https://wiki.teltonika-networks.com/view/Setting_up_a_SSTP_tunnel_between_RUTX_and_Mikrotik_device

Setting up a SSTP tunnel between RUTX and Mikrotik device

□

Contents

Introduction

Secure Socket Tunneling Protocol (SSTP) is a VPN protocol designed to transport PPP traffic via a secure SSL/TLS channel.

This article provides a guide on how to configure **SSTP** tunnel between RUTXxx (client) and Mikrotik (server) routers.

Prerequisites

- One RUTXxx router of any type
- One Mikrotik router (this configuration example was created using Mikrotik rb750gr3)
- Server must have a Public Static or Public Dynamic IP address
- At least one end device (PC, Laptop) to configure the routers
- WinBox application

Configuration scheme

Mikrotik (server) configuration

Connect to MikroTik by using **WinBox** application and press **New Terminal**.

Prerequisite for any VPN server is to get certificates sorted. Procedure is exactly the same as for OpenVPN server setup with the slight difference being that common-name really matters. It must match either external IP or external host name – no exceptions. Use these commands to create certificates:

```
/certificate

add name=ca-template common-name=example.com  days-valid=3650 key-size=2048
key-usage=crl-sign,key-cert-sign

add name=server-template common-name=example.com  days-valid=3650 key-
size=2048 key-usage=digital-signature,key-encipherment,tls-server

add name=client-template common-name=client.example.com  days-valid=3650 key-
size=2048 key-usage=tls-client

sign ca-template name=ca-certificate

sign server-template name=server-certificate ca=ca-certificate

sign client-template name=client-certificate ca=ca-certificate
```

You will need to export root certificate, to do so use these commands:

```
/certificate

export-certificate ca-certificate export-passphrase=""
```

Instead of editing the default encrypted profile, we can create a new one. Assumption is that your MikroTik will also be a DNS server. And while at it, create secure user/password:

```
/ppp

profile add name="vpn-profile" use-encryption=yes local-address=192.168.8.250
dns-server=192.168.8.250 remote-address=vpn-pool

secret add name=user profile=vpn-profile password=password
```

Enable SSTP VPN server interface:

```
/interface sstp-server server

set enabled=yes default-profile=vpn-profile authentication=mschap2
certificate=server-certificate force-aes=yes pfs=yes
```

Do not forget to adjust firewall if necessary (TCP port 443):

```
/ip firewall filter

add chain=input protocol=tcp dst-port=443 action=accept place-before=0
comment="Allow SSTP"
```

Now go to **Files** and export the certificate by simply dragging it to your desktop.

RUTXxx (client) configuration

Access RUTxxx WebUI and go to **Service > VPN > SSTP**. There create a new configuration by writing configuration name and pressing **Add** button. It should appear after a few seconds. Then

press **Edit**.

Now apply the following configuration.

1. **Enable** Instance.
2. **Write Server IP address** (MikroTik public IP address).
3. Write **Username** (write the username which you created with this command: secret add name=**user** profile=vpn-profile password=password).
4. Write **Password** (write the password which you created with this command: secret add name=user profile=vpn-profile password=**password**).
5. Upload **CA cert** (the file which you exported from MikroTik).
6. Press **Save & apply**.

Testing configuration

Try to ping the remote VPN endpoint via **CLI** or **SSH** using this command:

```
ping 192.168.8.250
```