MikroTik RouterOS - SSTP VPN with certificates

Help and Support

Help Desk

Homepage

SERVER MANAGEMENT

Managed Service Provider | Network Solutions | Information Systems | IT Projects | www.serman.ee

Overview

This article is written by Server Management Inc. IT systems administrator Timo Puistaja - 19.04.2017, Tartu, Estonia.

Need help configuring your device? Contact us

info@serman.ee

Usually we need VPN to connect to our come or office network. VPN is a good way to get the resources securely. Mostly its used as a part of "Working from home" method - user connects to VPN and is able to access fileserver or other internal resources (intranet for example) in the office. The best part about VPN is that you dont need to expose your internal resources to the world - the users just connect via VPN.

SSTP VPN is a nice way because it works on port 443 (same as HTTPS) so it´s allowed everywhere! Downside of that is you cant configure any HTTPS websites to your office because port 443 will be already used, but thats only issue when you have 1 Public Static IP but usually you have more - 3 or 5 depending on your ISP.

For security we use so called 2 step-authentification - username+password and certificate. When the hacker finds out the username and pass, the certificate is still needed to make VPN connetion. Unfortunatley Mikrotik doesnt support CA + SERVER + CLIENT certificates

at the moment, so we cant make new Client certificate to every user, but using certificate already is good. For advanced certificate security you should consider using OpenVPN for example.

NB! Most of the MikroTik SSTP VPN tutorials on the internet tell you to create CA, SERVER and CLIENT ceritiface, but in the end they use CA certificate in the Clients computer. So making Server and Client certificates is pointless and probably going to be fixed soon in MikroTik.

Im going to generate needed Certificate in MikroTik menu *System - Certificates.*

More coming soon....

Need help configuring your device? Contact us
info@serman.ee

Last update: 22/05/2019