

# L2TP IPsec

---

If possible, do not use this type of connection. This connection method can be unstable, has huge redundancy, has low performance, and does not support the strongest encryption. IPsec-IKEv2 is recommended instead.  
All modern operating systems support IKEv2, or there are applications for them.

---

## Configuring SafeUTM Global Settings

1. Go to **Users -> VPN connections.**
2. Check the box **L2TP/IPsec Connection.**
3. Enter the secret phrase (PSK key).
4. Click on **Save.**

## 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

.....



[PowerShell - script for configuring connections](#)

Save

## Configuring Users in SafeUTM

Allow the user to connect via VPN from the Internet by checking in the user settings (**Users -> User & Group -> General tab**) in the box **Allow remote access via VPN**.

L2TP IPsec clients behind the same NAT may experience connectivity issues if there is more than one client. [Instructions](#) can help solve the problem. We recommend using [IKEv2 IPSec](#) instead of L2TP IPsec.

---

## If a VPN connection is established, but you cannot access local network resources

Follow the recommendations in the article [Features of Routing and Access Organization](#).

---

Revision #7

Created 24 August 2022 21:14:53 by Val Redman

Updated 13 October 2022 14:39:19 by Val Redman