

Authorization by PPTP

Do not use this type of connection. This connection method is EXTREMELY insecure and has been left solely for compatibility with older solutions. Use **IPsec-IKEv2**.

Authorization by PPTP protocol involves authorization via a secure network tunnel between the user's network device and the SafeUTM internet gateway.

- A login/password bundle is used for user authorization and Active Directory users.
- To authenticate by PPTP protocol you need to assign an IP address to a network device, as well as configure a connection using the PPTP protocol, specifying the SafeUTM gateway IP address as the PPTP server address.

Upon successful authorization and establishment of a network tunnel, an additional IP address will automatically be assigned to the network device to gain access to internet resources. Using authorization by PPTP does not affect the ability of a network device to access LAN resources in any way.

Configuring SafeUTM Global Settings

To set up authorization by PPTP protocol you need to perform the following actions:

1. Go to **Users -> VPN connections**.

2. Select **PPTP Authorization** and click **Save**.

VPN connections ▾

Stopped

- 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

You can edit your login and password in the tab **Users -> User & Group** upon selection of a necessary user.

General Quota IP and MAC authorization

Username

Ryan Howard

Login

howard

Found in a group

Sales

Operations

Change password

Delete

Additional settings

☐ Deny access

☐ Allow remote access via VPN

Save

The user is assigned an IP address automatically from the pool of addresses for VPN configured in the section **Users -> VPN connections** (for example, 10.128.0.0/16).

In order to set up a **static** binding of addresses issued via VPN to certain users, go to **Users -> VPN connections -> Fixed VPN IP Addresses**, click "+ Add" and specify the intended user and IP address. An example of a fixed VPN IP address can be seen below:

VPN connections

Working

General

Fixed VPN IP addresses

Network for VPN connections: 192.168.0.0/16

+ Add

User	IP address	Operations
Ryan Howard	192.168.150.55	

When connecting from the internet, we recommend using IPsec IKEv2, L2TP IPsec, or SSTP for more reliable traffic encryption.

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**.

Possible Problems

- The provider from the gateway's side or from the connected client's side blocks the GRE protocol with which the PPTP connection takes place. In this case, when trying to connect to an external SafeUTM address, error 619 will occur. You can determine on which side the problem is by connecting from different places and from different providers. If it is possible to connect from some places, it means that the problem is on the side of those clients who cannot connect. When the provider is determined, you need to try to solve the problem with them or use **IPsec-IKEv2** or **SSTP**.
 - TCP port 1723 is blocked. You can check the port availability using standard network utilities such as telnet. If there is no connection to this port, then the tunnel cannot be established.
 - The user's username or password is incorrect. If this happens, it is often suggested to specify the domain when reconnecting. Try to create alphanumeric passwords, preferably in Latin, for your accounts. If the password is entered incorrectly more than 6 times, the user's IP address will be blocked by the password attack protection service.
 - If the connection is made with Windows OS, then in order for the packets to go through it, you need to make sure that the following box is checked in the connection settings **Use default gateway on the remote network** in the section **VPN connection properties -> Network tab -> Internet Protocol Version 4 (TCP/IPv4) properties -> Advanced**. If it is not necessary to route all packets to this interface, then the route must be written manually.
 - When the error **The connection was terminated by the remote computer** occurs, it is necessary to enable MPPE 128-bit support (In Windows this option is enabled by default) and only check MSCHAPV2 among authorization protocols.
-

If a VPN connection is established but it is not possible to access local network resources

Follow the recommendations in the article **Features of Routing and Access Organization**.

Revision #8

Created 22 August 2022 15:00:13 by Val Redman

Updated 12 October 2022 00:03:37 by Val Redman