

IKEv2

- [Basic concepts IKEv2 EAP](#)
- [Technical requirements and installation](#)
- [Create a root certificate](#)
- [Import the root certificate](#)
- [Create a server certificate](#)
- [Advanced settings](#)
- [Enable IKEv2](#)

Basic concepts IKEv2 EAP

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

Since version 1.2 **PUQVPNCP** supports VPN protocol **IKEv2** implemented with [strongSwan](#)

IKEv2 is a protocol that allows you to create direct IPsec tunnels between a server and a client. **IPsec** provides encryption of network traffic in IKEv2 virtual private networks. **IKEv2** is natively supported on a number of platforms (OS X 10.11+, iOS 9.1+, Windows 10) without additional applications and easily resolves client connectivity issues.

For the protocol to work correctly, it is necessary to configure certificates for encryption; using the panel, this process is easy and comes down to pressing literally two buttons.

It is worth remembering that the main VPN protocol in the panel is WireGuard, and the **IKEv2** protocol is an additional protocol. This means that before using **IKEv2**, you must configure the WireGuard protocol, and then enable **IKEv2** support on each **WireGuard** interface on which you want to use **IKEv2**.

IKEv2 protocol available to clients

- **Android** (Official application from strongSwan)
- **iOS** (integrated client)
- **macOS** (integrated client)
- **Linux** (network-manager-strongswan)
- **Windows** (integrated client)

Due to the specifics of Microsoft's implementation of the client in Windows, there is a technical nuance that requires you to enter the password twice each time you connect.

Usage features IKEv2 EAP

- To use the **IKEv2 EAP** protocol, the client must have the domain name of the VPN server, username and password for authorization, and there is a need to import the root

certificate to authenticate the server certificate.

- The **IKEv2 EAP** protocol uses **IPSec** encryption to encrypt traffic between the client and the server, this imposes a certain load on the server and we recommend taking this into account when choosing server parameters.
- The data transfer rate in the case of rate limiting is lower than declared, due to the fact that all data packets are consistent with the headers that are required for IPSec encryption to work. *This is especially noticeable at low limits of 1-10 megabits.*
- Due to the technical aspects of VPN client rate limiting, the data rate limit will be taken from the outgoing traffic parameter, this parameter in **IKEv2** connections will be for incoming and outgoing traffic

Technical requirements and installation

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

Technical requirements

- Operating systems: Debian 9+ (amd64), Ubuntu 18+ (amd64)
- Real ip address on server interface
- Domain name for the server
- **PUQVPNCP v1.2**
- Installed packages **strongswan strongswan-pki libstrongswan-extra-plugins**

Installation

We issue all commands after logging into the SSH terminal window as the root user.

```
apt-get update  
apt-get upgrade  
reboot
```

```
apt-get install strongswan strongswan-pki libstrongswan-extra-plugins -y
```

Checking installed packages

Checking the strongSwan

```
dpkg -s strongswan-starter
```

Output should look similar to this:

```
Package: strongswan-starter
Status: install ok installed
Priority: optional
Section: net
Installed-Size: 610
Maintainer: strongSwan Maintainers <pkg-swan-devel@lists.alioth.debian.org>
Architecture: amd64
Source: strongswan
Version: 5.9.1-1+deb11u3
Depends: adduser, libstrongswan (= 5.9.1-1+deb11u3), lsb-base (>= 3.0-6), debconf (>= 0.5) |
debconf-2.0, libc6 (>= 2.27)
Pre-Depends: init-system-helpers (>= 1.54~)
Recommends: strongswan-charon
Conflicts: openswan
Conffiles:
 /etc/apparmor.d/usr.lib.ipsec.stroke 3ddc2d056db9435ba0d421678308bee3
 /etc/init.d/ipsec a7b2d9de5749ee0bebcd6ac3f9fee732
 /etc/ipsec.conf 01485a8658db82dd781f9229f4151661
 /etc/ipsec.secrets d8e074734da10d2ec7bcd9913263d717
 /etc/strongswan.d/charon/stroke.conf effb1b5bc46a7c849754fada75bae0d2
 /etc/strongswan.d/starter.conf 2ba2784c18e268e34cec179d90e38437
Description: strongSwan daemon starter and configuration file parser
 The strongSwan VPN suite uses the native IPsec stack in the standard
 Linux kernel. It supports both the IKEv1 and IKEv2 protocols.
 .
 The starter and the associated "ipsec" script control the charon daemon from
 the command line. It parses ipsec.conf and loads the configurations to the
 daemon.
Homepage: http://www.strongswan.org
```

Checking the IPsec Version

```
ipsec version
```

Output should look similar to this:

```
Linux strongSwan U5.9.1/K5.10.0-10-amd64
University of Applied Sciences Rapperswil, Switzerland
```

See 'ipsec --copyright' for copyright information.

Checking the pki

pki

Output should look similar to this:

```
strongSwan 5.9.1 PKI tool
loaded plugins: test-vectors pkcs11 tpm aes rc2 sha2 sha1 md5 mgf1 random x509 revocation
pubkey pkcs1 pkcs7 pkcs8 pkcs12 dnskey sshkey pem openssl gcrypt af-alg gmp curve25519 hmac
drbg curl
usage:
  pki --acert    (-z)  issue an attribute certificate
  pki --dn       (-d)  extract the subject DN of an X.509 certificate
  pki --gen      (-g)  generate a new private key
  pki --issue    (-i)  issue a certificate using a CA certificate and key
  pki --keyid    (-k)  calculate key identifiers of a key/certificate
  pki --pkcs12   (-u)  PKCS#12 functions
  pki --pkcs7    (-7)  PKCS#7 wrap/unwrap functions
  pki --print    (-a)  print a credential in a human readable form
  pki --pub      (-p)  extract the public key from a private key/certificate
  pki --req      (-r)  create a PKCS#10 certificate request
  pki --self     (-s)  create a self signed certificate
  pki --signcrl  (-c)  issue a CRL using a CA certificate and key
  pki --verify   (-v)  verify a certificate using the CA certificate
  pki --help     (-h)  show usage information
```

Create a root certificate

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

If you already have a root certificate ready, use certificate import. More in the [certificate import instructions](#) section.

Go to menu item **VPN servers -> IKEv2**

PUQVPNCP

? HELP ? ruslan (79.184.3.204) Logout

Dashboard

VPN servers

WireGuard

IKEv2

VPN accounts

Settings

About us

IKEv2

Save Advanced settings

IKEv2 Enabled
NO

Starter: **not running**

Charon: **not running**

ROOT certificate
Certificate not found

Common name*
TEST_CN

Organization*
TEST_O

Organizational Unit
TEST_OU

Locality
TEST_L

State or Province Name
TEST_S

Country Name
TEST_C

Generate ROOT certificate

SERVER certificate
Certificate not found

SERVER Domain*

ROOT certificate **Certificate not found**

Import ROOT certificate and key

CaCert

CaKey

SERVER certificate info **Certificate not found**

You need to fill in the required fields such as:

- Common name
- Organization

Then click the button **Generate ROOT certificate**

After these steps, the **root certificate and private key** will be generated.
Information about the certificate will be available in the same place.

PUQVPNCP

? HELP ?ruslan (79.184.3.204)Logout

DashboardVPN serversVPN accountsSettingsAbout us

IKEv2

SaveAdvanced settings

IKEv2 EnabledNO

Starter: not running

Charon: not running

ROOT certificate
certificate trusted, lifetimes valid

Delete ROOT certificate

SERVER certificate
Certificate failed

Server Domain*dev.softkeel.com

Server IP*77.87.125.200

Common name*dev.softkeel.com

Organization*dev.softkeel.com

Organizational UnitTEST_OU

LocalityTEST_L

State or Province NameTEST_S

Country NameTEST_S

Generate SERVER certificate

Successfully

ROOT certificate certificate trusted, lifetimes valid

Download CA certificateDownload CA key

subject: "CN=TEST_CN, O=TEST_O, OU=TEST_OU, L=TEST_L, S=TEST_S, C=TEST_C"

issuer: "CN=TEST_CN, O=TEST_O, OU=TEST_OU, L=TEST_L, S=TEST_S, C=TEST_C"

validity: not before Dec 13 10:13:17 2022, ok

not after Dec 10 10:13:17 2032, ok (expires in 3650 days)

serial: 25:c6:13:87:bd:f4:93:00

flags: CA CRLSign self-signed

subjkeyId: 0f:1b:3c:bf:78:91:27:b7:f0:3b:2a:d9:d6:a4:e1:d2:cd:8f:4e:45

pubkey: RSA 4096 bits

keyid: e9:a8:b9:45:fa:ee:5c:48:2e:e7:e5:8e:fa:33:46:4c:cb:8c:20:f4

subjkey: 0f:1b:3c:bf:78:91:27:b7:f0:3b:2a:d9:d6:a4:e1:d2:cd:8f:4e:45

SERVER certificate info Certificate failed

To download the root certificate and private key, you can use the buttons **Download CA certificate** and **Download CA key**

To remove the root certificate, use the **Delete ROOT certificate** button

Import the root certificate

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

If you don't have a root certificate ready, use the certificate generation option. More in the certificate generation instruction section.

Go to menu item **VPN servers -> IKEv2**

PUQVPNCP ? HELP ? ruslan (79.184.3.204) Logout

Dashboard

VPN servers

WireGuard

IKEv2

VPN accounts

Settings

About us

IKEv2

Save Advanced settings

IKEv2 Enabled
NO

Starter: **not running**

Charon: **not running**

ROOT certificate
Certificate not found

Common name*
TEST_CN

Organization*
TEST_O

Organizational Unit
TEST_OU

Locality
TEST_L

State or Province Name
TEST_S

Country Name
TEST_C

Generate ROOT certificate

SERVER certificate
Certificate not found

Server Domain*
dev.softkeel.com

Server IP*
77.87.125.200

ROOT certificate **Certificate not found**

Import ROOT certificate and key

CaCert

```
AsIZL4YdXBtwqmmoj13zg6URslhXhLPeqw+0iqevfpPZE1a1IgXTEY0Xnba1B5o6
eRUCLcU04dYjv3Eg55WKKN4uPkmm0u1JiWZp8g13FBK1hss/g1qkh3ZW5nMVDjTP
GFGrY+eHLzEgM8RRieJpU+Jq9mmezp/r0pC0EqoDILx0Uz05qm/c892D8ZZVqVKP
TQnuHppAYATGcPBIOHURi4ufCfiEzba0jK6KLLJMRtGZEuMgTTz77HSvfugP0/C
+OVNv5WcXf26AUh0HXS5wjFo6eLTwfYi4ZegT9rTOUfwJ/x3hYcNxfGfsofgdh
bL6jLJkygi+tjQAiJzNmngRddDpun195Emc9yPYWQT5gz6qwy6ExhAmyfZ6fnIir
zWIYcS+oUh+mTfeqjBHSUAPfFSl0iWfeshx+XN1oun0SiPaeA9YAb/eiKF+L/0Fl
wX59Ea2Mr559mRB0Dg90HMRMqG5K52gyY3V3tXg2/ZZNKeXML00Vbctf+h5kdsT4
C2wL60LmJPQCBkNr6X0fBA==
-----END CERTIFICATE-----
```

CaKey

```
sVtqhpwsk14XfiuEMz0AsmJsFAhbd6+LPisBR+us9cJ4TH8+rCgPY2sa179LmZaV
VhgRmy+7Hscb5c4rLwMbYiul9nP42c6KYEElz/A58i9TC9109T+qCVmLAhaG1fg
fwKI/pB7HRhKd4iPxkcc/zk4RcAcBGuldzQRkrMazxxCzvdtnLfxls06KNQrPFkb
Ij/h6c8Yy9jBwU1V43dGBHDDsg0XBEcggEAN5TJ4PFR8PRE4/YlWDRWwXLEnFfr
TRfktvWyeDRnaQsSB9NgqF+I60ymIGYrcmu4Ej2Ix3U0Vul+yjI4j+jxBdw+hs2H
9z9AwVJdPuz9XLLC/odQTEbdLTymQCqrxm3QTJLMBQ3hyRdY95+Yd1VnJnTcNt
SDM5UJ1DEc+Xxx0/Z7Akn8s0U30RUda989Pmb25p5CKcrF9/Juk/5bgf0z6cdz8G
bGKG2DwJ/09RVd0BLJwKl166LexRjMp8Bhksf6aAb5bImfGFJ0k19amX3gn+TSotS
0BR5u+9CGRwt+SPONcxcXqs60TYu+WkAv3V23+0N8a1n17qKJVYvYnZQ0==
-----END RSA PRIVATE KEY-----
```

SERVER certificate info **Certificate not found**

You need to fill in the fields intended for the root certificate and for the private key

- **CaCert**
- **CaKey**

To import the root certificate and private key, click the **Import ROOT certificate and key** button

After these steps, the **root certificate and private key** will be imported.
Information about the certificate will be available there.

PUQVPNCP

Dashboard

VPN servers

VPN accounts

Settings

About us

?

HELP?

ruslan (79.184.3.204)

Logout

Successfully

IKEv2

Save

Advanced settings

IKEv2 Enabled

NO

Starter: not running

Charon: not running

ROOT certificate

certificate trusted, lifetimes valid

Delete ROOT certificate

SERVER certificate

Certificate failed

Server Domain*

dev.softkeel.com

Server IP*

77.87.125.200

Common name*

dev.softkeel.com

Organization*

dev.softkeel.com

Organizational Unit

TEST_OU

ROOT certificate

certificate trusted, lifetimes valid

Download CA certificate

Download CA key

subject: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"

issuer: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"

validity: not before Dec 05 12:32:38 2022, ok

not after Dec 02 12:32:38 2032, ok (expires in 3642 days)

serial: 31:86:4b:df:10:2f:81:fc

flags: CA CRLSign self-signed

subjKeyId: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60

pubkey: RSA 4096 bits

keyid: 34:92:a9:5d:0f:00:a0:65:c0:39:2a:33:b1:b8:ed:92:e4:ce:2e:11

subjkey: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60

SERVER certificate info

Certificate failed

To download the root certificate and private key, you can use the buttons **Download CA certificate** and **Download CA key**

To remove the root certificate, use the **Delete ROOT certificate** button

Create a server certificate

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

Before creating a server certificate, you must create or import a root certificate.

Go to menu item **VPN servers -> IKEv2**

PUQVPNCP ? HELP ? ruslan (79.184.3.204) Logout

Dashboard

VPN servers

- WireGuard
- IKEv2**

VPN accounts

Settings

About us

IKEv2

[Save](#) [Advanced settings](#)

IKEv2 Enabled
NO

Starter: not running

Charon: not running

ROOT certificate
certificate trusted, lifetimes valid

[Delete ROOT certificate](#)

SERVER certificate
Certificate failed

Server Domain*
dev.softkeel.com

Server IP*
77.87.125.200

Common name*
dev.softkeel.com

Organization*
dev.softkeel.com

Organizational Unit
TEST_OU

Locality
TEST_L

State or Province Name
TEST_S

Country Name
TEST_S

[Generate SERVER certificate](#)

ROOT certificate certificate trusted, lifetimes valid

[Download CA certificate](#) [Download CA key](#)

```
subject: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"
issuer:  "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"
validity: not before Dec 05 12:32:38 2022, ok
          not after  Dec 02 12:32:38 2032, ok (expires in 3642 days)
serial:   31:86:4b:df:10:2f:81:fc
flags:    CA CRLSign self-signed
subjkeyId: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60
pubkey:    RSA 4096 bits
keyid:     34:92:a9:5d:0f:00:a0:65:c0:39:2a:33:b1:b8:ed:92:e4:ce:2e:11
subjkey:   56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60
```

SERVER certificate info Certificate failed

You need to fill in the required fields such as:

- **Server Domain**
- **Server IP**
- **Common name**
- **Organization**

Then click the button **Generate SERVER certificate**

After these steps, the **Server certificate and private key** will be generated.
Information about the certificate will be available in the same place.

PUQVPNCP

? HELP ?

ruslan (79.184.3.204)

Logout

Dashboard

VPN servers

VPN accounts

Settings

About us

IKEv2

Save Advanced settings

IKEv2 Enabled

YES

Starter: PID: 2106159

Charon: PID: 2106160

ROOT certificate

certificate trusted, lifetimes valid

Delete ROOT certificate

SERVER certificate

certificate trusted, lifetimes valid

Delete SERVER certificate

ROOT certificate certificate trusted, lifetimes valid

Download CA certificate Download CA key

subject: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"

issuer: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"

validity: not before Dec 05 12:32:38 2022, ok

not after Dec 02 12:32:38 2032, ok (expires in 3642 days)

serial: 31:86:4b:df:10:2f:81:fc

flags: CA CRLSign self-signed

subjkeyId: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60

pubkey: RSA 4096 bits

keyid: 34:92:a9:5d:0f:00:a0:65:c0:39:2a:33:b1:b8:ed:92:e4:ce:2e:11

subjkey: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60

SERVER certificate info certificate trusted, lifetimes valid

subject: "CN=dev.softkeel.com, O=dev.softkeel.com, OU=TEST OU, L=TEST_L, S=TEST_S, C=TEST_S"

issuer: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"

validity: not before Dec 13 10:37:44 2022, ok

not after Dec 12 10:37:44 2027, ok (expires in 1824 days)

serial: 10:a4:8f:79:21:ec:b2:e8

altNames: dev.softkeel.com, 77.87.125.200

flags: serverAuth ikeIntermediate

authkeyId: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60

subjkeyId: d6:47:a2:4f:8f:2b:78:66:a7:d2:c6:77:ae:fb:71:47:e2:9f:46:79

pubkey: RSA 4096 bits

keyid: 8c:3f:a3:99:b7:45:7a:ed:d9:cb:b4:1c:a5:8b:97:f6:a0:e3:ee:93

subjkey: d6:47:a2:4f:8f:2b:78:66:a7:d2:c6:77:ae:fb:71:47:e2:9f:46:79

To remove the server certificate, use the **Delete SERVER certificate** button

After a successful server certificate generation process, the IKEv2 server transitions to the enabled state.

IKEv2 Enabled

YES

Starter: PID: 2106159

Charon: PID: 2106160

Advanced settings

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

For more precise server settings, you can use Advanced settings

On this page you can customize the server to suit your needs.

Use the official strongSwan documentation for parameter information

<https://wiki.strongswan.org/projects/strongswan/wiki/IpsecConf>

Go to menu item **VPN servers** -> **IKEv2** Click on the **Advanced settings** button

PUQVPNCP ? HELP ? ruslan (79.184.3.204) Logout

Dashboard

VPN servers

WireGuard

IKEv2

VPN accounts

Settings

About us

IKEv2

Save Advanced settings

IKEv2 Enabled

YES

Starter: PID: 2106159

Charon: PID: 2106160

ROOT certificate
certificate trusted, lifetimes valid

Delete ROOT certificate

SERVER certificate
certificate trusted, lifetimes valid

Delete SERVER certificate

ROOT certificate certificate trusted, lifetimes valid

Download CA certificate Download CA key

subject: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"
issuer: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"
validity: not before Dec 05 12:32:38 2022, ok
not after Dec 02 12:32:38 2032, ok (expires in 3642 days)
serial: 31:86:4b:df:10:2f:81:fc
flags: CA CRLSign self-signed
subjkeyId: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60
pubkey: RSA 4096 bits
keyid: 34:92:a9:5d:0f:00:a0:65:c0:39:2a:33:b1:b8:ed:92:e4:ce:2e:11
subjkey: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60

SERVER certificate info certificate trusted, lifetimes valid

subject: "CN=dev.softkeel.com, O=dev.softkeel.com, OU=TEST_OU, L=TEST_L, S=TEST_S, C=TEST_S"
issuer: "CN=PUQ VPN, O=PUQ sp. z o.o., OU=PUQ VPN, L=Warszaw, C=PL"
validity: not before Dec 13 10:37:44 2022, ok
not after Dec 12 10:37:44 2027, ok (expires in 1824 days)
serial: 10:a4:8f:79:21:ec:b2:e8
altNames: dev.softkeel.com, 77.87.125.200
flags: serverAuth ikeIntermediate
authkeyId: 56:c2:cc:8f:a3:d4:c7:7c:36:31:b5:a4:23:ea:fa:4b:0e:d0:c8:60
subjkeyId: d6:47:a2:4f:8f:2b:78:66:a7:d2:c6:77:ae:fb:71:47:e2:9f:46:79
pubkey: RSA 4096 bits
keyid: 8c:3f:a3:99:b7:45:7a:ed:d9:cb:b4:1c:a5:0b:97:f6:a0:e3:ee:93
subjkey: d6:47:a2:4f:8f:2b:78:66:a7:d2:c6:77:ae:fb:71:47:e2:9f:46:79

Go to the IKEv2 Advanced settings page

Dashboard

VPN servers

VPN accounts

Settings

About us

IKEv2 / Advanced settings

Save and restart

Set default and reset

config setup

Uniqueids: no ▼
Strictcrpolicy: no ▼

charondebug

how much charon debugging output
should be logged

dmn: 0 (audit) ▼
mgr: 0 (audit) ▼
ike: 0 (audit) ▼
chd: 0 (audit) ▼
job: 0 (audit) ▼
cfg: 0 (audit) ▼
knl: 0 (audit) ▼
net: 0 (audit) ▼
asn: 0 (audit) ▼
enc: 0 (audit) ▼
lib: 0 (audit) ▼
esp: 0 (audit) ▼
tls: 0 (audit) ▼
tnc: 0 (audit) ▼
imc: 0 (audit) ▼
imv: 0 (audit) ▼
pts: 0 (audit) ▼

conn default

Authby: pubkey ▼
Closeaction: none ▼
Compress: no ▼
Dpddelay: 300
Dpdtimeout: 150
Inactivity: 86400
Esp: aes256-sha256,chac
Forceencaps: yes ▼
Fragmentation: yes ▼
Ike: aes256-sha1-modp1
Ikelifetime: 86400
Installpolicy: yes ▼
Keyingtries: 5
Lifetime: 3600
Margintime: 600
Mobike: yes ▼
Modeconfig: pull ▼
Reauth: yes ▼
Rekey: no ▼
Rekeyfuzz: 100
Type: tunnel ▼

In order to restore the default settings, click the **Set default and reset** button

Enable IKEv2

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

It is worth remembering that the main VPN protocol in the panel is **WireGuard**, and the **IKEv2** protocol is an additional protocol. This means that before using **IKEv2**, you must configure the **WireGuard** protocol, and then enable **IKEv2** support on each **WireGuard** interface on which you want to use **IKEv2**.

For the inclusion of the **IKEv2** protocol, switch to the configuration of the **WireGuard** user interface

To enable the **IKEv2** protocol, switch to the desired **WireGuard** interface.

PUQVPNCP

Dashboard

VPN servers

WireGuard

IKEv2

VPN accounts

Settings

About us

? HELP ?

ruslan (79.184.3.204)

Logout

Create

Find By Name

Peers IKEv2

Find By Interface

Find By Network

Internal Traffic Port

External IP

DNS

Peer Download

Peer Upload

Keepalive

1-4819	0	YES	wg7	10.0.6.1/24	YES	51827	77.87.125.209	8.8.8.8	1.1.1.1	3M	4M	5	Edit	Delete
1-4820	1	YES	wg8	10.0.7.1/24	YES	51828	77.87.125.200	8.8.8.8	1.1.1.1	3M	4M	0	Edit	Delete
77_87_125_209	12	YES	wg110	10.0.110.1/24	YES	51930	77.87.125.200	10.0.110.1	77.87.125.200	30M	30M	5	Edit	Delete
Default	34	YES	wg0	13.11.11.10/24	NO	51820	77.87.125.200	8.8.8.8	1.1.1.1	10M	5M	0	Edit	Delete

PUQVPNCP

? HELP ?

ruslan (79.184.3.204)

Logout

Dashboard

VPN servers

VPN accounts

Settings

About us

WireGuard / Edit WireGuard

Save

Set Bandwidth

Name

77.87.125.209

Interface name

wg110

Private key

UAI3hlyFmkQpo+bX2WbfbF3lys3Vyyd

Public key

xbrwVHxNZ8UsjHQyyzFwmOEy1UC+

IP/MASK

10.0.110.1/24

Internal Traffic

ACCEPT

Port

51930

External IP

77.87.125.200

DNS 1

10.0.110.1

DNS 2

77.87.125.200

Peers configuration

Bandwidth download (in M) per peer

30

Bandwidth upload (in M) per peer

30

Persistent Keepalive

5

0 - disabled

IKEv2 Enabled

YES

Public key

xbrwVHxNZ8UsjHQyyzFwmOEy1UC+vvKQ0FG/cLoJh2w=

Port

51930

Firewall Nat

10.0.110.0/24 -> 0.0.0.0/0 SNAT to:77.87.125.200 Pkt:53 Bytes:3312

Firewall Filter

10.0.110.0/24 -> 10.0.110.0/24 ACCEPT Pkt:0 Bytes:0

Traffic Control

qdisc htb 1: root refcnt 2 r2q 10 default 0 direct_packets_stat 9 direct_qlen 1000
Sent 5200 bytes 18 pkt (dropped 0, overlimits 0 requeues 0)
backlog 0b 0p requeues 0

Name	Status	IP	Download Upload	Mangle	
dimon_pc	Enable	10.0.110.5	30M 30M	324	<div>Edit</div>
dimon_telefon	Enable	10.0.110.7	30M 30M	110	<div>Edit</div>
dino_pc	Enable	10.0.110.6	30M 30M	538	<div>Edit</div>
dino_telefon	Enable	10.0.110.8	30M 30M	209	<div>Edit</div>
galia_pc	Enable	10.0.110.11	30M 30M	211	<div>Edit</div>
peer_101	Enable	10.0.110.9	30M 30M	207	<div>Edit</div>
peer_215	Enable	10.0.110.2	30M 30M	323	<div>Edit</div>
ruslan_dom_pc	Enable	10.0.110.4	30M	377	<div>Edit</div>

Set the **IKEv2 Enabled** option to **YES** to keep the value of the **Save** button