge connections, see section 3.6 Local Bridges.) As explained previously, if the network you wish to connect to remotely has multiple segments, you must make local bridge connections between each static Virtual Hub and their respective physical LAN. (You will need multiple network adapters for this.)

Refer to section 10.4 Build a Generic Remote Access VPN for things to note when making local bridge connections.

Once the local bridges are configured that cluster is ready to go as a remote access VPN system. VPN Clients can make a VPN connection to the cluster controller via the Internet, at which point the controller will automatically redirect the connection to the VPN Server with the lowest current load. That VPN Server will then process that client's connection. The user never has to know about this process, and can connect just as they always would.

In addition, if an operating cluster member has a hardware failure or is taken down for maintenance, any VPN sessions being handled by the VPN Server on that member will automatically be assigned to a different VPN Server with no interruption of service. Even if something like this happens, the VPN Server administrator does not have to lift a finger.

10.8.9 Managing VPN Sessions on a Clustered VPN

Once you have finished setting up your clustered environment, there is usually no need to make an administrative connection to the cluster member servers. Administrative operations such as downloading log files, changing logging preferences, adding/removing/editing currently connected users, configuring external authentication servers, or configuring trusted authentication certificates can all be done on the cluster controller. The controller will then update all VPN Servers on the cluster to maintain consistency automatically.