

APPLICATION NOTE

APNUS015 OpenVPN tunnel

January 2020

Rev A1 / January 2020

Copyright © 2020 ACKSYS Communications & Systems. All rights reserved.



Content

Ι.	Ar	chitecture diagram
.	Re	ead before start4
.		VPN Server configuration5
A.		Set LAN1 interface
В.		Set LAN2 interface
C.		Set VPN6
D.		Set network zones7
	1.	LAN zone7
	2.	VPN zone7
	3.	WAN zone
IV.		VPN client configuration9
A.		Set LAN1 interface
В.		Set LTE interface9
C.		Set VPN interface
D.		Set network zones11
	1.	LAN zone11
	2.	VPN zone11
V.	Te	est PC's configuration
A.		Test PC1 configuration12
В.		Test PC2 configuration12
C.		Debug tips12
	1.	verify the routing tables in the device12
	2.	verify proper IP configuration12
	3.	wait after boot for tunnel to mount12

2





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.

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 Settinos Advanced Settinos	
Enable interface	
Network description	LAN
	6 Friendly name for your network
Protocol	static
IPv4-Address	192.168.33.1
IPv4-Netmask	255.255.0
Default IPv4 gateway	
Default gateway metric	0
	Ø Gateway priority when several default gateways are configured; lowest is chosen. (Used only when a default gateway is defined on this interface)
DNS server(s)	You can specify multiple DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.



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	(2) creates a bridge over specified interface(s)			
Interface				
МТU	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 :

ieneral Setup Interfaces Settings Advanced Settings		
nable interface		
stwork description	WAN	
	Priendly name for your network	
rotocol	static	
Pv4-Address	192.168.1.249	
2v4-Netmask	255.255.255.0	
efault IPy4 gateway	192.168.1.2	
efault gateway metric	0	
	② Gateway priority when several default gateways are configured. (oversit is chosen. (Used only when a default gateway is defined on this interface)	
NS server(s)	You can specify multiple DNS servers have noss anter to add a new antiv. Servers antered have will nuaride surformationally assigned noss	

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).

I COMMON CONFIGURATION				
General Setup Interfaces Settings Advanced Settings				
Bridge interfaces	(i) creates a bridge over specified interface(s)			
Interface	WFi adapter: WFi (currently disabled) - acksys_nm Z Ethernet adapter: LAN1 (network: LAN) Ethernet adapter: LAN2 (network: WAN)			
МТU	1500			

Save.

C. Set VPN

Go to Setup>VPN>Add Instance :

VP except for networks with protocol 'none'. this networks, should be brought up only by event rules. anne for this VPN instance alled V		
this network should be brought up only by event rules.		
name for this VPN instance alled) PP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms CCP pot that the server will listen to, and that the client will call fait LZD compression and		
name for this VPN Instance Billed) P. as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms CP pot that the server will listen to, and that the client will call fait IZD compression not		
Pr as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms PP as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms CP pot that the server will listen to, and that the client will call fast L2D compression fast L2D compression		
PP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms CCP port that the server will listen to, and that the client will call fait LZD compression and		
PP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms CCP port that the server will listen to, and that the client will call fair LZD compression and		
CP pot that the server will listen to, and that the client will call fast L2D compression and		
CP port that the server will listen to, and that the client will call fast L2O compression not		
fast LZO compression		
nnal		
tunnels are supported		
ss of the local VPN endpoint, not used in TLS dient mode since it is pulled from server		
255.0		
Subnet mask of the VPN subnet, not used in TLS dient mode		
e period (seconds). Every such time, a packet is sent to each peer to elicit a response.		
liv		

State at startup : Up, Description : vpn1, Role : Server, Protocol : TCP. Rememb

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) :

LOCAL ROUTES							
This section is used in both Server and Client modes. It	This section is used in both Server and Client modes. It lists the routes to be installed in the local IP stack.						
In the client, it lists the server subnets reachable using the server as gateway; In the server, it lists the client subnets reachable using the client as gateway; If the gateway is not indicated, it defaults to the VPN remote address.							
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.



Α	С	K٩	5Y	'S
COMM	NUNIC	CATIONS	& SY	STEMS

unnel settings Auth/Crypto Server settings	
ey type	No key (entails P2P, cleartext, no auth)
Data channel authentication digest	SHA1 (OpenVPN default)
	(2) Data channel authentication algorithm. Adds overhead to frames size and processing time.

Save.

CONFIGURATION

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.

EONE ENN_EONE	
This section defines common properties of "LAN_zone". Covered networks specifies which available networks are members of this	zone.
General Settings Advanced Settings	
Name	LAN_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
Covered networks	LAR &
NTER-ZONE FORWARDING	
Use this section only if NAT is disabled on this zone. The options below control the forwarding policies between this zone (LAN_ not imply a permission to forward from wan to lan as well.	zone) and other zones. Destination zones cover forwarded traffic originating from "LAN_zone". The forwarding rule is unidirectional, e.g. a forward from Ian to wan does
Allow forwarding to destination zones:	VPH_zone vph1:22 VAH_zone WAR:

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 Vo can restrict or open the local services in the firewall section below			
Covered networks	LAN 2			
	V vpnt:			
INTER-ZONE FORWARDING				
Use this section only if IAMT 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 Ian to wan does not imply a permission to forward from wan to ian as well.				
Allow forwarding to destination zones:	VAN_zone VAN			



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,

 $\label{eq:covered network:select(tick)} \mathsf{WAN},$

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 Y Of u can restrict or open the local services in the firewall section below			
Covered networks	LANE &			
INTER-ZONE FORWARDING				
Use this section only if NAT is disabled on this zone. The options below control the forwarding pulcies 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 Ian to wan does not imply a permission to forward from want lan as well.				
Allow forwarding to destination zones:	LAH.zone LAN: LAH.zone vent:			

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 :

General Setup Interfaces Settings Advanced Settings Enable interface Interfaces Settings Interfaces Settings Network description Local network Important Setup Interfaces Settings Interfaces Settings Protocol static Interfaces Settings Interfaces Settings IPx4-Address 192-168-23.1 Interfaces Settings Interfaces Settings Default IPx4 gateway Enable interfaces Interfaces Settings Interfaces Settings Default IPx4 gateway metric Interfaces Settings Interfaces Settings Interfaces Settings DBMS server(s) Interfaces Settings Interfaces Settings Interfaces Settings Interfaces Settings DMS server(s) Interfaces Settings Interfaces Settings Interfaces Settings Interfaces Settings	COMMON CONFIGURATION	
Enable interface Image: Color Interface Network description Local network Image: Color Interface Image: Color Interface Protocol static Image: Color Interface Image: Color Interface	General Setup Interfaces Settings Advanced Settings	
Network description Local network I friendly name for your network Protocol Isatic Ibb4-Address 192-168.23.1 Ibb4-States 255.255.00 Default Ibb4 gateway Image:	Enable interface	
Image: Pready name for your network Protocol tablic Itext-Address 192.168.23.1 Itext-Hetmask 255.255.00 Default (Px4 gateway Image: Page of table	Network description	Local network
Protocol static IPx4 Adress 192.168.23.1 IPx4 Hetmask 255.255.0 Default IPx4 gateway Impact of the several default gateway are configured; lowest is chosen. IUbes only when a setault gateway is defined on this interface) DHS server(s) Impact on the several default gateway is defined on this interface) DHS server(s) Impact on the several default gateway is defined on this interface)		(2) Friendly name for your network
IP2-164.ddress 192.166.23.1 IP2-1 Hetmask 255.255.0 Default IP4-d gateway Image: Comparison of the second of t	Protocol	static
IP-4-Hetmask 255.255.0 Default IP-4 gateway Default gateway metric O Odd gateway priority when several default gateways are configured, lowest is chosen. (Used only when a default gateway is defined on this interface) DHS server(s) Image: Constraint of the cons	IPv4-Address	192.168.23.1
Default []	IPv4-Netmask	255.255.255.0
Default gateway metric Image: Comparison of the several default gateways are configured. Iowest is chosen. (Used only when a seleault gateway is defined on this interface) DMS server(s) Image: Comparison of the several default gateway is defined on this interface) Image: Comparison of the several default gateway is defined on this interface) Image: Comparison of the several default gateway is defined on this interface) Image: Comparison of the several default gateway is defined on this interface) Image: Comparison of the several default gateway is defined on this interface)	Default IPv4 gateway	
Gateway priority when several default gateways are configured; lowest is chosen. (Used only when a default gateways is defined on this interface) DNS server(s) One of the several default gateway is defined on this interface) One of the several default gateway is defined on this interface) One of the several default gateway is defined on this interface) One of the several default gateway is defined on this interface)	Default gateway metric	0
DNS server(s)		Gateway priority when several default gateways are configured; lowest is chosen. (Used only when a default gateway is defined on this interface)
	<u>DNS</u> server(s)	(i) (ii) (iii) (iiii) (iiiii) (iiiiii) (iiiiii) (iiiiiii) (iiiiiii) (iiiiiii) (iiiiiiii) (iiiiiiii) (iiiiiiii) (iiiiiiiii) (iiiiiiiiii



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	<i>»</i> ••••	A&•
	Benter the correct SLOT 1 PIN code or you might lock your sim card!	
SIM card 1 access point (APN)	sl2sfr	
	Required except for LTE-only connections	
Authentication protocol	SIM only	

Populate SIM PIN and SIM APN. Save.



C. Set VPN interface

Go to Setup>VPN>Add Instance :

Tunnel settings Auth/Crypto Client settings	
nable virtual network	M
State at startup	
	Up (a) Default is turi except for networks with contact linear
	Use 'down' if this network should be brought up only by event rules.
DenVPN instance description	
	vpn1
	(i) Friendly name for this VPN instance
ole	Client (calling)
Protocol	TCP
	(g) Favor UDP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms
istener port	1198
	1100
	(2) UDP or TCP port that the server will listen to, and that the client will call
ata channel compression	Ø Use fast LZO compression
Tunnel type L3 (IP) tunnel	
	Only L3 tunnels are supported
/PN subnet local IP address	10.8.0.2
	IP address of the local VPN endpoint, not used in TLS client mode since it is pulled from server
/PN subnet mask	255 255 0
	Ø Subnet mask of the VPN subnet, not used in TLS client mode
Ceepalive period	10
	[**
	(2) Keepalive period (seconds). Every such time, a packet is sent to each peer to elicit a response.
Ceepalive timeout	30
	Keepalive timeout (seconds). Connection terminates if no traffic is received from the peer for such time.
	2 Mart - Mart



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.

		(
Tunnel settings Auth/Crypto Server settings		
Key type	No key (entails P2P, cleartext, no auth)	
Data channel authentication digest	SHA1 (OpenVPN default)	
	(g) Data channel authentication algorithm. Adds overhead to frames size and processing time.	

In client Settings tab set remote OpenVPN server address :

CONFIGURATION		
Tunnel settings Auth/Crypto Client settings		
Remote OpenVPN server address	Remote OpenVPN server address	

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) :

LOCAL ROUTES					
This section is used in both Server and Client modes. It lis	sts the routes to be installed in the local IP stack.				
In the client, it lists the server subnets reachable using the server as gateway, In the server, it lists the client subnets reachable using the client as gateway. If the gateway is not indicated, it defaults to the VPN remote address.					
TARGET NET	NETMASK	GATEWAY	METRIC	SORT	
192.168.33.0	255.255.255.0	10.8.0.1	Default: 0	* *	×

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.

ZONE "LAN"				
This section defines of Covered networks sp	common properties of "LA ecifies which available ne	AN". etworks are members of this zone.		
General Settings	Advanced Settings			
Name		LAN		
Enable NAT		🗌 🍘 Only	y on public zones. Warning: if using VRRP, the NATed network must be set to protocol NONE	
MSS clamping				
Default acceptance p	olicy for local services	All enabled	id v	
Covered networks			resarce of open are rocal services in the mewan section below	
COVERCE INCLINION			Local network: 🔬 🔬 🎡	
			vpn1: •••	
			Cellular:	
INTER-ZONE FORWARDING				
Use this section only if NAT is disabled on this zone. The options below control the forwarding policies between this zone (LAN) and other zones. Destination zones cover forwarded traffic originating from "LAN". The forwarding rule is unidirectional, e.g. a forward from Ian to wan does not imply a permission to forward from who to lar as well.				
Allow forwarding to	destination zones:	VPN_zc	zone vpn1: 🖳	

2. VPN zone

Browse back to Network Zones and add a $2^{\rm nd}$ 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.

ZONE "VPN_ZONE"	
This section defines common properties of "VPN_zone". Covered networks specifies which available networks are members of th	ils 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 V Vou can restrict or open the local services in the firewall section below
Covered networks	Local network 🖉 🖉 🚱
INTER-ZONE FORWARDING	
Use this section only if NAT is disabled on this zone. The options below control the forwarding policies between this zone (VPh not imply a permission to forward from wan to lan as well.	N_zone) and other zones. Destination zones cover forwarded traffic originating from "VPN_zone". The forwarding rule is unidirectional, e.g. a forward from ian to wan does
Allow forwarding to destination zones:	🗹 LAN Local network: 🔬 🧟 👷

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-icmprule

(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-icmprule

(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 IP	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.