Outgoing pfSense Connection to SafeUTM via IPsec

Setting up SafeUTM

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

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

Setting up pfSense

1. In the pfSense web interface, go to tab **VPN > IPsec > Advanced Options,** and in the **Child SA Start Action** field select option **None (Responder Only)**.
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 external interface SafeUTM.
- **Description** - any.
- **Authentication Method –** Mutual PSK.
- **My identifier -** My IP address.
- **Peer identifier** - KeyID tag. Enter the ID of the remote party, i.e. SafeUTM.
- **Pre-Shared Key** – enter the PSK key.

- **Encryption Algorithm**:

```
Algorithm - AES256-GCM;
Key length - 128 bit;
Hash - SHA256;
DH Group - Elliptic Curve 25519-256.
```

3. Save the connection.
4. Click the button **Show Phase 2 Entries** and add a new Phase 2 and enter the following values:

- **Encryption Algorithm**:

```
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).
7. 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.
8. Now go to tab **Status -> IPsec** (the connection that was created 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 are correct, you should recreate the connection to UTM by specifying in the field **Key ID** the value specified in My identifier and Peer identifier of pfSense, and try to connect again. On the pfSense side, no changes are necessary.

Revision #7
Created 27 August 2022 15:48:15 by Val Redman
Updated 13 October 2022 15:37:42 by Val Redman