Connecting Flexy to a Standard OpenVPN Server running Ubuntu Server

HMS Networks

May 3, 2019

This is a preliminary application note describing the steps required configure the Flexy VPN Client for use with the standard OpenVPN server. As of May 3rd 2019 limited testing has been performed on this solution. It is recommended customers develop a test system and verify every Flexy feature required for the customer specific application is tested prior to deploying.

The following software packages are used, version changes can impact the results. An effort should be made to use the identical software packages.

Openssl	version 1.1.0g
Unbuntu Server	version 18.04 LTS
EasyRSA	version 3.0.4
Flexy Firmware	version 13.0s0
OpenVPN	version
VirtualBox	version 6.0.6

References

This application note leverages the Digital Ocean web page describing the process of setting up a generic Linux OpenVPN server and client. Points where the Flexy configuration differs are described below. In this document "Digital Ocean OpenVPN Setup" refers to this page.
https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04

Step 0: Test Environment Setup

A VirtualBox box will be used to create Ubuntu Server VM. Download VirtualBox from Oracle. Download the Ubuntu Server LTS 18.04 iso. The default VirtualBox settings can be used with the following exceptions.

1) Settings > Network (Also the VM to get a IP address independent of the host)
    a. Ensure Adapter 1 is enabled
    b. Select Attached to: Bridged Adapter
    c. Select the host network interface with access to the internet
2) Settings > Shared Folders (Also the user to pass files back and forth between the host)
    a. Add a shared folder on the host (example Folder Path: c:\temp)
    b. Folder Name is VMshared
    c. Read-only and Auto-mount are no not checked
    d. Mount point is blank
    e. Check Make Permanent

3) Download the VBoxGestAdditions_6.0.0_RC1.iso from this site http://download.virtualbox.org/virtualbox/6.0.0_RC1/
4) Install the .iso in the Storage device for the VM (this is done in Settings > Storage)

Start the VM. Run the command ifconfig to verify the network adapter settings resulted in a IP address being assigned to the VM. The output should show a network interface with an IP address that is different from the Host but on the same subnet.

$ ifconfig

The following commands must be run at the Linux command line to mount the shared folder in the VM.

$ sudo mkdir /mnt/cdrom

$ sudo mount /dev/cdrom /mnt/cdrom

$ sudo /mnt/cdrom/./VBoxLinuxAdditions.run

$ mkdir ~/VMshared

$ sudo mount -t vboxsf - VMshared ~/VMshared

$ touch ~/VMshared/test

Check the host machine to verify a file "test" is now visible in the shared directory. This directory is used to pass files between the Linux VM and the host machine.

Step 1: Installing OpenVPN and Easy RSA

This section describes how to create both server and client keys and requests. A user generated CA will be used to sign the certification requests. A production system may want to use a corporate CA or 3rd party CA. If a CA other than the one defined in this document is used it is critical to use the CA configuration parameters as defined. Failure to do so will result in a certificate that is not usable in the Flexy system.

Execute the steps show in the Digital Ocean OpenVPN Setup Step 1 to install the EasyRSA and OpenVPN software packages on the VM.

If for development purposes the CA exists on the same machine ensure there is a sperate EasyRSA install directory for the CA.

Step 2: Installing OpenVPN and Easy RSA

Execute the steps shown in the Digital Ocean OpenVPN Setup Step 2 to build the CA. The default names will be used in this app note as shown in the Digital Ocean OpenVPN Setup. The following adjustments must be made to the vars file. The vars file must include the following lines uncommented.

set_var EASYRSA_KEY_SIZE 2048

set_var EASYRSA_NS_SUPPORT "yes"

set_var EASYRSA_NS_COMMENT "Easy-RSA Generated Certificate"

The EASYRSA_NS commands enable the certificate variable ns-cert-type. This variable is a legacy configuration variable that is embedded in the Flexy core configuration. It is used to fix the certificate usage to either a client only certificate or a server only certificate. There is no way to disable this feature in the Flexy firmware so it must be used. There is no security risk associated with using this legacy feature.

Step 3: Installing OpenVPN and Easy RSA

Execute the steps show in the Digital Ocean OpenVPN Setup Step 3 to build the CA. If executing this whole process on a single VM, the EasyRSA software must be installed in a separate directory from the CA EasyRSA install. Create a new directory for your key generator copy the EasyRSA tar file to the new directory and extract the software using this command.

$ tar xvf EasyRSA-3.0.4.tgz

Copy the vars file from the CA to this install of EasyRSA to ensure the configuration parameters are correct. (Not 100% sure this is required; it is possible the vars file is not used when generating keys and certificate requests)

The Digital Ocean OpenVPN Setup directions show coping the server.crt, ca.crt, ta.key, dh.pem to the OpenVPN install directory using the path /etc/openvpn. The current openvpn install includes to sub directories (server and client). HMS recommends placing the files in /etc/openvpn/server.

Step 4: Generating a Client Certificate and Key Pair

Execute the steps show in the Digital Ocean OpenVPN Setup Step 4 to build the CA. The same EasyRSA install location used to generate the server request and key can be used to generate the client request and key.

Step 5: Configuring the OpenVPN Service

Execute the steps show in the Digital Ocean OpenVPN Setup Step 5 to build the CA. HMS did not test the optional portions of this step. The server.conf files used during testing is included in appendix A of this document. The HMAC firewall feature was not enabled during testing. It is possible that an alternative set of options will work with this system. The following lines is required:

ns-cert-type client

Step 6: Adjusting the Server Networking Configuration

This step was not executed during the development of this application note. This section address network address routing at the server level. Customers are left to configure this portion of the system to meet their specific system needs.

Step 7: Starting and Enabling the OpenVPN Service

Execute the steps show in the Digital Ocean OpenVPN step 7. The Digital Ocean OpenVPN steps following step 7 are related to setting up a standard OpenVPN client. These steps will not be required to setup the Flexy service.

In addition to the status commands in step 7 it is useful to verify the OpenVPN service is accessible from another linux system or VM on the network. The following command will return success if the server is visible on the network. Ensure the IP address and port are updated to match the system under test.

$ nc -vu 172.16.0.45 1194

It may be useful during debug to start and stop the VPN server. Starting or restarting the server will cause the OpenVPN server to reread the server.conf file. The commands to do so are as follows:

Sudo systemctl status openvpn@servername

Sudo systemctl stop openvpn@servername

Sudo systemctl start openvpn@servername

Sudo systemctl restart openvpn@servername

Step 8: Configuring Flexy as a generic OpenVPN Client

The GUI interface can be used to configure a number of the OpenVPN Client setting but not all. As a result the use of the GUI will be minimized and a majority of the configuration will be done using configuration files.

In the Flexy GUI confirm the following settings:

1) Setup > System > Communications > Networking > VPN Connection > Main setup
    a. Ensure Establish outgoing VPN to server is selected
    b. No other options should be selected
2) Setup > System > Communications > Networking > VPN Connection > Global
    a. Internet connection proxy – No proxy
    b. Talk2M Account Name – Customers Account Name
    c. Talk2M Access Server – talk2m_pro
    d. Advanced settings Diagnosis level – High
    e. Advanced settings Port In – 0
    f. Advanced settings Port Out – This should be the port of the OpenVPN Server
    g. Advanced settings ‘keep alive’ interval – 120
    h. Advanced settings VPN Driver Mode – TUN
    i. Advanced settings VPN Protocol – UDP
3) Setup > System > Communications > Networking > VPN Connection > Incoming
    a. Leave as default
4) Setup > System > Communications > Networking > VPN Connection > Outgoing
    a. Establish VPN connection should be checked
    b. Primary server – IP address of OpenVPN Server

c. Secondary server – IP address of backup OpenVPN Server
d. Connect to…
    i. Select VPN Server in the drop down
    ii. The Private key, Certificate and CA certificate can be left unchanged or blank

Once the above GUI settings have been made reboot the Flexy. Using an FTP tool like FileZilla connect to the flexy once it has completed the reboot. The complete Flexy configuration is stored in multiple text files at the top level of the Flexy device. These file are overwrite by the GUI and should not be used to implement the VPN configuration. A link to a user configuration file is needed to create a user controlled file for configuration. This configuration link will be added to the top level comcfg.txt file.

1) FTP into the Flexy
2) Copy the /comcfg.txt file to a host PC
3) Edit the file and add this line

    VPNCfgFile:+/usr/client.ovpn

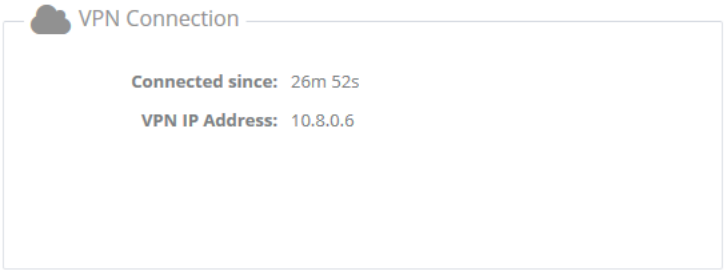
4) Edit the client.ovpn file used in this app note (attached)
    a. Different cipher files can be used for example auth SHA256 should work
    b. It is critical that if auth SHA256 is used an identical change is made to the server.conf
    c. ns-cert-type server is not included in the settings because it is automatically set by the Flexy firmware

FTP the following files over to the Flexy /usr directory: ca.crt, client.ovpn, client1.crt, client1.key.

Reboot the Flexy.

Verify the System is Working

If properly configured using the settings defined is this document the OpenVPN server will assign a IP address to Flexy in the 10.8.0.xxx range. In the Flexy GUI the top-level summary should show the following info in the VPN Connection section.



Still working on the sections below.

Useful tools

During the development of this application note the following commands and tools were used to debug the system. End users may find these tools useful in debugging the system.

1) Checking a Key, Certification pair. If the output of these two functions match the CRT and Key are a pair.
   $ openssl rsa -noout -modulus -in client1.key

   $ openssl x509 -noout -modulus -in client1.crt

2) Determining the version of ssl
   $ Openssl version -a

3) Command line reboot VirtualBox Linux box
   $ sudo shutdown -r now

Steps to enable the shared directory between the VirtualBox Ubuntu 18 server and windows host. In this case we used windows 10. The name of the shared folder in VirtualBox is shared.

sudo /mnt/cdrom/./VBoxLinuxAdditions.run

mkdir ~/shared

sudo mount -t vboxsf -t vboxsf shared ~/shared

need to add more

Attempted CA setup with this link and failed: https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04

The certificate request for the server could not be signed, not sure what the issue was.

Executing steps on this Wiki: https://wiki.archlinux.org/index.php/Easy-RSA

CA password is hms@123

Name of OpenVPN server is TomOpenVPNserver

OpenVPN is constantly trying to start which is making debug confusing: disable auto start by editing /etc/default/openvpn uncomment #AUTOSTART="none" , reboot the linux box, allows you to start clean. Sudo systemctl status openvpn@server will give you the status and point to a command called `journalctl --identifier ovpn-server to get a longer error file the issue is this error file accumulates errors from the beginning.`

`journalctl -xe #will also provide log into`

`Older client communications requirement`

`Make sure comp-lzo is uncommented in the openvpn configuration file`

`Log files in OpenVPN`

Define a status file in the openvpn configuration file by ensuring this line is uncommented in the configuration file.

status /var/log/openvpn/openvpn-status.log #current connection status 1 minute

log /var/log/openvpn/openvpn.log #logs to syslog truncated on startup

HMAC Firewall may not be supported in server.conf make sure the following two lines are commented. Also make sure these lines are not in the client config file.

;tls-auth /etc/openvpn/server/ta.key 0

;key-direction 0

EASYRSA Configuration. The eWON device uses OpenVPN 2.0.X and requires the ns-cert-type feature. This is a deprecated feature and must be explicitly requested when using EASYRSA to create server certificates.

Ensure these lines are uncommented in the var file:

set_var EASYRSA_NS_SUPPORT "yes"

set_var EASYRSA_NS_COMMENT "Easy-RSA Generated Certificate"

Digital Ocean Issues https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04

1) Copy the server key to /etc/openvpn/server (the page does not include the server directory)

Edit comcfg.txt in the Flexy top level directory, add the following line at the end of the file. Replace the file in the top level directory.

VPNCfgFile:+/usr/client.ovpn