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

Revision #9
Created 13 December 2022 08:01:39 by Ruslan
Updated 16 October 2023 08:58:10 by Yuliia Noha