



USER MANUAL

VPN Box HW

VPN BOX Virtual Machine SW

VIRTUAL PRIVATE NETWORK SERVER

SENECA s.r.l.



Via Austria, 26 - 35127 - PADOVA - ITALY

Tel. +39.049.8705355 - 8705359 Fax. +39.049.8706287

Web site: www.seneca.it

Technical assistance: support@seneca.it (IT), support@seneca.it (Other)

Commercial reference: <u>commerciale@seneca.it</u> (IT), <u>sales@seneca.it</u> (Other)

This document is the property of SENECA srl. Duplication and reproduction are forbidden, if not authorized. The contents of the present documentation refer to products and technologies described in it. All technical data contained in the document may be modified without prior notice The content of this documentation is subject to periodical revision.

To use the product safely and effectively, read the following instructions carefully before use. The product must be used only for the use for which it was designed and built. Any other use will be the user's responsibility. The installation, implementation and set-up are allowed only for authorized operators; these must be physically and intellectually suitable people. Set-up must be performed only after a correct installation and the user must perform every operation described in the installation manual carefully. Seneca will not be liable for any failure, breakdown or accident caused by ignorance or failure to apply the stated requirements. Seneca will not be liable for any unauthorized changes. Seneca reserves the right to modify the device, for any commercial or construction requirements, without the obligation to promptly update the reference manuals.

No liability for the contents of this document can be accepted. Use the concepts, examples and other content at your own risk. There may be errors and inaccuracies in this document, that may of course be damaging to your system. Proceed with caution, and although this is highly unlikely, the author(s) do not take any responsibility for that. Technical features subject to change without notice.

MI004180_102

Page 1

Date	Revision	Notes
24/11/2015	01	First revision.
12/04/2017	102	Added VM Ware Virtual Machine Appliance

Contents

1.	SOFTWARE OPEN SOURCE	6
2.	INTRODUCTION	6
2.1.	Hardware Specifications	6
2.2.	Virtual Machine Specifications	7
3.	VPN BOX INSTALLATION	7
3.1.	VPN Box Hardware	7
3.2.	Virtual VPN Box	8
4.	DEFAULT NETWORK CONFIGURATION	9
5.	FIRST CONFIGURATION WITH VPN BOX MANAGER	10
5.1.	General Parameters	11
5.2.	Network Setup	12
5.3.	Credentials	13
5.4.	Configuration Application	14
5.5.	Monitoring the Operation	14
5.	.5.1. Configure	15
5.	.5.2. Backup	15
5.	.5.3. Restore	15
5.	.5.4. System Log	16
6.	FACTORY RESET AND FIRMWARE UPDATE	16
6.1.	VPN Box Hardware	16
6.2.	Virtual VPN Box	23
7.	SINGLE LAN	23
7.1.	Router Configuration	24
7.2.	VPN Configuration	24
7.	.2.1. SENECA Device Configuration	24
7.	.2.2. VPN Accesses	

8.	POI		27
8.1.	Ro	outer Configuration	28
8.2.	VP	PN Configuration	29
8.	2.1.	SENECA Device Configuration	29
8.	2.1.	Group Configuration	
8.	2.2.	VPN Access Configuration	
8.3.	VP	PN Client Communicator	31
9.	CO	NNECTION TO THE VPN NETWORK WITH VPN CLIENT CON	MMUNICATOR32
9.1.	VP	PN Client Connection	32
9.2.	VP	PN Client Communicator in Service Mode	33
10.	CO	NNECTION VIA ANDROID CLIENT (MOBILE AND/OR TABLE	ET)34
11.	GLC	OSSARY	36

Seneca VPN-BOX

ATTENTION!

UNDER NO CIRCUMSTANCES, WILL SENECA S.R.L. OR ITS SUPPLIERS BE RESPONSIBLE FOR ANY LOSS OF RECORDING DATA/INCOME OR FOR CONSEQUENTIAL OR INCIDENTAL DAMAGE DUE TO NEGLIGENCE OR RECKLESS MISHANDLING OF THE VPN-BOX, EVEN THOUGH SENECA IS WELL AWARE OF THESE POSSIBLE DAMAGES.

SENECA, ITS SUBSIDIARIES, AFFILIATES, COMPANIES OF THE GROUP, SUPPLIERS AND RETAILERS WILL NOT GUARANTEE THAT THE FUNCTIONS COMPLETELY SATISFY CUSTOMERS' EXPECTATIONS OR THAT THE VPN-BOX, THE FIRMWARE AND THE SOFTWARE HAS NO ERRORS OR WORKS CONTINUOUSLY.

1. Software Open Source

The VPN Box software and firmware contain Open Source software under GPL license. In compliance with section 3b of GPL, we provide the sources of this software. It is possible to get them from SENECA s.r.l. asking for them via email to support@seneca.it.

2. Introduction

VPN Box is a server device that allows centralizing the management and connection of the SENECA devices enabled to use a VPN.

In a company's (suitably configured) LAN network, the field remote equipment can connect among themselves or to a PC (via Ethernet or 3G modem) and communicate using TCP/IP protocols. With this device it is possible to organize a VPN Single Lan (or Remote Control) or Point to Point (or Remote Service) network.

The Single LAN method solves the cases where it is necessary to create a connection allowing the communication between devices installed in different sites and far from each other, so as to form one network that can include, if so wished, also the device sub-networks; these cases are typical in SCADA and Remote control environments.

The Point to Point method allows a maintenance technician to reach a single device and, optionally, its subnetwork to work on it; the typical use is field remote Service of machines and reprogramming of a PLC/HMI, verification of some functions and problem solving.

The VPN Box is a server device that needs to be configured by a software provided with: VPN Box Manager;

To create the VPN tunnel between a remote PC and the network/device the VPN Client Communicator software is provided.

Type of device	Industrial server
Motherboard Form Factor	Mini-ITX
Cooling	Passive (fanless)
Front I/O	2 x USB 2.0
Back I/O	2 high current USB 2.0
	2 USB 2.0
	1 VGA
	1 HDMI
	1 Gb LAN
	1 Jack DC (8 V to 19 V)
Processor	Intel Atom N2800
Processor speed	1.86 GHz

2.1. Hardware Specifications

6

Socket	Onboard (BGA)
Number of cores	2
Chipset	Intel NM10
Type of memory	DDR3 SO-DIMM (non-ECC)
Amount of memory	2 GB 1066MHz
LAN Controller	Intel 82579L GbE
Supply voltage	8~19 V
Supply connector	Jack DC Onboard
Operating temperature	0°C ~ 40°C
Dimensions (WxHxD)	185.14 x 32 x 205 mm
Certifications	CE, FCC, RoHS
Storage	32 GB SSD Drive

2.2. Virtual Machine Specifications

The virtual machine is supplied in OVF (see VM installation chapter) and has no specific hardware characteristics. It needs to work on an ATOM processor of at least 64 bit and 1Gb of RAM; the operating system is Debian and therefore the host must be compatible with this LINUX distribution.

3. VPN Box Installation

3.1. VPN Box Hardware





Socket

To install VPN Box, proceed as follows:

Position the server horizontally on a flat surface, or use the appropriate brackets that make it possible to fit it against the wall (included in the supply).

Connect the power supply (to the round plug on the back) and the network cable. The device needs no keyboard or mouse to operate, but these are required in case of recovery or firmware update; they can therefore be left disconnected.

Start the device with the front button: nothing else is required.

ATTENTION: this being a server, it needs to be correctly switched on and off, that is the power must not be disconnected when the server is ON. To avoid power surges and/or blackouts, we recommend a UPS is used.

The device is switched off with the front button that must be pressed only once, briefly; the prolonged pressure of this button switches the unit off immediately giving the operating system no time to close the various processes.

3.2. Virtual VPN Box

In this case, it is necessary to install the packet provided as virtual machine, consisting of an ".ovf" file saved in OVF 1.0.

This file can be imported to a virtual host such as VMWare. To start installation, double-click on the packet this will start the installation that will take up to several minutes. You will then follow a wizard and the first screen is as shown in the figure below.

Import Virtual Machine		
Store the new Virtual Machine Provide a name and local storage path for the new virtual machine.		
Name for the new virtual machine:		
VPN Box Release.1.1.3.		
Storage path for the new virtual machine:		
C:\Users\USERNAME\Documents\Virtual Machine Browse		
Help Import Cancel		

Once the disk have been created, start the device. On first start-up, once the Login screen is displayed, the system will create the encryption keys; this operation might take some time, wait till completed (The VM restarts and the login screen representing only a maintenance terminal is displayed again: nothing else is therefore required).



The VMWare host will detect a Guest Managed machine, VMWare tools are already installed (the package is the Debian 8.x one). Compatibility is set as follow:

ESXi: 6.0, 5.5, 5.1, 5.0 - Fusion: 8.x, 7.x, 6.x, 5.x, 4.x - Workstation: 12.0, 11.x, 10.x, 9.x, 8.x

WARNING! This virtual machine is a 64 bit virtual machine this means that the host must be compatible with Intel-VT or AMD-V technology that has to be enabled on the PC bios: this feature is implemented by the CPU.

4. Default Network Configuration

The VPN Box's default configuration is the network configuration obtained via DHCP, therefore, once connected to the network it will try and acquire an IP address, gateway and DNS via the DHCP server.

If this operation is not successful, the following network parameters are set: IP address 192.168.90.101 and subnet-mask 255.255.255.0. From a functional point of view, the VPN Box must be configured since on first start-up no mode is available to be used; if a device tries to connect to the VPN Box, it will be ignored. For the VPN Box to communicate with the outside, when behind a router, the NAT must be configured on it; for any configuration details, see the section about the server's individual operating method (Remote Service or Remote Control).

5. First Configuration with VPN BOX Manager

To configure the VPN, the VPN Box Manager software will be used, available for Windows 7 or higher.

This software is also available on the www.seneca.it website, in the VPN BOX section.

The PC you will carry out the *first configuration* from and on which the VPN Box Manager is installed, **must** be in the same LAN as the VPN Box.

Therefore, the VPN Box Manager software allows editing/modifying:

- Operating modes and Configuration
- Device management
- VPN Client accesses

When the software starts, an access login is displayed; the first thing to do is to find out the IP address of the VPN Box for the connection.

To find it, you can use the discovery system in the software that can be accessed from the login panel via the appropriate button shown in the figure:

Server Address		٩
User Name	Passwor	rd
LANG: EN	Connect	Cancel

ATTENTION! If this button is disabled, it means another process is using the UDP 49161 port. You must identify what application is using this port and close it down.

When the discovery system is started, the network is scanned to identify the VPN Box devices, their IP addresses and versions.

			VPN BOX I	Discover		
Local network Sca	n, VPN BOX found	Ŀ				
IP	Ping	Operating Mode	MAC	Name	Version	
15:15:0:10	0 ms	STATIC		VPN Box	1.0	Seleziona
						Close

By pressing Select the login screen will display the IP address found and selected.

ATTENTION: if the network configuration of the PC you connect from is not compatible with the VPN Box, you must add a compatible IP address from Windows network management.

When you connect for the first time, the device has default credentials (all in small letters):

USERNAME: supervisor

PASSWORD: seneca

More generally, these credentials are the same in case of a factory reset or firmware update. As soon as you log in, the device will display the configuration panel with all the parameters.

5.1. General Parameters

The section has a Name field that allows assigning a label to the VPN Box; this option is useful since the defined name will always be displayed on the VPN Box Manager and VPN Center Client softwares. The following option defines the operating mode, that is

Point to Point (also called Remote Service) or Single Lan (called Remote Control as well).

ATTENTION: the mode can be modified only during the first configuration, after that it will be possible to modify it only with a factory reset.

VPN BC	DX Setup
General Network Credentials	
VPN BOX Operating mode Operating mode Point to Point Image: Access to the SENECA device local network	
MAC 08:00:27:4E:C6:B9, version 1.0.0.10	OK Cancel

Once the mode has been selected, it is possible to check/uncheck the "Access to local network" that allows specifying if other peripherals connected to the Seneca device via Ethernet must be visible remotely to the other devices (in Single Lan Mode) or PC Clients (in both Single Lan and Point to Point modes).

5.2. Network Setup

The following window shows the classical network settings of an Ethernet-based device that can be static or dynamic through the aid of the DCHP.

VPN BC	OX Setup
General Network Credentials	
Network Setup	
IP	Netmask
192.168.90.101	255.255.255.0
Server DNS 8.8.8.8	Gateway 192.168.90.1
MAC 08:00:27:4E:C6:B9, version 1.0.0.10	OK Cancel

ATTENTION! On first installation it is *highly recommended* to provide VPN BOX with a static IP address

5.3. Credentials

In the last screen the default password for both the supervisor account and for all the Seneca devices can be modified.

The password of the devices is necessary for the VPN configuration (i.e. Z-TWS4/Z-PASS1/2) of the devices to be registered on the VPN Box to create a network, it must coincide with the one set up on the devices.

The supervisor's default password is "seneca".

The default password of the devices is "seneca".

Take care so that the user name for the supervisor account remains always the same, that is "supervisor".

VPN BC	DX Setup
General Network Credentials VPN BOX SUPERVISOR Password	(Confirm)
•••••	
SENECA Devices Password	(Confirm)
MAC 08:00:27:4E:C6:B9, version 1.0.0.10	OK Cancel

5.4. Configuration Application

When OK is pressed, the program will configure all the parameters, to do this it must restart the VPN BOX, so wait for a few minutes before reconnecting. Once the modifications are applied, the software will log out automatically.

5.5. Monitoring the Operation

This section is common to all operating modes and allows managing the device and its configuration. The central section, that can be updated with the "Refresh" button at the top, is a status panel showing the version, VPN Box model, selected operating mode; it is important to have the machine MAC address available so as to identify the devices. Immediately underneath there is the network configuration, showing what has been previously defined.

	<table-cell> Refresh 🌣 Setup 🖬 Backup 🖾 Restore 📲 Logs</table-cell>
Server	
Version 1.0.0.10 - M	odel B - Operating Mode Single Lan - Mac Address 00:22:4D:B6:08:8F
Network	
IP 192.168.1.230/2	55.255.255.0, Gateway 192.168.1.1, DNS 8.8.8.8
Statistics	
Statistic	Value
CPU Load	0.0
RAM	In use 142 MB, Total 1993 MB
bandwidth in use	Input 0 kB/s, Output 0 kB/s
Temperature	Core 0: 40.00, Core 1: 38.00 (MAX 100 °C)

The grid contains the status data reflecting the operation at that very moment and these are updated every minute by the machine. The first one is the CPU load, that is what the system is processing: it is a number starting from zero, that is no processing taking place, and reaching 1 or more. Between 0 and 1 the machine is within its operational limit, higher numbers mean unsuitable work loads that the machine might, sooner or later, no longer be able to process and that might cause a block; we recommend the load is kept below 0.8.

Then the following is displayed: the status of the whole memory and of the memory used by both the operating system and the services. The band shows how much the network card is working while the temperature displays the values detected by the CPU and chipset sensors.

5.5.1. Configure

This section reopens the VPN Box configuration that can be totally modified but for the mode and visibility of the device local network.

5.5.2. Backup

This function creates an image of the VPN Box configuration that can be registered as a local file, for future use. We recommend you often back up the whole configuration so as not to lose any data.

5.5.3. Restore

Restoring the Configuration data takes place by selecting the file previously created by the backup. Restoring carries out a complete rollback that needs however time to be received by the devices registered on the VPN Box. A complete reset, covering also the devices, requires a few minutes (according to the connection speed). This to allow each device to reload all the credentials.

5.5.4. System Log

The logging window is useful to check the status of the services in case of errors. It is divided into system (SYSLOG) and application logs. The first one shows the status of the VPN services while the second one filters only the application part of the VPN Box. Both are useful only to check any errors or malfunctions. Please remember that VPN Box keeps these logs only for the current day and then deletes them.

6. Factory Reset and Firmware Update

6.1. VPN Box Hardware

The factory reset and firmware update are carried out the same way, that is by resetting a factory image. In both cases, do a configuration backup first to be used for the reset. To perform these operations, the following material is required:

- USB keyboard and Monitor with HDMI socket (ATTENTION!! The monitor must support HD 1920 x 1080 resolutions and 72Hz refresh frequencies at least)
- 1 x 2Gb (at least) USB stick for the UPDATE software
- 1 x 2Gb (at least) USB stick for the firmware

We recommend you connect to VPN Box Manager first and carry out a backup, since the procedure will clear the whole disk, configuration data included. The software required for the update is Clonezilla and can be downloaded from http://clonezilla.org/downloads.php, paying attention to download the Debian version in ISO 64bit format. To prepare the first USB stick with the Clonezilla reset program, download the program used to create the stick http://sourceforge.net/projects/usbwriter/. Now insert the USB stick, the previously downloaded USBWriter program opens, select the ISO image and the unit the stick is connected to.

		USBWrite	r		
Source file	vclopezilla-live-2 (1 2-32-amd64 is			Browse
			-		2
Target device					Defrech
G: [7.6 GB]				*	Refresh
Progress					

ATTENTION! All the data on the stick will be deleted.

When writing is complete, close the program, disconnect the Clonezilla stick and insert the second stick. The firmware must be saved on this stick and it can be obtained from the Seneca site or server. The firmware packet must be unpacked in root, where there must be just one folder containing a series of files as per the following figure: ATTENTION! The folder must not be renamed and there must be no spaces in its name, it must be of the VPNBOX-1.0.0.6 type. Once the second stick is disconnected you are ready to reset.

11 💽 11 = I			VPNBOX-1.0.0.6		
File Home Condividi Visualizza					
Copia Incolla Incolla incolla collegamento	Sposta Copia in * in *	Nuova elemento ▼ Nuova cartella	Proprietà	Seleziona tutto Deseleziona tutto Inverti selezione	
Appunti	Organizza Nuovo Apri Selezi			Seleziona	
(→ + ↑) G:\VPNBOX-1.0	0.6				
🔶 Preferiti	Nome	Ultima modifica	Tipo Di	imensione	
E Desktop	blkdev.list	03/11/2015 10:09	File LIST	1 KB	
🐌 Download	blkid.list	03/11/2015 10:09	File LIST	1 KB	
📃 Risorse recenti	clonezilla-img	03/11/2015 10:12	File	5 KB	
	dev-fs.list		File LIST	1 KB	
Oreative Cloud Files	📄 disk	03/11/2015 10:11	File	1 KB	
💱 Dropbox	𝗭 efi-n∨ram.dat	03/11/2015 10:11	dat files	1 KB	
le SkyDrive	📔 Info-dmi.txt	03/11/2015 10:11	File TXT	9 KB	
	📔 Info-Ishw.txt	03/11/2015 10:11	File TXT	15 KB	
쥺 OneDrive	📔 Info-Ispci.txt	03/11/2015 10:11	File TXT	2 KB	
	📔 Info-packages.txt	03/11/2015 10:11	File TXT	1 KB	
💐 Gruppo home	📔 Info-saved-by-cmd.txt	03/11/2015 10:12	File TXT	1 KB	
	parts 📄	03/11/2015 10:11	File	1 KB	
🕎 Questo PC	sda1.ext4-ptcl-img.gz.aa	03/11/2015 10:11	File AA	657.433 KB	
📜 Desktop	sda-chs.sf 03/11/2015 10:09 File SF		1 KB		
Documenti	sda-hidden-data-after-mbr	03/11/2015 10:09	File	1.024 KB	
🗼 Download	sda-mbr	03/11/2015 10:09	File	1 KB	
╞ Immagini	sda-pt.parted	03/11/2015 10:09	File PARTED	1 KB	
🔰 Musica	sda-pt.parted.compact	03/11/2015 10:09	File COMPACT	1 KB	
Jideo	sda-pt.sf	03/11/2015 10:09	File SF	1 KB	
Windows8_OS (C:)	📄 swappt-sda5.info	03/11/2015 10:11	File INFO	1 KB	

Connect the VPN Box to a monitor and to a keyboard and insert the first stick with the Clonezilla reset program into the front left port. Start the VPN Box and wait for the stick to boot, a selection screen shall be displayed, select "Clonezilla live (default settings, VGA 800x600)".



Press Enter and wait for the operating system to boot, this might take a few minutes according to the speed of the stick used. A selection screen for the keyboard layout will be displayed first.

Free Software Labs	Choose language Which language do you prefer: ca_ES.UTF-8 Catalan Català de_DE.UTF-8 German Deutsch en_US.UTF-8 English hu_HU.UTF-8 Hungarian Magyar es_ES.UTF-8 Spanish Español fr_FR.UTF-8 French Français it_IT.UTF-8 Italian Italiano ja_JP.UTF-8 Brazilian Portuguese Português do Brasil ru_RU.UTF-8 Brazilian Portuguese Português do Brasil ru_RU.UTF-8 Slovak Slovenský tr_TR.UTF-8 Turkish Türkçe zh_CN.UTF-8 Chinese (Simplified) 简体中文	
	<ok></ok>	

Select "en_US.UTF-8 English", press Enter and continue with the English configuration; the system will continue asking for the keyboard to be remapped, press Enter again and continue.

Configuring console-data The keymap records the layout of symbols on the keyboard. - 'Select keymap from arch list': select one of the predefined keymaps specific for your architecture (recommended for non-USB keyboards); - 'Don't touch keymap': don't overwrite the keymap in /etc/console, which is maintained manually with install-keymap(8); - 'Keep kernel keymap': prevent any keymap from being loaded next time the system boots; - 'Select keyman from full list': list all the predefined keymans
Configuring console-data The keymap records the layout of symbols on the keyboard. - 'Select keymap from arch list': select one of the predefined keymaps specific for your architecture (recommended for non-USB keyboards); - 'Don't touch keymap': don't overwrite the keymap in /etc/console, which is maintained manually with install-keymap(0); - 'Keep kernel keymap': prevent any keymap from being loaded next time the system boots; - 'Select keyman from full list': list all the predefined keymans
Configuring console-data The keymap records the layout of symbols on the keyboard. - 'Select keymap from arch list': select one of the predefined keymaps specific for your architecture (recommended for non-USB keyboards); - 'Don't touch keymap': don't overwrite the keymap in /etc/console, which is maintained manually with install-keymap(8); - 'Keep kernel keymap': prevent any keymap from being loaded next time the system boots; - 'Select keyman from full list': list all the predefined keymans
 'Select keymap from arch list': select one of the predefined keymaps specific for your architecture (recommended for non-USB keyboards); 'Don't touch keymap': don't overwrite the keymap in /etc/console, which is maintained manually with install-keymap(8); 'Keep kernel keymap': prevent any keymap from being loaded next time the system boots; 'Select keymap from full list': list all the predefined keymaps
Recommended when using cross-architecture (often USB) keyboards.
Policy for handling keymaps:
Select keymap from arch list D <mark>on't touch keymap</mark> Keep kernel keymap Select keymap from full list
<ok> (Dancel></ok>

The system is now ready and will ask if you want to start with the wizard program or enter shell, select the first option as in the figure.

NCHC Free Software I	Labs, Taiwan	
	Start Clonezilla Start Clonezilla or enter login shell (command line)? Select mode: Start_Clonezilla Start Clonezilla Enter shell Enter command line promot	
	<dk> <cancel></cancel></dk>	
	ă.	

The reset is based on image, so proceed with the selection of the first item as per the following figure.

N	CHC Free Software Labs, Taiwan
ſ	Clonezilia – Opensource Clone System (OCS)
I	*Clonezilla is free (GPL) software, and comes with ABSOLUTELY NO WARRANTY*
I	///Hint! From now on, if multiple choices are available, you have to press space key to mark
I	your selection. An asterisk (*) will be shown when the selection is done///
I	(1) closed are dvariable, god can
I	(2) disk to disk or partition to partition clone/restore.
I	Select mode:
I	device image work with disks on partitions using images
I	device-device work with disks of partitions dank in the addition
I	
I	
I	<dk> <cancel></cancel></dk>
l	
Γ	
Ι.	
E.	

The operation carried out is a reset from local device, that is from USB peripheral, for this reason you have to select "local_dev" in the screen shown below. After pressing Enter (bottom yellow), the system will ask you to enter the peripheral you want to use for the reset. Insert the stick with the firmware into the second front right USB port, wait 5 seconds and press Enter. The connected devices will be assessed, wait for the procedure to complete.



When scanning is completed, a window appears where you are asked to select the device containing the firmware. The situation should be as follows: SDA1 is the fixed disk of the VPN Box, SDB1 is the Clonezilla update program and SDC1 is the firmware. Choose the last one to carry out the reset.

NCHC Free Software Lab:	, Taiwan			
Now we need to mount read or save the imay //NOTE/// You shoul The partition name is "hda1" or "sda1", th in the second disk is C: is hda1 (for PATA) sda5) sda1 28.66_e sdb1 1.3G(In, sdc1 7.76_vfa	Clonezilla - Opensou a device as /home/par je in /home/partimag. NOT mount the partit is the device name in G 2 And partition in the i "hdbl" or "sdbl" or sdal (for PATA, S thdt:_orsdal(for PATA, S xt4(In_VBOX_HARDDISK_) VBOX_HARDDISK_) VBOX at Ox41: Dirty (In_VB	Ince Clone System (timag (Clonezilla Storn you want to ba SNU/Linux. The firs: e first disk is "hdu If the system you SATA or SCSI), and I U-VBOX_HARDDISK_VB73 HARDDISK_VB755b7a2 KHARDDISK_VB75b7a2	OCS) Mode: image(s) repository) so that we can ckup as /home/partimag t partition in the first disk is a2" or "sda2", the first partition want to save is MS windows, normally D: could be hda2 (or sda2), hda5 (or 55b7a22–91ebb941 HARDDISK_VB4191b9ee—dfa347fc	
	<ok></ok>		<cancel></cancel>	

A window will then appear, as per the following picture, asking what folder must be used; since everything is in root, select "Top directory_in_the_local_device". Once selected, press Enter and its contents will be shown, continue by pressing Enter again.

NUMU Free Suffware Labs, Taiwan	
Clonezilla - Opensour	ce Clone System (OCS)
Which directory is for the Clonezilla image (onl the Clonezilla image (i.e. directory) itself wil	y the first level of directories are shown, and l be excluded. If there is a space in the
directory name, it will _NOT_ be shown)?:	
/ Top_directory_i	n_the_local_device
<0k>	<cancel></cancel>
	t
	Ţ
	Ţ

You are then asked for the level of detail of the options that, in this case, must be left as "Beginner": press Enter and continue.

NCHC	Free	Software	Labs,	Taiwan	
		Choose	the n	Clonezilla – Opensource Clone System (OCS)	
				Beginner Beginner mode: Accept the default options	
				Expert Expert mode: Choose your own options	
				(Ok) (Cancel)	
				Non-Neurice 17	

Having to reset the firmware, proceed selecting "restoredisk" followed by the unit to reset.

Clonezilla is This software backup importa ///Hint! From your selection	Clonezilla – (clonezilla – (s free (GPL) software will overwrite the (ant files before rest now on, if multiple n. An asterisk () w.	Opensource Clone System (OCS): Select mode , and comes with ABSOLUTELY NO WARRANTY* Jata on your hard drive when restoring! It is recommended to toring!*** choices are available, you have to press space key to mark ill be shown when the selection is done///
	savedisk saveparts restoredisk restoreparts 1-2-mdisks recovery-iso-zip chk-img-restorable cvt-img-compression encrypt-img decrypt-img exit	Save_local_disk_as_an_image Save_local_partitions_as_an_image Restore_an_image_to_local_disk Restore_an_image_to_local_partitions Restore_an_image_to_multiple_local_disks Create_recovery_Clonezilla_live Check_the_image_restorable_or_not Convert_image_compression_format_as_another_image Encrypt_an_existing_unencrypted_image Decrypt_an_existing_encrypted_image Exit. Enter command line prompt
	<0k>	\> <cancel></cancel>

The system is now ready to be reset and will ask what unit to carry it out on: the disks compatible with the restore will be displayed, as shown in the figure below; only one compatible disk should be displayed, the 32Gb system disk that is the main VPN Box disk, an SSD that should take the name SDA.

NCHC Free Software Labs, Taiwan	
	na Quatan (000) Nada, pastanadisk
Choose the target disk(s) to be overwritten	(ALL DATA ON THE ENTIRE DISK WILL BE LOST AND
REPLACED!!) The disk name is the device name in GNU/Linu	v The first disk in the sustem is "hda" or "sda"
the 2nd disk is "hdb" or "sdb" Press space	e key to mark your selection. An asterisk (*) will
be shown when the selection is done	
sda 36.5GB_VBOX_HARDDISK_	_VBOX_HARDDISK_V8755b7a22-91ebb941
sda 36.5GB_VBOX_HARDDISK_	_VBOX_HARDDISK_VB755b7a22-91ebb941
sda 36.5GB_VBOX_HARDDISK <ok></ok>	_vB0X_HARDDISK_vB755b7a22-91ebb941 <cancel></cancel>
<mark>sda 36.5GB_VBOX_HARDDISK</mark> _ <ok></ok>	_vB0X_HARDDISK_vB755b7a22-91ebb941 <cancel></cancel>
<mark>sda 36.5GB_VBOX_HARDDISK_</mark> <ok></ok>	_vB0X_HARDDISK_vB755b7a22-91ebb941 <cancel></cancel>
<mark>sda 36.5GB_VBOX_HARDDISK_</mark> <ok></ok>	_vB0X_HARDDISK_vB755b7a22-91ebb941 <cance1></cance1>
<mark>sda 36.568_VBOX_HARDDISK.</mark> <ok></ok>	_VBOX_HARDDISK_VB755b7a22-91ebb941 <cance1></cance1>
sda 36.5GB_VBOX_HARDDISK_ <ok></ok>	_VBOX_HARDDISK_VB755b7a22-91ebb941 <cancel></cancel>
sda 36.5GB_VBOX_HARDDISK_ <ok></ok>	_VBOX_HARDDISK_VB755b7a22-91ebb941 <cance1></cance1>
sda 36.5GB_VBOX_HARDDISK_ <ok></ok>	_VBOX_HARDDISK_VB755b7a22-91ebb941 <cancel></cancel>

Once the disk has been selected, the procedure will start and further confirmation to proceed will be requested (by pressing y or Enter), this because this operation involves the complete loss of the previous data. At the end you will be asked how you want to proceed, select "poweroff" and then take the USB sticks out. Restart the VPN Box and wait for the machine to reboot that, once the operating system has been reloaded, will create the encryption keys: this is a long operation, so leave the VPN Box switched on until it

restarts automatically. *ATTENTION!* The machine must not be switched off and restarted during this configuration operation.

6.2. Virtual VPN Box

In the first place, back up the current VPN Box configuration. The new appliance must then be reset in the destination host machine (importing the file in OVF) and a Restore must be performed with the file created with the previous backup. Note: the reset is the same as the first installation of the Virtual VPN BOX, therefore, on first start-up, the system will calculate the encryption keys: **it must not be switched off or restarted manually**, it will restart automatically when the operation is complete. For the complete procedure, see the chapter about the first installation of the virtual machine.

7. Single Lan

This mode allows creating a VPN network interconnecting two or more devices with a PC, SCADA or Mobiles.

ATTENTION: this mode configures a virtual LAN network requiring the allocation of different local IPs on all Seneca devices belonging to the network, since the VPN clients are all connected at the same time and always visible to the rest of the network. This requirement is necessary above all if you want the networks downstream from the ZPASS to be visible.



7.1. Router Configuration

In this mode, VPN Box is a server and needs to expose the following ports on public network to work correctly:

Port	Туре	Compulsory	Description
443	ТСР	Yes	Service channel necessary to communicate with the devices and VPN clients.
1193	ТСР	Optional	For possible Seneca support
1194	ТСР	Yes	VPN data channel

These ports must be open on the router, therefore unfiltered by a possible firewall rule. They must then be re-directed from the router, from the outside towards the inside, modifying the NAT and making them converge towards the local IP address of the VPN BOX: on commercial routers, this option is normally called "Virtual Server" or "Port Mapping".

When the configuration is complete, make a note of the router IP public address, required (with the password) for the VPN configuration of the SENECA devices. Refer to your in-house system administrator about how to acquire this IP address. The modification of the router ports is compulsory **only** if the VPN Box is in a LAN (addresses 192.168.x.x, 10.x.x.x and 172.x.x.x), if it is installed on a public network (therefore with a public IP address visible from the Internet) no router configuration shall be needed.

7.2. VPN Configuration

The configuration of the Remote Control mode (Single Lan) is divided into two operations: Configuration of the *Seneca devices* and Configuration of the *VPN accesses* (Users). The former are clearly the connection points to various field systems and their configuration is dealt with in the specific user manual of every SENECA device compatible with the VPN Box.

On the other hand, VPN Accesses are accounts allowing the maintenance or monitoring PCs (such as a SCADA server) to connect to the network. VPN Box Manager has a dedicated control panel for each type of operation, as shown in the figure.



7.2.1. SENECA Device Configuration

Once configured locally via their Web Server, Seneca devices will register on the VPN Box and the Device section of VPN Box Manager will start to fill up: this operation will take about 2 minutes. This time is important because each device will communicate any changes of status and receive new configurations.

8	VPN Box Ma	nager - 3.0.1.0	- 🗆 ×
NOME VPN BOX Single Lan, User Connected SUPERVISOR			SENECA
Status SENECA DEVICES VPN Access Devices			(2) Refresh
TAG	MAC	IMEI	STATUS
zpass_C8F9	Service (BOF) (B	Rep84401-01885	SERVICE OFF - VPN DOWN
Configuration CONFIGURED, last refree	sh 11/27/2015 6:16:28 PM		🗘 Setup
Connection Network 192.168.90.0/2	55.255.255.0 (VPN 10.9.1.9)		Delete
			.::

The status of the device determines its colour according to the following table, the polling offline status has priority over the machine status setting it to red.

Status	Colour
New	Orange
Configured	Green
Configuration in progress	Yellow
Service OFF	Red

Immediately after registering, the device status is "NEW" and the device itself is waiting to be configured by VPN Box Manager; in this status the device will perform no operation and will not connect to the network. While registering, the device provides various details such as its MAC address, IMEI (if provided with an integrated modem), TAG name and Local network configuration. The TAG name is the name of the installation and can be modified with the *Edit* button at the bottom so as to give it a talking name; please remember that the change of name is just an alias at VPN Box's level, the name shall remain the original one locally on the device.

Another important parameter is the network the Seneca device belongs to that, if local network visibility has been enabled, allows the device to reach the connected devices via Ethernet (for instance HMI or PLC). Exactly like the TAG name, this addressing can be modified with the Edit button, clearly if this is modified, this configuration must be applied also locally on the device.

USER MANUAL – VPN-BOX

EditDevice
Tag
zpass_C8F98
Network
Network 192 v 168 ÷ 90 ÷ .0/255.255.255.0
Apply Cancel

To proceed and make the device work within the VPN network, press the *Edit* button and accept the configuration with the *OK* button; polling time will be required to apply this configuration. The status of the device will pass from "NEW" to "CONFIGURATION IN PROGRESS" until the modification is applied, then it will go to "CONFIGURED" and the device will connect to the network. Devices are considered offline if no polling is carried out for over 3 minutes. The device can also be removed by pressing the *Cancel* button. If the VPN configuration on the device remains unchanged, this will try and register again.

7.2.2. VPN Accesses

Once the devices are connected you can connect to this new network with a PC, but you need to create accesses first. Every access created is a connection to the VPN network, it is therefore necessary to define as many users as the VPN Client PCs required to monitor/maintain the Network.

ATTENTION: each access can be used by just one user at a time.

a	VPN Box Manager - 3.0.1.0		- 🗆 ×
NOME VPN BOX			SENECA
Status SENECA DEVICES VPN Access			
Users		+ New × Delete	♥ Refresh
Usemame	Network	Level	
anna an	VPN 10.9.1.5		EDIT

Users can be added, edited and deleted at will; clearly, if an account is deleted while it is being used, this will effectively be closed only when it disconnects.

ATTENTION: usernames and passwords are case sensitive.

Once this is completed, the account is operational and VPN Client Communicator must be used for the connection, but we will talk about this in the appropriate section.

8. Point To Point

This scenario is typical when you have numerous sites with identical systems and networks. Since it is not possible to create a network with several identical IP addresses, it is necessary to create several networks that must be independent.

The user can choose to which one to connect (one at a time) and carry out the necessary maintenance. This mode is designed for field support scenarios, it is not a connection to use permanently like Single Lan.

Moreover it is possible to group the devices and assign them to the users that must connect: each user will therefore be able to connect only to the devices assigned to it.



The following figure shows an example of how groups are used. There are three users, A, B and C that have 8 ZPASS available and a precise access discipline is required.



By creating a group for each user, A will see ZPASS 1, 2, 3 while B will see all the devices and C will access only 1, 2, 5 and 6.

8.1. Router Configuration

In this mode the devices create a tunnel towards the VPN Box and wait for the connection. For this reason each device is associated to a separate port. In this operating mode the VPN Box is a concentrator that sorts the connections.

Port	Туре	Compulsory	Description
443	ТСР	Yes	Service channel necessary to communicate with the devices and clients.
1193	ТСР	Yes	Necessary to drive the tunnel
1195	TCP	Yes	Necessary for device 1
	ТСР		
1195+N	ТСР	Yes	Necessary for device N

In this configuration the number of ports is fixed but variable according to how many devices you want to have. The system automatically assigns the port starting from 1195; if you have 10 devices, the ports from 1195 to 1204 must be opened on the router.

These ports must be open on the router, therefore unfiltered by a possible firewall rule. Once opened, they must then be re-directed from the router, from the outside towards the inside, modifying the NAT and

making them converge towards the local IP address of the VPN BOX: on commercial routers, this option is normally called "Virtual Server" or "Port Mapping".

When the configuration is complete, make a note of the router IP public address, required (with the password) for the VPN configuration of the SENECA devices.

Refer to your in-house system administrator about how to acquire this IP address. The modification of the router ports is compulsory **only** if the VPN Box is in a LAN (addresses 192.168.x.x, 10.x.x.x and 172.x.x.x), if it is installed on a public network (therefore with a public IP address visible from the Internet) no router configuration shall be needed.

8.2. VPN Configuration

The configuration of the VPN network in Point to Point mode is divided into three parts: *Seneca device* VPN configuration, via Web Server, following which the devices will be able to register with the system to make their network available via tunnel. Configuration of the *Groups* that contain the devices and are used to isolate the VPN Accesses (Users) and make only some devices "visible" to them.

This operation allows therefore creating sets of devices and associate them to one or more VPN Accesses as a kind of access list. A device can be part of one or more groups and the same group can be associated to one or more VPN Accesses; this gives wide scope for configuration. The configuration of the *VPN Accesses* will allow maintenance technicians to access the VPN Client Communicator that, displaying just the list of the associated devices, will connect them to the required one.



8.2.1. SENECA Device Configuration

As previously mentioned, once the devices are configured locally with their web server, they will register with the VPN Box and the Seneca device section will start to fill up: the device will take about two minutes for this operation. This time is important because the device will communicate via polling any changes of status and receive new configurations.

		VPN	Box Manager - 3.0.1.0		
LASCIO VPN int to Point, User	BOX Connected SUPERVISOR				S SENEC
Status SENECA D	Devices Groups VPN Access				
Devices					🖏 Refresh
TAG	MAC		IMEI	STATUS	
ZPASS_2S	C8:F9	0.0509.057	862264	SERVICE ON	
zpass_Q1	C8:F9	E el caso astro	862264	SERVICE OFF	
zpass_lan2	C8:F9	t de caso as caso	862264	SERVICE ON	
zpass_Q2	C8:F9	t descesses	862264	SERVICE OFF	
zpass_lan1	C8:F9	ter cesses and	862264	SERVICE ON	
zpass_giovanni	C8:F9	E Constantine (MODEM NOT INSTALLED	SERVICE OFF	
Configuration		20 2015 0 40 44 44			
Configuration	CONFIGURED, last refresh 11/	30/2015 9:40:44 AM			¢ Setup
Configuration	CONFIGURED, last refresh 11/ Port: 1195 network 192.168.10	30/2015 9:40:44 AM 2.101/255 255 255.0 (VPN	10.9.0.0)	_	¢ Setup

As shown in the figure, waiting for polling, the devices register and are immediately ready to connect. They can assume different colours according to their status as per the table shown below:

Status	Colour
Configured	Emerald green
Configuration in progress	Pea green
Service OFF	Red

If the polling service has timed out, the system will impose the red colour to highlight an anomaly: this can be due to a loss of connection of the Seneca device or lack of synchronism. In this operating mode, the devices are always green and therefore ready to connect. A change in status takes place if a Group or User is added, edited or deleted; in fact these occurrences involve an update of the device configuration. Two operations are therefore possible on the panel: the deletion that involves the elimination of the Seneca device from the VPN Box (ATTENTION: the support must be first disabled from the VPN configuration of the web server of the device) and the change of TAG that is nothing more than the change of name of the device.

ATTENTION: Changing the TAG, this is modified only on the VPN Box, the device will keep its original name.

8.2.1. Group Configuration

This section represents the connection element between users and devices. Each group can contain all or just some devices: let's suppose there are two users (X and Y) and 4 Seneca devices (Z, X, Q, K). If user X has to see everything and Y only Q and K, two groups must be created, one with Z, X, Q and K and another one with just Q and K. Once assigned, users will see only what is applicable to them.

3	VPN Box Manager - 3.0.1.0	- 🗆 🗙
RILASCIO VPN BOX Point to Point, User Connected SUPERVIS	in and a second s	S SENECA
Status SENECA Devices Groups VPN	Access	
Groups	Group test_rd devices	
Group	TAG	IMEI mac
Test01 Ed	zpass_Q1	86226 C8:F9:
Test02 Ed	zpass_lan2	86226 C8:F9:
All Ed	zpass_Q2	86226 C8:F9:
Group03 Ed	zpass_lan1	86226 C8:F9:
+ New		
× Delete		
€2 Refresh		+ Add X Delete

The group interface is divided into two sections, the left one consists of the group lists containing also the *Edit* button and the *New*, *Delete* and *Update* buttons. On the right the content of the selected group is displayed, with the device Add and Delete buttons at the bottom.

8.2.2. VPN Access Configuration

VPN Accesses represent users that will then connect to the individual Seneca devices. They can be created by giving them a name and a password and assigning them to a group. They must be assigned to a group to access the device list; if this is not the case, no device will be seen on connection.

3	VPN Box Manager - 3.0.1.0			- 🗆 ×
RILASCIO VPN BOX (194.184.235.249) Point to Point, User Connected SUPERVISOR				SENECA
Status SENECA Devices Groups VPN Access				
Users		+ New	× Delete	€2 Refresh
Usemame	Network	Level	Group	
			Test02	EDIT
Tandar Barris (Brode)	VPN 10.9.1.13	USER	All	EDIT
1000000000	VPN 10.9.1.5	USER	Test01	EDIT

8.3. VPN Client Communicator

The connection client is used to connect to an individual Seneca device.

ATTENTION! Each device will accept just one connection at a time, if one user is already connected, the second one will be rejected.

•		VPN Clie	nt Communicat	or - 3.1.0.0		- 🗆 ×
RIL Poin	ASCIO VPN BOX t To Point, Logged Use	er MANUTENZIONE	1)		S	SENECA
Available devic	es list				65	Refresh
TAG	MAC	IMEI	CONNECTION	CONFIGURATION		
ZPASS_2S	C8:F9	862264	SERVICE ON	CONFIGURED / P	Connect	Export
zpass_Q1	C8:F9	862264	SERVICE ON	CONFIGURED / P	Connect	Export
zpass_lan2	C8:F9	862264	SERVICE ON	CONFIGURED / P	Connect	Export
zpass_Q2	C8:F9	862264	SERVICE ON	CONFIGURED / P	Connect	Export
zpass_lan1	C8:F9	862264	SERVICE ON	CONFIGURED / P	Connect	Export
VPN Device 2	ZPASS_2S					
Status: Local Addres VPN Address	Connecting ss: 192.168.102.101 s: 10.9.0.0	[AF_INET] Mon Nov 30 09:48:02 2 Mon Nov 30 09:48:02 2 [AF_INET]	015 TCPv4_CLIENT I 015 TCPv4_CLIENT I	link local: [undef] link remote:	^ ○ ₽ ↓	Disconnect Web

Once logged in, the program will display the list of assigned devices. Each one is accompanied by its operating status and port. By pressing Connect, the system will start a session, connect to the ZPASS, projecting you into the destination network and allowing you to see also the devices downstream from the ZPASS (only if you chose this option when you first configured the device). Your configuration can be exported and used with an OpenVPN client such as an Android (for smartphone); see the paragraph on exporting.

9. Connection to the VPN Network with VPN Client Communicator

This software is a VPN connection client and must be installed on the PCs you want to use to access the VPN network. It gives the possibility of three different uses, two of which will be dealt with later on.

9.1. VPN Client Connection

In this mode, access is possible with the previously created credentials, creating a VPN tunnel with the server and making the network and connected devices accessible. On entering you get a panoramic view of the connected Seneca devices and their status. The configured devices that are online are considered as operational, the network they belong to appears on each line.

3		VPN Clier	nt Communicate	or - 3.1.0.0		- 🗆 ×
\$	NOME VPN BOX iingle Lan, Logged User VEI	RONICA			S	SENECA
Available d	evices list				0	Refresh
TAG	MAC	IMEI	CONNECTION	CONFIGURATION		
zpass_C8F	981020 C8:F9:81:02:01:D	6 862264020120993	SERVICE ON	CONFIGURED / N	Export	Web
Single Lar	1 Connection					
Status:	Connecting	Mon Nov 30 09:51:48 2	015 Control Channel:	TLSv1, cipher TLSv1/SS	v3 ^ 🖸	Disconnect
Server A	ddress: 10.9.0.1	DHE-RSA-AES256-SH/ Mon Nov 30 09:51:48 2	A, 1024 bit RSA 2015 [SERVER] Peer (Connection Initiated with		
VPN add	dress: 10.9.1.5					Connect
						.:i

By pressing the *Connect* button you get into the network and communicate with the devices, in the centre the system operations during the connection are logged. On the bottom left-hand side, the configuration data at VPN addresses' level are displayed while on the device panel the addresses of both the device local network and of the VPN are shown. Your configuration can be exported and used with a standard OpenVPN client such as an Android (for smartphone); see the paragraph on exporting.

ATTENTION! If you connect from a PC with IP addresses compatible with those of the VPN network, some IP addresses might not work locally.

9.2. VPN Client Communicator in Service Mode

There are cases when it is necessary for a PC wanting to connect to the VPN network to be able to do so autonomously and automatically, without an operator logging in and starting the connection via VPN Client Communicator; these situations are often connected to SCADAs installed on servers. To activate the automatic mode, log into VPN Client Communicator, click on the gear icon in the top left-hand corner and select "Service" from the menu.

It is necessary to install the configuration onto the machine and to do it, press *Install*. The system will carry out all the operations automatically, moving the service to "run" and starting it straight away. It is possible to load the system log into the bottom box, to check the operations carried out or any connection problems.

	Service	
VPN Service Status		
Start	Stop C Restart	Stopped
Setup		
III Install	With this option the service will start automatically at startup (a	(also without login)
O Uninstall	Stop the automatic service startup	
Connection Log		
		🔍 Refresh Logs
		^
		~

Always from this panel, you can stop and restart the service, cancelling also the configuration.

ATTENTION: if you install the automatic mode, you will not be able to use the account in normal mode.

10. Connection via Android Client (Mobile and/or Tablet)

Exporting the configuration, you can save it in a folder to be used on OpenVPN-compatible systems. An example is the configuration of a mobile for the connection, the client for Android can be found at this address:

https://play.google.com/store/apps/details?id=net.openvpn.openvpn&hl=it

Connect the mobile to the computer in mass-storage mode and copy all the exported files to the device; they must be all in the same folder and must be renamed. Typically it is possible to use the Download folder, create a folder and copy the files into it.

spia percorso	Sports Copis Elimina Disemina	Accesso raciinato ·	Moderica no veseleziona tutto			
colla collegamento	in * in * *	cartella *	北口口口中日	ovpn	- C ×	
nti	Organizza	Nuovo	File Home Condividi Vi	sualizza	^ f	8
▶ export_mobile	Nome	Ultima modifica	Copia Incola collegement	Sposta in - X Elimina -	Proprietà Composicia	
			Annunti	Organizza Nugro	Anti Seleziona	
	zpass_C8F9810201D6.auth	22/10/2015 14:31	00.000			
	Lad zpass_C8P9810201D6.crt	22/10/2015 14:31	🔄 🕘 * T 🌲 > Questo PC >	Nexus 5 Memoria interna Download o	Jvpn v C Cerca in ovpn JP	tutto
	zpass_C8F9810201D6.key	22/10/2015 14:31				>> na tutto
an frank	zpass_C8F9810201D6_ca.crt	22/10/2015 14:31	Download ^ Si Risorse recenti	zpass_C8F9810201D6.auth File AUTH	zpass_C8F9810201D6.crt Certificato di sicurezza	ezione 1a
			Creative Cloud Files Dropbox StyOnive Dropbox StyOnive Construive Construive Coursto PC Destop Destop	Para CHP02010E.key Para CHP02010E.key Para CHP02010E.ca.cft Para CHP0102010E.ca.cft ChP02010E.ca.cft 1,05108	2944 CH791020105Avpn Opent091 Config File 073 byte	
1/52 8 8 - (1.0000-071)			Documenti Documenti Musica Musica Nexus 5 Video Udochand DS (fr) Video Oelementi		E	9
			Elementi: 0		1 Computer	1.00

Open the application on the smartphone or tablet and open the menu in the top right-hand corner that will appear as in the figure:



Select "*Import Profile from SD Card*" from the menu, a window will be displayed where you can navigate your folders; look for the folder you have just created, select the .ovpn file and press "*Select*". Now the connection is ready, just press *Connect*. It is important to note that also the user created by the VPN Box, in this case "*rd*", has been imported with the profile; only the OpenVPN clients compatible with this mode can be used.

 S ■ M S ■ J 14:34 	😂 🚱 🖬 🔰 🔺 🖇 🖨 🕶 🐨 🖌 🖬 14:34			
OpenVPN Connect :	OpenVPN Connect :			
Profile Imported To create a shortout to this profile or access the profile context menu (for rename, delete, etc.), touch the edit icon on the right. To switch to a different profile, tap the profile name briefly.	OpenVPN Profile: 82.106. [zpass_C8F9810201D6] → OpenVPN: Connected Disconnect			
OpenVPN Profile: 82.106. [zpass_C8F9810201D6]	Connection stats: Duration 0:00:04 Packet received 3 seconds ago Bytes in 3,79 KB Bytes out 2,88 KB Connection info: IPv4 10.9.1.25 User rd			
Connect Your Secure and Private Path to the Internet https://www.privatetunnel.com/ VPN Solution for your Business	Server 82.106. Server IP 82.106. Port 1194 Protocol TCPv4 Tap for less detail Your Secure and Private Path to the Internet			

11. Glossary

• VPN Box Manager

It is a software that allows configuring the VPN Box hardware or VPN Box Virtual Machine software.

• VPN Client Communicator

It is the software that allows users (PCs) to connect to the VPN Box via VPN.

• PTP (Point To Point)

This acronym is used to indicate a point-to-point connection between the client PC and the remote device. This configuration is useful when there are many networks to connect to, all with the same configuration, that cannot therefore remain on the same LAN. This mode is non permanent, that is it must be used for the necessary operations and then disconnected.

• SL (Single Lan)

It indicates the VPN Box mode called Remote Control that allows creating a unique (and therefore single) virtual network between the equipment and the connection clients. It is designed for monitoring systems such as SCADAs, where the connection is stable. In this mode the devices cannot have identical network configurations.