Setting up an IPsec tunnel between RUTX and Fortigate device

Setting up an IPsec tunnel between RUTX and Fortigate device

Introduction IPsec (Internet Protocol Security) is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet within a communication session. Operating at the network layer, IPsec protects and authenticates IP packets between devices like routers, firewalls, or hosts. Its primary use is to create VPN tunnels, enabling secure communication over insecure networks such as the Internet. An IPsec VPN tunnel ensures that data transmitted between two points is encrypted and secure from unauthorized access. This makes IPsec VPNs ideal for connecting remote offices, enabling secure remote access, and linking different network parts. IPsec provides data confidentiality through encryption, data integrity via cryptographic checksums, and data origin authentication. Its versatility allows it to be configured for various security needs, using either transport mode for end-to-end security or tunnel mode for site-to-site VPNs. Tunnel mode encrypts the entire IP packet and encapsulates it in a new IP packet with new headers. Despite its robust security, IPsec can be complex to configure and manage, requiring a solid understanding of networking and cryptography. When properly implemented, IPsec VPNs offer a highly secure method for transmitting sensitive information, making them essential in modern network security. Prerequisites • One RUTXxx router of any type • One Fortigate router • At least one router must have a Public Static or Public Dynamic IP address • At least one end device (PC, Laptop, Tablet, Smartphone) to configure the routers • (Optional) A second end device to configure and test remote LAN access

Configuration scheme

RUTX configuration From the WebUI, go to Services > VPN > IPsec. Enter a name you wish for your IPsec instance, click ADD and when it appears in IPsec Configuration field, click edit.

Then apply the configuration presented below.

1. Enable instance. 2. Add Remote endpoint (the Public IP address of the Fortigate router). 3. Write Pre shared key (a shared password used for authentication between the peers. The value of this field must match on both instances). 4. Set Local identifier (device identifier for IPsec tunnel, write RUTX LAN IP address). 5. Set Remote identifier (remote device identifier for IPsec tunnel, write Fortigate LAN IP address). 6. Write Local subnet (an IP address/Subnet mask of the router on which the IPsec instance is configured). 7. Write Remote subnet (LAN IP address/Subnet mask of the Fortigate router).

Below configuration needs to be done on Advanced Settings.

Next step in configuring IPsec instance is Phase settings. In this example, Encryption Algorithm set to AES 128 and DH Group is set to MODP2048. Match this configuration in both Phase 1 and Phase 2 settings.

When you're finished with the configuration, click Save&Apply button and then you will be prompted back to IPsec window.

Fortigate configuration From the WebUI of the Fortigate router, go to System window and do the below changes.

1. Open System Settings.. 2. Click Feature Visibility section. 3. Enable Multiple Interface Policies.

`From the VPN > IPsec window. Give your desired name and choose Custom on the Template Type window.`

Choose Static IP Address for the Remote Gateway and write the Public IP of the Teltonika Router in the IP Address section.

Choose Pre-shared Key for Authentication method and write the password.

Leave the other settings as default.

After IPsec configuration is done, click Save.

From the WebUI of the Fortigate Router go to Network > Static Routes and add Teltonika Router’s subnet mask as a destination.

And lastly, Firewall Policies needs to be updated on the Fortigate Router. Below changes needs to be done.

Testing the setup If you've followed all the steps presented above, your configuration should be finished. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. In order to test an IPsec connection, login to the RUTX WebUI and go to Services → CLI. Login with user name: root and the router's admin password. From there you should

then be able to ping the opposite instance's LAN IP address. To use a ping command, type ping <ip_address> and press the "Enter" key on your keyboard: