

APPLICATION NOTE

APNUS015 OpenVPN tunnel

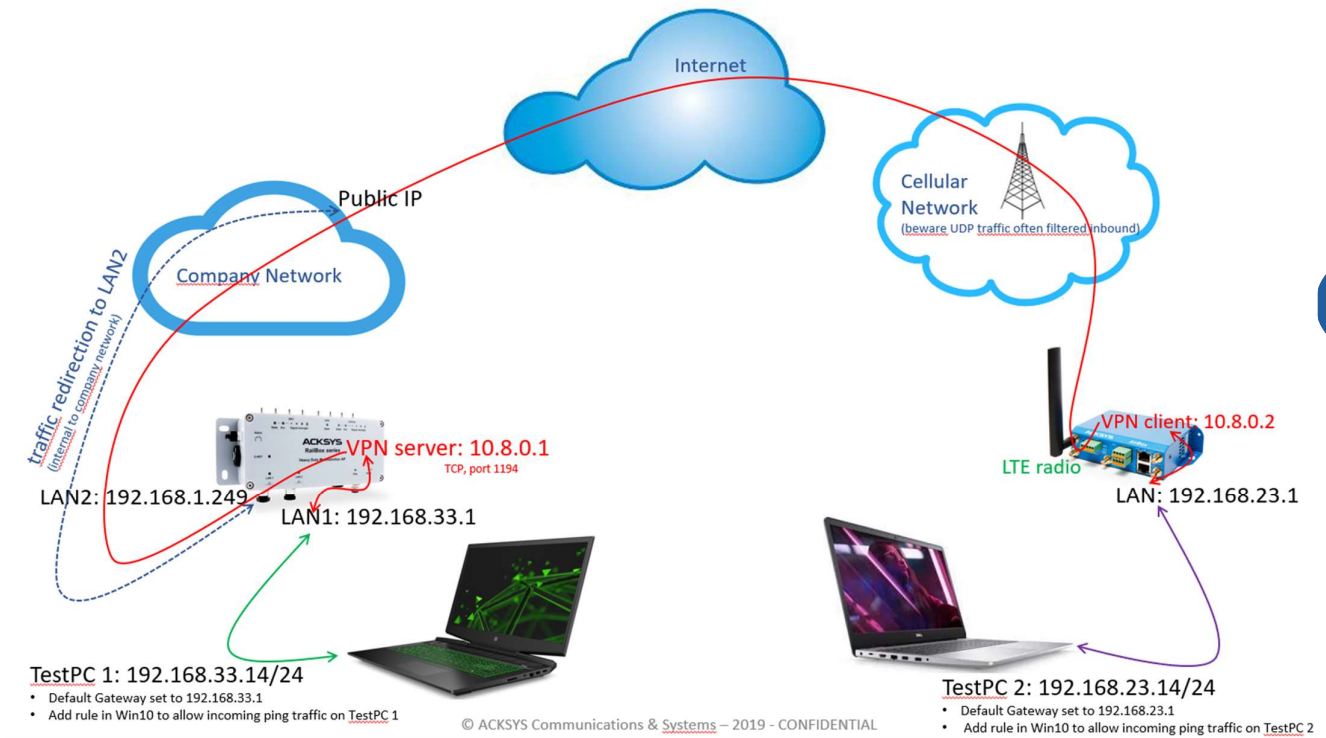
January 2020

Content

- I. Architecture diagram3
- II. Read before start4
- III. VPN Server configuration5
 - A. Set LAN1 interface5
 - B. Set LAN2 interface5
 - C. Set VPN6
 - D. Set network zones.....7
 - 1. LAN zone7
 - 2. VPN zone7
 - 3. WAN zone.....8
- IV. VPN client configuration.....9
 - A. Set LAN1 interface9
 - B. Set LTE interface9
 - C. Set VPN interface10
 - D. Set network zones.....11
 - 1. LAN zone11
 - 2. VPN zone11
- V. Test PC's configuration12
 - A. Test PC1 configuration.....12
 - B. Test PC2 configuration.....12
 - C. Debug tips.....12
 - 1. verify the routing tables in the device.....12
 - 2. verify proper IP configuration12
 - 3. wait after boot for tunnel to mount12



I. Architecture diagram



This scenario exhibits a connection from a cellular VPN client, in the field, to a VPN server at a company backbone.

For example's sake we do run both server and client on Acksys devices.

An internal traffic redirection rule forwards incoming VPN traffic from the company public IP address to the VPN server IP in the backbone.

For the sake of clarity and easier troubleshooting it is advised to first build a tunnel without certificate/key. Once the tunnel is up and one can ping from one test pc to the other test pc, authentication and encryption must be added.

II. Read before start

1)

Cellular network operators filter incoming UDP traffic in general and ports (udp or tcp) in general.

This means that vpn client might well be able to send openVPN traffic but VPN server might not receive it (in case one deploys the server over cellular too, running it on a LTE/5G device).

Or in case server is in a wired infrastructure, it might well answer incoming VPN traffic but answers are filtered when entering the cellular network and not forwarded back to the VPN client.

In this case either negotiate with your carrier to have necessary protocols and ports open for your SIM plan, or more easily, tweak the protocols and ports used to bypass the carrier filters (use TCP instead of UDP and/or use other port than 1194).

This is the reason why, in following examples, TCP protocol is used instead of UDP.

4

2)

On Windows10 ping answer is disabled by default.

Any incoming ping request is dropped by Windows firewall.

One must add a rule to allow incoming ping traffic on the test PC's. See appropriate section below.

<https://docs.microsoft.com/fr-fr/windows/security/threat-protection/windows-firewall/create-an-inbound-icmp-rule>

3)

Upon creation, VPN instance (client or server) is not explicitly attached to an interface.

When in server mode, it will listen to all available interfaces.

When in client mode, it will mount on the interface from which the VPN server IP address can be reached. On a cellular device, this will typically be the cellular interface.

4)

In case using the cellular device as VPN server :

the SIM card must be able to get a public IP address from the carrier.

Do contact your carrier representative to get such service activated on your SIM.

Standard SIM plans do not provide public IP, only private IP.

With reason. Having a public IP on your device makes it visible and open to any malware and attack from the internet.

In case you need to set the VPN server on the cellular device, you MUST :

- set and define a strong and unique password on the Acksys device (to access the MMI)

- if possible block all incoming traffic on the WAN interface and only allow known traffic

- purchase a private APN at your carrier.

This is to protect you against device being hacked and used for malware purpose, for example generating or receiving loads of traffic in the frame of DoS attacks or flood attacks that will result in bill shock and high data consumption costs charged by the network provider.

III. VPN Server configuration

A. Set LAN1 interface

Go to Setup>Network>Add Network :

COMMON CONFIGURATION

General Setup | **Interfaces Settings** | Advanced Settings

Enable interface

Network description: LAN

Protocol: static

IPv4-Address: 192.168.33.1

IPv4-Netmask: 255.255.255.0

Default IPv4 gateway:

Default gateway metric: 0

DNS server(s):

Description : LAN,
IPv4 address : 192.168.33.1,
netmask : 255.255.255.0,
Save.

Assign this network to Ethernet port 1.

By default all device interfaces (ethernet ports and WiFi interfaces) are bridged to a common lan. In this scenario we do not need WiFi and we want to isolate the 2 ethernet interfaces on 2 distinct LAN. Go to Interface Settings tab.

COMMON CONFIGURATION

General Setup | **Interfaces Settings** | Advanced Settings

Bridge interfaces creates a bridge over specified interface(s)

Interface: Ethernet adapter: LAN1 (network: LAN)

MTU: 1500

Bridge Interfaces : unchecked,
Interfaces : assign only the ethernet port 1 (for some reasons called « LAN1 ») to the LAN network.
Save.

B. Set LAN2 interface

Go to Setup>Network>Add Network :

COMMON CONFIGURATION

General Setup | **Interfaces Settings** | Advanced Settings

Enable interface

Network description: WAN

Protocol: static

IPv4-Address: 192.168.1.249

IPv4-Netmask: 255.255.255.0

Default IPv4 gateway: 192.168.1.2

Default gateway metric: 0

DNS server(s):

Description : WAN (it is called WAN as this LAN interface will provide a WAN access over the company internal network),
IPv4 address : any relevant IP matching your own setup,
netmask : 255.255.255.0,
Default Gateway : any relevant IP matching your own setup,

Save.

Note if you plan a field-only scenario (where both Acksys devices, client and server are in the field using cellular connection as WAN access) you can skip this step and do not need to create a second LAN network.

Assign this network to Ethernet port 2 :

Go to Interface Settings tab and verify ticked interface is Ethernet adapter LAN2 (WAN).

Save.



C. Set VPN

Go to Setup>VPN>Add Instance :

State at startup : Up,

Description : vpn1,

Role : Server,

Protocol : TCP. Remember carriers do filter UDP inbound (traffic from the internet to the Airbox LTE),

Listener port : 1194,

Local IP address : 10.8.0.1.

Add route for VPN server to be able to find remote subnet on testPC 2 (beyond VPN client) :

TARGET NET	NETMASK	GATEWAY	METRIC	SORT
192.168.23.0	255.255.255.0	10.8.0.2	Default: 0	

Set authentication and cryptographic parameters. As explained above it is advised to set them in a second step only after the tunnel can mount and remote test pc's can see each other.

Save.

D. Set network zones

A zone is a network or a group of networks which will obey user defined firewall policies. We will add 3 zones, one for LAN1 (aka LAN), one for LAN2 (aka WAN), one for the VPN.

1. LAN zone

Go to Setup>Routing / Firewall>Network Zones>Add zone :

ZONE section :

Name : LAN_zone,

Enable NAT : disable (untick) parameter,

Covered network : select (tick) LAN,

INTER ZONE FORWARDING section :

Select « VPN » zone (you might want to create this zone prior to selecting it),

Save.

2. VPN zone

Browse back to Network Zones>Add zone and add a 2nd zone :

ZONE section :

Name : VPN_zone,

Enable NAT : disable (untick) parameter,

Covered network : select (tick) VPN1,

INTER ZONE FORWARDING section :

Select « LAN » zone,

Save.

ZONE "VPN_ZONE"

This section defines common properties of "VPN_zone".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: VPN_zone

Enable NAT: Only on public zones. Warning: If using VRRP, the NATed network must be set to protocol NONE

MSS clamping:

Default acceptance policy for local services: All enabled
You can restrict or open the local services in the firewall section below

Covered networks: LAN, WAN, vpn1

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (VPN_zone) and other zones. Destination zones cover forwarded traffic originating from "VPN_zone". The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forwarding to destination zones: LAN_zone LAN, WAN_zone WAN

3. WAN zone

Browse back to Network Zones>Add zone and add a 3rd zone :

ZONE section :

Name : WAN zone,

Enable NAT : enable (tick) parameter,

Covered network : select (tick) WAN,

Save and apply.

ZONE "WAN_ZONE"

This section defines common properties of "WAN_zone".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: WAN_zone

Enable NAT: Only on public zones. Warning: If using VRRP, the NATed network must be set to protocol NONE

MSS clamping:

Default acceptance policy for local services: All disabled
You can restrict or open the local services in the firewall section below

Covered networks: LAN, WAN, vpn1

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (WAN_zone) and other zones. Destination zones cover forwarded traffic originating from "WAN_zone". The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forwarding to destination zones: LAN_zone LAN, VPN_zone vpn1

At this point you can loose access to the IHM and, in order to get it back, you might want to set your test laptop ip to 192.168.33.14 as explained below in testpc 1 setup.

Note for a field only scenario (server running on a cellular device too) you do not need to create a WAN zone.

IV. VPN client configuration

A. Set LAN1 interface

Go to Setup>Network>Add Network :

COMMON CONFIGURATION

General Setup | Interfaces Settings | Advanced Settings

Enable interface

Network description: Local network

Protocol: static

IPv4-Address: 192.168.23.1

IPv4-Netmask: 255.255.255.0

Default IPv4 gateway:

Default gateway metric: 0

DNS server(s):

Description : Local network,
IPv4 address : 192.168.23.1,
netmask : 255.255.255.0,
Save.

(There is no need to specify the default gateway).

B. Set LTE interface

Go to Setup>Physical Interfaces and enable LTE interface :



Then Edit the network :



Choose the SIM tray (1 or 2). Verify the SIM card is in this tray.

Go to either SIM1 or SIM2 tab :

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

SIM card 1 PIN code: ●●●●

SIM card 1 access point (APN): sl2sfr

Authentication protocol: SIM only

Populate SIM PIN and SIM APN.
Save.

C. Set VPN interface

Go to Setup>VPN>Add Instance :

The screenshot shows the 'CONFIGURATION' tab for adding a new VPN instance. The 'Tunnel settings' sub-tab is active. Key configurations include:

- Enable virtual network:** Checked.
- State at startup:** Set to 'Up'.
- OpenVPN instance description:** 'vpn1'.
- Role:** 'Client (calling)'.
- Protocol:** 'TCP'.
- Listener port:** '1198'.
- Data channel compression:** 'Use fast LZO compression' is selected.
- Tunnel type:** 'L3 (IP) tunnel'.
- VPN subnet local IP address:** '10.8.0.2'.
- VPN subnet mask:** '255.255.255.0'.
- Keepalive period:** '10'.
- Keepalive timeout:** '30'.



State at startup : Up,

Description : vpn1,

Role : client,

Protocol : TCP. Remember carriers do filter UDP inbound (traffic from the internet to the Airbox LTE),

Listener port : 1198.

Note here different port than the actual one the server has been set to listen to. This is due to the redirection rule on the backbone side that listens on this particular port on the public IP and will redirect internally to 192.168.1.249:1194. You might want to set in this parameter any relevant port matching your own setup.

Local IP address : 10.8.0.2.

Set authentication and cryptographic parameters. As explained above it is advised to set them in a second step only after the tunnel can mount and remote test pc's can see each other.

The screenshot shows the 'Auth/Crypto' sub-tab. Key configurations include:

- Key type:** 'No key (entails P2P, cleartext, no auth)'.
- Data channel authentication digest:** 'SHA1 (OpenVPN default)'.

In client Settings tab set remote OpenVPN server address :

The screenshot shows the 'Client settings' sub-tab. The 'Remote OpenVPN server address' field is highlighted with a black box, indicating where the server IP should be entered.

Do populate the relevant IP where the VPN server can be reached. In our case the public IP on the company network.

Add route for VPN client to be able to find remote subnet on testPC 1 (beyond VPN server) :

The screenshot shows the 'LOCAL ROUTES' configuration. It includes a table for defining routes:

TARGET NET	NETMASK	GATEWAY	METRIC	SORT
192.168.33.0	255.255.255.0	10.8.0.1	Default: 0	

An 'Add' button is located below the table.

Save.

D. Set network zones

A zone is a network or a group of networks which will obey user defined firewall policies. We will add 2 zones, one for LAN1 (aka LAN), one for the VPN.

1. LAN zone

Go to Setup>Routing / Firewall>Network Zones>Add zone :

ZONE section :

Name : LAN,

Enable NAT : disable (untick) parameter,

Covered network : select (tick) Local Network,

INTER ZONE FORWARDING section :

Select « VPN » zone (you might want to create this zone prior to selecting it),

Save.

2. VPN zone

Browse back to Network Zones and add a 2nd zone :

ZONE section :

Name : VPN_zone,

Enable NAT : disable (untick) parameter,

Covered network : select (tick) VPN1,

INTER ZONE FORWARDING section :

Select « Local network » zone,

Save and apply.

At this point you can loose access to the IHM and, in order to get it back, you might want to set your test laptop ip to 192.168.23.14 as explained below in testpc 2 setup.

V. Test PC's configuration

A. Test PC1 configuration

- Open the network adapter settings and set static IP 192.168.33.14/24 and default Gateway 192.168.33.1
- Allow incoming ping traffic on pc:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-icmp-rule>

[\(french version\)](#)

B. Test PC2 configuration

- Open the network adapter settings and set static IP 192.168.23.14/24 and default Gateway 192.168.23.1
- Allow incoming ping traffic on pc:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-icmp-rule>

[\(french version\)](#)

C. Debug tips

1. verify the routing tables in the device

Routing table are available under STATUS>NETWORK>ROUTES.

Example here on the routing table from the server side :

ROUTES

The following rules are currently active on this system.

ACTIVE IPV4-ROUTES				
NETWORK	TARGET	IPV4-NETMASK	IPV4-GATEWAY	METRIC
WAN	default	0.0.0.0	192.168.1.2	0
vpn1	10.8.0.0	255.255.255.0	local	0
WAN	192.168.1.0	255.255.255.0	local	0
vpn1	192.168.23.0	255.255.255.0	10.8.0.2	0
LAN	192.168.33.0	255.255.255.0	local	0

Do send a screenshot of this table on both client and server side in case you need to contact support.
In case you run the server side on a linux machine (non Acksys) do send the result of route -n command.

2. verify proper IP configuration

in following order :

- Check the public IP address is reachable from the client side

Ping from the Acksys client to the VPN server public IP address. If not working, especially in the case of the VPN server being a cellular device, verify the IP address is well public and possibly come back to your cellular network provider.

- Check both client and server can ping each other

Trigger a ping from 10.8.0.1 to 10.8.0.2 and reverse-wise.

- Check both LAN interfaces can ping each other

Trigger a ping from client to eg 192.168.33.1 and from server to eg 192.168.23.1

- Check both test pc's can ping each other

Trigger a ping from Test PC1 to test PC2 and reverse-wise.

3. wait after boot for tunnel to mount

Tunnel will require a certain time to establish between client and server. Typically a couple of minutes.