https://wiki.teltonika-networks.com/view/Setting_up_a_Site-to-Site_IPsec_Tunnel_between_Teltonika_Networks_and_Microsoft_Azure

Setting up a Site-to-Site IPsec Tunnel between Teltonika Networks and Microsoft Azure

The information on this page is updated in accordance with the **00.07.07.1** firmware version .

□

Contents

Introduction

A site-to-site connection using an IPsec tunnel between Teltonika devices and an Azure Virtual Network Gateway is a secure method to link two separate networks over the internet. This setup ensures that data transmitted between the on-premises network, managed by Teltonika routers, and the Azure cloud environment is encrypted and secure.

If You have trouble seeing any of the settings, be sure to enable "**Advanced mode**"

Topology

Prerequisite

The user needs an Azure account with an active subscription.

Azure Platform

Create a VPN Gateway on the Azure Platform

Log into the Azure portal, search for "Virtual Network Gateways" and click on **Create**.

Use the information and images below as reference to complete the settings:

Projects details

- **Suscription:** Your suscription.
- **Resource Group:** Your resource group.

Instance details

- **Name:** VNet1GW.
- **Region:** Your prefered Region.
- **Gateway type:** VPN.
- **SKU:** VpnGW2AZ.
- **Generation:** Generation2 (mandatory).
- **Virtual Network:** Select or create a new one.
- **Gateway Subnet Address Range:** 10.1.1.0/24 (if using Virtual Network default configuration).

Public IP address

- **Public IP address:** Create new.
- **Public IP address name:** Vnet1GWpip.
- **Assigment:** Static.
- **Enable active-active mode:** Disabled.
- **Configure BGP:** Disabled.

Create a Virtual Network

In case you do not have previously created a virtual network, click on the blue URL link to create one and use the default settings as shown in the image below:

Finish the VPN gateway configuration

After finishing the previous configuration, you can continue with the tags. This section is not mandatory; therefore, we left it as default and clicked on **Review + create** to check that the network gateway has the parameters shown below, and then click on the **Create** button to finish the configuration.

Create a local network Gateway

In the search bar, look for "Local Network Gateways" and click on **Create**.

Fill in the configuration fields accordingly and add the remote router address space (LAN network) and the FQDN if the router does not have a static public IP address on its WAN interface.

Projects details

- **Suscription:** Your suscription.
- **Resource Group:** Your resource group.

Instance details

- **Region:** Your prefered Region.
- **Name:** toRegion.
- **Endpoint:** FQDN.
- **FQDN:** The fully qualified domain name of the router's remote connection.
- **Address Space:** The router's LAN network(s)
- **Configure BGP settings:** No.

Verify the configuration and click on **Create** to finish.

Create a connection

Search for "Connections" and create a new one:

Complete the connection settings using the information and images below as reference:

Projects details

- **Suscription:** Your suscription.
- **Resource Group:** Your resource group.

Instance details

- **Connection type:** Site-to-Site (IPsec).
- **Name:** SiteToSite.
- **Region:** Your prefered Region (It must match the one selected above).

Virtual network Gateway

- **Virtual network gateway:** Vnet1GW.
- **Local network gateway:** toRegion.
- **Shared Key(PSK):** Your Pre-shared key (It must match the one in the router IPsec configuration).
- **Use Azure Private IP Address:** Unchecked.
- **IPsec/IKE policy:** Custom.
- **IKE Phase 1:** Encryption: AES256 , Integrity/PRF: SHA1 , DH Group: DHGroup2.
- **IKE Phase 2:** Encryption: AES256 , IPsec Integrity: SHA1 , PFS Group: None.
- **IPsec SA lifetime in KiloBytes:** 0.
- **IPsec SA lifetime in seconds:** 10800.
- **Use policy based traffic selector:** Disable.
- **DPD timeout in seconds:** 45.
- **Connection mode** Default or ResponderOnly.

NAT Rules Associations

- **Ingress NAT Rules:** 0 selected.
- **Egress NAT Rules:** 0 selected.

Note: You can use different crypto proposals; however, you must ensure that they match on the router.

Click on **Review + Create**, then verify the configuration and click on **Create** to finish.

Teltonika Device Configuration

DDNS configuration

Log into the router via WebUI.

In case you don’t have a static public IP address on the WAN interface, you can enable the Dynamic DNS service as explained here: DDNS Configuration Examples

Path: WebUI > Services > Dynamic DNS.

Note: On devices other than the RUTX series, you will need to download the DDNS service from the Package Manager.

After finishing the configuration, you should get the public IP address of the created domain.

IPsec configuration

Locate the following path: **WebUI > Services > IPsec** ; and a new instance:

Instance details

- **Enable:** On.
- **Authentication method:** Pre-shared key.
- **Pre-shared key:** Your pre-shared key (must match the pre-shared key configured in the Azure platform's IPsec settings).
- **Local Identifier:** Empty.
- **Remote Identifier:** Empty.

General Settings

- **Mode:** Start.
- **Type:** Tunnel.
- **Default route:** off.
- **Local Subnet:** The router local network(s).
- **Remote Subnet:** The virtual network you want to access remotely hosted in your virtual environment in Azure.
- **Key Exchange:** IKEv2

Advanced Settings

- **Dead peer detection:** On.
- **DPD action:** Restart.
- **DPD delay:** 45.
- **Leave all other advanced settings as default..**

Proposal Settings

- **Phase 1:** Encryption: AES256 , Authentication: SHA1 , DH Group: MODP1024.
- **Phase 2:** Encryption: AES256 , Hash: SHA1 , PFS Group: No PFS.
- **Force crypto Proposal:** off.
- **lifetimes:** Empty.

Note: in this example, we use DH Group equals to MODP1024 which is the same to Group 2 selected on the Azure platform.

Check Site to Site Communication

If you followed the configuration steps, you should see that the Site to Site connection has been successfully established.

You can also check in the Azure platform that the connection has been established:

Check connectivity between the router LAN and a VM inside the Azure virtual network you may have:

Test connectivity from a host in the router’s LAN to the VM:

Connect to the VM in Azure, test connectivity to the Router’s LAN interface.

See Also

- Dynamic DNS - general information on the DDNS service.
- DDNS Configuration Examples - additional examples for different DDNS providers.

External links

- https://www.noip.com
- https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal