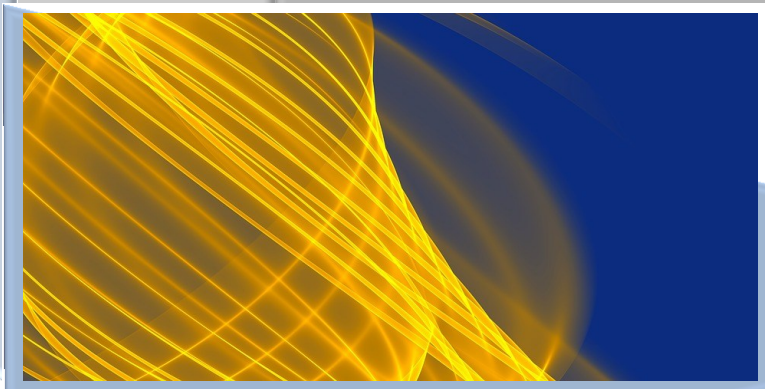
**Hubyka LTD**

# Virtual Private Network SmartHubyHome

## Technical description

**Version 1.2**

**Do not leave home network, take it with you and be unlimited mobile with secure network transport. Manage your home and be close to the people you love.**



**One is to want, another is to be able to, third and fourth is to configure and administer professionally.**

# TECHNICAL DESCRIPTION

# of Virtual Private Network SmartHubyHome

## 1. Description

Virtual Private Network **SmartHubyHome** is a technical solution for a virtual connection system (tunneling) that provides certified access and encrypted data transport in an Internet environment based on **OpenVPN** technology between the server and clients. They share a common **Ethernet** segment and a common segment of **IP** addresses, unified **WiFi** access parameters at any point on the virtual network, and share the public IP address of the Internet access server. The OpenVPN client receives Internet access and connectivity to the server through the Internet Service Provider or through a mobile operator, and is provided with a technical capability to work in a car or other means of transport in the presence of a mobile data network.

## 2. Purpose

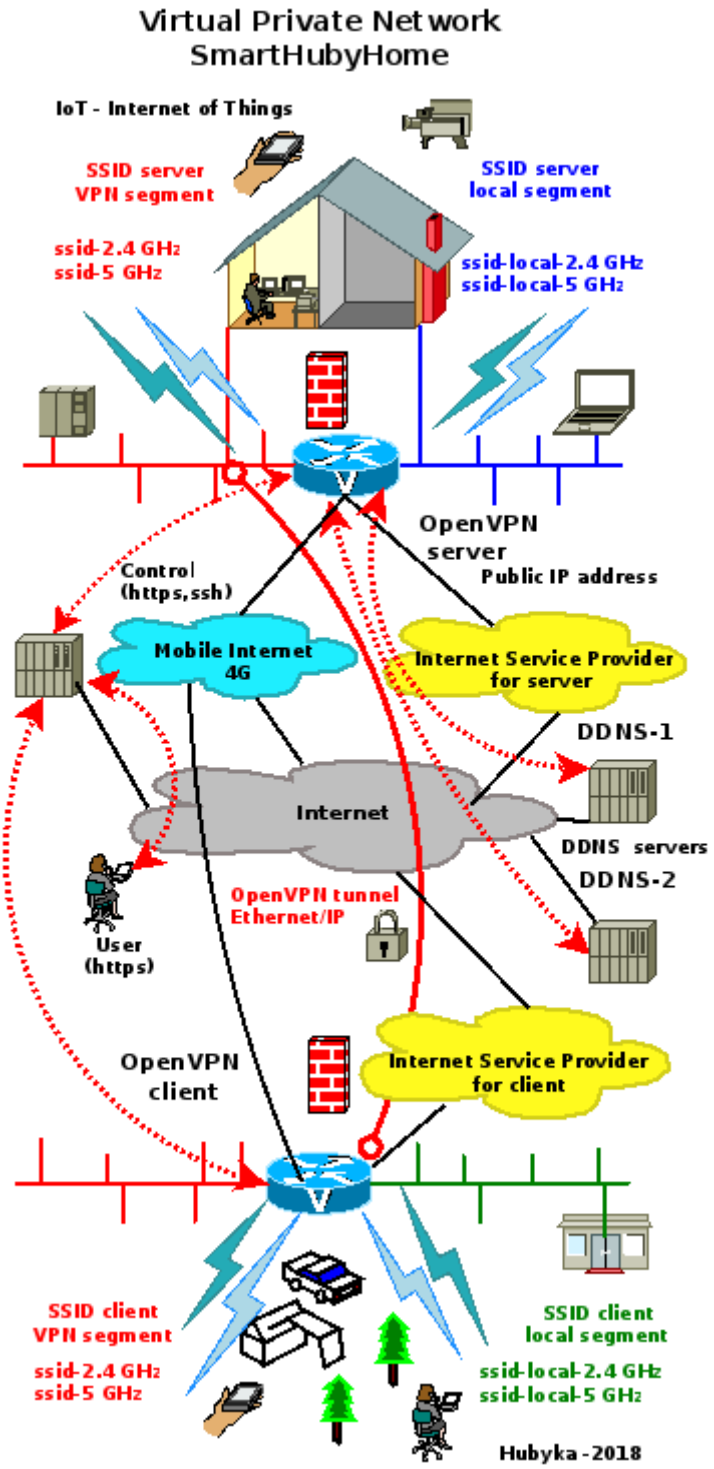
**SmartHubyHome** is designed for remote or mobile access to the Ethernet and IP segments of the internal home network with Internet access for the OpenVPN server with a public IP address. The Virtual Private Network provides direct access to peripherals in the internal home network with private IP addresses - IP cameras, smart home devices (IoT), home appliances with internet access, home data server. The **SmartHubyHome** virtual network functionality on the server's dynamic IP address is provided with a Dynamic Domain Name Server (**DDNS**).

## 3. Service composition

**The service includes:**

- Router for OpenVPN server for stationary operation and power supply adapter for 220V/50Hz
- OpenVPN client router capable of stationary operation with a 220V / 50Hz power adapter and 12V vehicle power and grounded minus from the lighter socket with a power cable
- Maximum number of routers for OpenVPN clients - 4 - option
- 4G/3G modems with USB interface with prepaid cards for mobile Internet access. Modems are used for mobile access by OpenVPN clients and for Internet access to the OpenVPN server - option
- Two wireless access points with different security levels at 2.4 GHz and 5 GHz at any point on the virtual network
- Access to the OpenVPN server by name for a public IP address with Dynamic Name Service (DDNS)
- Names for devices with a fixed IP address in the internal network (IP cameras, smart-TV, universal control panel)
- Client-side management of the network under the "publish-subscribe" scheme - an option
- Maintenance and configuration support
- Interface for home server with public access, redirecting to a private IP address (port forwarding) and limitation of administrative access to the server – option

## 4. Structure of the virtual network




The Virtual Private Network **SmartHubyHome** is powered by **OpenVPN** technology to share a common Ethernet and address segment (Ethernet / IP) between OpenVPN server and OpenVPN clients with Internet traffic tunneling.The authentication of OpenVPN clients is with a name, password and digital certificate and the data is encrypted with a dynamic key. Each of the OpenVPN clients has a permanent IP address from the shared IP segment of the internal network.

The network topology is a star in which the OpenVPN server router is central, with full connectivity between all the nodes of the virtual network - client-server and client-client. An obligatory condition for running, monitoring, and managing the virtual network is Internet connectivity and a public IP address for the OpenVPN server. The network structure for a dynamic address of OpenVPN server is provided by a double reserved dynamic name server DDNS for a name zone supported by the service provider. OpenVPN client routers can work with a connection to the OpenVPN server and an Internet-based network with private IP addresses network address translation (NAT) including in a mobile data network.

## 5. Technical parameters

### 5.1. Router for OpenVPN server

**Mikrotik - Product code RBD52G-5HacD2HnD-TC - hAP ac², System RouterOS**
**https://mikrotik.com/product/hap_ac2**

**5.1.1.** Dimensions 34 x 119 x 98mm
**5.1.2.** Maximum power consumption 15 W at supply voltage 18-28 V DC
**5.1.3.** Number of power supply ports 2. (DC connector, PoE-IN - Passive PoE)
**5.1.4.** Tested ambient temperature -40 ° C .. + 50 ° C

**5.1.5. Specifications**
- **5.1.5.1.** Product Code: RBD52G-5HacD2HnD-TC
- **5.1.5.2.** Architecture ARM 32bit
- **5.1.5.3.** CPU IPQ-4018
- **5.1.5.4.** CPU core count - 4
- **5.1.5.5.** Nominal CPU frequency 716 MHz
- **5.1.5.6.** License level 4
- **5.1.5.7.** Operating system RouterOS
- **5.1.5.8.** RAM 128 MB
- **5.1.5.9.** 16 MB memory - FLASH type

**5.1.6. Supported WiFi standards**
- **5.1.6.1.** WiFi 2.4 GHz
  Chip model IPQ-4018
  Number of channels – 2
  Standards - 802.11b/g/n
  Antenna gain 2.5 dBi
- **5.1.6.2.** WiFi 5 GHz
  Chip model IPQ-4018
  Number of channels – 2
  Standards - 802.11ac
  Antenna gain 2.5 dBi

**5.1.7.** Ethernet ports 10/100/1000 Mbps – 5
**5.1.8.** USB slot – type A
**5.1.9.** Productivity 1518 Bytes – 162.5 kpps / 1973.4 Mbitps

### 5.2. Router for OpenVPN client

**Mikrotik - Product code RB952Ui-5ac2nD-TC - hAP ac lite tower , System RouterOS**

**https://mikrotik.com/product/RB952Ui-5ac2nD-TC#fndtn-specifications**

**5.2.1.** Dimensions 34 x 119 x 98mm
**5.2.2.** Maximum power consumption 8 W at supply voltage 10-28 V DC.

**5.2.3.** Number of power supply ports 2. (DC connector, PoE-IN - Passive PoE).
**5.2.4.** Tested ambient temperature -40 ° C .. + 50 ° C
**5.2.5. Specifications**
**5.2.5.1.** Product Code: RB952Ui-5ac2nD-TC
**5.2.5.2.** Architecture MIPSBE
**5.2.5.3.** CPU QCA9531
**5.2.5.4.** CPU core count -1
**5.2.5.5.** Nominal CPU frequency 650 MHz
**5.2.5.6.** License level 4
**5.2.5.7.** Operating system RouterOS
**5.2.5.8.** RAM 64 MB
**5.2.5.9.** 16 MB memory - FLASH type
**5.2.6. Supported WiFi standards**
**5.2.6.1.** WiFi 2.4 GHz
Chip model QCA-9887
Number of channels – 2
Standards - 802.11b/g/n
Antenna gain - 2 dBi
**5.2.6.2.** WiFi 5 GHz
Chip model -9531
Number of channels – 2
Standards - 802.11ac
Antenna gain 2 dBi
**5.2.7.** Ethernet ports 10/100 Mbps – 5
**5.2.8.**USB slot – type A
**5.2.9.** Productivity 1518 Bytes – 40.6 kpps / 493.0 Mbitps

## 5.3. Tunneling Technology - OpenVPN

**5.3.1.** Transport Protocol - TCP
**5.3.2.** OpenVPN server port - 988 (port 443 - optional)
**5.3.3.** Mode of operation - Ethernet/IP (Ethernet-bridge, TAP virtual interface)
**5.3.4.**Authentication of OpenVPN clients - SHA-1, MD5 with name, password and certificate
**5.3.5.** Encryption of traffic in the tunnel - Blowfish algorithm with 128-bit key length (blowfish128)

## 5.4. Network Parameters

**5.4.1. Topology of the virtual private network SmartHubyHome**. The logical topology of the virtual private network is star type. The central node is an OpenVPN server.
**5.4.2. Connectivity type between virtual private network nodes - full mesh**. Each node is connected to each if an OpenVPN server is available. All nodes share a common Ethernet segment and a common IP address segment.
**5.4.3.Number of OpenVPN Clients -1. Option - up to 4.**

**5.4.4. OpenVPN server**
**5.4.4.1. IP address plan**
WAN IP address - public, received by DHCP from the Internet service provider
VPN shared network segment (private addresses on RFC1918):

- network - 10.10.10.0/23 (netmask 255.255.254.0)
- default gateway - 10.10.10.1

- Reserved - 10.10.10.2 - 10.10.10.99
- OpenVPN server - reserved - 10.10.10.100
- OpenVPN pool -10.10.10.101-10.10.10.199
- Reserved address - 10.10.10.200
- Free IP addresses for user equipment with static settings - /23 (netmask 255.255.254.0) :
  10.10.10.201-10.10.10.255
  10.10.11.0 – 10.10.11.10
- IP addresses for DHCP user equipment:
  DHCP VPN pool - 10.10.11.11-10.10.11.239
- Reserved - 10.11.11.240 - 10.10.11.254

Local Network Segment (Private RFC1918 addresses):

- network 10.12.12.0/23 (netmask 255.255.254.0)
- default gateway 10.12.12.1
- Reserved - 10.12.12.2 - 10.12.12.199
- Reserved address - 10.12.12.200
- Free IP addresses for user equipment with static settings - /23 (netmask 255.255.254.0) :
  10.12.12.201-10.12.12.255
  10.12.13.0 – 10.12.13.10
-
- IP addresses for DHCP user equipment:
  DHCP local pool 10.12.13.11-10.12.13.239
- Reserved - 10.12.13.240 - 10.12.13.254

#### 5.4.4.2. Layout of interfaces

- WAN interface - ether1
- - LAN interfaces for VPN shared network segment - ether2, ether3
- - LAN interfaces for a local network segment - ether4, ether5

#### 5.4.4.3. WiFi access

- SSID for a local network segment 5 GHz and 2.4 GHz
- SSID for a VPN network segment 5 GHz and 2.4 GHz

#### 5.4.4.4. Home server port redirection – option

- IP address 10.10.10.240/23 (netmask 255.255.255.254)
- default gateway 10.10.10.1
- number of ports - up to 8
- physical interface - ether2 or ether3 - VPN shared network segment for both routers

### 5.4.5.OpenVPN client

#### 5.4.5.1. IP address plan

WAN IP address - public, received by DHCP from the Internet service provider

VPN shared network segment (private addresses on RFC1918):

- network - 10.10.10.0/23 (netmask 255.255.254.0)
- default gateway - 10.10.10.2
- Reserved - 10.10.10.2 - 10.10.10.99
- OpenVPN client - reserved - 10.10.10.101

- OpenVPN pool -10.10.10.101-10.10.10.199
- Reserved address - 10.10.10.200
- Free IP addresses for user equipment with static settings - /23 (netmask 255.255.254.0) :
  10.10.10.201-10.10.10.255
  10.10.11.0 – 10.10.11.10
- IP addresses for DHCP user equipment:
- DHCP VPN pool - 10.10.11.11-10.10.11.239
- Reserved - 10.11.11.240 - 10.10.11.254

Local Network Segment (Private RFC1918 addresses):

- network 10.12.12.0/23 (netmask 255.255.254.0)
- default gateway 10.12.12.1
- Reserved - 10.12.12.2 - 10.12.12.199
- Reserved address - 10.12.12.200
- Free IP addresses for user equipment with static settings - /23 (netmask 255.255.254.0) :
  10.12.12.201-10.12.12.255
  10.12.13.0 – 10.12.13.10
-
- IP addresses for DHCP user equipment:

- DHCP local pool 10.12.13.11-10.12.13.239
- Reserved - 10.12.13.240 - 10.12.13.254

#### 5.4.5.2. Layout of interfaces

- WAN interface - ether1
- LAN interfaces for VPN shared network segment - ether2, ether3
- LAN interfaces for a local network segment - ether4, ether5

#### 5.4.5.3. WiFi access

- SSID for a local network segment -5 GHz and 2.4 GHz
- SSID for the VPN network segment -5 GHz and 2.4 GHz

### 5.4.6. Mobile Internet - Option

**5.4.6.1. Functions.** Mobile Internet connectivity is configured for 3G and 4G USB modems. Not all modems are compatible with Mikrotik routers. Traffic at maximum speed for most carriers is limited. The different base stations provide different speeds. It is necessary to plan the traffic in accordance with the operator's tariff plan and refer to the map of the provided speeds.

#### 5.4.6.2. OpenVPN server

In the OpenVPN server, mobile connectivity is used to provide redundancy. The reservation works automatically when the modem is turned on and provided if the default route is dropped via DHCP through the WAN port.

If there is a problem with the main provider's network without dropping this route, it is necessary to remove the network cable from the WAN port to redirect traffic over the mobile data network. Because mobile operators typically do not provide a public IP address, the virtual private network does not work when the OpenVPN server is running a mobile Internet.

**OpenVPN client**
For the OpenVPN client, mobile connectivity can be the main mode in a car or rural area. When working in a vehicle, it is necessary to provide the router with power supply equipment that conforms to the voltage of the on-board network..

### 5.4.7.Dynamic Domain Name Server (DDNS)

**5.4.7.1. Purpose.** The work of the Virtual Private Network on OpenVPN technology in an Internet environment with a dynamic IP address on the server is provided with a double reserved dynamic domain name server - DDNS. Two name servers work in parallel, simultaneously and independently. They provide address resource records (A) for the IP address of the OpenVPN server WAN interface. **Предназначение.** Работата на виртуалната частна мрежа по технологията OpenVPN в Интернет среда с динамичен IP адрес на сървъра се осигурява с двойно резервиран динамичен сървър за имена - DDNS. Два именни сървъра работят паралелно, едновременно и независимо. Те осигуряват адресни именни ресурсни (A) записи за IP адреса на WAN интерфейса на OpenVPN сървъра.

**5.4.7.2. Parameters of name records**

- Update period - 300 s
- Time to live (TTL) - 600 s
- Transport protocol of DDNS requests – TCP
- Authentication and encryption - HTTS with public certificate

### 5.4.8. Managing and Network Security

Router management is performed on a two-way client-server schema "Publish-subscribe". The configuration elements of each router are the metadata needed to operate the system. The metadata are transported between the control server and the routers in encrypted form. Configurations support network administration only from fixed network addresses. The certificates required for the virtual private network operation are stored in the router's memory.

The storage of the equipment and the provision of normal working conditions is the responsibility of the user.

The user information and management features with authentication and authorization (name and password) are provided on secure protocol - HTTPS with public certificate. One user profile manages all routers in the virtual private network. E-mail information is provided after anonymization and does not contain personal information about the user. There are also no bases for the history of DDNS queries and records. All options and configurations not covered by this document are negotiated but not in contradiction with the Agreements on Integrity and Compliance with the Legal and Ethical Frameworks.