RAK Industrial LPWAN Gateway Remote Management - OpenVPN

Version V1.0 | April 2020

RAKwireless.com

Visit our website for more document.

Contents

1 Overview

This document introduces a method of remote management of RAK Industrial LPWAN Gateways based on OpenVPN. A virtual private network (VPN) is created where a server is deployed that both the Gateway and any number of customer devices (PC, Phone, etc.) can connect to via a public IP address. This is possible to implement using any of the backhaul connectivity options the Gateway supports (Ethernet, Wi-Fi, LTE).

Thus, by connecting to the server via a remote client the user can remotely manage the Gateway from any point, at any time.

2 Network Topology

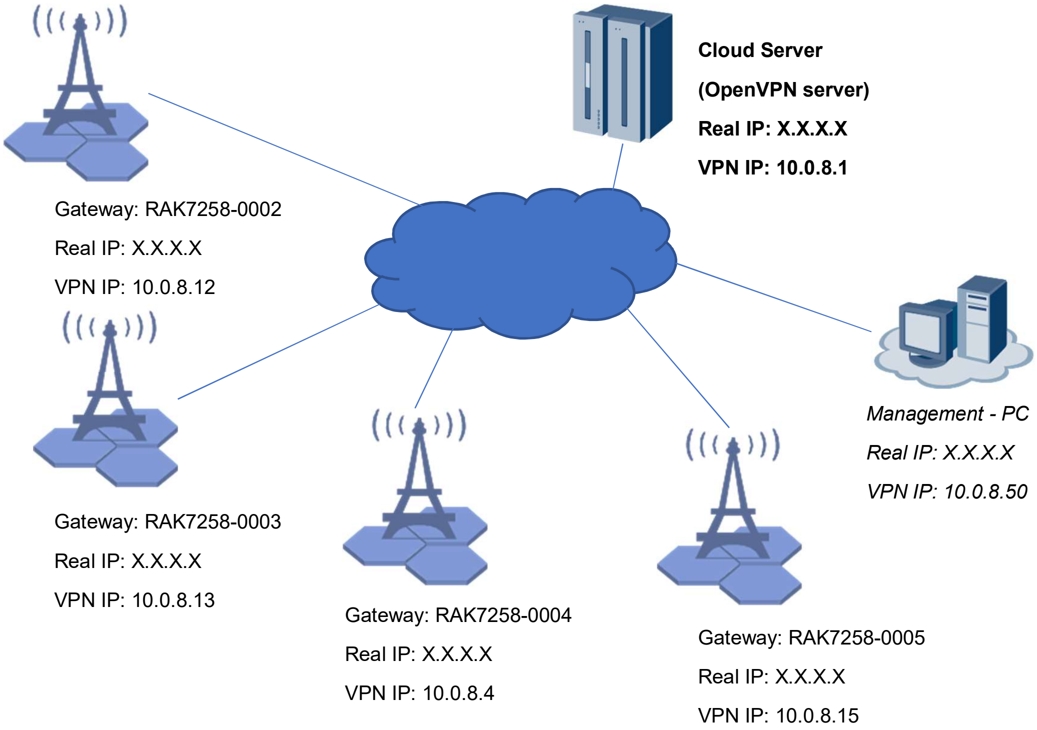


Figure 1 | Network Topology

3 Deploy the OpenVPN Server

This tutorial assumes you already have an AWS EC2 Instance with Ubuntu Server 18.04 LTS running on it. You can find a tutorial on how to deploy one at the link below:

Deployment and Management of Ubuntu on an AWS EC2 Instance

3.1 Install OpenVPN

First, we need to install the Open VPN package:

```
sudo apt install openvpn -y
```

3.2 Download a certificate management tool suite

We are going to be using Easy RSA:

```
wget https://github.com/OpenVPN/easy-rsa/archive/v3.0.6.tar.gz -O easyrsa.tar.gz
```

3.3 Initialize Easy RSA to generate a CA certificate and a server certificate

step 1. Extract and copy easyrsa to */etc/openvpn/easyrsa/*

```
sudo mkdir -p /etc/openvpn/easyrsa
tar zxvf easyrsa.tar.gz
sudo cp -rf easy-rsa-3.0.6/easyrsa3/* /etc/openvpn/easyrsa/
```

step 2. Initialize the pki

```
cd /etc/openvpn/easyrsa
sudo ./easyrsa init-pki
```

step 3. Generate the CA certificate

```
sudo ./easyrsa build-ca
```

Enter the required information according to the prompt.

Note: When asked for a password make sure to write it down as it will be required later on.

step 4. Generate the Server certificate

```
sudo ./easyrsa build-server-full server nopass
```

step 5. Generate the DH parameters file

```
sudo ./easyrsa gen-dh
```

step 6. Generate the crl.pem file

```
sudo ./easyrsa gen-crl
```

3.4 Generate the OpenVPN Server configuration and running files

step 1. Created the OpenVPN server configuration file and fill it in:

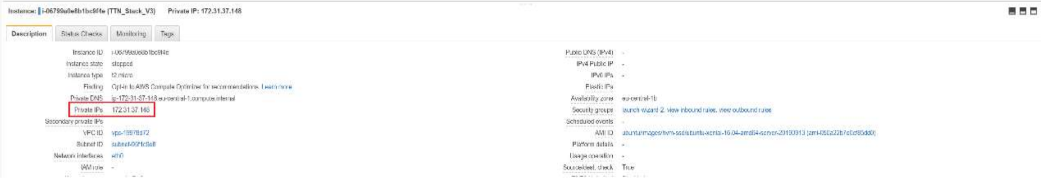
Create the folder the file will reside in:

```
sudo mkdir -p /etc/openvpn/server
```

Create the file and open it for editing

```
sudo nano /etc/openvpn/server/config.ovpn
```

Note: Change the ***local 123.56.96.211*** IP with your private AWS IP.

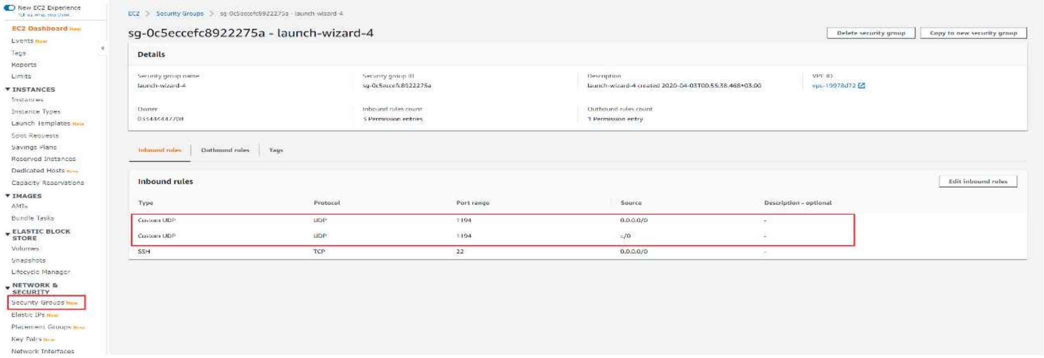


Instance: i-06799a0e8b1bc9f4e (TTN_Stack_V3) Private IP: 172.31.37.148

Instance ID	i-06799a0e8b1bc9f4e	Public DNS (IPv4)	-
Instance state	stopped	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-172-31-37-148.eu-central-1.compute.internal	Availability zone	eu-central-1b
Private IPs	172.31.37.148	Security groups	launch-wizard-2. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	-
VPC ID	vpc-19978d72	AMI ID	ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20190913 (ami-050a22b7e0cf85dd0)
Subnet ID	subnet-0971c9a8	Platform details	-
Network interfaces	eth0	Usage operation	-
IAM role	-	Source/dest. check	True

Figure 2 | AWS Instance Private IP

Note: You have to add an inbound rule in the AWS Security Group for UDP port 1194.



sg-0c5eccefc8922275a - launch-wizard-4

Details

Security group name: launch-wizard-4
Security group ID: sg-0c5eccefc8922275a
Description: launch-wizard-4 created 2020-04-03T00:55:38.468+03:00
VPC ID: vpc-19978d72
Owner: 035444447708
Inbound rules count: 3 Permission entries
Outbound rules count: 1 Permission entry

Inbound rules

Type	Protocol	Port range	Source	Description - optional
Custom UDP	UDP	1194	0.0.0.0/0	-
Custom UDP	UDP	1194	::/0	-
SSH	TCP	22	0.0.0.0/0	-

Figure 3 | Security Group Inbound Rules

```
# openvpn server
cd /etc/openvpn/server
daemon
dev tap
proto udp

#local ipaddr to bind. Change it with Server IP.
local 123.56.96.211
port 1194

server-bridge 10.0.8.1 255.255.255.0 10.0.8.11 10.0.8.100
ifconfig-pool-persist ip_pool.txt

up interface-up.sh

client-to-client
keepalive 10 120
comp-lzo
user root
group root
persist-key
persist-tun

ca /etc/openvpn/easyrsa/pki/ca.crt
cert /etc/openvpn/easyrsa/pki/issued/server.crt
key /etc/openvpn/easyrsa/pki/private/server.key
dh /etc/openvpn/easyrsa/pki/dh.pem
crl-verify /etc/openvpn/easyrsa/pki/crl.pem


status /var/log/openvpn-status-server.log
log /var/log/openvpn-server.log
verb 3
script-security 2
```

step 2. Create and fill in the *interface-up.sh*. This is a script that will create the virtual *tap* interface:

```
sudo nano /etc/openvpn/server/interface-up.sh
```

Fill in the content of the file with the lines below:

```
#!/bin/sh
/sbin/ifconfig $1 10.0.8.1 netmask 255.255.255.0 broadcast 10.0.8.0
```

Make the script executable:

```
sudo chmod +x /etc/openvpn/server/interface-up.sh
```

3.5 Start OpenVPN

step 1. Start OpenVPN

Note: If you want to OpenVPN to run on instance startup run the command:

```
sudo systemctl enable openvpn
```

Execute the following in order to get your *tap* interface up:

```
sudo openvpn --config /etc/openvpn/server/config.ovpn
```

Note: If you want OpenVPN to execute the configuration file automatically you should rename the config.ovpn to config.conf and move it to the /etc/openvpn folder.

This way if the Operating System is rebooted, OpenVPN will automatically load the tap interface.

```
cd /etc/openvpn/server
sudo mv config.ovpn /etc/openvpn/config.conf
```

step 2. Check whether the OpenVPN virtual interface is up:

```
 ifconfig tap0
```

You should see a similar output if the *tap0* interface is up and running.

```
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.8.1  netmask 255.255.255.0  broadcast 10.0.8.0
        ether 3a:37:f6:5a:bb:32  txqueuelen 100  (Ethernet)
        RX packets 45125  bytes 8292906 (7.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16611  bytes 2205218 (2.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4 Setup the OpenVPN Management Client

4.1 Generate the OpenVPN Server client certificate for your PC

Note: We use ***management*** as the name for the client PC.

```
cd /etc/openvpn/easyrsa
# ./easyrsa build-client-full <client_name> nopass
sudo ./easyrsa build-client-full managment nopass

# Update certificate control file
sudo ./easyrsa gen-crl
```

4.2 Make the OpenVPN Client profile file.

The <*ca*>*,* <*cert*>*,* and <*key*> in the configuration file are the CA certificate, Client certificate and Client secret key.

The CA certificate is located in:

/etc/openvpn/easyrsa/pki/ca.crt

The Client certificate together with the Client secret key we generated in **Section 4.1**.

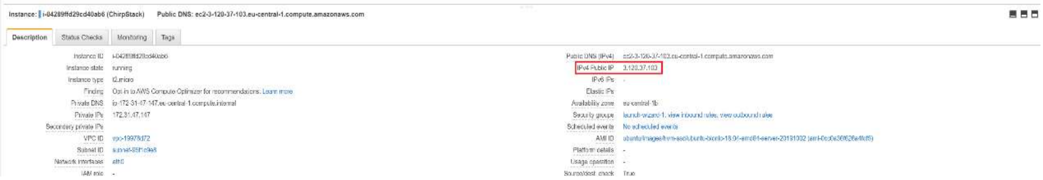
Client certificate:

/etc/openvpn/easyrsa/issued/<*client_name*>.crt

Client secret key:

/etc/openvpn/easyrsa/private/<*client_name*>.key

Open a text editor in your PC and copy this template. Change the remote IP with your Amazon Instance Public IP and add each certificate in its corresponding section by copying the content from the locations mentioned above and replacing the corresponding section in the template.



Instance: i-04289ffd29cd40ab6 (ChirpStack)   Public DNS: ec2-3-120-37-103.eu-central-1.compute.amazonaws.com

Instance ID	i-04289ffd29cd40ab6	Public DNS (IPv4)	ec2-3-120-37-103.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	3.120.37.103
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-172-31-47-147.eu-central-1.compute.internal	Availability zone	eu-central-1b
Private IPs	172.31.47.147	Security groups	launch-wizard-1. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-19978d72	AMI ID	ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20191002 (ami-0cc0a36f626a4fdf5)
Subnet ID	subnet-85f1c9e8	Platform details	-
Network interfaces	eth0	Usage operation	-
IAM role	-	Source/dest. check	True

Figure 4 | AWS Instance Public IP

```
dev tap
client
remote 123.56.96.211 1194
proto udp
nobind
resolv-retry infinite

persist-key
persist-tun

remote-cert-tls server

comp-lzo
verb 3

# copy from openvpn-server /etc/openvpn/easyrsa/pki/ca.crt
<ca>
-----BEGIN CERTIFICATE-----
MIIDNTCCAh2gAwIBAgIJANYEjCM+cqsxMA0GCSqGSIb3DQEBCwUAMBYxFDASBgNV
BAMMC1JBS1dpcmVsZXNzMB4XDTE5MTEyNTAxMzIyOVoXDTI5MTEyMjAxMzIyOVow
FjEUMBIGA1UEAwwLUkFLV2lyZWxlc3MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDZS/8PCehr3TSTvidQLFVYT5EydKDVidEUm6/yOE0BZs99kZKGn6eF
mFQnBfve4mAHzPnC3amiuCh+01kf97P7MDpS/cYTdR9RB9Xng/jyBQqMVVHLbwoG
IS7mQmBpV0NdU8RYKsLCARPn50eRGiL2AS6cPDSjrrj2xsBEydTsjE/95gJ7AvWQ
RPRoVTI9S31mY6tLrs16zydtEXWicDVaRFkvultijCmCiUhfaDE8lt1dQxd5jkvw
cHtm1EBdHjyce7oXa+Og0p2c5EmTb1K2pjHZHG0jINv9lErC049g/ey7CcddDd+Q
Bm7fqArIaov7kk+U7zKhBrTVH3dmPWEHAgMBAAGjgYUwgYIwHQYDVR0OBBYEFLd+
eVD4IqyA84ABBeFupjEV0+bOMEYGA1UdIwQ/MD2AFLd+eVD4IqyA84ABBeFupjEV
0+bOoRqkGDAWMRQwEgYDVQQDDAtSQUtXaXJlbGVzc4IJANYEjCM+cqsxMAwGA1Ud
EwQFMAMBAf8wCwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBCwUAA4IBAQABFT6ZgK7Y
tM5tZEfEKSCMUxfESJ+4pPN2lryZVskXtD6BfjvKkQpj3A+R6MRNloOPvZ4spAvH
5fFvfI97Ts40rQjWpgPLQDEBcgBi6dzzmMSap/iw9wLtgqWFVm+LXPMHQnqBKfs2
HksTlKOhiKZlvtGYfxay6kbMU35LX8WdRxx8JNvRNIDL68lLdreXB7vTKQYAvcKP
o1GuZFqKV2KFxpjxzLg1BeM3U4X5k4xDQDaOHENKJO4pdWBfMLP3AAyC9wq481PO
hgA1R8ZAt+psYxOAB6O3A1SzDJ/df5ciPdsp1Kia0HCB2cGIZ7ZwfzPDNivH8/bT
n7UOb+khvmsD
-----END CERTIFICATE-----
</ca>

# Client certificate PEM
# Copy from server /etc/openvpn/easyrsa/pki/issued/managment.crt
#

<cert>
-----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQVm22YDcNRRzycbFHSEkkFjANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDAtSQUtXaXJlbGVzczAeFw0yMDAyMDUwMjI5MzZaFw0yMzAxMjAw
MjI5MzZaMBcxFTATBgNVBAMMDFJBSzcyNThfNjY2NjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAK53T6vlbm4xVgM5z8fC6ul5WsdT3gfEGEOKu0MWcxq4
YP0jrhXAwJV20EdUXYiFIOdf9woYvv8ANTFYHIBAT+jZrGhbhph7QSzmb1xzc3g/
nGJVJAW7L10EmQ0mSsi64NTv/8Ou7wZQpqd8+FuIjDbMFJMP24GbqswG6nnhJCST
1b1hfAgijK/dagRFJTcYhJcutwJrpUjhdAwVBG/GuXQwyI82WXzpqvVyfPgCb4Ek
9ehHuA1Zsmgp68ChGFM+WrEZ1sETDlxlNAfsON7hihf3xYZ2iZ/6rq5RpUczJm3P
9dxO74I8/dxe9TnNcIvqasxGg3jZW4UvQyATqnb+z5kCAwEAAaOBlzCBlDAJBgNV
```

```
HRMEAjAAMB0GA1UdDgQWBBRQkqjMkMV4u8R0EKDDG08qjxJb4TBGBgNVHSMEPzA9
gBS3fnlQ+CKsgPOAAQXhbqYxFdPmzqEapBgwFjEUMBIGA1UEAwwLUkFLV2lyZWxl
c3OCCQDWBIwjPnK67dATBgNVHSUEDDAKBggrBgEFBQcDAjALBgNVHQ8EBAMCB4Aw
DQYJKoZIhvcNAQELBQADggEBAGDGH6+b1EGkVj//EDyJUBISWWcXC8EwmrT25Tga
WDid21QQatQahriVOFHu0B7DGSJb6kw4Om8Mz+kef1v529VIip56wP4I7aVQdcTg
SoVBCc0ToXxGO+EXPWc0jBwPReofMzYeaZ+hZcSHeFOYAso5aFSMfk5Z7qwYQfaj
ZQ7AdTj2NcxH92bIv7JUzW6Xh8OcTuTzQd4J2dtJr4ObnRkYrqg27dzlV1dz73hJ
JIs7AXUH4wivehV3VGd95am6ejs4Hedhaw23h+pV91LmG4gdb6EPHm0JPCHbaQAb
JzF75JEh0CLOlDFBK419Dgg10n0gqLkSTcp+CzNlCx7k+24=
-----END CERTIFICATE-----
</cert>
# Client key PEM
# Copy from server /etc/openvpn/easyrsa/pki/private/managment.key
#
<key>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCud0+r5W5uMVYD
Oc/HwurpeVrHU94HxBhDirtDFnMauGD9I64VwMCVdtBHVF2IhSDnX/cKGL7/ADUx
WByAQE/o2axoW4aYe0Es5m9cc3N4P5xiVSQFuy9dBJkNJkrIuuDU7//Dru8GUKan
fPhbiIw2zBSTD9uBm6rMBup54SQkk9W9YXwIIoyv3WoERSU3GISXLrcCa6VI4XQM
FQRvxrl0MMiPNll86ar1cnz4Am+BJPXoR7gNWbJoKevAoRhTPlqxGdbBEw5cZTQH
7Dje4YoX98WGdomf+q6uUaVH11Ztz/XcTu+CPP3cXvU5zXCL6iIMRoN42VuFL0Mg
E6p2/s+ZAgMBAAECggEAGGwPNQra2IYDelQfZ+E7LQ+Vy41L6V5j3yCOcie0WSsy
OH1EIztmOgX1xeZjaXbpUjo2xK0OH3gR+iRRaQqXpQrDfaBCSRoH15cyQ4jNwyl0
ZLdyYXMAgE7iddrEYTD3xBcMgIH+Z63mhk+SHI4SwqDyyFtR6OS3lfPp4sHHY28r
FJPXW7a10M+pxjEX+A8m3UM4VJiLy2YeklB7laJkQjHcA/Gh+sh/0NjZwCYyWWAi
irATLDSa3z6N7yr3xAO/J4vEZVaGxyyJRvR4qmr0xE15xyCfQQcWdw1DpGT9uBk/
4z/1Tq2sJUekzYebeENliJY3ADVsVS0JszRRHCYwGQKBgQDhRlwvrjvRP8ZCd9th
ssKXgkJBUSqxp8VvFtylMKy2koNq6S2S3yiGmiNWd7JxdGk+77MGmA8kTdpORMcN
L9xSLMWiuMLHGEYf79TkON0ZBqN/wwuPttJG8ICWhqAjL+dDcLoqz8j4dO6FwKPo
z+fVjVupXgYKfqLpm9SAD1apewKBgQDGQuyhzv0Ru7o29MDg5YZ0dwj9bV1KzlFf
3DAdcX+k4Z48R50e5VhewIedA3eafy+UER63CAWLQru96sbRoGkk8aKBk9AGJPFb
i4NVWWaiUA2A2WVUKkdIQsNrr2xHBTwiFPftTxWRWUT1DKgF+uHvSzBKfn13PReS
KCjxzPis+wKBgQDVeW9yX5GfwOeHpTznYBa2rGFMtDXZFDssAmYkw/NnL4AJl93w
CDjHFNnX3qXijYYOdecYoI/4vy3YbaSTAn+t/29pu9wX/xC0wvjjLF+Yj4nwUExs
a7roLpAsFHc74PEuH2zLlQvFJknBxcONozb2T3ZFESx4VXjcFydQEzj0cQKBgANq
Wbs73p40lrOlqcD2E0fkWRJMlQPZ5Ar7txR6xREpFdnB/hHvL4OKW4u36JKPyFkL
pnTOvZG1l5hg+AXadpU9WGhVDItejY3fLGcHAD6hlGn41McLZ2j2RXmQbxQWIgAQ
TmkXKK71U7vI+QgJV2UQ7YcLAMxSEBrjeDkaJ9qLAoGAEiSjuv5X0PbZpiyH6/GX
YuMhFYWZnk/IwoxQW4alBIRuI7EQ+fLvrFUxikMOIsLKtKrcVLjJBgFSz4hIE9YE
YnaQ5Vx+RMzTwakRJtPook55pS1HpdK7Y/0oiUOsJGCEzVj8P/e/WrhFqWPGalIJ
ENCGBuhos/YdITFeKQ381zk=
-----END PRIVATE KEY-----
</key>
```

Save the file with the name *management_client.ovpn*

4.3 OpenVPN PC client

Download the OpenVPN Client from here and install it.

Start the OpenVPN GUI Client. You will see an icon in the taskbar.

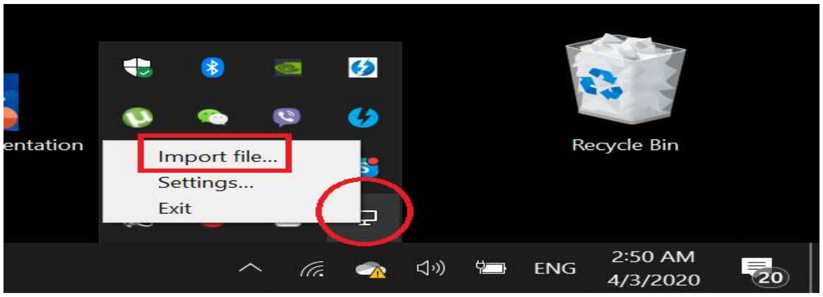
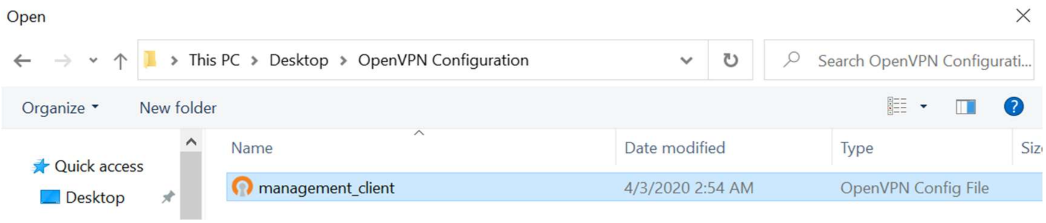


Figure 5 | Open VPN Taskbar Icon

Right click → Import file. Navigate to the *management_client.ovpn* file and open it.


Open
This PC > Desktop > OpenVPN Configuration
Search OpenVPN Configurati...
Organize
New folder
Quick access
Desktop

Name	Date modified	Type	Siz
management_client	4/3/2020 2:54 AM	OpenVPN Config File	

Figure 6 | Importing OpenVPN client file

Make sure to go into the OpenVPN menu again and press Connect (it will not initiate automatically).

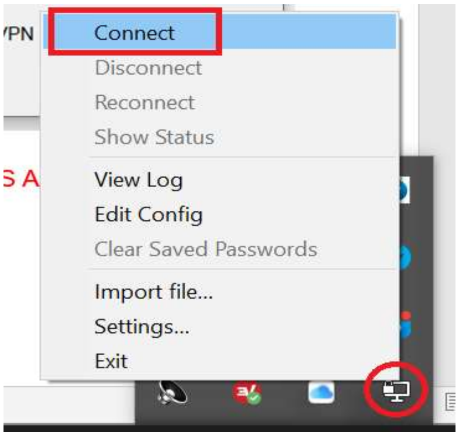
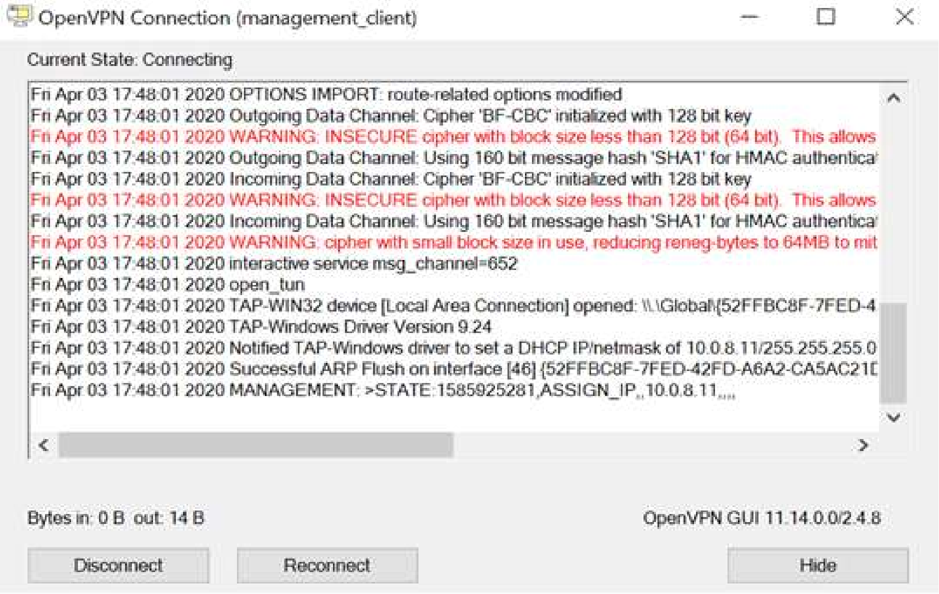


Figure 7 | Open VPN Connection initiation

If everything is set up properly there will be a connection log window that will disappear after the procedure runs through (refer to Figure 8).



Current State: Connecting

```
Fri Apr 03 17:48:01 2020 OPTIONS IMPORT: route-related options modified
Fri Apr 03 17:48:01 2020 Outgoing Data Channel: Cipher 'BF-CBC' initialized with 128 bit key
Fri Apr 03 17:48:01 2020 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This allows
Fri Apr 03 17:48:01 2020 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentica
Fri Apr 03 17:48:01 2020 Incoming Data Channel: Cipher 'BF-CBC' initialized with 128 bit key
Fri Apr 03 17:48:01 2020 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This allows
Fri Apr 03 17:48:01 2020 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentica
Fri Apr 03 17:48:01 2020 WARNING: cipher with small block size in use, reducing reneg-bytes to 64MB to mit
Fri Apr 03 17:48:01 2020 interactive service msg_channel=652
Fri Apr 03 17:48:01 2020 open_tun
Fri Apr 03 17:48:01 2020 TAP-WIN32 device [Local Area Connection] opened: \\.\Global\{52FFBC8F-7FED-4
Fri Apr 03 17:48:01 2020 TAP-Windows Driver Version 9.24
Fri Apr 03 17:48:01 2020 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.0.8.11/255.255.255.0
Fri Apr 03 17:48:01 2020 Successful ARP Flush on interface [46] {52FFBC8F-7FED-42FD-A6A2-CA5AC21D
Fri Apr 03 17:48:01 2020 MANAGEMENT: >STATE:1585925281,ASSIGN_IP,,10.0.8.11,,,,
```

Bytes in: 0 B out: 14 B

OpenVPN GUI 11.14.0.0/2.4.8

Figure 8 | Open VPN Connection log

The OpenVPN should now be in green (Figure 9), meaning the connection has been successful.

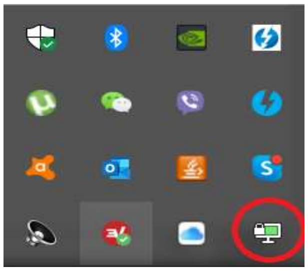
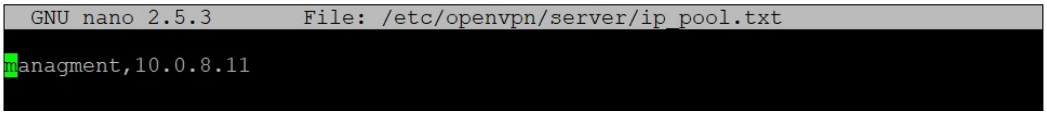


Figure 9 | Open VPN Connection log

You can check which clients are currently connected to the OpenVPN Server and their corresponding IP addresses by executing the following command in your Ubuntu console:

```
sudo nano /etc/openvpn/server/ip_pool.txt
```



```
  GNU nano 2.5.3         File: /etc/openvpn/server/ip_pool.txt

managment,10.0.8.11
```

Figure 10 | Open VPN connected clients 1

There should be only one client and its IP address visible now. This is the PC connected to the OpenVPN Server. Later the Gateway also should be visible.

5 Setup OpenVPN client on LoRa gateway

The procedure for generating the Keys for the Gateway is the same as the one for the Management PC, with the exception of there being a different Client name.

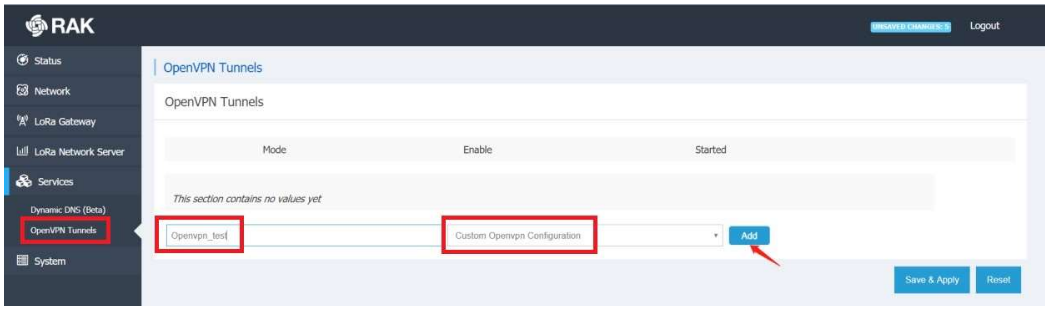
You can go through **Section 4.1** and **Section 4.2** again, and do the same procedure, not forgetting to replace the "management" name we used for the Client with the one for the Gateway. We have used "***rak7258-001***".

Once you have assembled your certificates into a single file you need to import the contents into the OpenVPN client section of your Gateway.

5.1 Log into the Gateway via the Web UI (locally)

Make sure you still have local network access to your Gateway and connect to it in order to access the Web UI.

Go to the **Services → OpenVPN Tunnels** in the sidebar menu section. Enter a name and choose "Custom Openvpn Configuration" from the drop-down menu. Finalize by pressing the "Add" button. Use Figure 11 as reference.



OpenVPN Tunnels

OpenVPN Tunnels

Mode	Enable	Started

This section contains no values yet

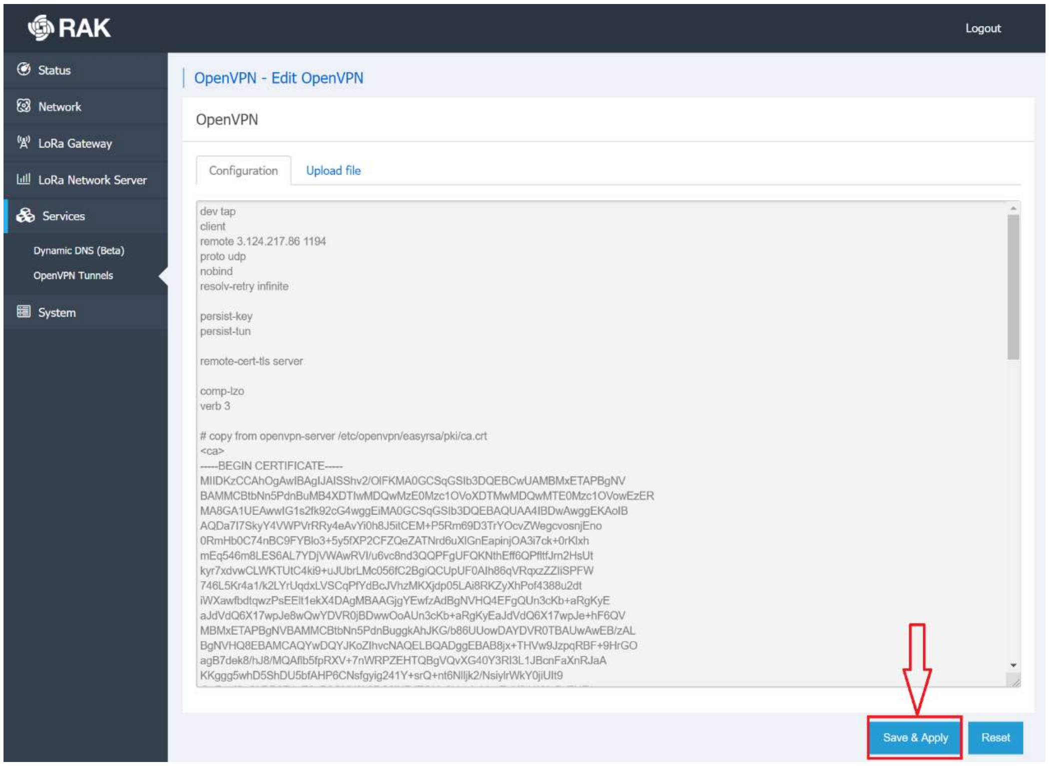
Openvpn_test

Custom Openvpn Configuration

Figure 11 | Creating an OpenVPN tunnel

In the next window simply copy/paste the content of the file you created in the beginning of **Section 5**, "Save & Apply" (Figure 12).

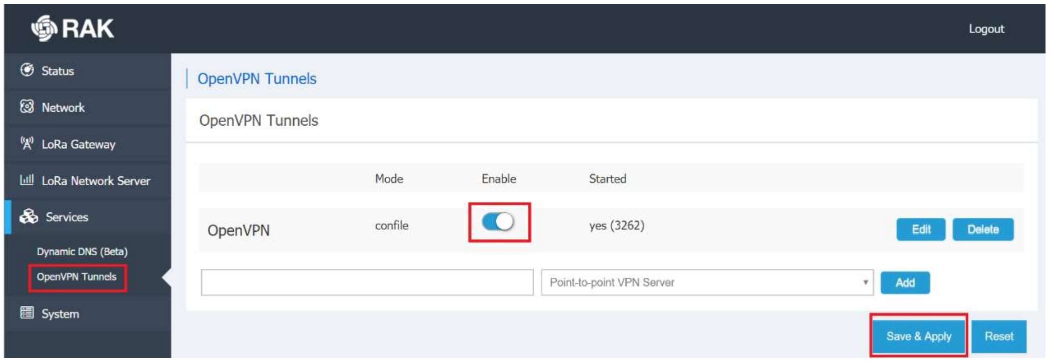
Finally, as shown in Figure 13, go back to the OpenVPN Tunnels section, flip the "Enable" switch into the on state and "Save & Apply". This will finalize things and the Gateway should now be connected to the OpenVPN Server. The process might take a few minutes to complete.



OpenVPN

```
dev tap
client
remote 3.124.217.86 1194
proto udp
nobind
resolv-retry infinite

persist-key
persist-tun

remote-cert-tls server

comp-lzo
verb 3

# copy from openvpn-server /etc/openvpn/easyrsa/pki/ca.crt
<ca>
-----BEGIN CERTIFICATE-----
MIIDKzCCAhOgAwIBAgIJAISShv2/OIFKMA0GCSqGSIb3DQEBCwUAMBMxETAPBgNV
BAMMCBtbNn5PdnBuMB4XDTIwMDQwMzE0Mzc1OVoXDTMwMDQwMTE0Mzc1OVowEzER
MA8GA1UEAwwIG1s2fk92cG4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDa7I7SkyY4VWPVrRRy4eAvYi0h8J5itCEM+P5Rm69D3TrYOcvZWegcvosnjEno
0RmHb0C74nBC9FYBlo3+5y5fXP2CFZQeZATNrd6uXIGnEapinjOA3i7ck+0rKlxh
mEq546m8LES6AL7YDjVWAwRVI/u6vc8nd3QQPFgUFQKNthEff6QPfltfJm2HsUt
kyr7xdvwCLWKTUtC4ki9+uJUbrLMc056fC2BgiQCUpUF0AIh86qVRqxzZZIiSPFW
746L5Kr4a1/k2LYrUqdxLVSCqPfYdBcJVhzMKXjdp05LAi8RKZyXhPof4388u2dt
iWXawfbdtqwzPsEEIt1ekX4DAgMBAAGjgYEwfzAdBgNVHQ4EFgQUn3cKb+aRgKyE
aJdVdQ6X17wpJe8wQwYDVR0jBDwwOoAUn3cKb+aRgKyEaJdVdQ6X17wpJe+hF6QV
MBMxETAPBgNVBAMMCBtbNn5PdnBuggkAhJKG/b86UUowDAYDVR0TBAUwAwEB/zAL
BgNVHQ8EBAMCAQYwDQYJKoZIhvcNAQELBQADggEBAB8jx+THVw9JzpqRBF+9HrGO
agB7dek8/hJ8/MQAflb5fpRXV+7nWRPZEHTQBgVQvXG40Y3RI3L1JBcnFaXnRJaA
KKggg5whD5ShDU5bfAHP6CNsfgyig241Y+srQ+nt6NIljk2/NsiylrWkY0jiUIt9
```

Figure 12 | Importing the OpenVPN certificate data



OpenVPN Tunnels

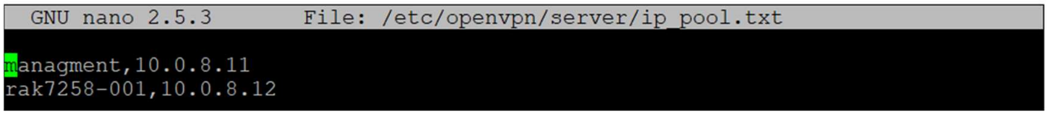
	Mode	Enable	Started
OpenVPN	confile	●	yes (3262)

Point-to-point VPN Server

Figure 13 | Enabling OpenVPN

Check again in the client list file on the OpenVPN Server for the IP address of the Gateway:

```
sudo nano /etc/openvpn/server/ip_pool.txt
```



```
  GNU nano 2.5.3          File: /etc/openvpn/server/ip_pool.txt

managment,10.0.8.11
rak7258-001,10.0.8.12
```

Figure 14 | Open VPN connected clients 2

The IP address of the Gateway should be in the second entry.

5.2 Log into the Gateway (remotely)

You can now log into the Gateway by using the IP address (Figure 14) assigned to it by the OpenVPN Server. This can be utilized for an SSH2 connection, the Web UI (via a browser), etc.

This concludes the tutorial.