

# Business-VPN WHMCS module

The module is intended as an opportunity for IT companies to expand their offer for customers by offering paid VPN accounts. After installation, the module will fully manage the creation, edition, and suspension of VPN accounts and interact with the WHMCS billing system, exchanging data needed for settlements with customers, activations or service blocking.

- [Description](#)
- [Changelog](#)
- [Installation and configuration guide](#)
  - [Basic concepts and requirements](#)
  - [WHMCS setup\(install/update\)](#)
  - [Mikrotik preparation and configuration](#)
  - [Add server \(router Mikrotik\) in WHMCS](#)
  - [Product Configuration](#)
- [Client Area](#)
  - [Home screen](#)
  - [Add VPN account](#)
  - [Edit VPN account](#)
  - [Statistics](#)
- [Admin Area](#)
  - [Product Home Screen](#)

# Description

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

The Business VPN module provides an opportunity to sell the Virtual Private Network service for business clients.

The module is designed as a professional solution for companies and corporations, which enables remote access to company resources from anywhere in the world in a safe and monitored manner. The biggest difference from common VPN solutions such as NordVPN, EasyVPN etc. is the professional nature of the service.

### What makes Business VPN different from regular, widely offered VPNs

The end customer of the service receives such opportunities as:

- Dedicated permanent IP address
- Full management of VPN accounts to the end buyer: Create, modify, delete and block VPN accounts
- Forward TCP/UDP protocol ports from a public address to any IP address on the internal network
- Convenient and informative VPN account connection statistics

Thanks to our solution, the client does not have to delegate the company's resources to carry out this activity, but focus on the practical side of using it, thanks to which he saves money.

This model of operation allows IT departments in companies to configure in detail and securely internal Firewall, passing specific ports, detailed traffic monitoring, or to keep through internal IDS *which is not possible when using commonly offered solutions.*

Such a VPN becomes an integral part of the company's IT infrastructure and is ideally suited to the conditions of a given client.

### Who and why needs such a service that this module

provides.

The service offers to the end customer a fully fledged private network.

1. The service combines all nodes that are connected via VPN into one private network. This allows you to communicate with each other from different physical locations. An example of use is, the remote work of the company's staff, having private remote access to each other. Also, due to the fact that each connected VPN user will be presented on the Internet with the public address of the service, it is possible to configure access to the company's servers only from the IP address of the service. Thus restrict access only to everyone except users of the service.
2. If your employees need to have access to some sites on the Internet and be represented by a public address of a certain geographic location, then this service allows you to implement it. The public address of the service is not changed during the entire time of using the service.
3. Ability to connect network devices, such as measuring instruments, to the same network, creating remote access to network equipment.

## Module Functions:

- Auto create and deploy VPN account/accounts
- Suspend/Unsuspend/Terminate/Change Package/Change Password/Reset connection
- Use only Mikrotik API
- Possibility to set Bandwidth speed limits
- Module supports multilingualism
- Account limit per package
- Bandwidth Limit per account

## Functions of the client area:

- Creating VPN Accounts
- Deleting a VPN account
- Blocking VPN account
- VPN account online statistics. For control



★ Overview ^

i Information

+ Add VPN account

▶ Port Forwarding

📊 Statistics

**Dev License:** This installation of WHMCS is running under a Development License and is not authorized to be used for production use. Please report any cases of abuse to [abuse@whmcs.com](mailto:abuse@whmcs.com)



Business-VPN  
100  
Business-VPN

ACTIVE

Registration Date

Saturday, October 8th, 2022

Recurring Amount

0.00\$

Billing Cycle

Free Account

Next Due Date

-

Payment Method

Bank Transfer

🌐 Manage

Network configuration

VPN server:	vpn-test.puq.pl
Dedicated IP:	77.87.125.205
Private internal network:	172.16.205.0/25
VPN Protocols:	PPtP L2TP
L2TP IPsec PSK key:	QWEqwe123
Number of VPN accounts:	5/10
Bandwidth download/upload:	10/5 M



Add VPN account



Port Forwarding



Statistics

Enabled	Username	Online	Uptime	
✓	1-4806-r1 (172.16.205.2)	✓	1m33s pptp	<a href="#">Reset connection</a> <a href="#">Edit</a>
✓	1-4806-r2 (172.16.205.3)	✓	1m32s pptp	<a href="#">Reset connection</a> <a href="#">Edit</a>
✓	1-4806-r3 (172.16.205.4)	✓	1m31s pptp	<a href="#">Reset connection</a> <a href="#">Edit</a>
✓	1-4806-r4 (172.16.205.5)	✓	1m30s	<a href="#">Reset connection</a>

★ Overview ^

i Information

+ Add VPN account

» Port Forwarding

📊 Statistics

**Dev License:** This installation of WHMCS is running under a Development License and is not authorized to be used for production use. Please report any cases of abuse to [abuse@whmcs.com](mailto:abuse@whmcs.com)

## Add VPN account

Username:

1-4806-

Password:

[Generate](#)

IP address:

172.16.205.7



[+ Add VPN account](#)

★ Overview ^

i Information

+ Add VPN account

» Port Forwarding

📊 Statistics

**Dev License:** This installation of WHMCS is running under a Development License and is not authorized to be used for production use. Please report any cases of abuse to [abuse@whmcs.com](mailto:abuse@whmcs.com)

## Edit VPN account

Username:

1-4806-r1

Password:

2A8Jkfs4vbyG

[Generate](#)

IP address:

172.16.205.2



Enabled:



[✕ Delete](#)

[✎ Save](#)

★ Overview ^

i Information

+ Add VPN account

➡ Port Forwarding

📊 Statistics

**Dev License:** This installation of WHMCS is running under a Development License and is not authorized to be used for production use. Please report any cases of abuse to [abuse@whmcs.com](mailto:abuse@whmcs.com)

## Port Forwarding

From:    ⌵

To:  ⌵

+ Add port forwarding

Public IP:PORT	To IP:PORT	Bytes (Packets)	
77.87.125.205:333 udp	172.16.205.5:50 (1-4806-r4)	0 (0)	<button>✕ Delete</button>
77.87.125.205:500 tcp	172.16.205.3:23 (1-4806-r2)	144 (3)	<button>✕ Delete</button>

★ Overview ^

i Information

+ Add VPN account

» Port Forwarding

📊 Statistics

**Dev License:** This installation of WHMCS is running under a Development License and is not authorized to be used for production use. Please report any cases of abuse to [abuse@whmcs.com](mailto:abuse@whmcs.com)

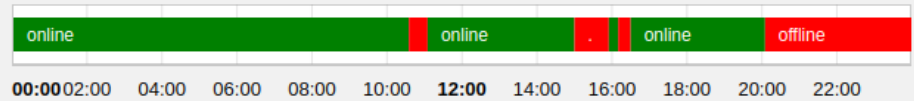
2022-10-17



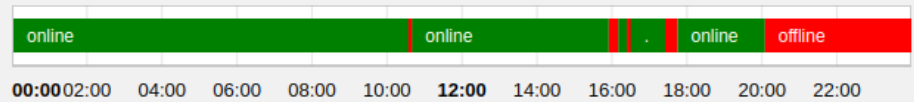
📊 Show statistics

## Statistics for: 2022-10-17

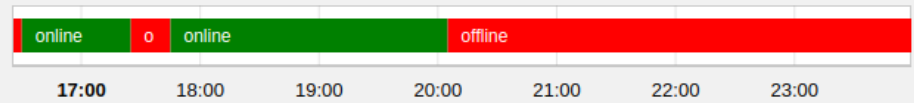
Username: 1-4806-r1



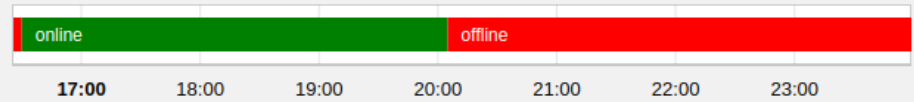
Username: 1-4806-r2



Username: 1-4806-r3



Username: 1-4806-r4





Go

More ▾

Non[Change Package](#)

API answer OK

## VPN accounts

## Port Forwarding

## Addons

No Records Found

Servers

Edit Server

Name	<input type="text" value="vpn-test.puq.pl-B"/>
Hostname	<input type="text" value="vpn-test.puq.pl"/>
IP Address	<input type="text"/>
Assigned IP Addresses (One per line)	<div>77.87.125.205   25   172.16.205.0   25 77.87.125.206   25   172.16.206.0   25 77.87.125.207   25   172.16.207.0   25 77.87.125.208   25   172.16.208.0   25 77.87.125.209   25   172.16.209.0   25</div>
Monthly Cost	<input type="text" value="0.00"/>
Datacenter/NOC	<input type="text"/>
Maximum No. of Accounts	<input type="text" value="200"/>
Server Status Address	<div><input type="text"/> To display this server on the server status page, enter the full path to the server status folder (required to be uploaded to each server you want to monitor) - eg. <a href="https://www.example.com/status/">https://www.example.com/status/</a></div>
Enable/Disable	<input type="checkbox"/> Tick to disable this server

Nameservers

Primary Nameserver	<input type="text"/>	IP Address:	<input type="text"/>
Secondary Nameserver	<input type="text"/>	IP Address:	<input type="text"/>
Third Nameserver	<input type="text"/>	IP Address:	<input type="text"/>
Fourth Nameserver	<input type="text"/>	IP Address:	<input type="text"/>
Fifth Nameserver	<input type="text"/>	IP Address:	<input type="text"/>

Server Details

Module	<div><div>PUQ Business-VPN</div><div>Test Connection</div></div>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Access Hash	<div></div>
Secure	<input checked="" type="checkbox"/> Tick to use SSL Mode for Connections
Port	<div><input type="text" value="443"/><input type="checkbox"/> Override with Custom Port</div>

Save ChangesCancel Changes

# Changelog

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

### v2.0 Released 23-09-2024

**Module is coded ionCube v13**

Supported php version:

- php 7.4 WHMCS 8.11.0 -
- php 8.1 WHMCS 8.11.0 +
- php 8.2 WHMCS 8.11.0 +

---

### v1.1.5 Released 11-10-2023

1. Supported WHMCS v8.8.0
2. Translations added/updated (**Arabic, Azerbaijani, Catalan, Chinese, Croatian, Czech, Danish, Dutch, English, Estonian, Farsi, French, German, Hebrew, Hungarian, Italian, Macedonian, Norwegian, Polish, Romanian, Russian, Spanish, Swedish, Turkish, Ukrainian**)

---

### v1.1 Released 03-03-2023

1. Support Mikrotik v7.8
2. Support WHMCS v8.6
3. Support IonCube PHP Loader v12
4. Support for PHP 8.1 and PHP 7.4
5. Change in the way statistics are collected and cleaned
6. Design change, icons added

---

### v1.0 Released 20-10-2022

First version

# Installation and configuration guide

# Basic concepts and requirements

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

### Requirements for the successful operation of the module

- Minimal WHMCS version 8+
- Mikrotik/CHR router OS 7+
- Public network for the needs of NAT implementation

An IP address class must be reserved for the solution. Each end customer receives one IP address after activating the service.

Please refer to the basic mode of operation of the module to better understand its operation and functionality.

### The basic logic of the module

During the creation of a service for the end client, the module does the following actions:

1. Automatically selects a free public IP address from the server available in the settings. When choosing an available IP address, services in the terminated state are not taken into account, i.e. previously used IP. *(Previously used IP addresses for services that have not been extended and have expired will be used to activate the service for the new client.)*
2. The module configures the selected public IP address on the network interface of the router.
3. The module *creates firewall rules* such as:
  - NAT rules for accessing the Internet private network
  - Allowing firewall rules for communication between IP's of a private network

- Block rules that block traffic between all other private networks.

## Mikrotik management schema

- When a user creates a VPN account, the module creates a VPN user Mikrotik on the router, adds queues with a bandwidth limit.
- When a user deletes a VPN Account, the module deletes the VPN user on Mikrotik and deletes the bandwidth-limiting queue.
- When a user creates port forwarding, the module creates rules on the Mikrotik router in the firewall that implement port forwarding from a public address to a private one.
- During service suspension, the module disables all VPN client accounts and resets all active connections.
- During service unsuspension, the module enables all VPN client accounts.
- During service termination, the module deletes all VPN client accounts, deletes all firewall rules associated with the service, and also deletes the public IP from the router's network interface.

# WHMCS

## setup(install/update)

### Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

**Module is coded ionCube v13**

Supported php version:

- php 7.4 WHMCS 8.11.0 -
- php 8.1 WHMCS 8.11.0 +
- php 8.2 WHMCS 8.11.0 +

To install and update a module, you must perform one and the same action.

#### 1. Download the latest version of the module.

PHP 8.2

```
wget http://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Business-VPN/php82/PUQ_WHMCS-Business-VPN-latest.zip
```

PHP 8.1

```
wget http://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Business-VPN/php81/PUQ_WHMCS-Business-VPN-latest.zip
```

PHP 7.4

```
wget http://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Business-VPN/php74/PUQ_WHMCS-Business-VPN-latest.zip
```

All versions are available via link:

[https://download.puqcloud.com/WHMCS/servers/PUQ\\_WHMCS-Business-VPN/](https://download.puqcloud.com/WHMCS/servers/PUQ_WHMCS-Business-VPN/)

## 2. Unzip the archive with the module.

```
unzip PUQ_WHMCS-Business-VPN-latest.zip
```

## 3. Copy and Replace "puqBusinessVPN" from "PUQ\_WHMCS-Business-VPN" to "WHMCS\_WEB\_DIR/modules/servers/"



# Mikrotik preparation and configuration

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

Note: **Enter the following commands one by one and wait for the command to complete.**

### I. Check RouterOS version

**Make sure that the version of RouterOS is 7+**

```
system/package/print
```

### II. Enabling HTTPS Create your own root CA on your router

```
/certificate  
add name=LocalCA common-name=LocalCA key-usage=key-cert-sign,crl-sign
```

### III. Sign the newly created CA certificate

```
/certificate  
sign LocalCA
```

## IV. Create a new certificate for Webfig (non-root certificate)

Note: as common-name=XXX.XXX.XXX.XXX You enter public IP address of the router.

```
/certificate  
add name=Webfig common-name=XXX.XXX.XXX.XXX
```

## V. Sign the newly created certificate for Webfig

```
/certificate  
sign Webfig ca=LocalCA
```

## VI. Enable SSL (*www-ssl*) and specify to use the newly created certificate for Webfig

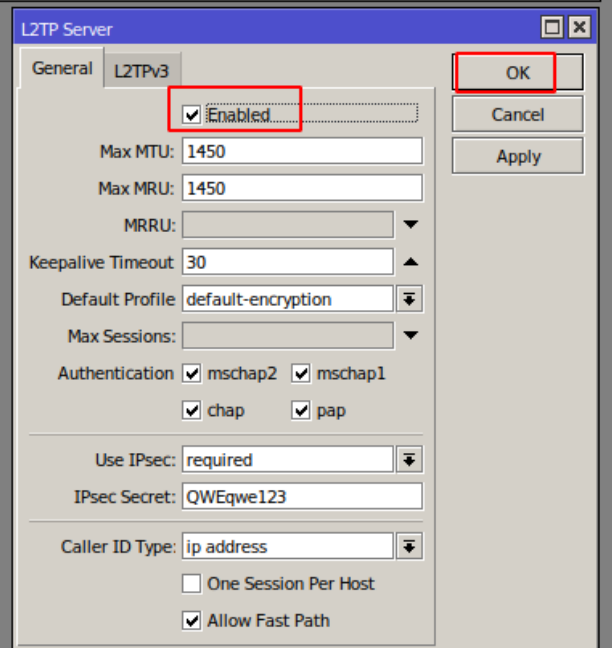
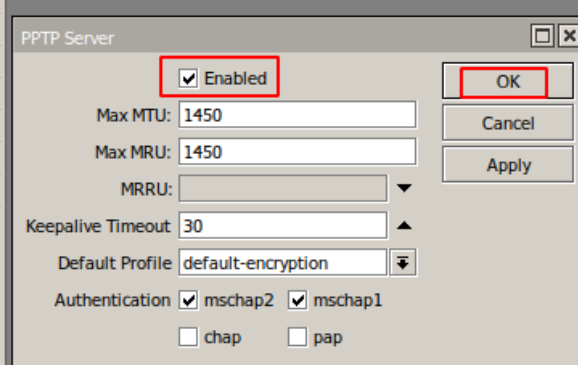
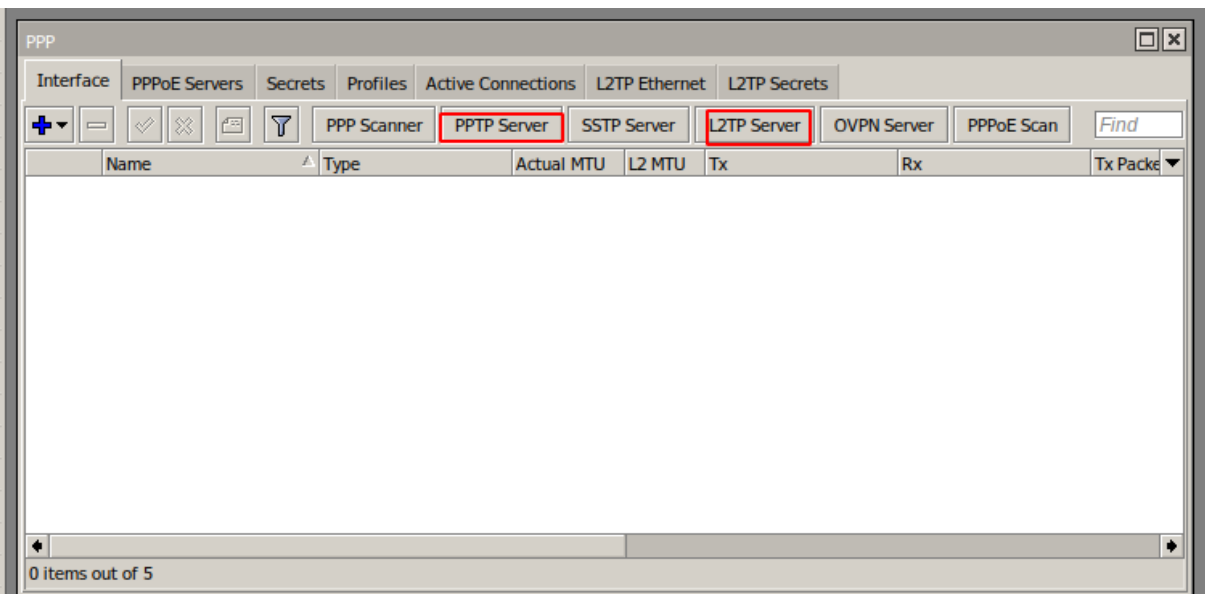
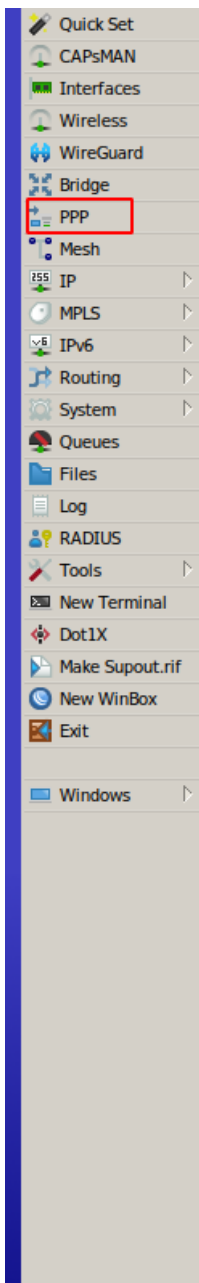
```
/ip service  
set www-ssl certificate=Webfig disabled=no
```

## VII. Enable api-ssl and specify to use the newly created certificate for Webfig

```
/ip service  
set api-ssl certificate=Webfig disabled=no
```

## VIII. Enable VPN server

To enable the VPN server



# Add server (router Mikrotik) in WHMCS

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

Add a new server to the system WHMCS.

Login to Your WHMCS panel and create new server in WHMCS (*System Settings->Products/Services->Servers*)

System Settings->Servers->Add New Server

[Products/Services](#)  
[Configure the correct](#) **Name** and **Hostname**  
[Product Addons](#)  
[Product Bundles](#)  
[Domain Pricing](#)  
[Domain Registrars](#)

**Name is just for Your convenience and You can put there anything You like ie: Mygreat mikrotik routr**

**You can choose whatever hostname You want. Valid entries look similar to: vpn.mydomain.com, ourgreatvpn.mydomain.net. You can also dedicate whole domain ie: myVPNservices.com if You like. The important thing is to resolve the choosen IP address of the Mikrotik router in DNS server for Your domain.**

- In the "**Assigned IP Addresses field**", enter a list of IP addresses that will be issued to users.

The format in which you need to enter a list of public IP addresses and private subnets is as follows.

To define the available pool of IP addresses, for each available IP number you should enter another line where the data is separated by the "|" separator. Each line with an IP number definition has the following structure:

```
<PUBLIC_IP>|<MASK_OF_PUBLIC_NETWORK>|<PRIVATE_NETWORK>|<MASK_OF_PRIVATE_NETWORK>
```

Servers

Edit Server

Name	<input type="text" value="vpn-test.puq.pl-B"/>
Hostname	<input type="text" value="vpn-test.puq.pl"/>
IP Address	<input type="text"/>
Assigned IP Addresses (One per line)	<div>77.87.125.205 25 172.16.205.0 25 77.87.125.206 25 172.16.206.0 25 77.87.125.207 25 172.16.207.0 25 77.87.125.208 25 172.16.208.0 25 77.87.125.209 25 172.16.209.0 25</div>
Monthly Cost	<input type="text" value="0.00"/>
Datacenter/NOC	<input type="text"/>
Maximum No. of Accounts	<input type="text" value="200"/>
Server Status Address	<div><input type="text"/> To display this server on the server status page, enter the full path to the server status folder (required to be uploaded to each server you want to monitor) - eg. <a href="https://www.example.com/status/">https://www.example.com/status/</a></div>
Enable/Disable	<input type="checkbox"/> Tick to disable this server

Enter the correct data in the username and password field

- In the **Server Details** section, select the **"PUQ Business-VPN"** module and enter the correct **username** and **password** for the **Mikrotik**.
- To check, click the **"Test connection"** button

Server Details

Module	<div>PUQ Business-VPN ▾<div>Test Connection</div></div> <div>✓ Connection successful. Some values have been auto-filled.</div>
Username	<div>admin</div>
Password	<div>.....</div>
Access Hash	<div></div>
Secure	<div><input checked="" type="checkbox"/> Tick to use SSL Mode for Connections</div>
Port	<div><div>443</div><div><input type="checkbox"/> Override with Custom Port</div></div>

# Product Configuration

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

### Add new product to WHMCS

System Settings->Products/Services->Create a New Product

In the **Module settings** section, select the "**PUQ Business-VPN**" module

License key: 4XPRUF [redacted]-GPPJNL  
success: 2022-11-07T15:26:10+01:00

Interface for public IP: ether1-pub (CE:08:BD:0F:C9:61)  
The public IP address will set on this interface

VPN users settings

Number of VPN users: 10

Bandwidth Download: 10 M

Bandwidth Upload: 5 M

Mikrotik configuration

Automatically add settings to Mikrotik

Public IP on interface: ☒

NAT rules on public ip: ☒

Firewall Accept Rules: ☒

Firewall Drop Rules: ☒

The settings will be added when the service is created. And they will be deleted at the moment the service switches to the terminated state

PPP Profile: default  
Profile that connects to the VPN user

Basic settings

Description prefix: WAW

Service: any  
PPP Secret Service

Support PPTP: ☒ Information in the client panel about PPTP protocol support

Support L2TP: ☒ Information in the client panel about L2TP protocol support

L2TP IPsec PSK key: QWEqwe123

- **License key:** A pre-purchased license key for the "**PUQ Business-VPN**" module. For the module to work correctly, the key must be active
- **Interface for public IP:** Interface on the router on which the public IP address will be set
- **PPP Profile:** PPP secret profile on Mikrotik router

### VPN users settings

- **Number of VPN users:** The number of VPN accounts that a client can create
- **Bandwidth Download:** Download bandwidth that will apply per VPN connection
- **Bandwidth Upload:** Upload bandwidth that will apply per VPN connection

### Mikrotik configuration

- **Public IP on interface:** If checked, the module will automatically set the IP address on

the interface in the Mikrotik router

- **NAT rules on public ip:** If checked, then the module will automatically make firewall rules that will make NAT, for Internet access of all connected VPN accounts of the client in the Mikrotik router
- **Firewall Accept Rules:** If checked, then the module automatically creates firewall rules that will allow traffic between VPN client accounts
- **Firewall Drop Rules:** If checked, then the module automatically creates firewall rules that will drop traffic between VPN client accounts and other private networks on the router

## Basic settings

- **Description prefix:** The prefix that will appear in all descriptions that will be on the Mikrotik router
- **Service:** A service that will be available to a VPN user on a Mikrotik router
- **Support PPTP/Support L2TP:** If checked, it will be reflected in the client zone
- **L2TP IPsec PSK key:** it will be reflected in the client zone



# Client Area

# Home screen

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

### Basic information on client panel page

**VPN server:** The VPN server address that is entered when creating a VPN connection for the end user

**Dedicated IP:** The public IP address that is reserved for the service and through which all users of the VPN service will be represented on the Internet.

**Private internal network:** Private subnet whose IP addresses are available to the client to create VPN accounts. When adding a new VPN account, it will be assigned an IP address from this internal pool of addresses.

**VPN Protocols:** VPN protocols that are available (*by default you can easily enable two protocols in Mikrotik router: PPPtP i L2TP* )

**L2TP IPSec PSK key:** In the case of L2TP, this is the encryption key

**Number of VPN accounts:** Number of used and available VPN client accounts from the pool available based on the defined package.

**Bandwidtht download/upload:** The bandwidth rate that will be available on each VPN client account








### Function buttons for service management.

- **Add VPN account:** To create a new VPN account
- **Port Forwarding:** To configure port forwarding from a public IP address to a private one
- **Statistics:** To access connection statistics of VPN

List of VPN accounts with technical/dynamic data and also buttons **Edit** and **Reset connections**



## Network configuration

 VPN server:	vpn-test.puq.pl
 Dedicated IP:	77.87.125.205
 Private internal network:	172.16.205.0/25
 VPN Protocols:	PPpTtP L2TP
 L2TP IPsec PSK key:	QWEqwe123
 Number of VPN accounts:	8/10
 Bandwidtht download/upload:	10/5 M































Add VPN account



Port Forwarding



Statistics

 Enabled	 Username	 Online	 Uptime
	1-4806-4 (172.16.205.7)		 Edit
	1-4806-asd (172.16.205.8)		 Edit
	1-4806-dupa (172.16.205.17)		 Edit
	1-4806-r1 (172.16.205.2)		 Edit
	1-4806-r2 (172.16.205.3)		 Edit
	1-4806-r3 (172.16.205.4)		 Edit
	1-4806-r4 (172.16.205.5)		 Edit
	1-4806-ruslan (172.16.205.6)		 Edit



# Add VPN account







## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

This is how the page for adding a new VPN account looks like.

Each VPN account has a unique client ID, the ID is generated according to the scheme <user\_id>-<service\_id>-Manually entered value. <user\_id>-<service\_id> are generated automatically by module. You can modify manually the last part.

## Add VPN account

 Username:	<input type="text" value="1-4806- Enter username"/>
 Password:	<input type="password" value="Enter password"/>  Generate
 IP address:	<input type="text" value="172.16.205.9"/> 
	

To create a new account, the client must enter the following.







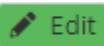


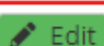


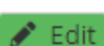


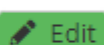


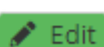
Username, Password, Select an available IP address from the dropdown list. Then click the **Add VPN account** button.

# Edit VPN account

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

In order to edit a VPN account, you must click on the **Edit** button on the selected account.

 Enabled	 Username	 Online	 Uptime
	1-4806-4 (172.16.205.7)		
	1-4806-asd (172.16.205.8)		
	1-4806-dupa (172.16.205.17)		
	1-4806-r1 (172.16.205.2)		
	1-4806-r2 (172.16.205.3)		









You can edit the following parameters:

- Password
- IP address
- Enable/Disable VPN account

Also on the editing page there is an opportunity to delete a VPN account.

By pressing the DELETE button

## Edit VPN account

 Username:	<input type="text" value="1-4806-r2"/>
 Password:	<input type="password" value="C1CS81fejEdu"/>  Generate
 IP address:	<input type="text" value="172.16.205.3"/> 
 Enabled:	<input checked="" type="checkbox"/>
 Delete	 Save



# Statistics

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

The module provides visual online statistics of VPN accounts.

It is possible to select a specific data to display statistics.

Statistics are available for the last 60 days.

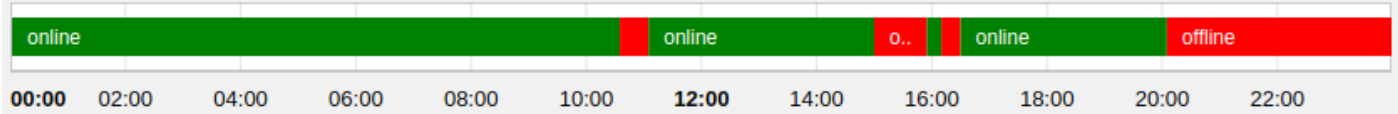
2022-10-17



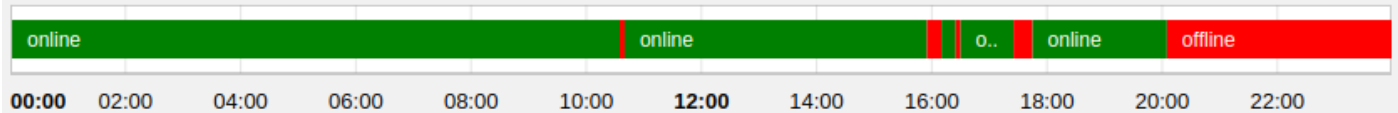
Show statistics

## Statistics for: 2022-10-17

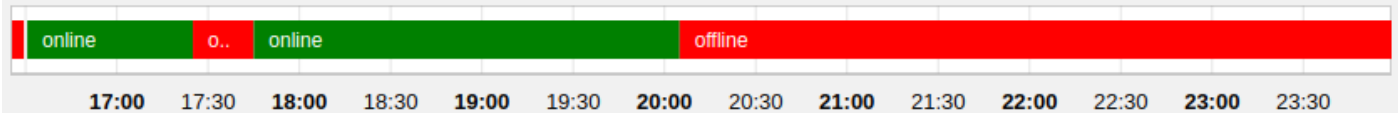
Username: 1-4806-r1



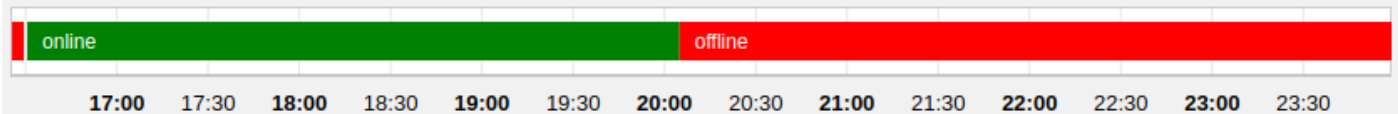
Username: 1-4806-r2



Username: 1-4806-r3



Username: 1-4806-r4



# Admin Area

# Product Home Screen

## Business-VPN module **WHMCS**

[Order now](#) | [Download](#) | [FAQ](#)

The main screen of the product contains the following items.

- List of VPN client accounts
- List of all forwarded client ports.

Go

More ▾

Non[Change Package](#)

API answer OK

## VPN accounts

## Port Forwarding

## Addons

No Records Found