Incoming pfSense connection to SafeUTM via IPsec

Following the steps in this article, you can combine pfSense and SafeUTM networks via IPsec using PSK.

> The combined LANs should not overlap!

Setting up SafeUTM

1. In the SafeUTM web interface, open tab **Services -> IPsec -> Devices.**
2. Add a new connection:

- **Connection name** – any.
- **Type** – incoming.
- **Authorization type** – PSK.
- **PSK** – specify the PSK key to be used for the connection.
- **Remote side identifier** – any.
- **Home local network** – Specify the SafeUTM local area network that will be visible from the pfSense subnet.
- **Remote local networks –** Specify the pfSense local network that will be visible from the SafeUTM subnet.

3. Save the created connection, then click on the "Enable" button.
4. Two configuration files will be generated on SafeUTM in the `/etc/strongswan/autogen/` folder. You need to go to the console and open the file of the type `device_<number>.peer` for editing.
5. From this file, you need to copy the value of the `rightid` line (approximate type –@#746573745f70736b). In the future, this value will need to be registered on pfSense.
6. The setup is complete, now let’s set up pfSense.

Setting up pfSense

1. In the pfSense web interface, go to tab VPN **-> IPsec –> Tunnels.**
2. Add a new connection:

- **Key Exchange version** – IKEv2.
- **Internet Protocol** – IPv4.
- **Interface** – Select the pfSense external interface that will be used to connect to SafeUTM.
- **Remote Gateway** – IP of the SafeUTM external interface.
- **Description** – any.
- **Authentication Method** – Mutual PSK.
- **My identifier and Peer identifier** – insert the value of the rightid line on SafeUTM here (see step 5 in setting up SafeUTM).
- **Pre-Shared Key** – insert the PSK key that was previously registered on SafeUTM.
- **Encryption Algorithm: For SafeUTM version 13.0 and later**, use the following parameters: Algorithm **-** AES256-GCM; **Key length -** 128 bit; **Hash -** SHA256; **DH Group -** Elliptic Curve 25519- 256.

All other values can be left by default.

3. Save the connection.
4. Click on the button **Show Phase 2 Entries** and add a new Phase 2. Specify here:

- **Encryption Algorithm**: **For SafeUTM version 13.0 and later**, use the following parameters: Algorithm **-** AES256-GCM; **Key length -** 128 bit; **Hash -** SHA256; **DH Group -** Elliptic Curve 25519- 256.
- **Local Network** – pfSense LAN which will be accessible from the SafeUTM subnet.
- **Remote Network** – SafeUTM LAN, which will be accessible from the pfSense subnet.

All other values can be left by default.

5. Save the connection.
6. Then you need to allow traffic to flow between the pfSense and SafeUTM local networks in the pfSense firewall (go to tab **Firewall -> Rules -> IPsec** and create two rules that allow traffic to flow between the SafeUTM and pfSense local networks).
Also, pay attention to the WAN firewall section – by default, incoming traffic from "gray" subnets is prohibited in it, so you need to remove this restriction.

7. Now go to tab **Status -> IPsec** (the created connection should appear there), and click on the Connect VPN button.

The setup is complete, the connection should be successfully established.

If the connection could not be established, and the pfSense firewall settings were made correctly, you should recreate the connection on UTM by specifying in the Key ID field the value that was specified in My identifier and Peer identifier for pfSense and try to connect again. No changes are required on the pfSense side.

Revision #5
Created 2022-08-27 15:44:45 UTC by Val Redman

Updated 2022-10-13 15:37:21 UTC by Val Redman