

# IPSec IKEv2

This VPN protocol is preferable and recommended for all usage scenarios. Instructions for setting up VPN connections on different operating systems are available [here](#).

---

## Setting up VPN Server in SafeUTM

1. To enable authorization by IKEv2, check the corresponding box **Connection via IKEv2/IPsec** in the Web interface section **Users -> VPN connections**.
2. Routes are transmitted to clients to your local networks automatically. To control access to networks, use **Firewall**.

3. Connection is possible only by domain name (not by IP address), therefore it is necessary to have a domain name that resolves to the IP address of the SafeUTM external interface. In the **Domain** field, this DNS name must be specified. It is necessary to issue a Let's Encrypt certificate.

## VPN connections ▾

Working

General

Fixed VPN IP addresses

### General settings

Network for VPN connections

192.168.0.0/16

☐ PPTP connection

☐ PPPoE connection

☒ IKEv2/IPSec Connection

Domain

safeutm.com

☐ SSTP Connection

Domain

Port

1443

☐ L2TP/IPSec Connection

PSK

.....



Save

4. For users who need to connect from outside via VPN, check the box **Allow remote access via VPN** in the user tree. The username and password specified here will be used to connect.

## IPsec IKEv2 Support in Client OS

- Microsoft **Windows 7** (2009). Requires installation of a Let's Encrypt root certificate

- Apple **MacOS X 10.11** "El Capitan" (2015)
  - Linux **NetworkManager plugin** (since 2008)
  - Google **Android 11** (2020). On older versions, you can use the **StrongSwan** application
  - Apple **iOS 9** (iPhone 4S) (2015)
  - **KeeneticOS 3.5**
  - Mikrotik
  - Cisco routers
- 

Revision #6

Created 22 August 2022 15:01:06 by Val Redman

Updated 12 October 2022 00:04:22 by Val Redman