Cloud Simulation

VPN Connectivity Guide

Table of contents

DISCLAIMER: Although we provide basic instructions for you to establish a VPN connection to your CLOUDSIM instance, we DO NOT officially support the installation and use of OpenVPN or IPsec/GRE. Use at your own risk.

1. Introduction

This document is intended to explain in detail the methods of connecting to your Cloud Simulation instance (referred to as CloudSim from here on) via the Internet, as well as over a leased-line connection using Deutsche Boerse's N7 network. These methods are meant to provide strong security, while at the same time allowing the customer the flexibility to choose which option is best for their network infrastructure.

Whether you connect to your CloudSim instance over the internet, or the leased-line option, both connectivity types require you to establish a VPN tunnel using either GRE encapsulation and IPSEC encryption, or SSL encryption with the configuration files supplied during the creation of your CloudSim instance.

For those customers who have chosen to connect using a dedicated channel on their N7 connectivity, they must, in addition to establishing a VPN connection, ensure that they have defined a route through their network, to their N7 CloudSim connection, for any computers that will be used to access Instance Control on their CloudSim instance. Instance Control can only be accessed via the N7 CloudSim connection. Details on this can be found in Section 4.

2. OpenVPN

OpenVPN is a VPN software solution which uses the industry standard SSL/TLS protocol for data encryption. The OpenVPN tunnel connectivity to CLOUDSIM is strictly a host-to-host solution, meaning that the tunnel to your CLOUDSIM instance should terminate on a host on your client side. OpenVPN tunnel connectivity to CLOUDSIM can be terminated on Windows, Linux, or Mac OSX.

2.1 Possible Endpoints

For official documentation and more detailed installation instructions about OpenVPN please visit http://openvpn.net/howto#install

The following instructions assume that you have downloaded the OpenVPN configuration files associated with your CLOUDSIM instance, available after logging in at https://CloudSim.deutsche-boerse.com. After the creation of your CLOUDSIM instance, you will be able to download your pre-configured OpenVPN configuration file, as well as associated keys and certificates, to create a VPN tunnel for access to your CLOUDSIM instance.

NOTE: The OpenVPN endpoint on your instance is designed for use with the OpenVPN client version 2.3.2. Other versions of the client may not be compatible with your instance's server.

2.1.1 Windows

2.1.1.1 Installation

OpenVPN for Windows can be installed from the self-installing exe file on the OpenVPN download page. Note that OpenVPN will only run on Windows XP or later, and must be installed and run by a user who has administrative privileges (this restriction is imposed by Windows, not OpenVPN). Click here for information on running OpenVPN without administrative privileges

Official OpenVPN Windows installers include OpenVPN-GUI, which allows managing OpenVPN connections from a system tray applet.

During the install process, when confronted with the "Choose Components" state, leave the default options selected.

IMPORTANT: When the installation prompts you to confirm the installation of the "TAP-Windows Adapter V9", select "Continue Anyway". This installs the necessary virtual network interface that the tunnel will be established on.

After you've run the Windows installer, OpenVPN is ready for use and will associate itself with files having the .ovpn extension.

2.1.1.2 Connection initiation

Extract the contents of the downloaded .zip file into any directory on your client.

Right click on the client.ovpn file that you had previously extracted and select Start OpenVPN on this configuration file. OpenVPN should proceed to establish a secure connection to the your running instance.

Alternative connection methods:

Run OpenVPN from a command prompt Window with a command such as:

```
openvpn client.ovpn
```

Run OpenVPN as a service by extracting all files downloaded from your instance to \Program Files\OpenVPN\config and starting the OpenVPN Service, which can be controlled from Start Menu -> Control Panel -> Administrative Tools -> Services.

Additional Windows install notes.

2.1.2 Linux

These instructions assume you have root privileges and have access to the appropriate commands (apt-get/yum, unzip, service).

If you are using Debian, Ubuntu, Fedora 16 or RHEL/CentOS/Scientific Linux 6, OpenVPN is available through your distribution's repositories.

If using *Debian/Ubuntu* run:

```
apt-get install openvpn
```

If using *RHEL/Fedora* run:

```
yum install openvpn
```

Once OpenVPN has been successfully installed, unzip the contents of the "openvpn" directory from the .zip archive for your instance into /etc/openvpn/ and run restart OpenVPN:

```
unzip -j 31_171_244_59.zip 'openvpn/*' -d /etc/openvpn

service openvpn restart
```

If everything has been done correctly and no errors have occurred, you should be able to see the successfully established VPN tunnel to your instance.

Note: If OpenVPN is not available in your repositories, the OpenVPN source can be downloaded here: http://openvpn.net/index.php/open-source/downloads.html

2.1.3 Mac OSX

OpenVPN does not provide an official GUI for Mac OSX, but we have found that the application Tunnelblick works well.

You can find the Tunnelblick download link and official instructions at https://code.google.com/p/tunnelblick/

Once the Tunnelblick .dmg file has been downloaded, double click it. On the new window, double click the "Tunnelblick" icon and confirm the installation. When prompted for configuration files, click "Quit".

Once Tunnelblick has been successfully installed, simply double click XX_XX_XX_XX.tblk provided with the .zip archive and your VPN tunnel to the instance should automatically be configured.

In the taskbar, click the Tunnelblick icon and connect to your instance.

If everything has been done correctly and no errors have occurred, you should be able to see the successfully established VPN tunnel to your CLOUDSIM instance.

2.2 Firewall ports

Required firewall ports when using OpenVPN:

• OpenVPN tunnel	TCP port 1194 (SSL)
• Instance control (web interface for controlling instances)	TCP port 8000 (SSL)

3. IPsec/GRE

IPsec/GRE connectivity to CLOUDSIM is an alternate connection method meant to accommodate customer networks that are incompatible with our OpenVPN solution. Our IPsec/GRE connectivity leaves more of the configuration up to the customer, allowing for flexibility when it comes to larger internal networks whose security policies may not allow for direct host-to-host access.

In order to use IPsec/GRE as your tunnel method, you'll first need to have a static IP assigned to your CLOUDSIM account that you can attach to your instances.

This solution consists of two components. The first component is IPsec, which provides encryption of all traffic between your CLOUDSIM instance and your internet-facing entry point into your network. Because IPsec alone is incapable of transporting multicast traffic (required for CLOUDSIM's market data), a separate GRE tunnel is required. The GRE tunnel is also between the same endpoints as the IPsec tunnel, as the IPsec tunnel is simply meant to just encrypt all of the traffic sent via the GRE tunnel.

All traffic is sent via the GRE tunnel interface. The exchange backend is directly available via this GRE tunnel, and all exchange interfaces (market data interfaces, trading interfaces) need to be addressed via this interface.

Because of the flexibility of our IPsec/GRE connection solution, we are unable to provide an officially supported configuration, but this document will list several example network configurations that have been tested and work for us.

To clarify basic terminology, we will refer to the following IP addresses throughout our documention.

Term	Refers to
<CLOUDSIM_END-POINT_IP>	Publically addressable IP address assigned to your CloudSim instance.
<CUSTOMER_END-POINT_IP>	Publically addressable IP address assigned to the interface the customer chooses to terminate the IPsec tunnel upon. This is usually assigned by the customer's ISP.

3.1 IPsec Settings

3.1.1 Phase 1 (IKE-AES-256-SHA-DH5) Parameters

Setting	Parameter
Encryption Algorithm	AES256
Hashing Algorithm	SHA-1
Diffie-Hellman Group	Group 5 (1536-bit)
Authentication Mode	Pre-Shared Key
IKE Negotiation Mode	Main
IKE Timeout (ISAKMP)	3600 Seconds (1 Hour)

3.1.2 Phase 2 (ESP-AES-128-SHA-HMAC) Parameters

Setting	Parameter
Encryption Algorithm	AES128
Hashing Algorithm	SHA-1
PFS Diffie-Hellman Group	Group 5 (1536-bit)
IPsec Timeout (SA)	3360 Seconds (56 Minutes)

3.1.3 Pre-Shared Key

The Pre-Shared Key (PSK) for your CLOUDSIM instance is available for download on the CLOUDSIM homepage (https://CloudSim.deutsche-boerse.de) after you have configured your initial set of keys for your instance's IP address.

3.2 GRE Settings

10.8.0.1 is the CLOUDSIM instance's IP address on the GRE tunnel interface. This is the peer on the other side of the GRE tunnel from the customer endpoint. This 10.8.0.1 address is the T7 "backend", being the address of multicast sources as well as TCP/IP connections. Explain how GRE endpoint is the "next router hop"

3.3 Possible Endpoints

Many different hardware and software platforms support IPsec encryption. It is impossible to certify all available options. We've tested permutations of the following platforms, however, our tests are neither absolutely inclusive of every option under these platforms, nor should they be considered endorsement.

3.3.1 Linux

Due to its flexibility, IPsec/GRE can work as a host-to-host solution when using Linux as an endpoint.

3.3.2 Cisco

We have also tested a Cisco-based device as an endpoint for IPsec/GRE connectivity to CLOUDSIM, enabling the use of multiple clients behind the customer's endpoint.

4. Accessing CloudSim via an N7 Connection

It is now possible to access CloudSim via a dedicated CloudSim channel on an N7 connection. However, customers are still required to make a VPN connection to their instance using either SSH or IPSEC/GRE.

Additionally, any internal machine that you wish to have connect to your CloudSim instance's static IP address must have a route to the correct network. This includes any machines or workstations that will connect to your instance's Instance Control page.

There are many different ways to ensure a route to your CloudSim instance, and your networking staff is the best resource to approach regarding this. They will have their own preferences for publishing this route within your network. However, it is possible to configure a static route on a machine-by-machine basis. Below, strictly for reference, you will find instructions on setting a static route on three popular OS platforms; Windows, Linux, and MacOS.

The instructions for creating static routes for your specific OS and version number may vary. We recommend that you confirm these steps with your IT department before executing them.

In each of these examples, xxx.xxx.xxx.0 refers to the N7 IP address assigned to your instance; and yyy.yyy.yyy.yyy refers to the LAN IP address on your router that connects to N7.

4.1 Windows

To add a static route to your instance for Windows-based machines, type the following at a CMD prompt:

```
route -p ADD xxx.xxx.xxx.0 MASK 255.255.255.0 yyy.yyy.yyy.yyy
```

The "*-p*" switch on the *route* command makes this route persistent. If you would prefer to make this route temporary, than omit the "*-p*".

4.2 Linux

To add a temporary static route, simply run, as **root**, the *ip route add* command with the right network information:

```
ip route add xxx.xxx.xxx.0/24 via yyy.yyy.yyy.yyy dev eth0
```

To add a permanent static route

To make the route permament, you need to create a static route configuration file. Create a file with the name route-interface in your /etc/sysconfig/network-scripts, such as:

```
touch /etc/sysconfig/network-scripts/route-eth0
```

Then, add the line:

```
xxx.xxx.xxx.0/24 via yyy.yyy.yyy.yyy dev eth0
```

to your /etc/sysconfig/network-scripts/route-eth0 file. Make sure to restart your network settings so they take effect:

```
service network restart
```

4.3 Mac OS X

To add a temporary static route, simply run the *route add* command from a console window:

```
sudo route add xxx.xxx.xxx.0/24 yyy.yyy.yyy.yyy
```

To add a permanent static route, create a new, executable bash script, and set it to run at start up. For example:

```
vim /usr/local/bin/static-routes.sh
```

To this file, add the line:

```
sudo route add xxx.xxx.xxx.0/24 yyy.yyy.yyy.yyy
```

Be sure to make this file executable:

```
chmod +x /usr/local/bin/static-routes.sh
```