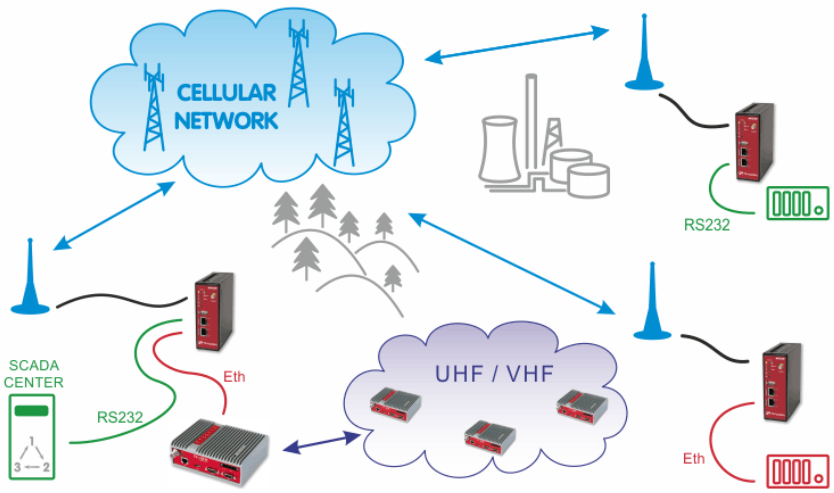
RACOM
RADIO DATA NETWORKS

Application notes



M!DGE/MG102i - VPN Configuration

version 1.3
2021-04-09

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

Table of Contents

Introduction

M!DGE/MG102i units support several VPN types. Based on your application, number of clients, topology and other factors, the most suitable option should be selected.

RACOM recommends using either **OpenVPN** or **IPsec**. Both are very secure and robust solutions. IPsec is very common for point-to-point tunneling or it's typically used with some bigger VPN concentrator such as CISCO. OpenVPN is very common for interconnecting large environments and M!DGE/MG102i can serve as the VPN server for up to 25 clients. If higher number of clients is required, a special VPN concentrator needs to be installed.

Note

A special software feature key (Server extension) must be ordered to provide the support for 25 OpenVPN clients. Our routers support up to 10 OpenVPN clients without this key.

PPTP is a very common solution, usually for connecting Windows PC to the M!DGE/MG102i, but should be used only if other options are not possible. The PPTP security algorithms have already been broken and it's not as secure as IPsec or OpenVPN. **GRE** tunnel is useful for routing subnets among the units, because it also creates a special “greX” interface and it's possible to define as many routes as needed. Keep in mind that GRE is not encrypted, the packets are just wrapped into the GRE header and they can be easily eavesdropped. These notes are not issues of RACOM, but they come from general implementation of those protocols.

Important

Refer to our *Introduction application note*[1] for APN and IP differences obtained from your mobile operator. In general, VPN or any other service can work over Mobile connection smoothly, but take into account several "must-have" requirements. In case of public APN, the VPN server must have a public IP address. It can be a static IP (optimal solution) or dynamic IP, but in such a case Dynamic DNS service has to be configured and set in M!DGE2 and third party service provider. All the VPN clients can have dynamic IP addresses, but the server hast to be accessible from the Internet - i.e. it has to have a public IP address. Another option is to have a closed and private APN (no Internet access) in which all your devices can "see" each other. Talk to your operator about services and options they can offer you. All the examples within this application note use our private RACOM APN.

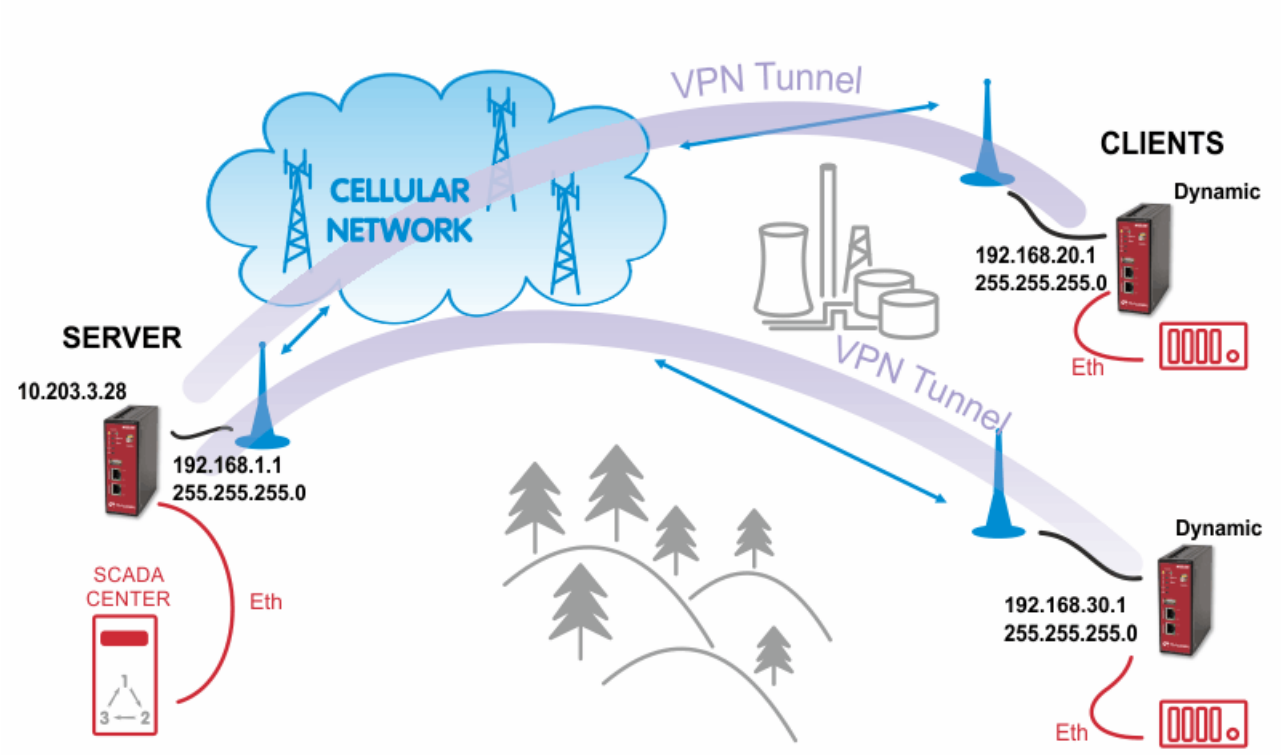
See the following examples for details.

[1] https://www.racom.eu/download/hw/midge/free/eng/1_app/midge-app-intro-en.pdf

1. OpenVPN

The OpenVPN tunnel can be operated in two modes – either in the Routed mode or in the Bridged mode. If the VPN network consists of one subnet only, the bridged mode should be used. The whole network seems to be just bridged within the local switches. If you need to interconnect several networks/subnets, you need to utilize the Routed mode. See the detailed examples below.

1.1. OpenVPN – Routed mode



1.1.1. OpenVPN Server Configuration

The first step is configuring the Server. Make sure you are connected to the cellular network and so you have the WAN interface active.

Note

You can also use the Ethernet interface as a WAN interface.

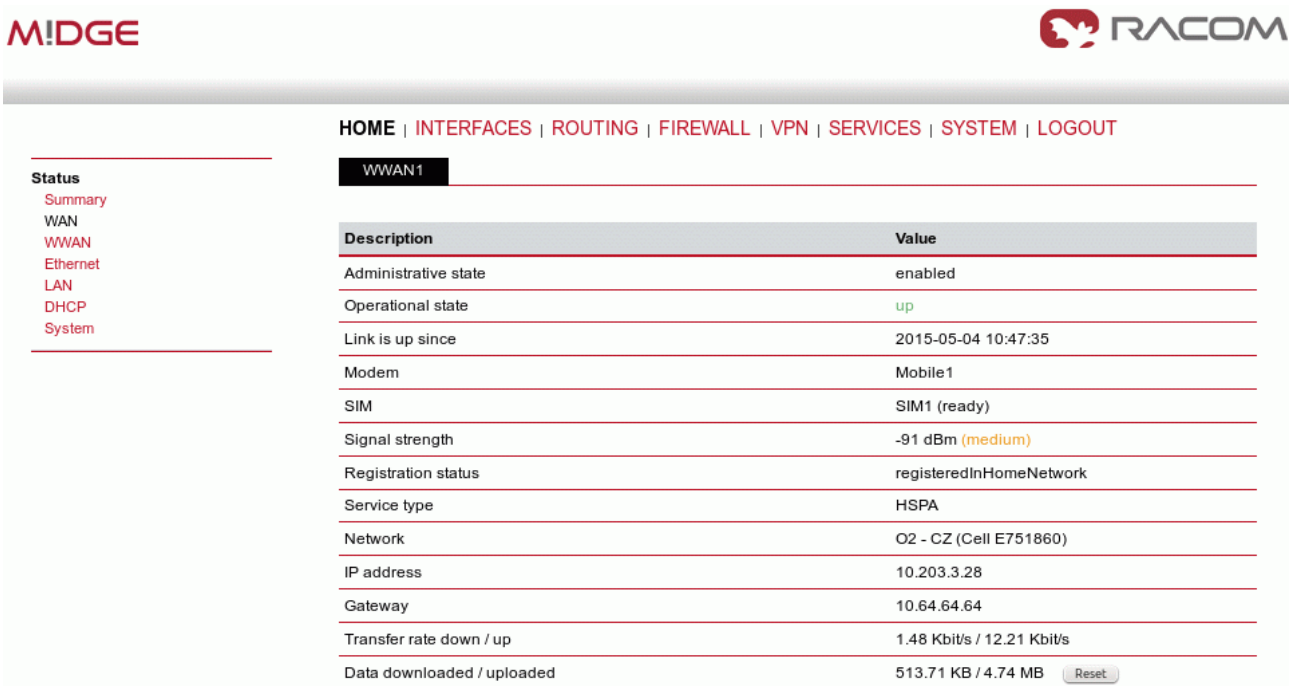


Fig. 1.1: Server WAN status

With OpenVPN, it is required to have a correct time. One possibility is to set the NTP server synchronization. Go to the **SYSTEM – Time & Region** menu and configure the unit with a reachable NTP server.

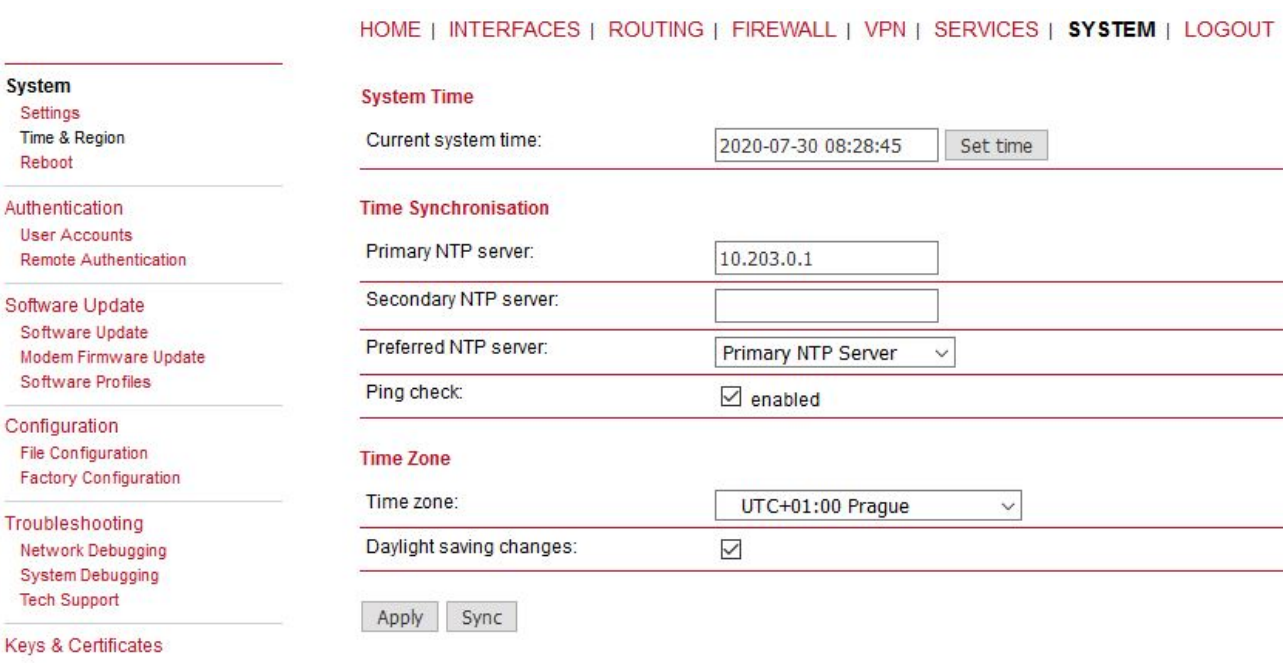


Fig. 1.2: NTP synchronization

When you are successfully connected and the time is correct, start configuring the OpenVPN server. The default values can be used or read the manual for parameter descriptions.

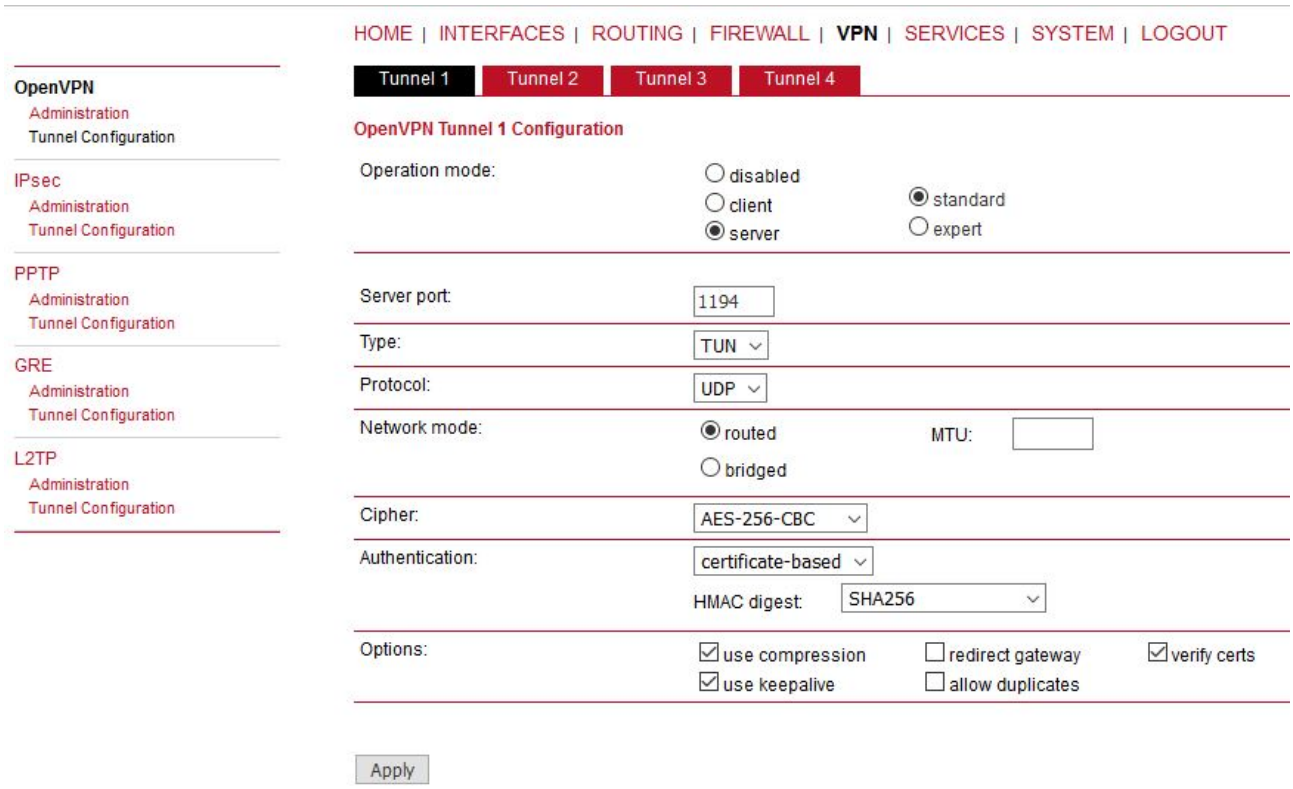


Fig. 1.3: OpenVPN Server Configuration

After applying the configuration, the certificates need to be created. Click on the given link or go to the **SYSTEM – Keys & Certificates** menu.

Fig. 1.4: Missing certificates

In this menu, create the certificates. By default, the Action is set to “generate locally”, but you can also upload the certificates or enroll them via SCEP.

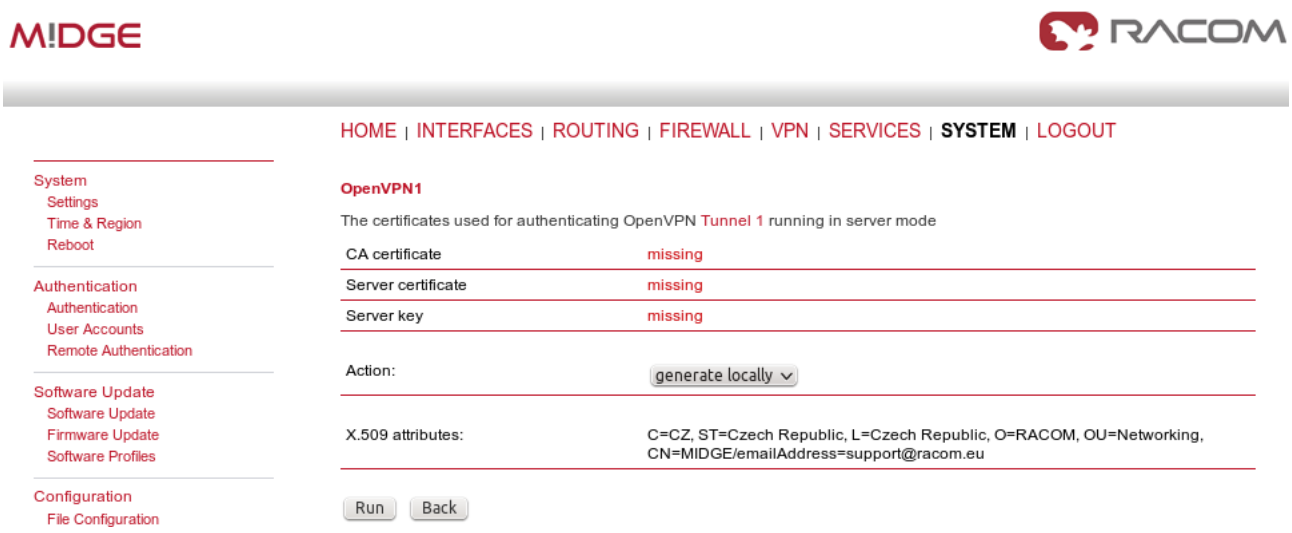


Fig. 1.5: Creating certificates

Important

The Passphrase must be configured first in the SYSTEM – Keys & Certificates – Configuration menu. The Certificates can be configured to contain specific Organization, Country, e-mail, etc.

See the following example where the certificates are created.

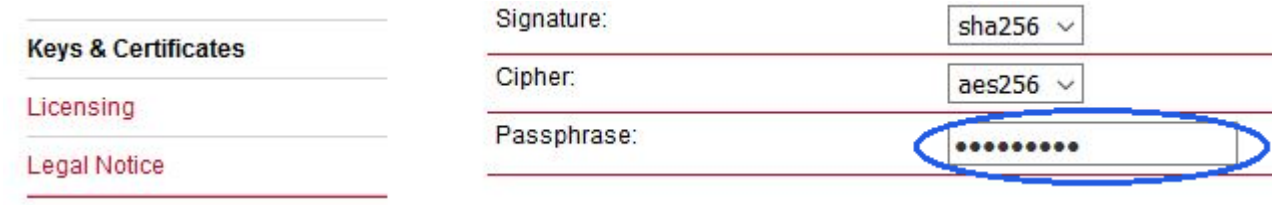


Fig. 1.6: Configuration of Certificates' passphrase

In the same menu, you can generate or upload certificates for individual clients or go back to the OpenVPN – Client Management menu, configure required hosts and the certificates will be locally created automatically after downloading the Expert mode file.

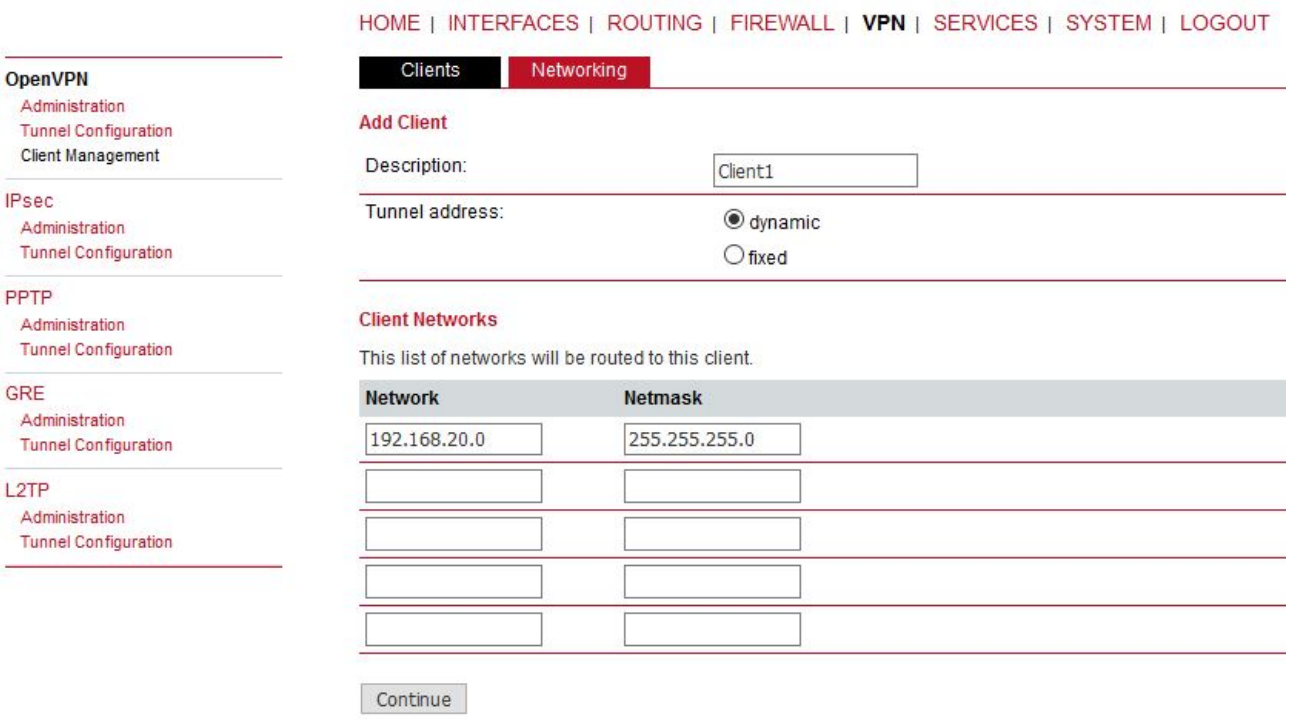


Fig. 1.7: OpenVPN Client

In the Clients menu, you can define the clients' networks or leave it empty. Each client can have its own network/mask. In our example, configure the network 192.168.20.0/24 for midge1 and 192.168.30.0/24 for midge2. The tunnel address can be dynamic.

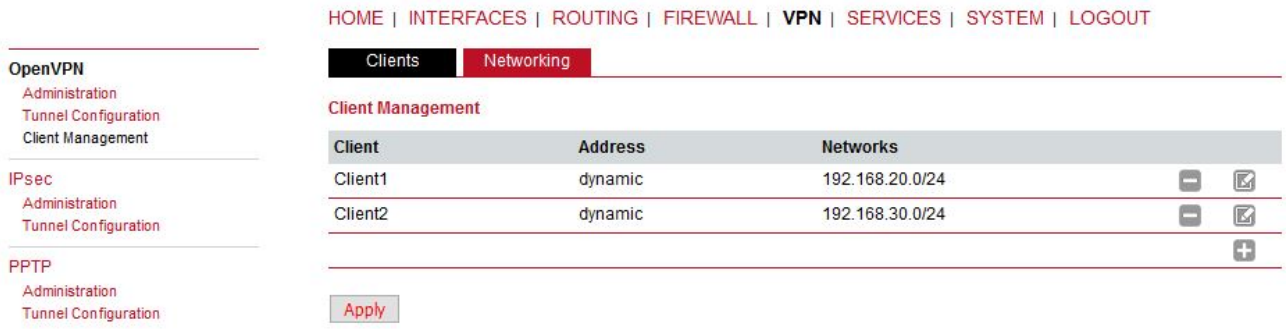


Fig. 1.8: OpenVPN clients list

In the Networking menu, you can add networks which will be pushed into all clients' Routing menu so that matching packets will be routed back to the server. Routing between the clients can be enabled too. Fill in the Server's IP subnet 192.168.1.0/24.

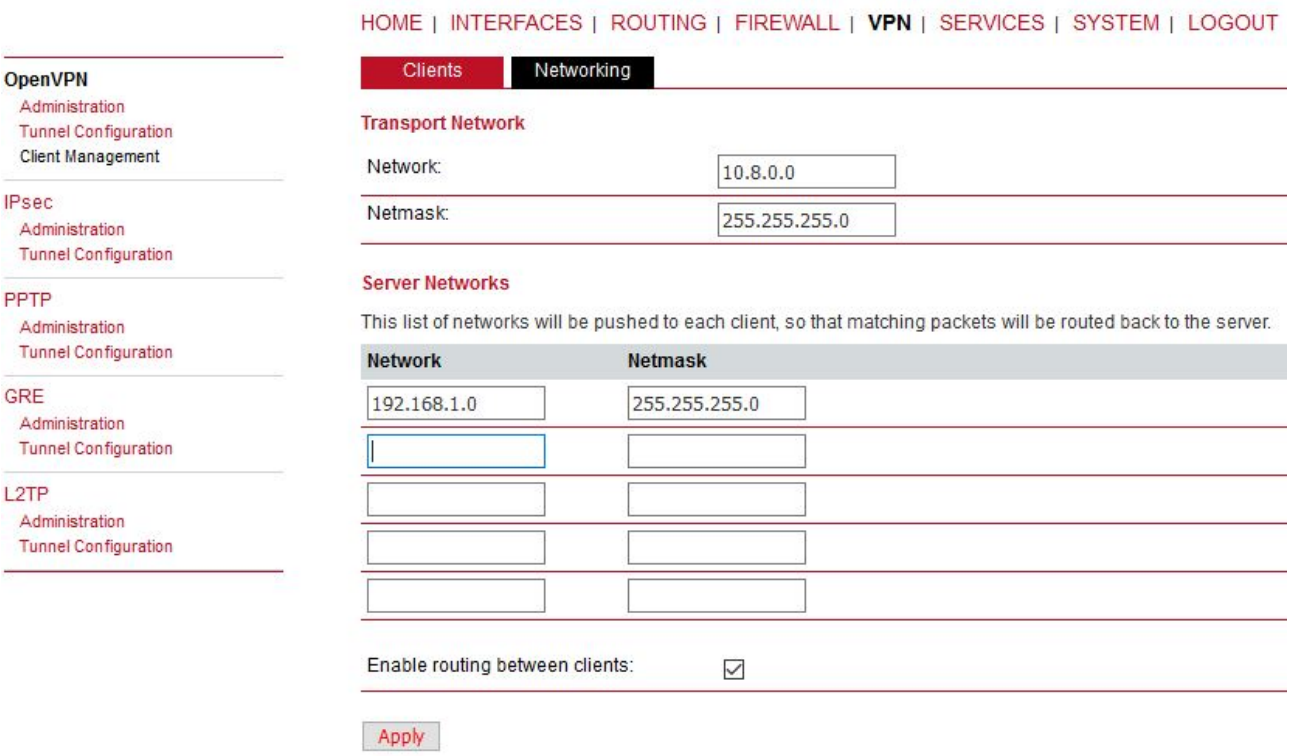


Fig. 1.9: OpenVPN Routes (Server's subnet)

Another step is to download the Expert file for all the configured clients. Fill in the server's WAN IP address.

Note

The IP address depends on your APN configuration. If you use DynamicDNS service with a dynamic public IP address, fill the DNS hostname here and not a current IP address.

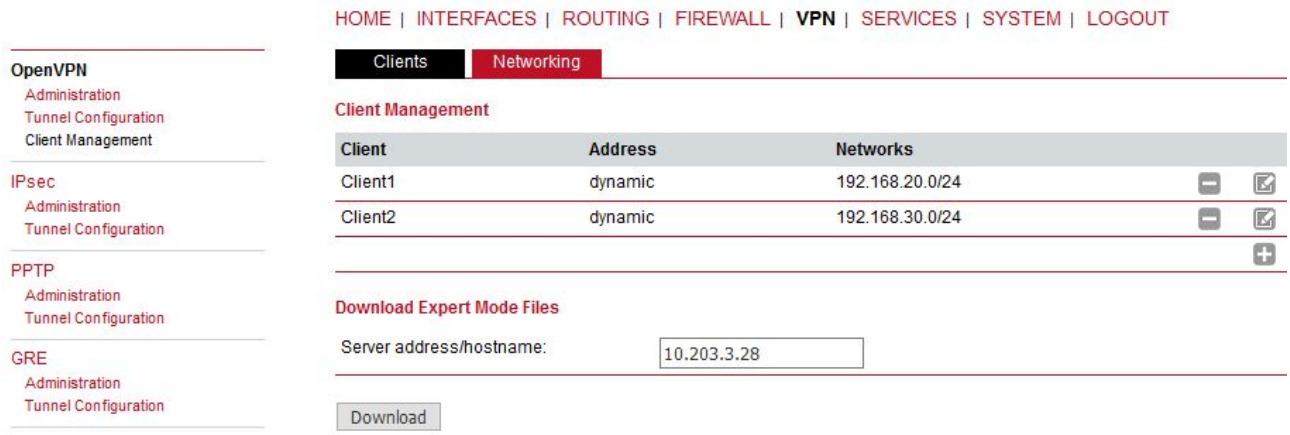


Fig. 1.10: OpenVPN downloading Expert file

The last step is Enabling the OpenVPN server.

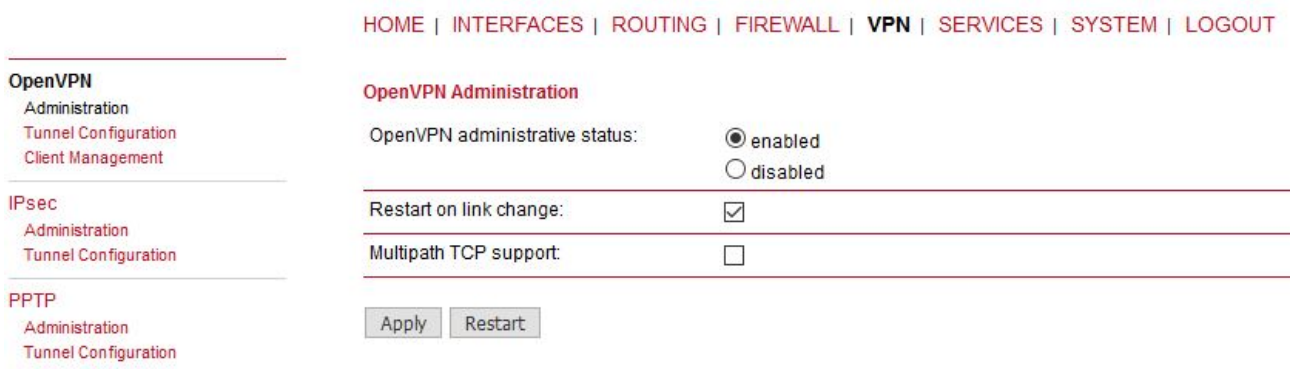


Fig. 1.11: Enabling OpenVPN server

The OpenVPN server configuration is now complete. The server is running and listening for all VPN clients.

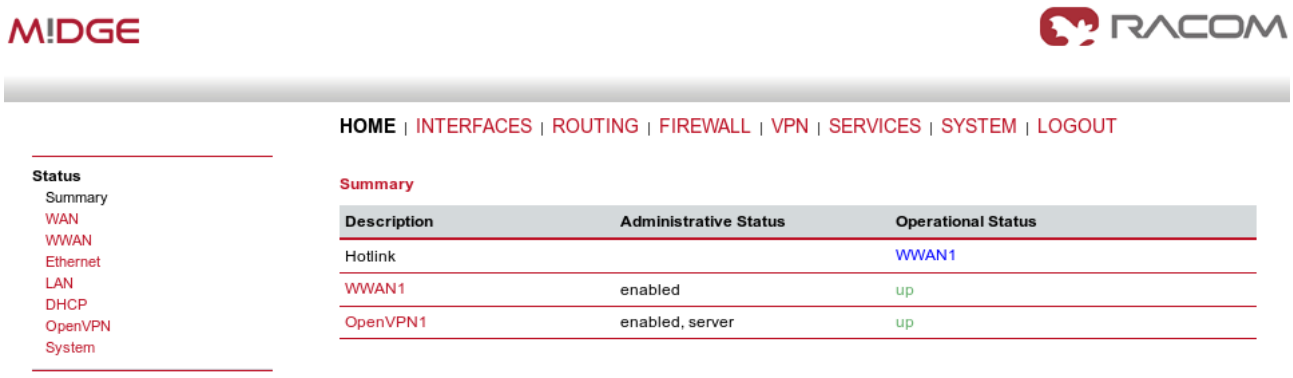


Fig. 1.12: OpenVPN server is running

1.1.2. OpenVPN Client Configuration

The easiest way how to configure the client is to upload the Expert file downloaded from the server. Unzip the file to obtain Expert files for individual clients.

Configure the APN on both clients and set the correct NTP server for time synchronization. Afterwards, go to the OpenVPN menu and upload the expert file.

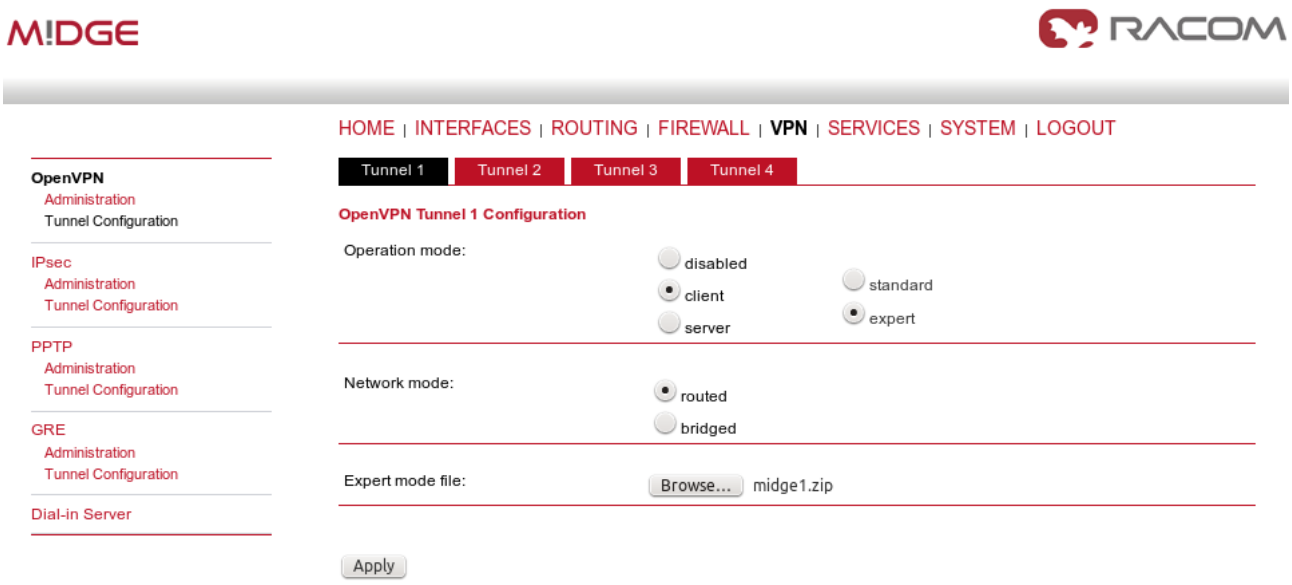


Fig. 1.13: OpenVPN client configuration (midge1)

The Expert mode file should be installed. Now, enable the OpenVPN client and check the VPN status.

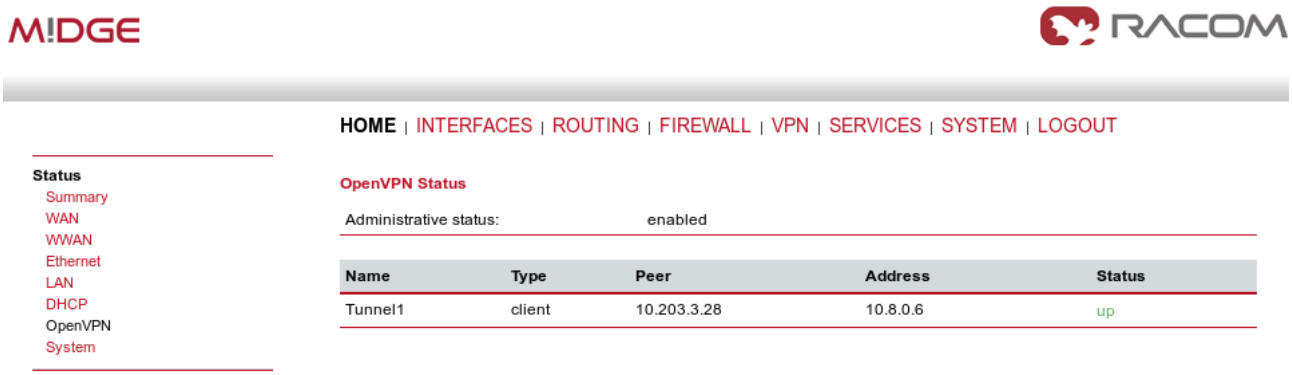


Fig. 1.14: OpenVPN client – connected successfully

1.1.3. Testing OpenVPN tunnel

On both the client and the server, you should see the updated Routing menu. There is a new TUN interface. See the Server's Routing menu.

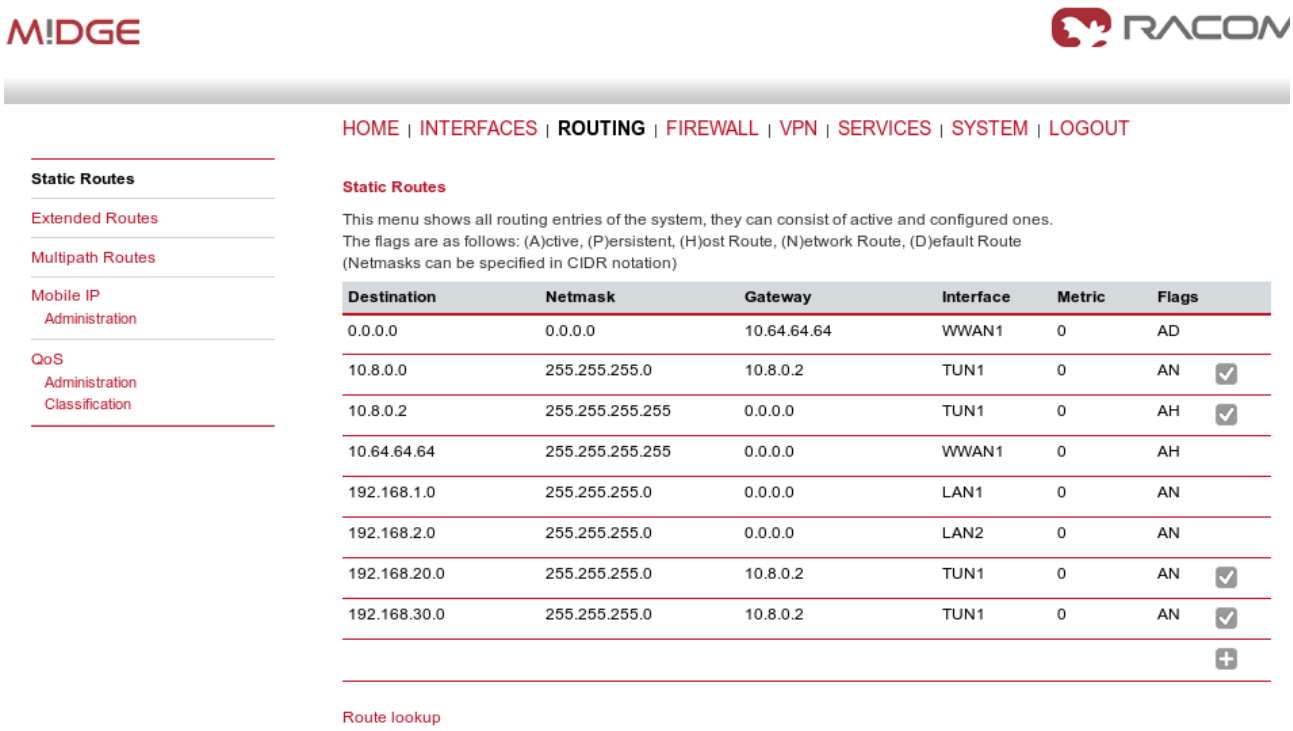


Fig. 1.15: OpenVPN Routing

You can define new routes in the Routing menu manually, just choose the correct TUN interface. Note that adding routes this way is not possible with the Bridged tunnel type or with IPsec.

Check the reachability of remote network by issuing the PING command from the SYSTEM – Troubleshooting – Network Debugging menu. Ping the remote M!DGE Ethernet IP address or you can even try to ping a device behind the remote M!DGE. In the example below, a ping from the server to the client is displayed.

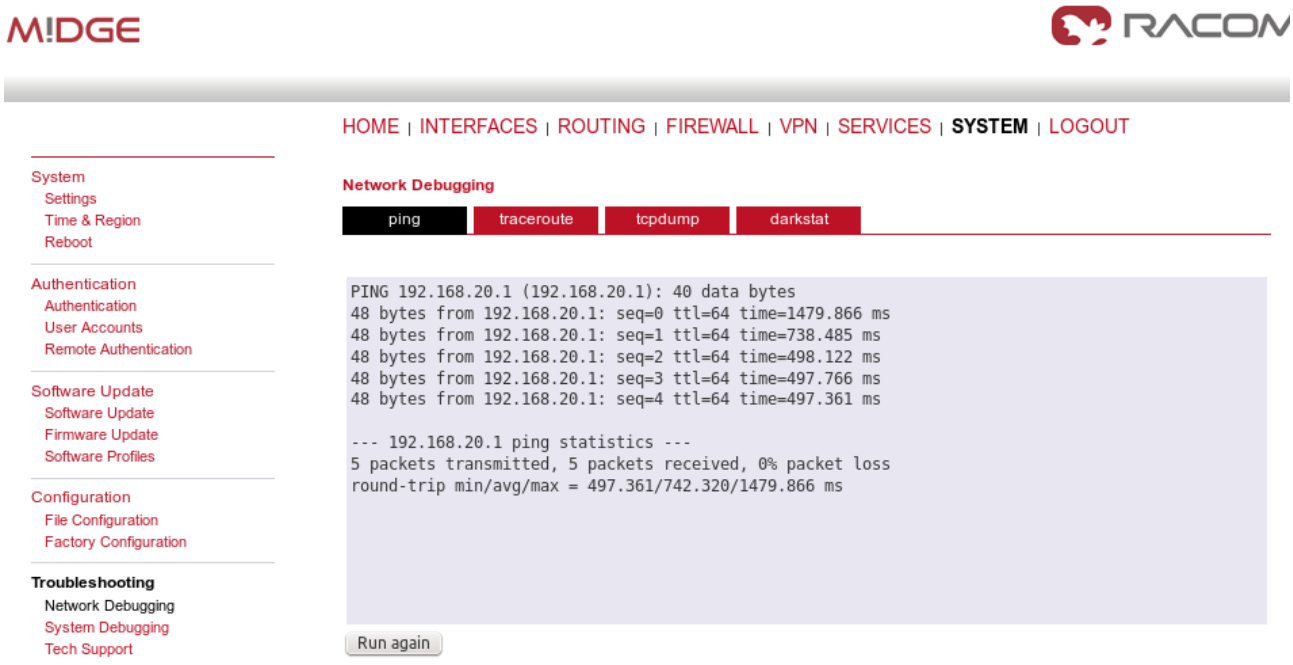


Fig. 1.16: Checking OpenVPN tunnel via ping

1.2. OpenVPN – Bridged mode

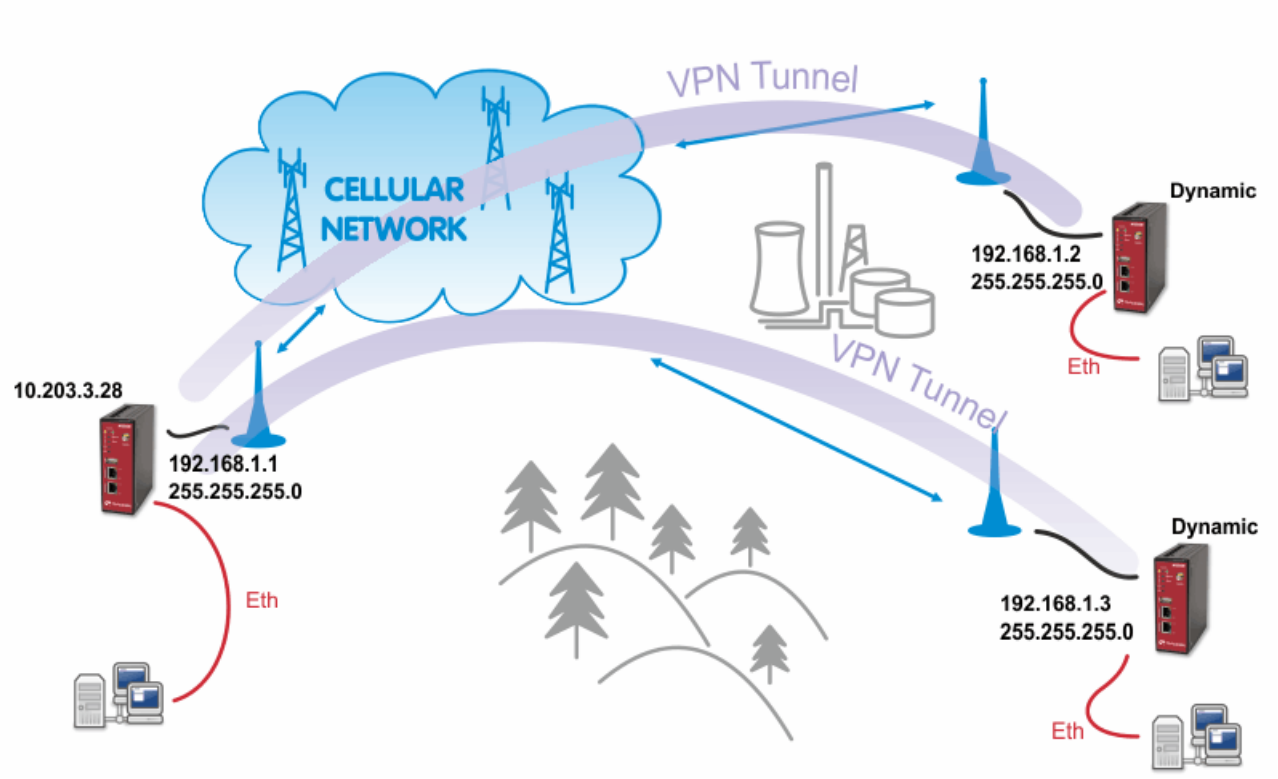


Fig. 1.17: OpenVPN Bridged mode

The Bridge type of the OpenVPN tunnel used when you need to interconnect the devices within one IP subnet so we create “transparent” network. In our example, we will use the 192.168.1.0/24 subnet. The center has the IP address 192.168.1.1. The clients have 192.168.1.2 and .1.3. You can attach any device (e.g. notebook) to any M!DGE so you can test the reachability of not just M!DGE units, but even the connected devices.

Note

Make sure you have the correct IP addresses on all M!DGE units (INTERFACES – Ethernet – IP settings).

1.2.1. OpenVPN Server Configuration

The configuration is very similar to the previous example. In the Tunnel configuration, set the Type to “TAP”, Network mode to “bridged” and select the correct LAN interface.

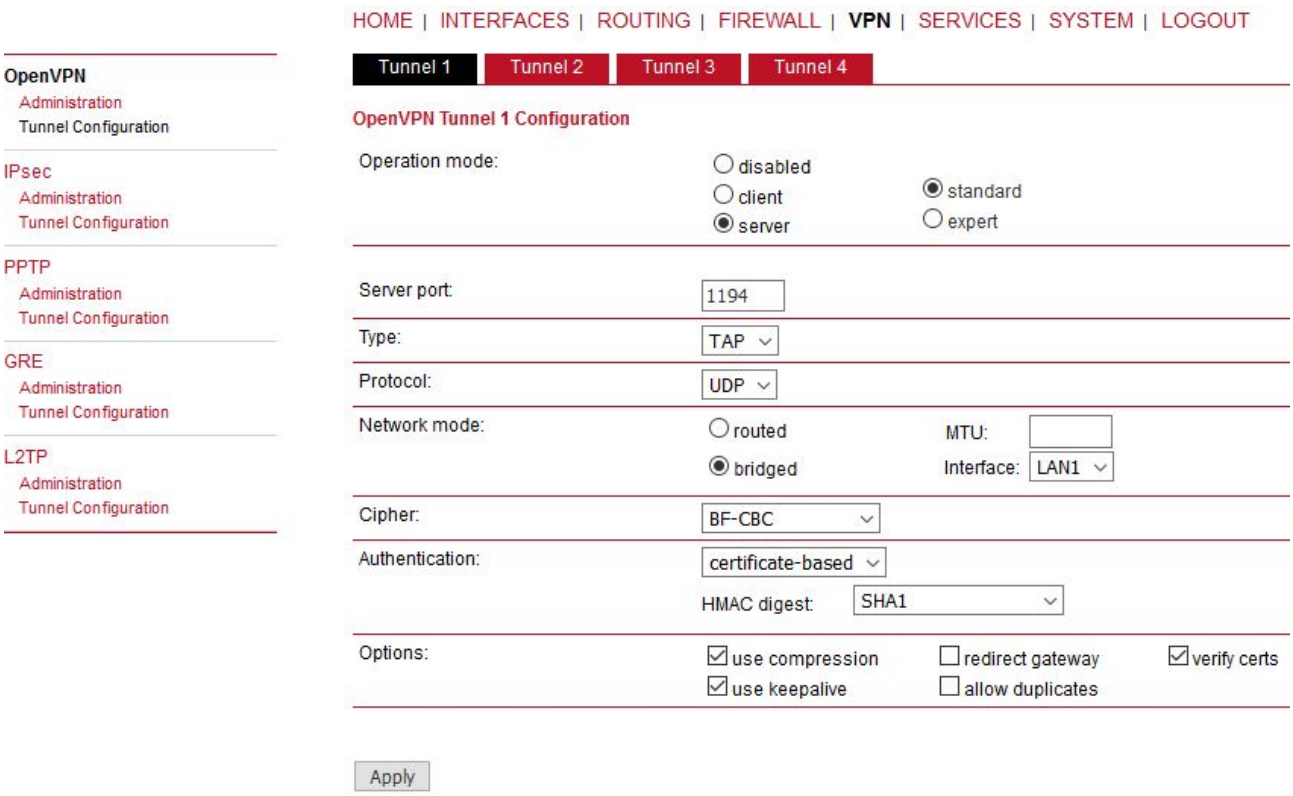


Fig. 1.18: OpenVPN Server – bridged mode

Create the required certificates and enable two clients in the Management menu. See the details in *Section 1.1, "OpenVPN – Routed mode"*.

The Networking and Routes menus do not require anything to change. We are NOT defining any routes in this mode.

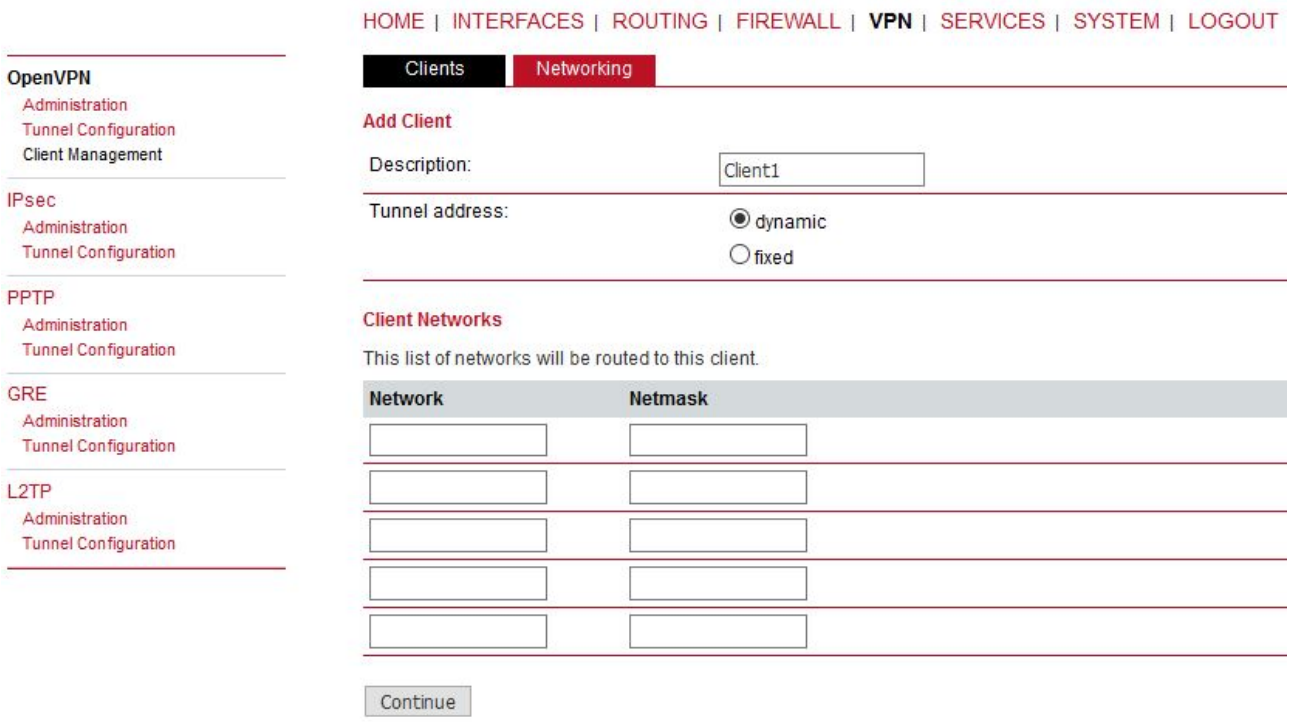


Fig. 1.19: OpenVPN Clients – bridged mode

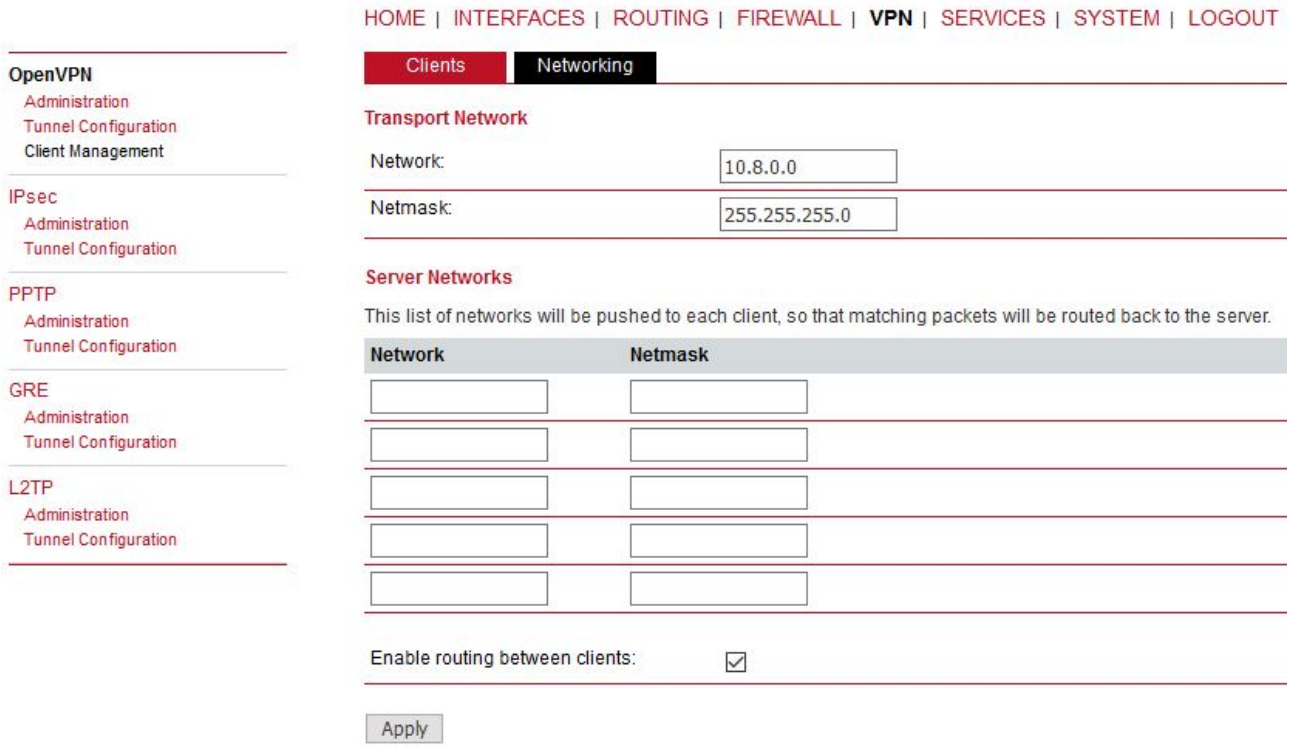


Fig. 1.20: OpenVPN Networking – bridged mode

Download the Expert file and Enable the tunnel.

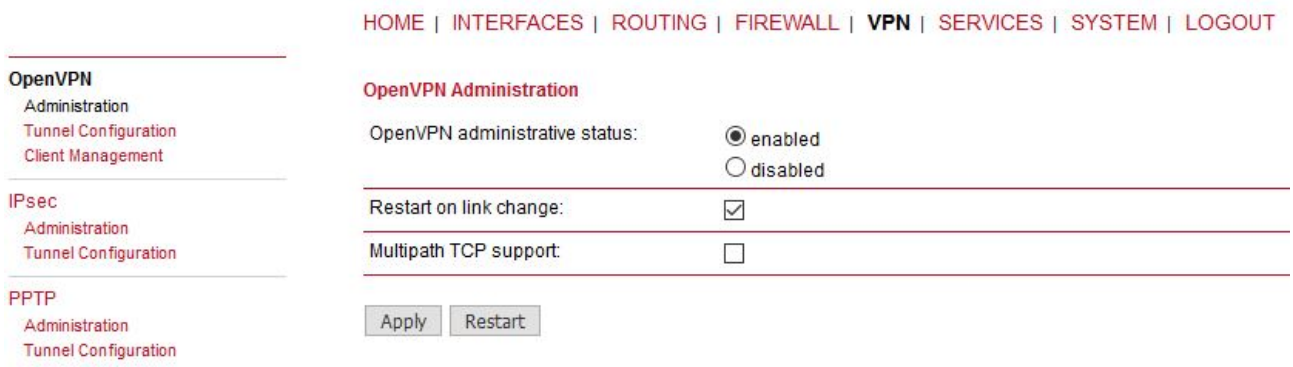


Fig. 1.21: Enabling OpenVPN server

Finally, you check the OpenVPN status in the HOME menu.

1.2.2. OpenVPN Client Configuration

The client's configuration is very simple, just upload the Expert file.

Note

You could, of course, use the Standard Operation mode, but using Expert file is simpler.

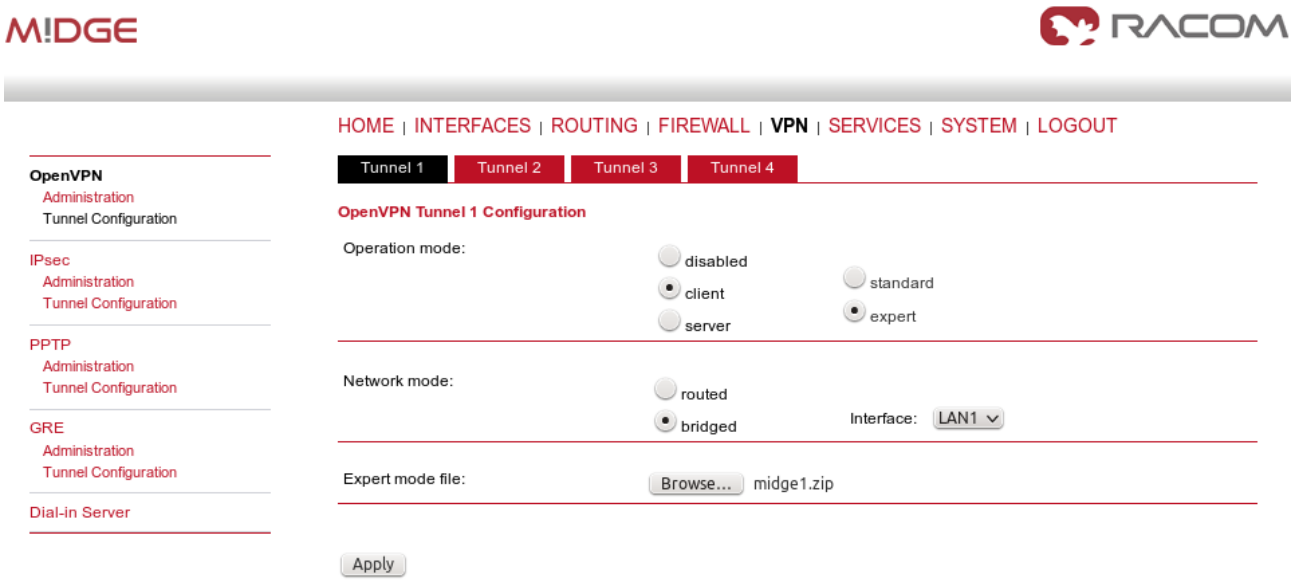


Fig. 1.22: OpenVPN client configuration – bridged mode

Enable the tunnel and check the VPN status.

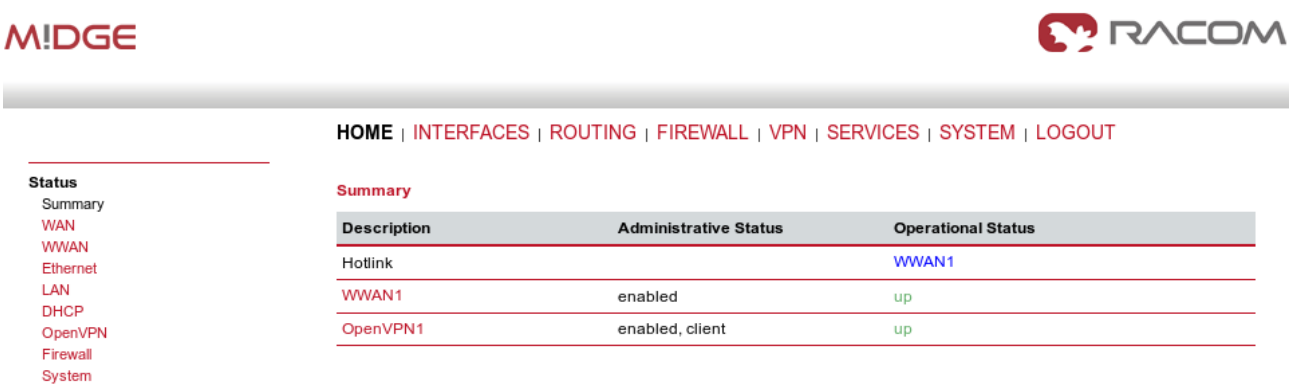


Fig. 1.23: OpenVPN client HOME menu

1.2.3. Testing OpenVPN tunnel

Test the tunnel using the Ping functionality.

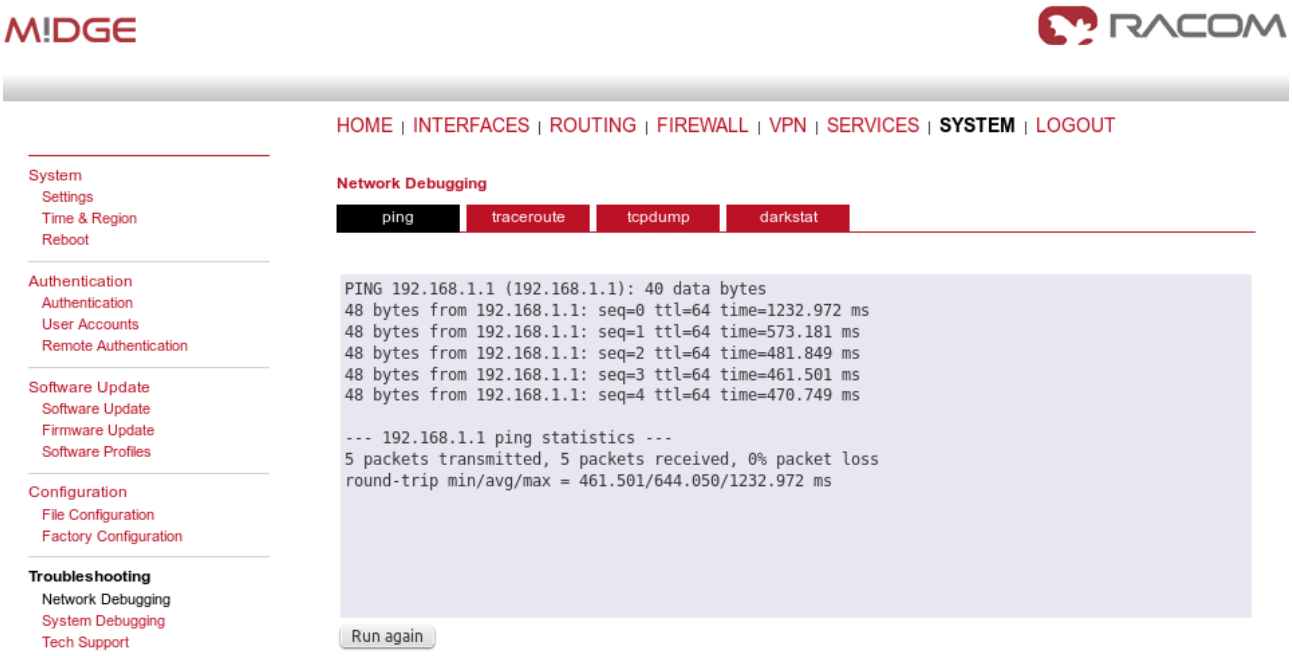


Fig. 1.24: Testing OpenVPN (ping from the client to the server)

Remember that there is no route in the Routing menu, because we are using TAP interface instead of TUN.

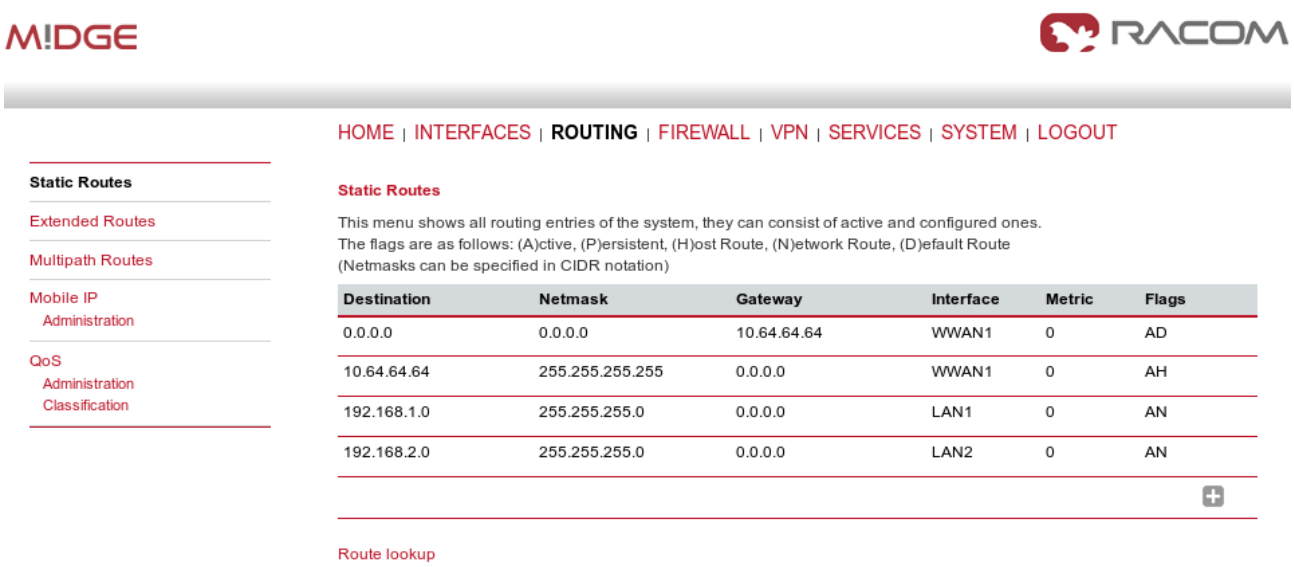


Fig. 1.25: Routing menu – bridged mode

Note

You can ping among the devices connected via M!DGE units. The link should be transparent and no extra routes are needed on the devices.

```
$ ping -c 5 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1636 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1327 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1477 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1207 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1097 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 1097.632/1349.279/1636.959/191.392 ms, pipe 2
```

OpenVPN is a very powerful tool. If you need to know more about the possible options, use the M!DGE/MG102i manual for more details.

2. IPsec

IPsec can be used in a network of any size. A dedicated router (or several routers) serve(s) as the VPN concentrator. The choice of vendor and type depends on the SLA requirements and the size of the network - RACOM has positive experience with Cisco routers (IOS or ASA based), however routers from other vendors (e.g. Juniper, Netgear, WatchGuard or others) can certainly be used.

The following routers were used as IPsec VPN concentrators:

- M!DGE/MG102i – up to 4 tunnels
- Cisco 1700 – up to 100
- Cisco ASA 5510 – up to 250
- Cisco 871-K9 – up to 10 tunnels
- Cisco 1841-HSEC/ K9 – up to 800 tunnels

Please follow the instruction in the user manual of the specific router for IPsec tunnel settings. RACOM support team can assist you with basic settings for Cisco routers. A short description of the IPsec tunnel configuration in M!DGE/MG102i follows.

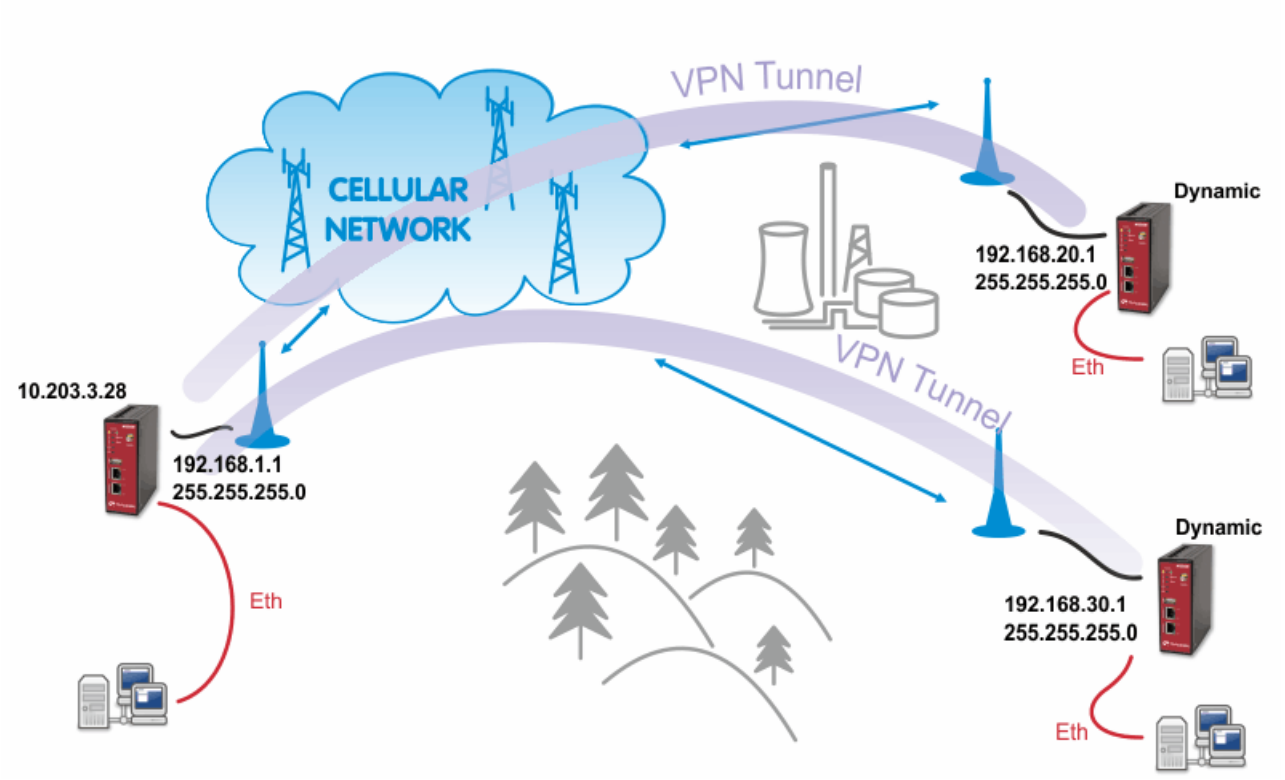


Fig. 2.1: IPsec

The topology is the same as with the routed OpenVPN example. Remember that it is not possible to have a bridged mode of IPsec as it was possible with OpenVPN.

Both remote M!DGE/MG102i units in the example have dynamic mobile IP addresses. We will set the center's peer IP to 0.0.0.0 so it will accept the connections from any IP address.

With IPsec, the most common way to authenticate each other is via a pre-shared key. Due to this, it is not essential to have a correct time using the NTP server.

2.1. IPsec Configuration

2.1.1. Server's configuration

Go to the **VPN – IPsec – Tunnel Configuration** menu and create a new tunnel by pressing the “+” sign.

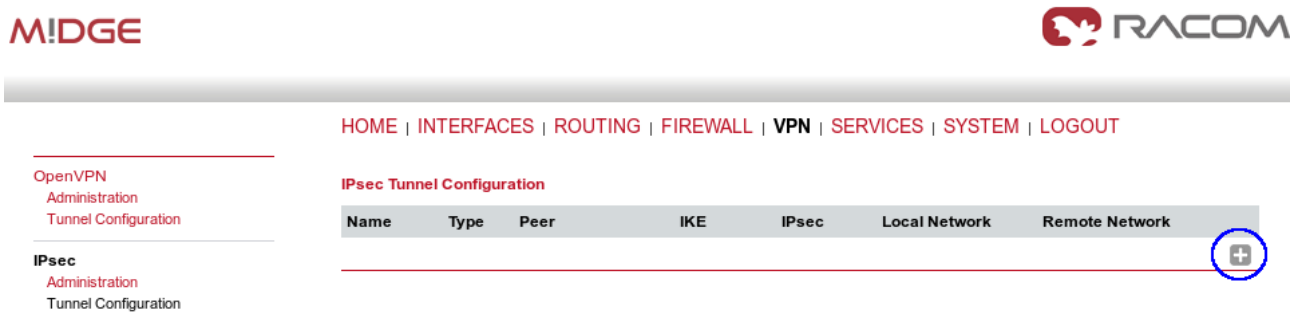


Fig. 2.2: Creating IPsec tunnel

In the General tab, fill in 0.0.0.0 into the IP address field. Due to this address, any remote unit can establish the connection with the central unit if the credentials are correct. The remote unit's IP address is not an issue.

Note

From our experience, change the Action to “restart”.

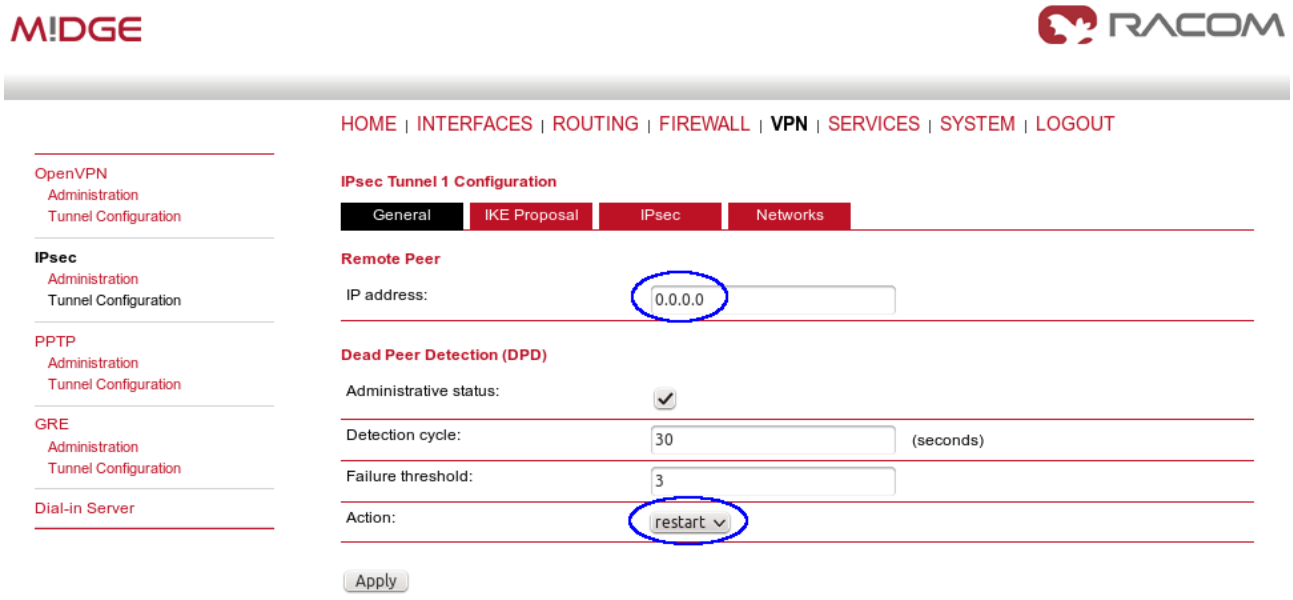


Fig. 2.3: IPsec server's General configuration

Apply the changes and go to the next tab, IKE Proposal. Define any pre-shared key, which must be the same on the center and the remote sites. Fill in the Local and Peer IDs. In our example, FQDNs are used. The central ID is “midge-central” and the ID for the first client is “midge-client1”.

Note

You need to add a second tunnel if you need to connect M!DGE “client2”.

Other parameters can stay in defaults or you can enable PFS for higher security.

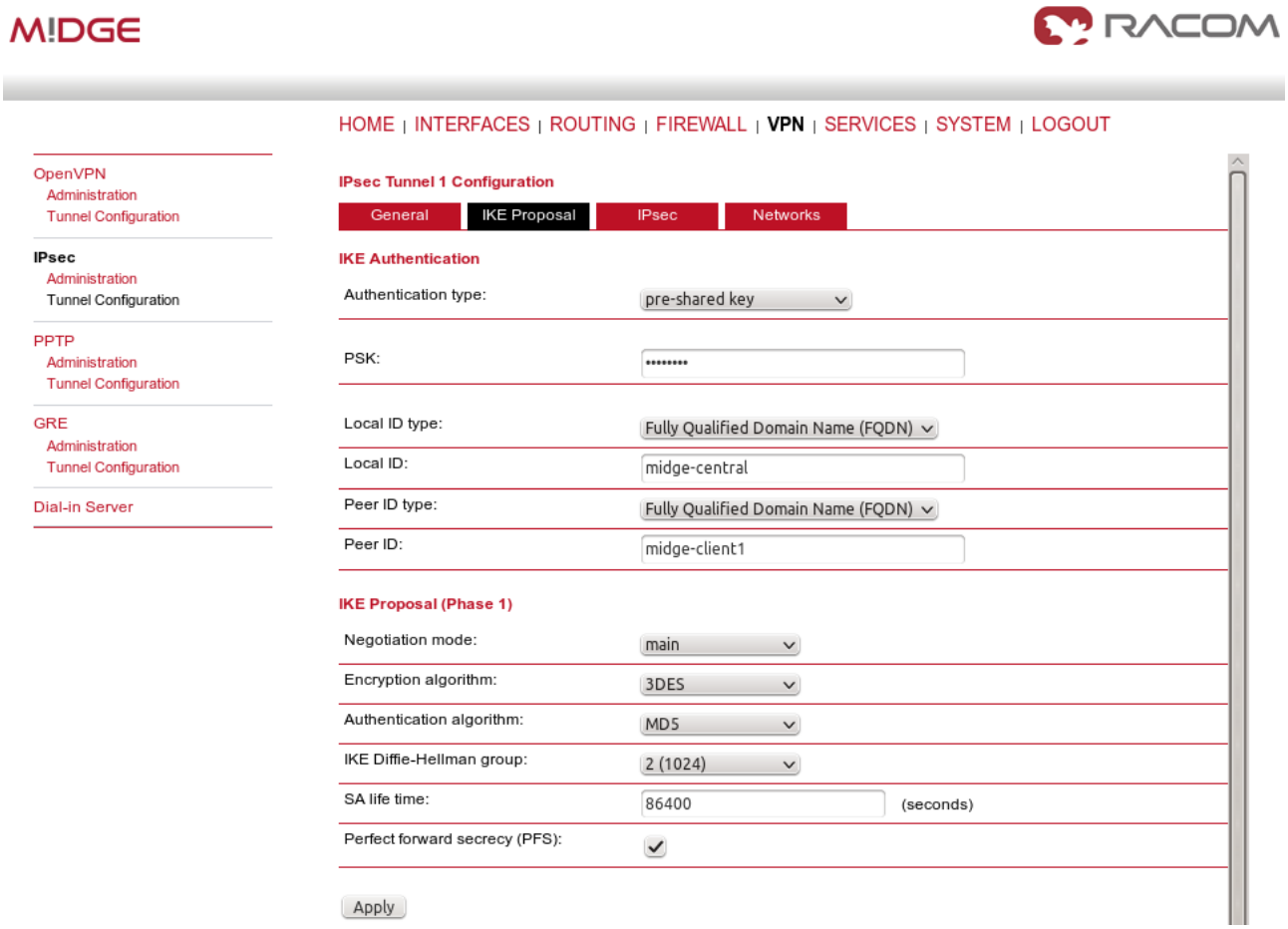


Fig. 2.4: IPsec central's IKE Proposal tab

After applying the changes, you can leave everything in defaults within the IPsec Proposal tab.

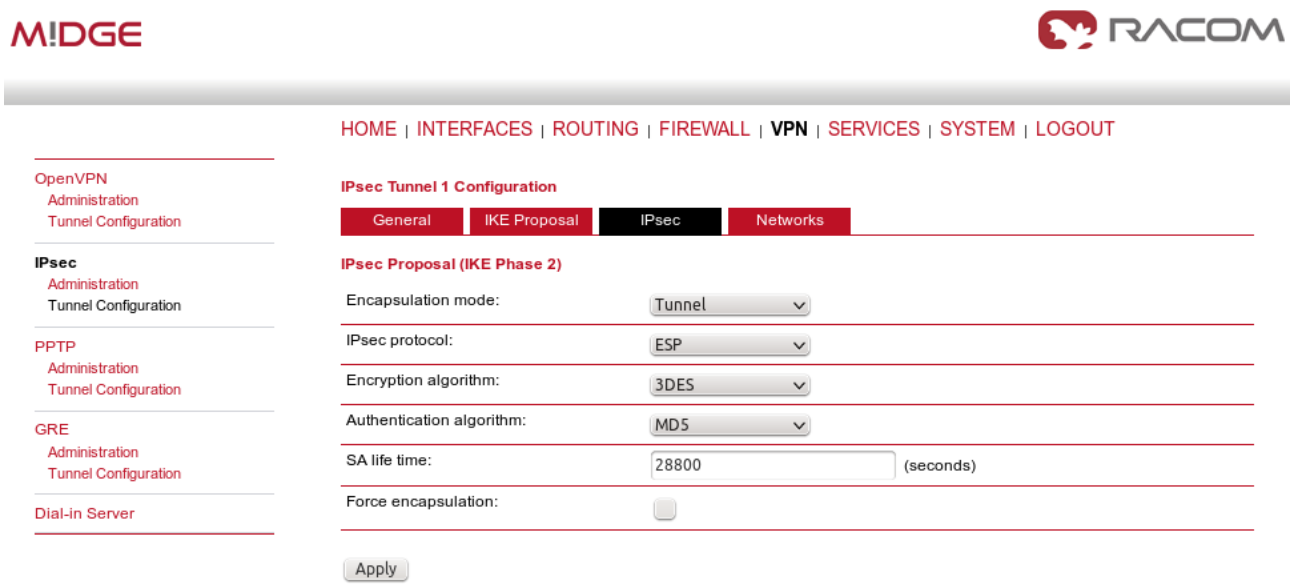


Fig. 2.5: IPsec central's IPsec Proposal tab

In the last tab, define the required routable networks. In our example, we interconnect server's 192.168.1.0/24 subnet with client's 192.168.20.0/24 subnet. Leave the “NAT address” blank.

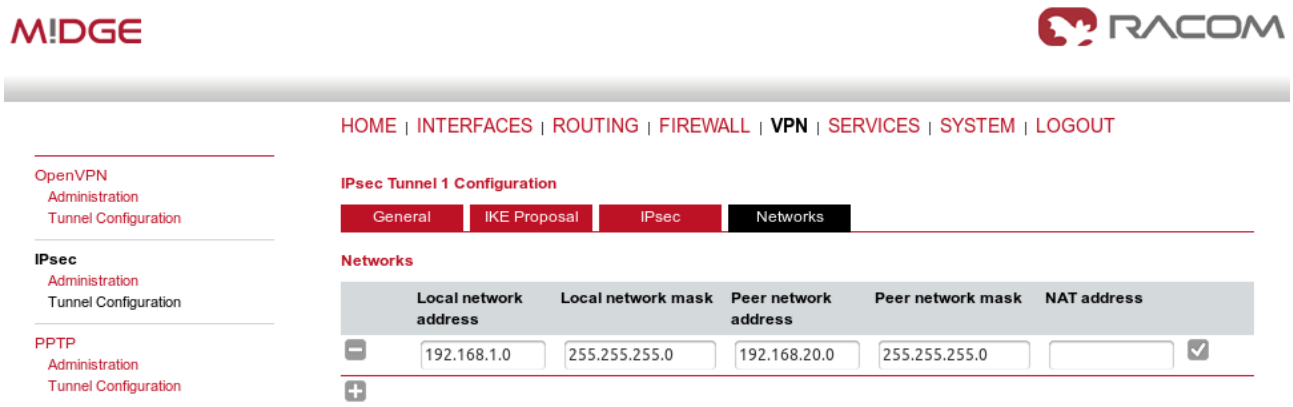


Fig. 2.6: IPsec central's Networks tab

Return back to the Administration menu and enable the tunnel. Check both parameters – Propose NAT traversal and Restart on link change.

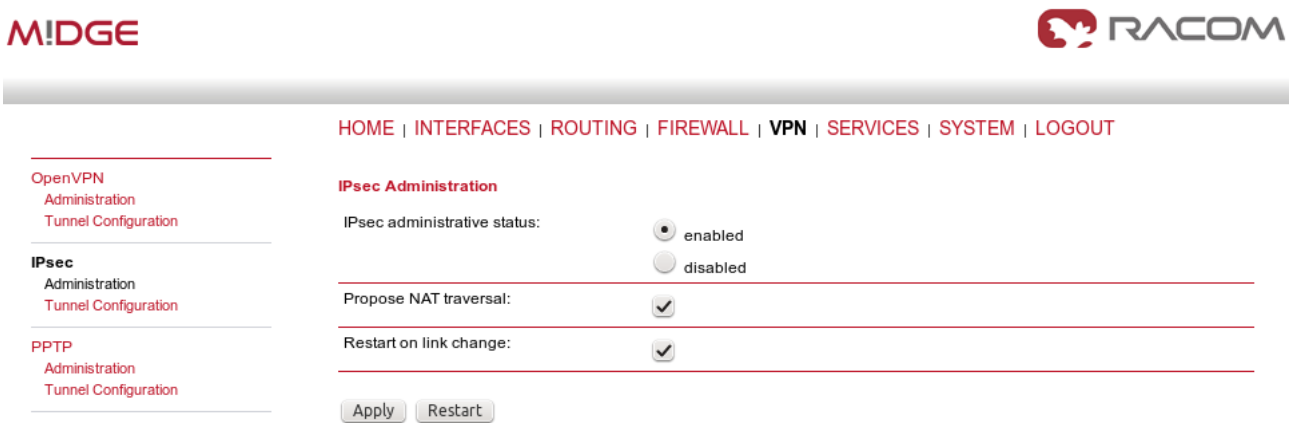


Fig. 2.7: Enabling IPsec tunnel

The pop-up window will appear asking you to confirm the MSS to be decreased due to IPsec overhead. Confirm this change.

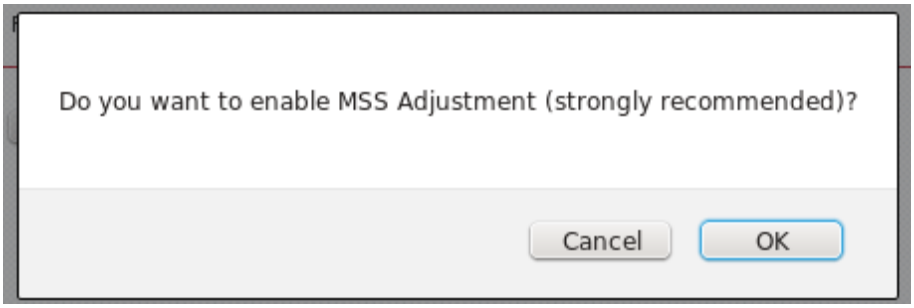


Fig. 2.8: MSS Adjustment

If you now check the tunnel status, it will be “down”, because the client's configuration is not yet finished.

2.1.2. Client's configuration

The client's configuration must follow the server's one. The Peer IP address must be the server's IP address.

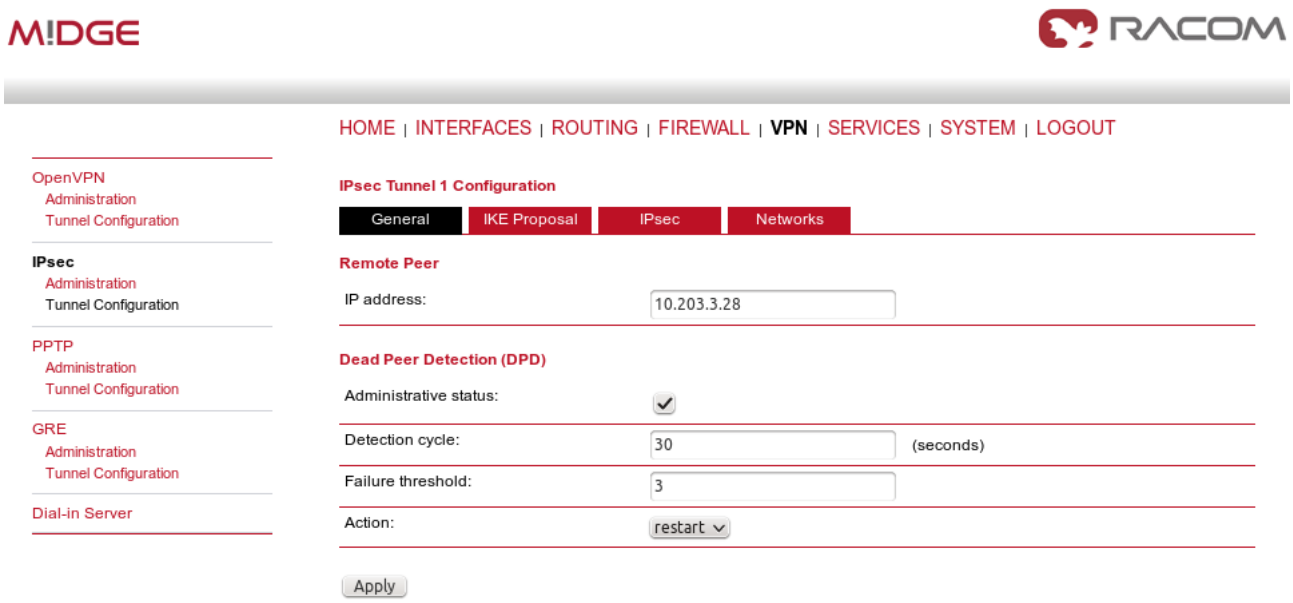


Fig. 2.9: Client's IPsec General tab

In the IKE Proposal tab, the PSK must be the same as on the server's side and switch the IDs. Do not forget to enable PFS if checked on the server.

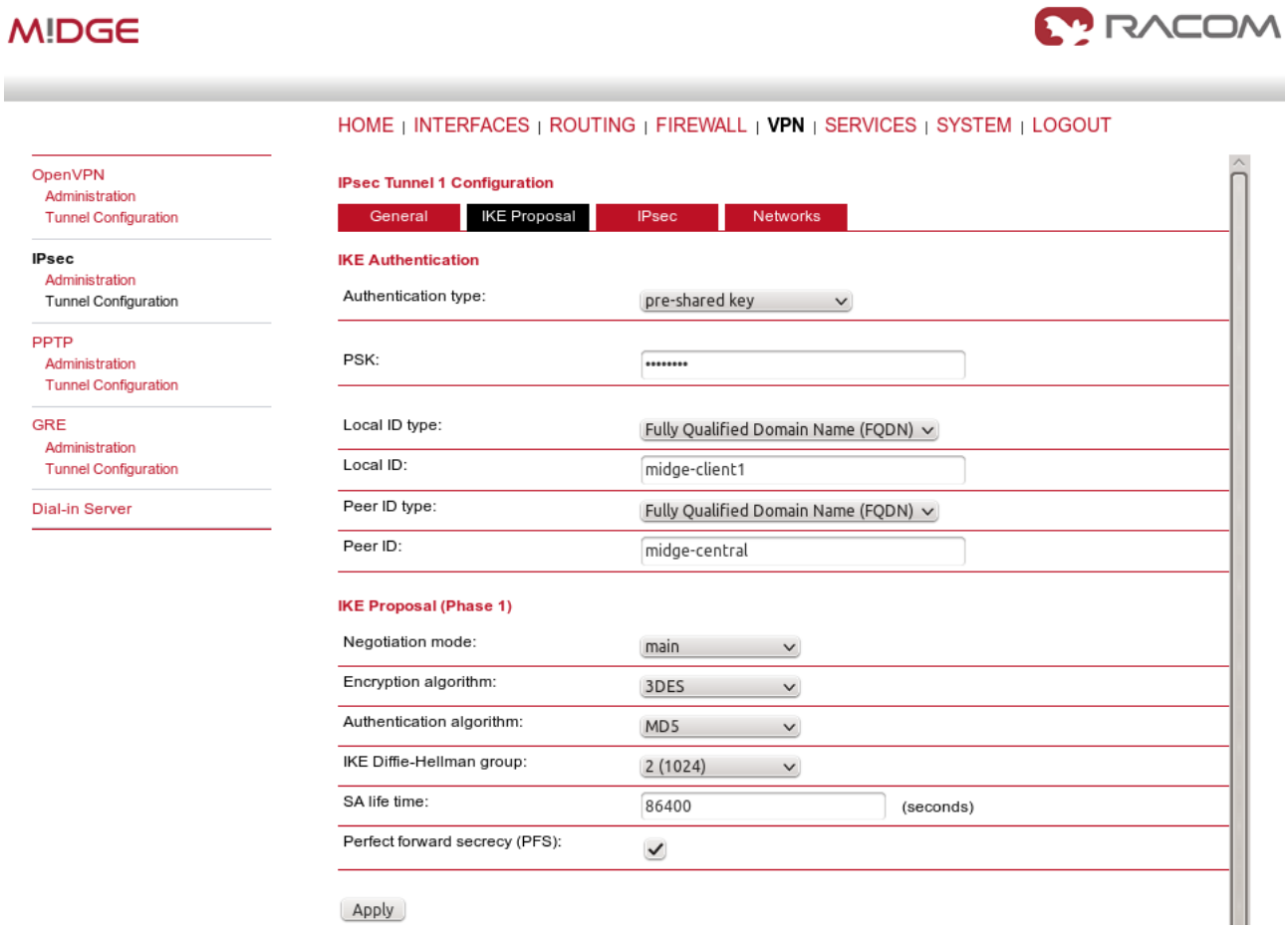


Fig. 2.10: Client's IPsec IKE Proposal

Leave IPsec proposal in defaults and configure the Networks. Just switch the subnets (compared to the central's configuration).

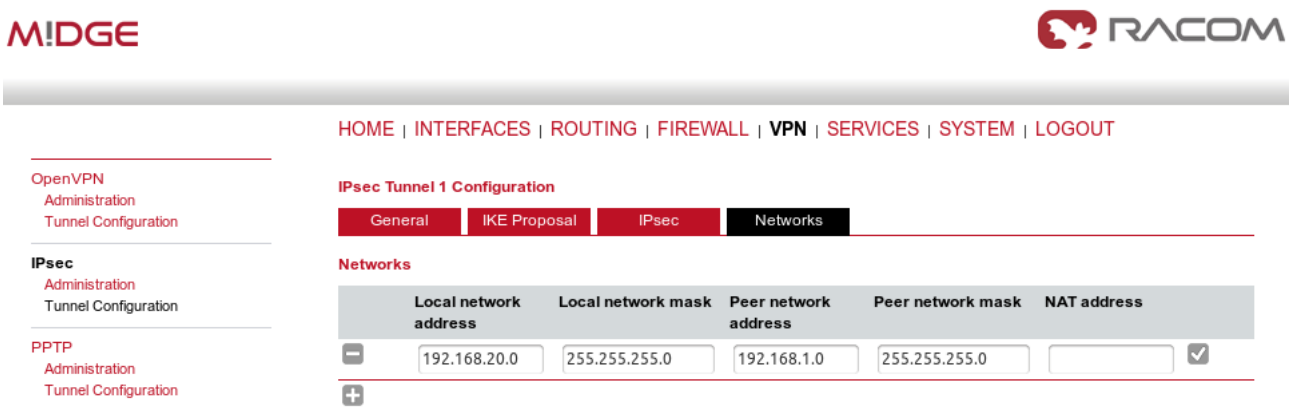


Fig. 2.11: Client's IPsec Networks tab

We can now Enable the tunnel and confirm the MSS adjustment.

After the algorithmcompletes the tunnel establishment, the tunnel should be marked “up” on both units. Check the HOME menu.

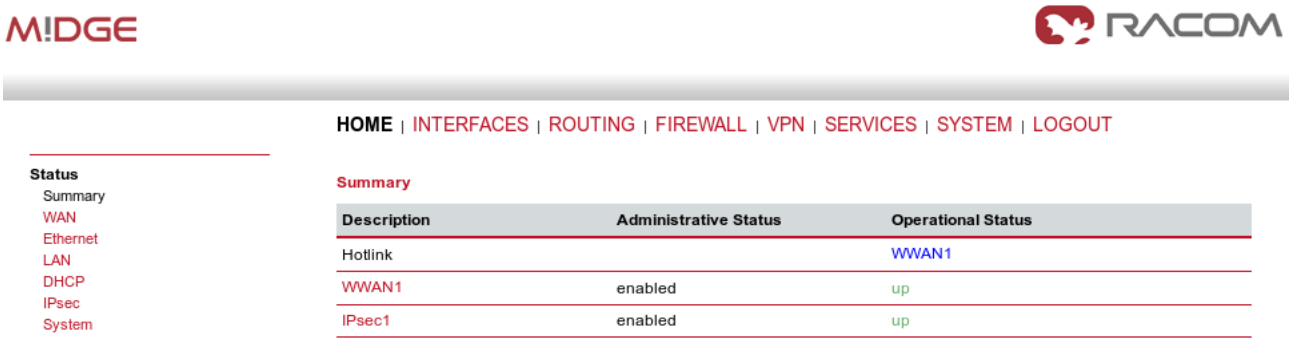


Fig. 2.12: IPsec is established successfully

Once the tunnel is UP, you can check the functionality via the ping, e.g. from the command shell:

```
~ $ ping -I 192.168.1.1 192.168.20.1
PING 192.168.20.1 (192.168.20.1) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.20.1: seq=0 ttl=64 time=849.734 ms
64 bytes from 192.168.20.1: seq=1 ttl=64 time=1058.866 ms
64 bytes from 192.168.20.1: seq=2 ttl=64 time=918.134 ms
```

You need to set the source IP address so the IPsec routing would work. Otherwise, there could be no route back from the remote M!DGE.

Use M!DGE/MG102i manual for more details.

3. GRE

GRE (Generic Routing Encapsulation) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. The GRE Tunnel can be configured between any two devices that are compatible with this protocol.

- There are 2 modes of GRE operation: TUN (Tunnel mode) or TAP (L2 transparent connection) with SW bridge.
- Packets passing through the GRE tunnel are not encrypted. You can combine GRE with IPsec for encryption purposes.
- The GRE tunnel neither establishes nor maintains a connection with the peer. The GRE tunnel is created regardless of peer status (peer need not exist at all).
- The GRE tunnel has its own IP address and mask. Network defined by this address and mask contains only 2 nodes – each end of the tunnel.

See *Chapter GRE*[1] in the manual M!DGE for descriptions of parameters.

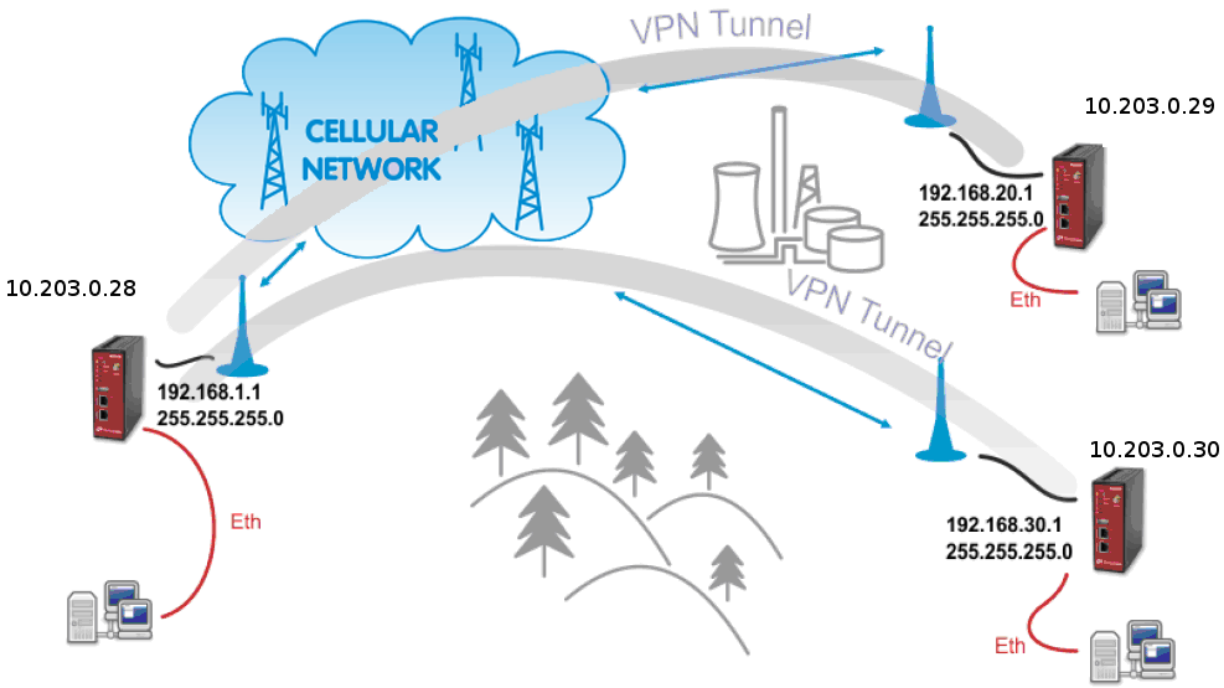


Fig. 3.1: GRE topology

The topology for GRE tunnel example is very similar to IPsec and OpenVPN topologies. The main difference are mobile (WWAN) IP addresses. In GRE, both units are equal to each other, i.e. there are no “server” and “client” roles. One important requirement is that both ends of the tunnel must be able to access/reach the remote end mobile IP. In this example, the unit 10.203.0.28 must be able to access both 10.203.0.29 and 10.203.0.30 IP addresses; and in the same time both these units must be able to access 10.203.0.28 mobile IP address.

[1] https://www.racom.eu/eng/products/m/midge1/web_conf.html#gresec

The following example explains the configuration of 10.203.0.28 and 10.203.0.29 M!DGE units only. If you test a second tunnel as well, there must be two GRE tunnels configured in 10.203.0.28 unit.

Note

If you utilize a public APN, the GRE requires all the mobile IPs to be public so that they can access/reach each other.

Note

The maximum number of GRE tunnels is 4.

3.1. GRE Configuration

The following example explains the TUN (tunnel, routed) version. If you need to interconnect the L2 topology, just select the “TAP” Interface type and choose a required Ethernet interface.

Fig. 3.2: TAP mode

M!DGE 10.203.0.28

Go to the **VPN – GRE – Tunnel Configuration** menu and enable the “Tunnel 1”.

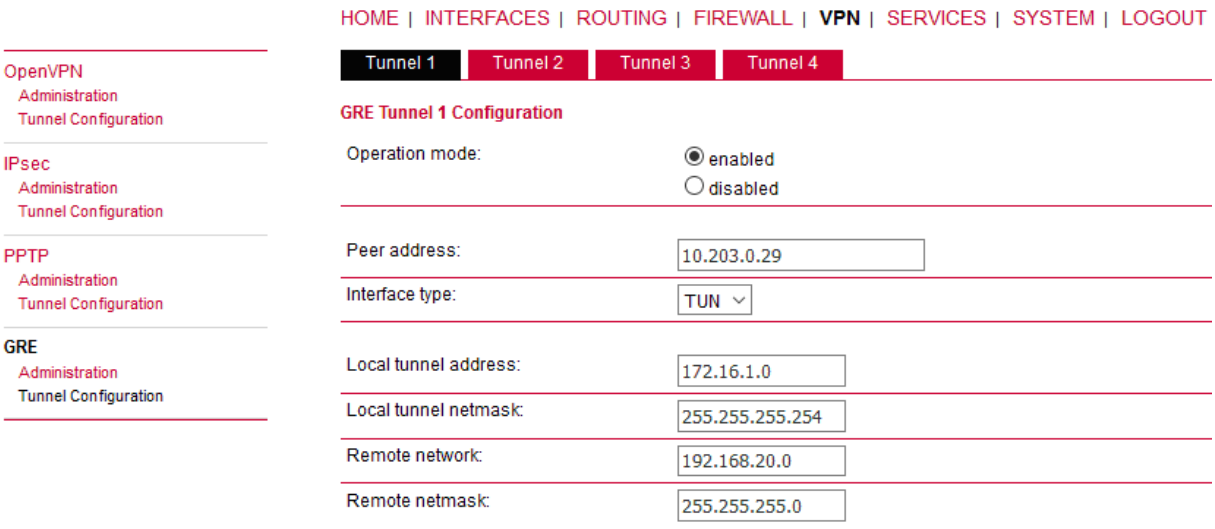


Fig. 3.3: TUN mode, 10.203.0.28 unit

Parameters:

Peer address	“10.203.0.29” (the remote M!DGE unit’s mobile WWAN IP address)
Interface type	“TUN” (tunnel/routed mode)

Local tunnel address	“172.16.1.0” (the local IP address of newly created GRE tunnel)
Local tunnel netmask	“255.255.255.254” (/31 mask in CIDR notation – only two IP addresses are required, but any wider mask is also acceptable, e.g. /30, /29, …)
Remote network	“192.168.20.0” (remote subnet)
Remote netmask	“255.255.255.0” (/24 mask of remote subnet)

Click on the “Apply” button.

Go to the GRE Administration menu and Enable the GRE tunneling.

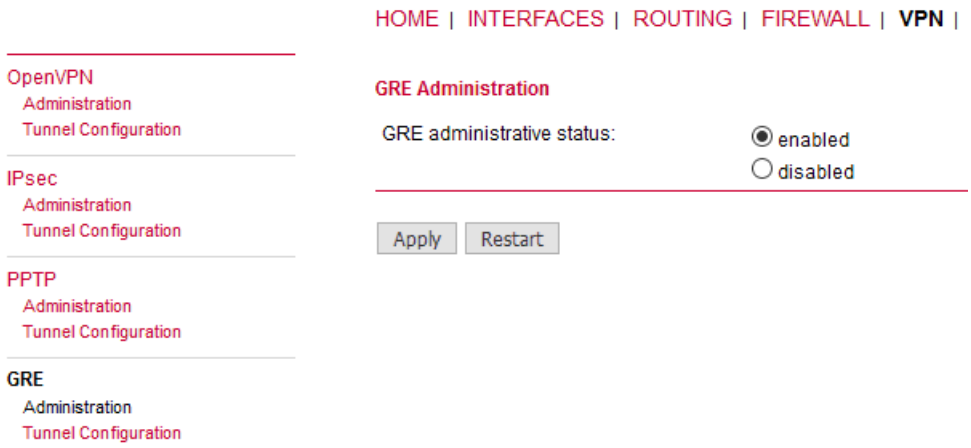


Fig. 3.4: GRE administration status – enabled

Check the Status menu – the GRE tunnel should be “up” and running. As explained, the GRE tunnel does not establish or maintain the connection and so it is “up” even though the remote end is not configured yet.

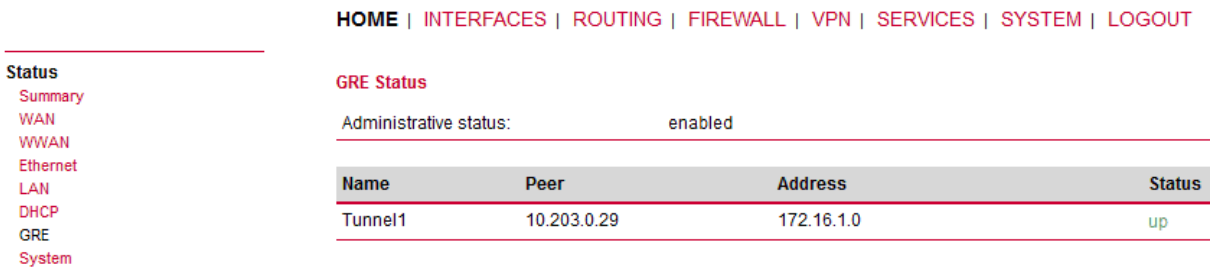


Fig. 3.5: GRE tunnel up, 10.203.0.28 unit

M!DGE 10.203.0.29

Go to the VPN – GRE – Tunnel Configuration menu and enable the “Tunnel 1”.

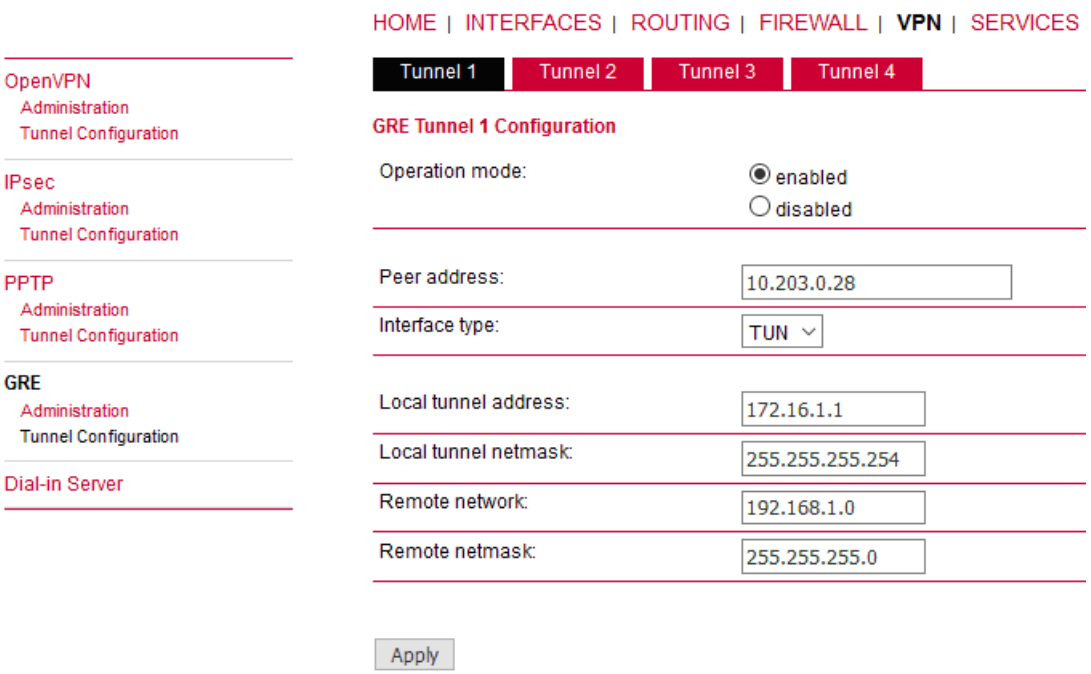


Fig. 3.6: TUN mode, 10.203.0.29 unit

Parameters:

Peer address	“10.203.0.28” (the remote M!DGE unit’s mobile WWAN IP address)
Interface type	“TUN” (tunnel/routed mode)
Local tunnel address	“172.16.1.1” (the local IP address of newly created GRE tunnel)
Local tunnel netmask	“255.255.255.254” (/31 mask in CIDR notation – only two IP addresses are required, but any wider mask is also acceptable, e.g. /30, /29, …)
Remote network	“192.168.1.0” (remote subnet)
Remote netmask	“255.255.255.0” (/24 mask of remote subnet)

Click on the “Apply” button.

Go to the GRE Administration menu and Enable the GRE tunneling.

Check the Status menu – the GRE tunnel should be “up” and running.

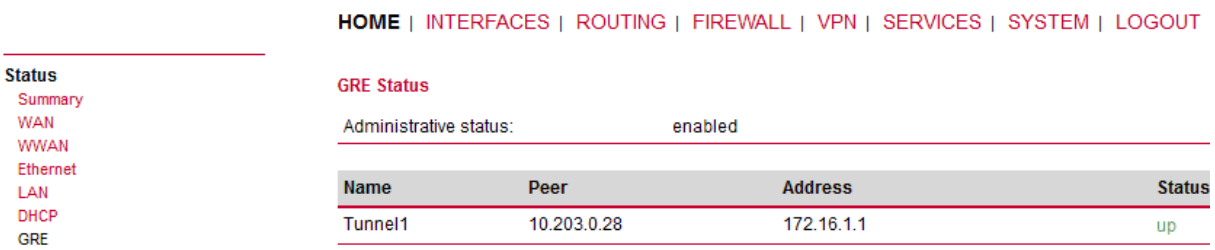


Fig. 3.7: GRE tunnel up, 10.203.0.29 unit

3.2. GRE Tunnel Verification

The easiest way to test the GRE tunnel functionality is to run a ping command. Go to the **System – Troubleshooting – Network debugging** menu and fill in the remote Ethernet IP address.

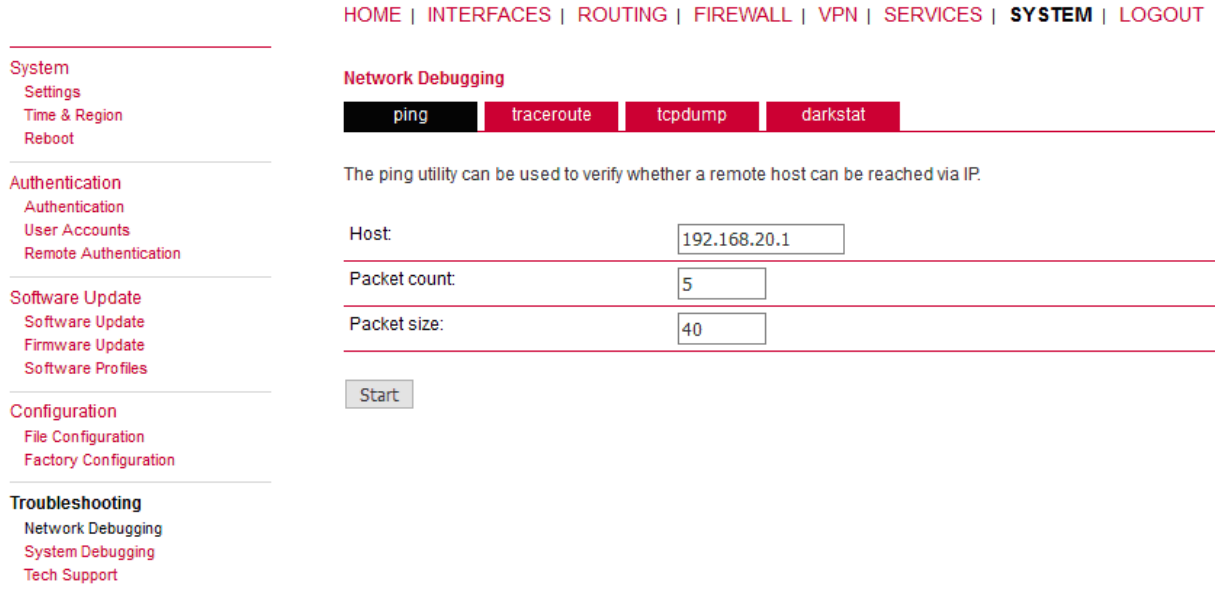


Fig. 3.8: Ping test

Press the “Start” button and check the results.

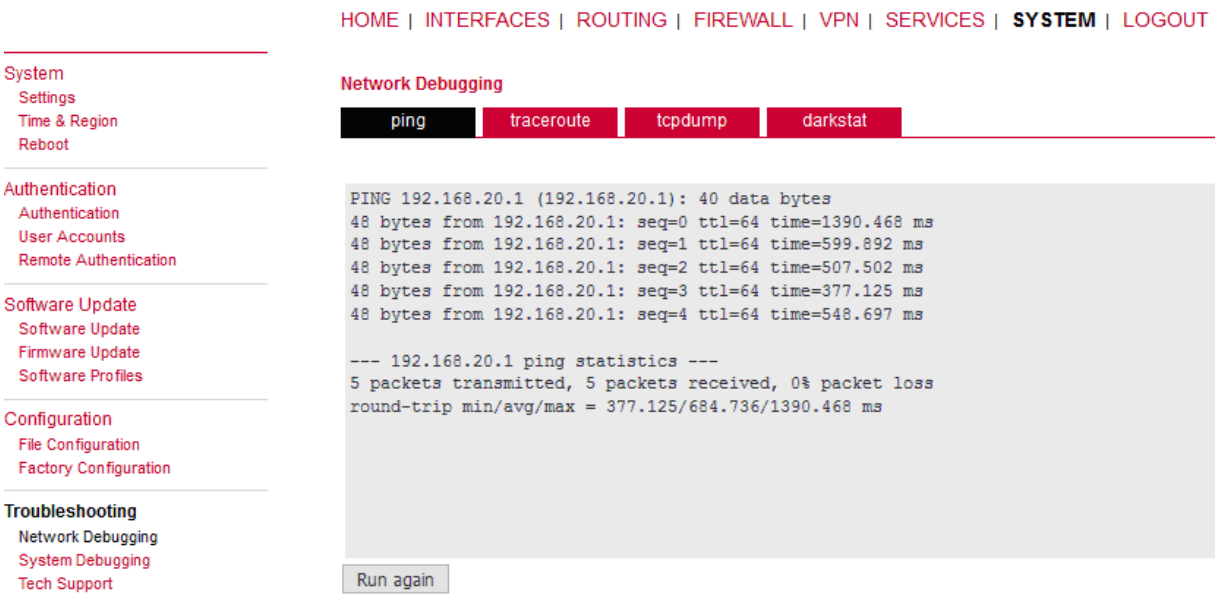


Fig. 3.9: Successful Ping test results

The remote IP is accessible successfully.

The Routing tables should be updated as well – including the configured remote subnets.

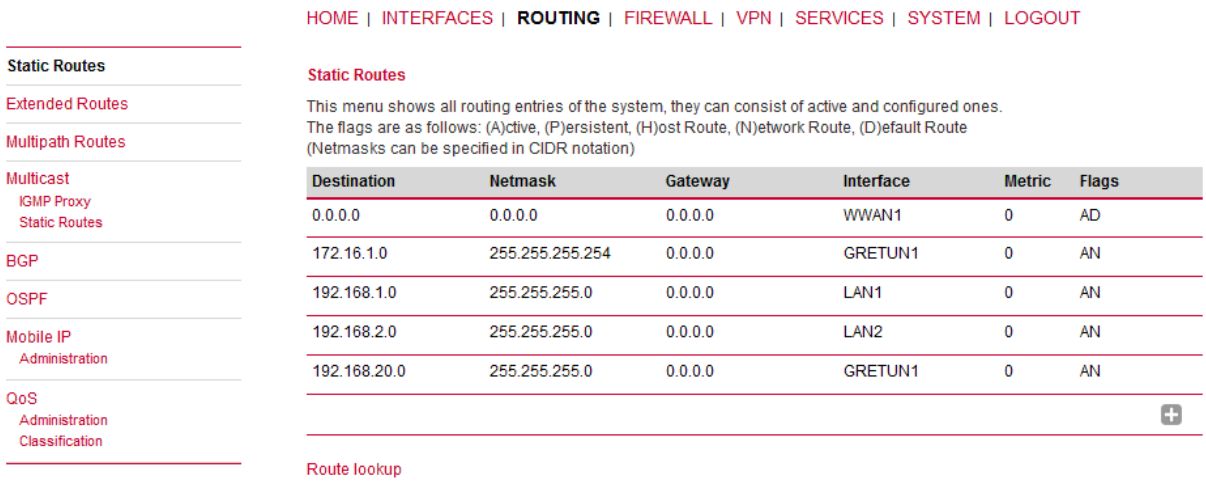


Fig. 3.10: Routing menu with GRE routes

Note

If you need to add other remote subnets, configure them in Static Routes menu – use the same GRETUN Interface and set the gateway to 0.0.0.0.

3.3. Troubleshooting

What can be wrong if remote subnets are not accessible?

- Are both remote WWAN mobile IP addresses accessible?
- Is firewall turned off or configured to pass through GRE traffic?
- Is the GRE network configured correctly? (IP and netmask)
- Are the remote subnets configured correctly? Are Routing tables updated?
- If you test the accessibility from connected PLCs/PCs, are there static routes (or default gateway) configured?

4. L2TP over IPsec

The Layer 2 Tunneling Protocol is a tunneling protocol which does not support any encryption or confidentiality. It relies on an encryption protocol that it passes within the tunnel to provide privacy. L2TPv3 is supported. Tunnel can be bridged to the local interfaces.

In this example, IPsec is configured to provide mentioned encryption and confidentiality. The topology is very simple, just point-to-point and connecting devices within 192.168.1.0/24 LAN subnet over M!DGE2 cellular connection (private APN).

Note

The L2TP is supported in M!DGE2 since the FW version 4.3.40.100.

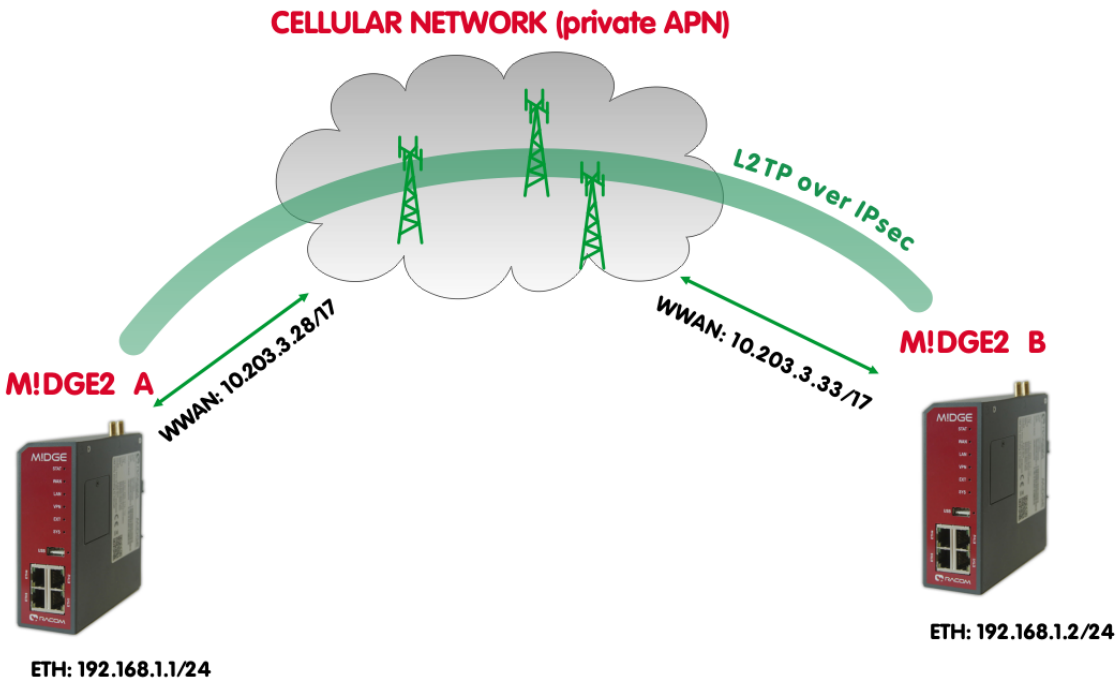


Fig. 4.1: Topology diagram, L2TP over IPsec

Note

Only L2TP and IPsec parameters are displayed and explained. Configuring private APN, ETH IP addresses etc. is not included.

4.1. L2TP Configuration

M!DGE2 A

Go to the VPN -> L2TP -> Tunnel configuration menu.

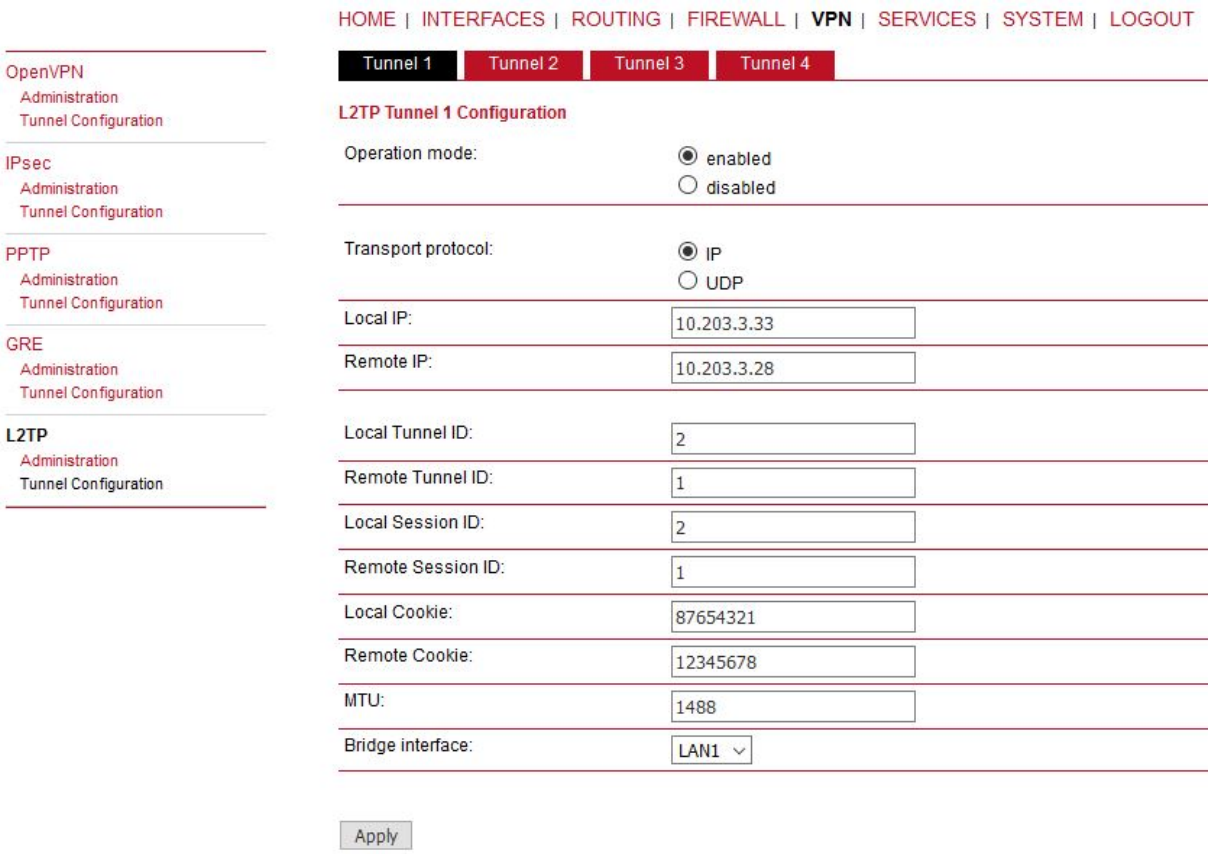


Fig. 4.2: M!DGE2 A - L2TP configuration

Parameters:

Operational mode	enabled
Transport protocol	IP (default value, UDP can be better in environment with NAT and firewalls)
Local IP	10.203.3.28 (local WWAN IP address)
Remote IP	10.203.3.33 (remote WWAN IP address)
Local Tunnel ID	1 (L2TP tunnel numeric ID of local unit)
Remote tunnel ID	2 (L2TP tunnel numeric ID of remote unit)
Local Session ID	1 (L2TP tunnel session ID of local unit)
Remote Session ID	1 (L2TP tunnel session ID of remote unit)
Local Cookie	12345678 (optional parameter, 8digit value)
Remote Cookie	87654321 (optional parameter, 8digit value)
MTU	1488 Bytes (default)
Bridge interface	LAN1 (the interface for which we create “*pseudowire*” over L2TP)

Apply the changes and enable the L2TP in Administration menu.

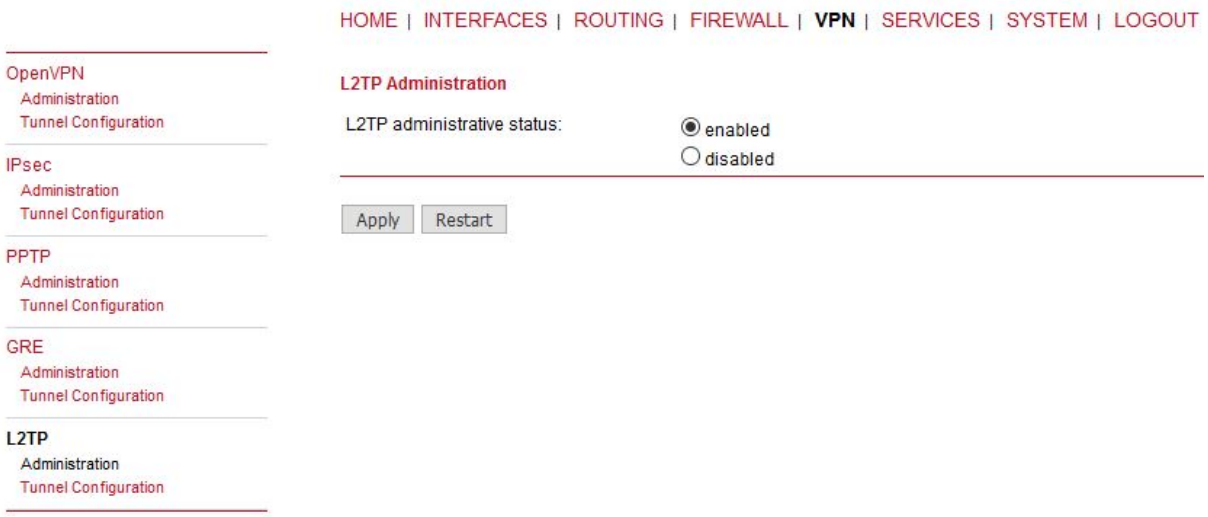


Fig. 4.3: L2TP administration

M!DGE2 B

Do the same configuration in B unit as well, but just switch the IPs, IDs and cookies so they match each other with A unit.

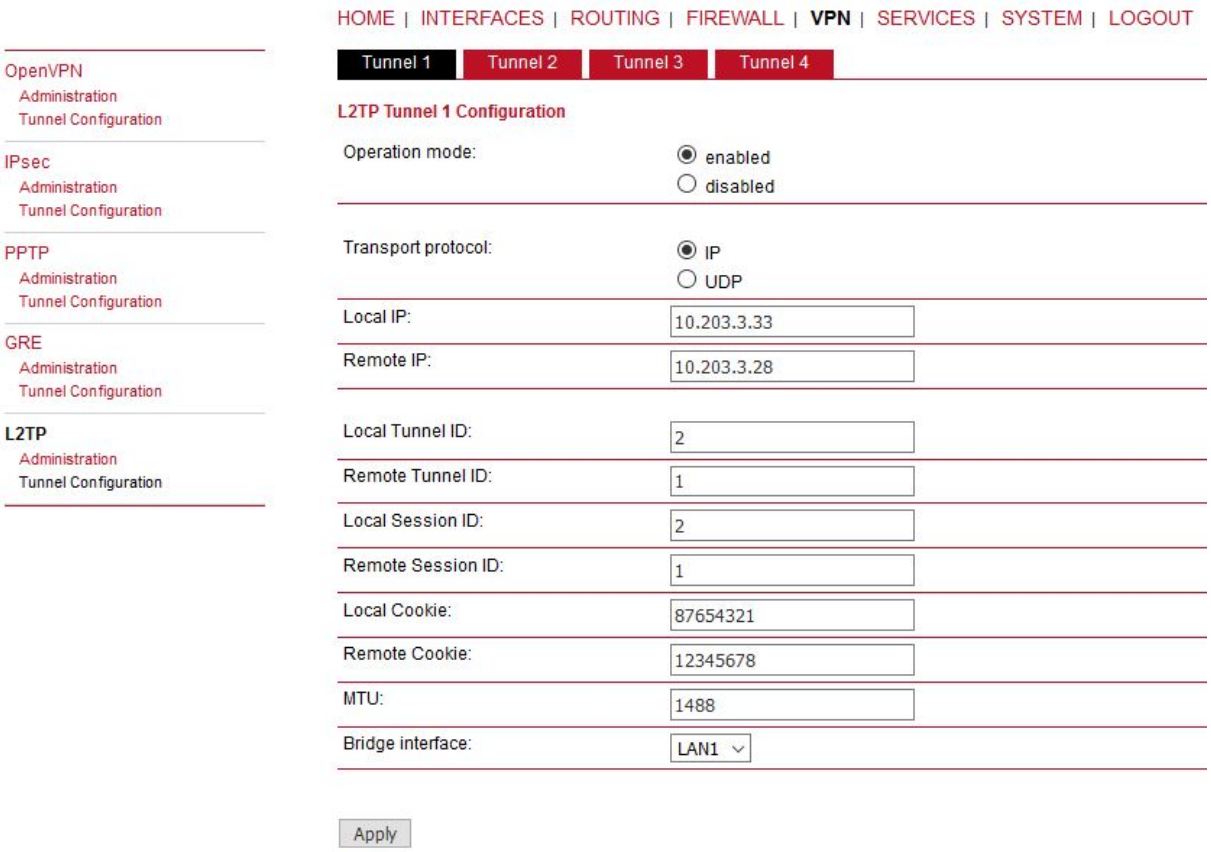


Fig. 4.4: M!DGE2 B - L2TP settings

This should enable non-secure L2TP only communication between our M!DGE2 units and all devices connected via LAN1 in 192.168.1.0/24 network. You can verify the accessibility via PING tool.

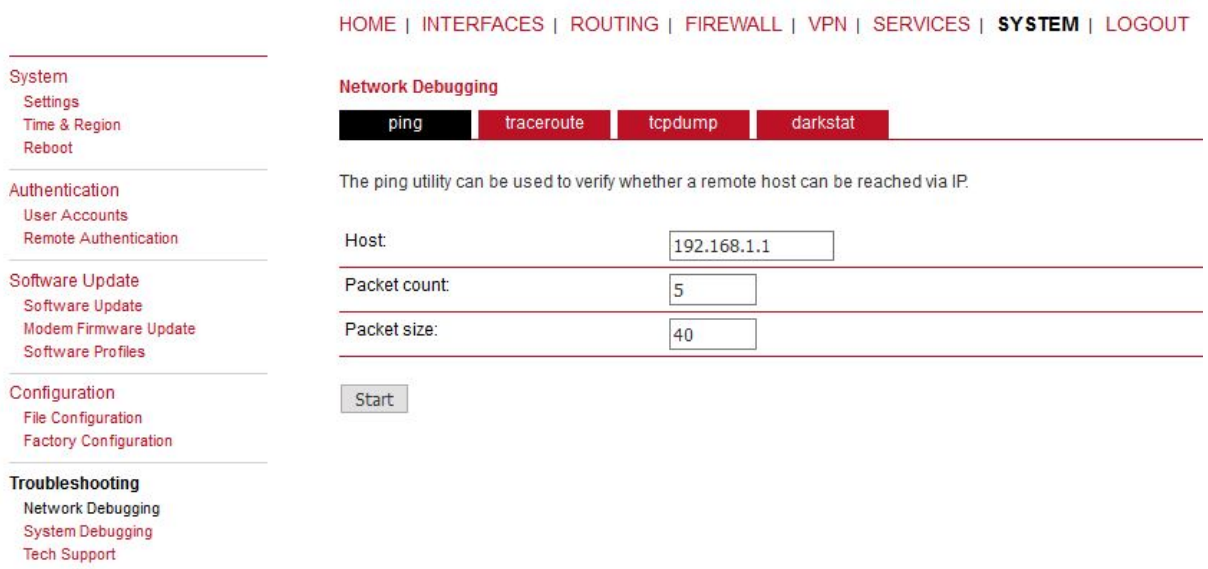


Fig. 4.5: Run the PING to verify accessibility

Check the results.

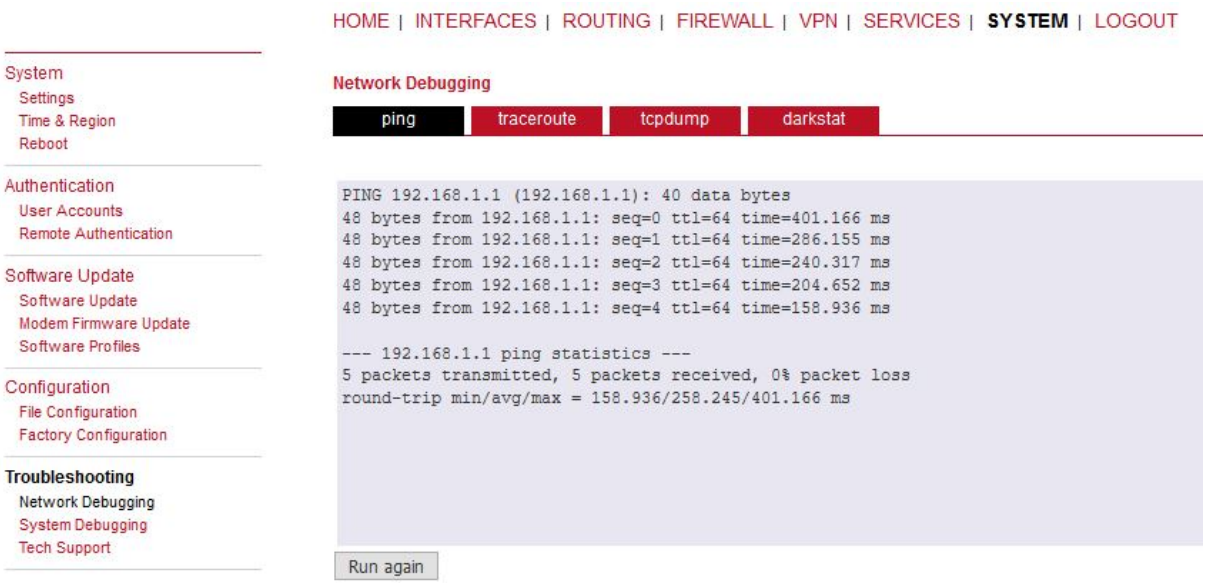


Fig. 4.6: PING results over L2TP non-secure tunnel

4.2. IPsec configuration

Go to the VPN -> IPsec -> Configuration menu and configure the IPsec tunnel.

M!DGE2 A

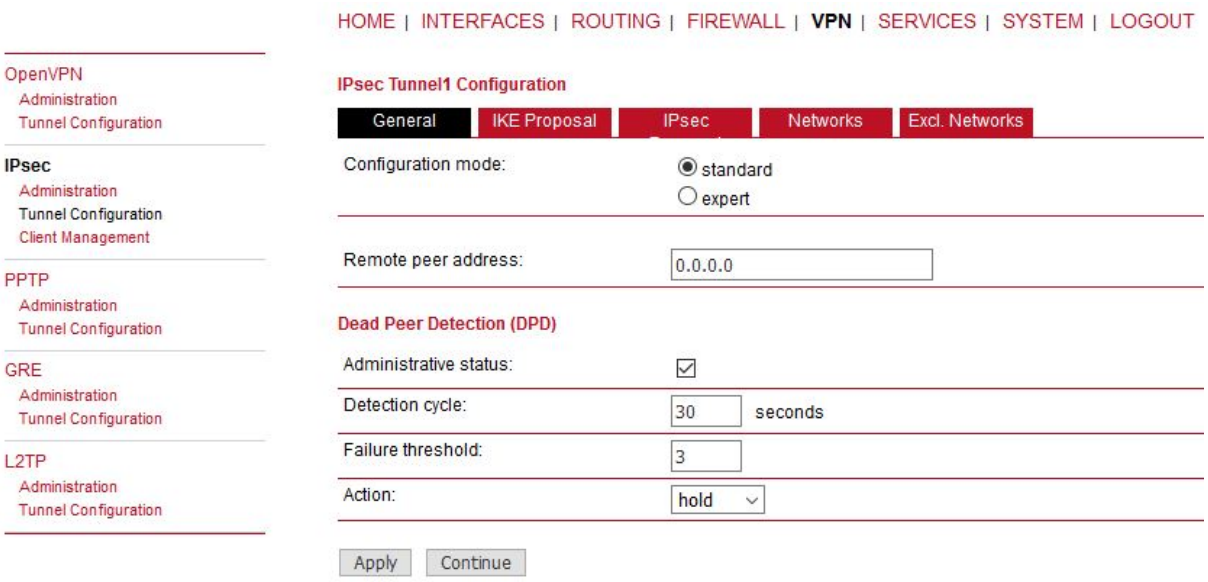


Fig. 4.7: M!DGE2 A – General IPsec configuration

Parameters:

Remote peer address 0.0.0.0 (passive mode)

Other values can stay in default or set them as required. Set the IKE Proposal to match 2nd M!DGE2.

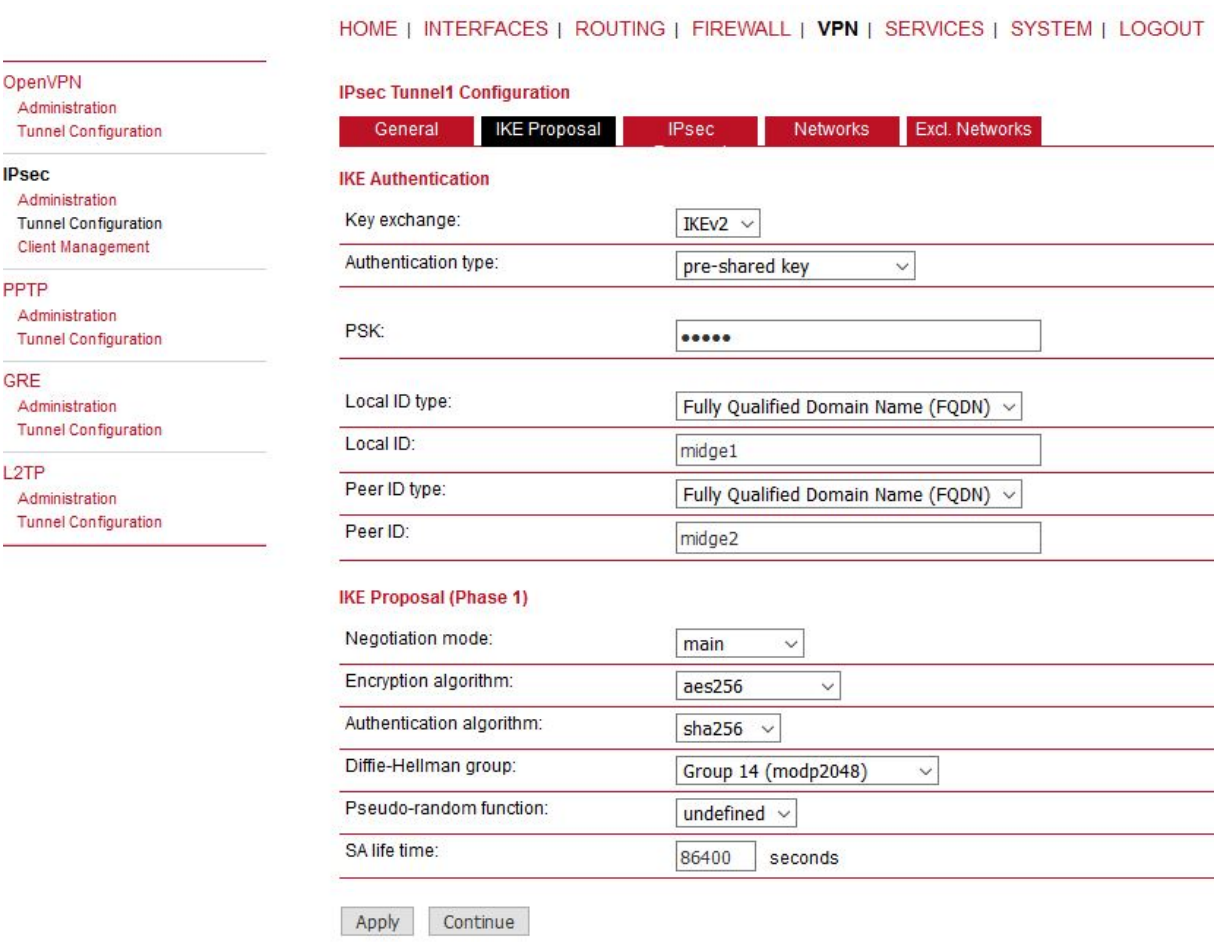


Fig. 4.8: M!DGE2 A – IPsec IKE Proposal

Configure the parameters as required. We configured the IKEv2 with PSK “midge”. The IDs are set to FQDN “midge1” and “midge2”. Other parameters are in default settings.

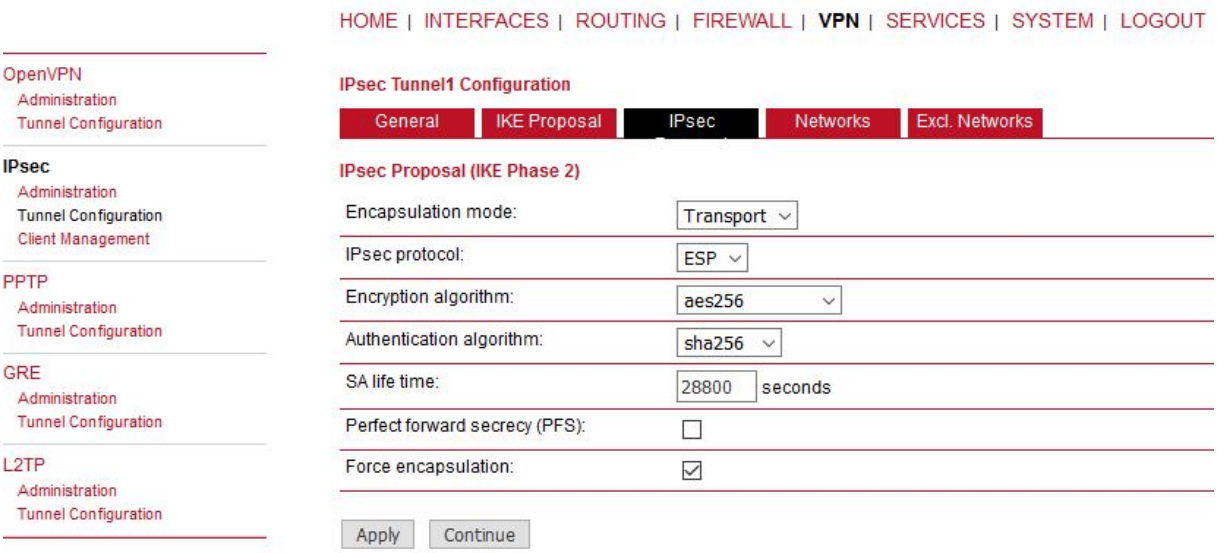


Fig. 4.9: M!DGE2 A – IPsec Proposal

The **Encapsulation mode** is important. Set it to **Transport** mode, otherwise it will not work. The mode enables usage with other tunneling protocols such as L2TP or GRE.

Check the **Force encapsulation** to make sure IPsec runs over **UDP**.

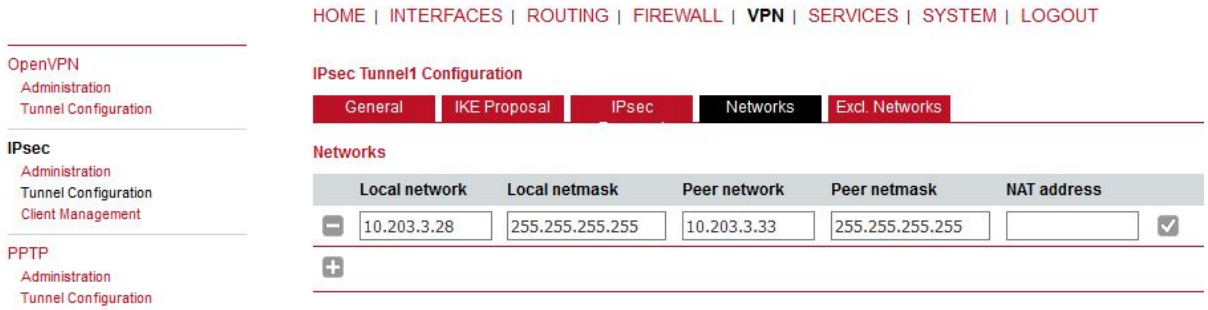


Fig. 4.10: M!DGE2 A – IPsec Networks

This can seem strange, but the WWAN IP addresses must be set as networks so that L2TP (or GRE) is built over IPsec – i.e. once IPsec is up, all the communication between these 2 units is via IPsec tunnel.

M!DGE2 B

Do almost the same configuration as with M!DGE2 A. See the screenshots below.

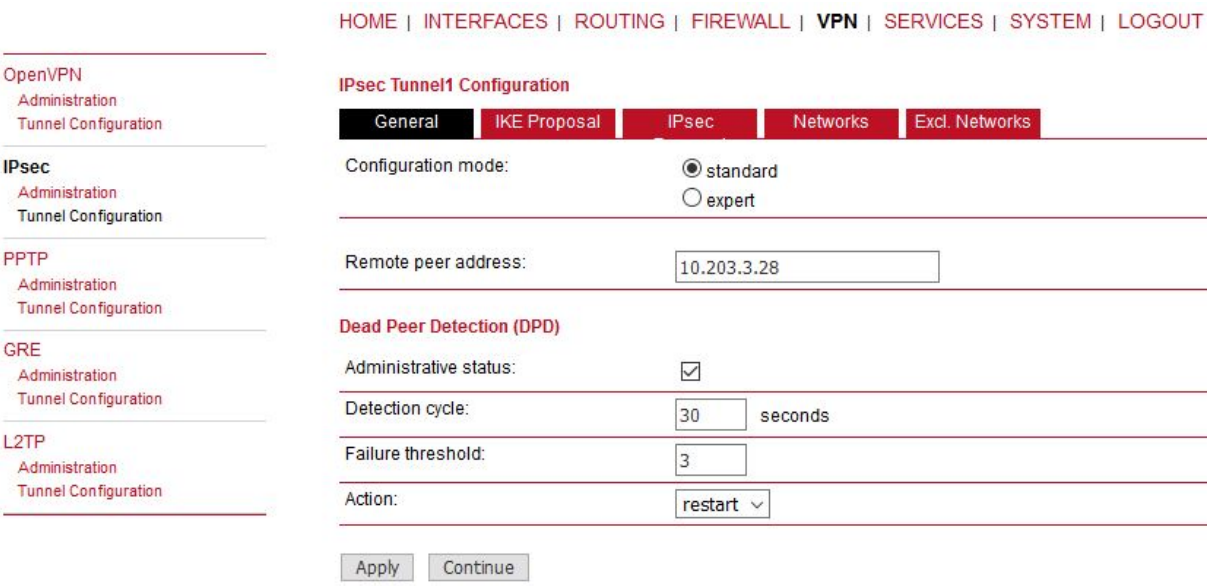


Fig. 4.11: M!DGE2 B – General IPsec configuration

Make sure to provide correct Peer address – i.e. M!DGE A WWAN IP (10.203.3.28). The DPD action can be “restart”.

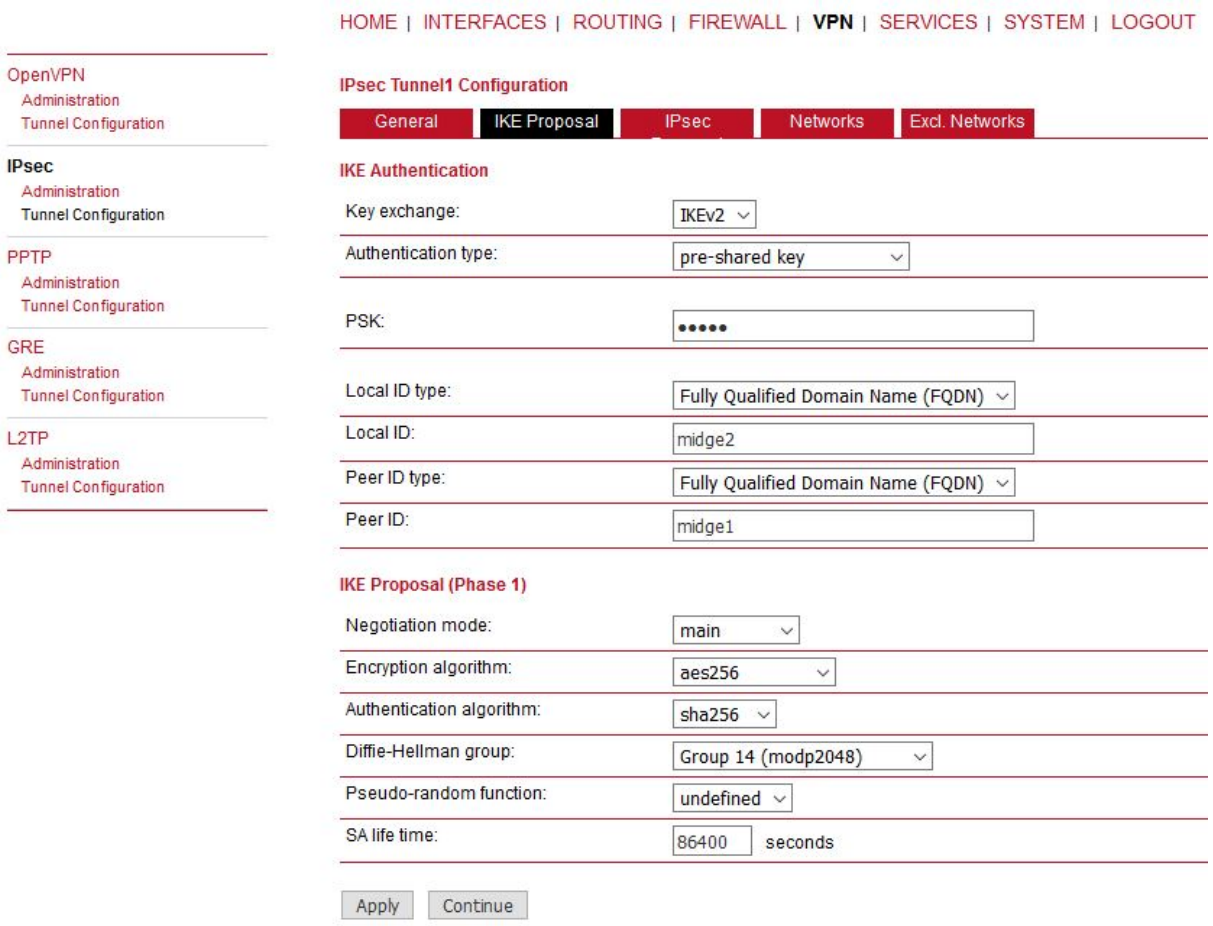


Fig. 4.12: M!DGE2 B – IPsec IKE Proposal

Make sure to set parameters the same as in M!DGE2 A, but with switched IDs. IPsec proposal is the same. The Networks are just switched.

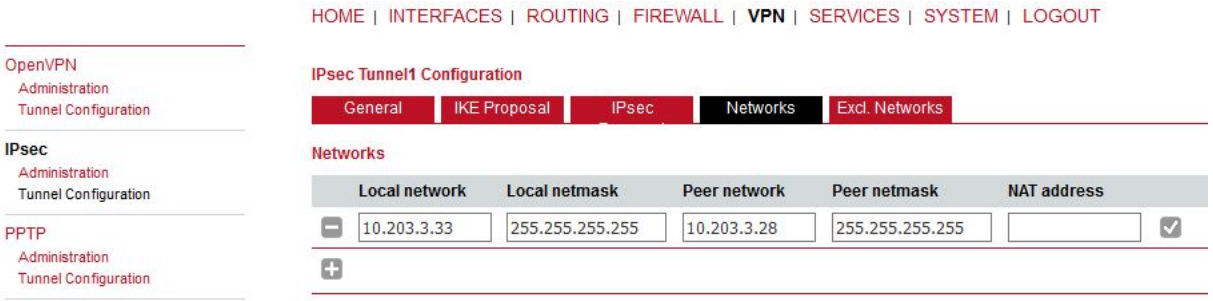


Fig. 4.13: M!DGE2 B – IPsec networks

Enable IPsec on both ends and wait until the tunnel is established.

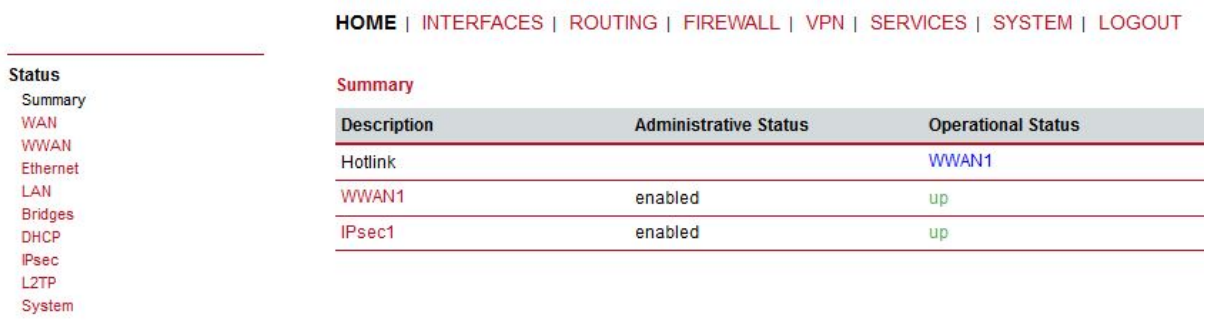


Fig. 4.14: IPsec tunnel being up

Verify the remote LAN IP accessibility again.

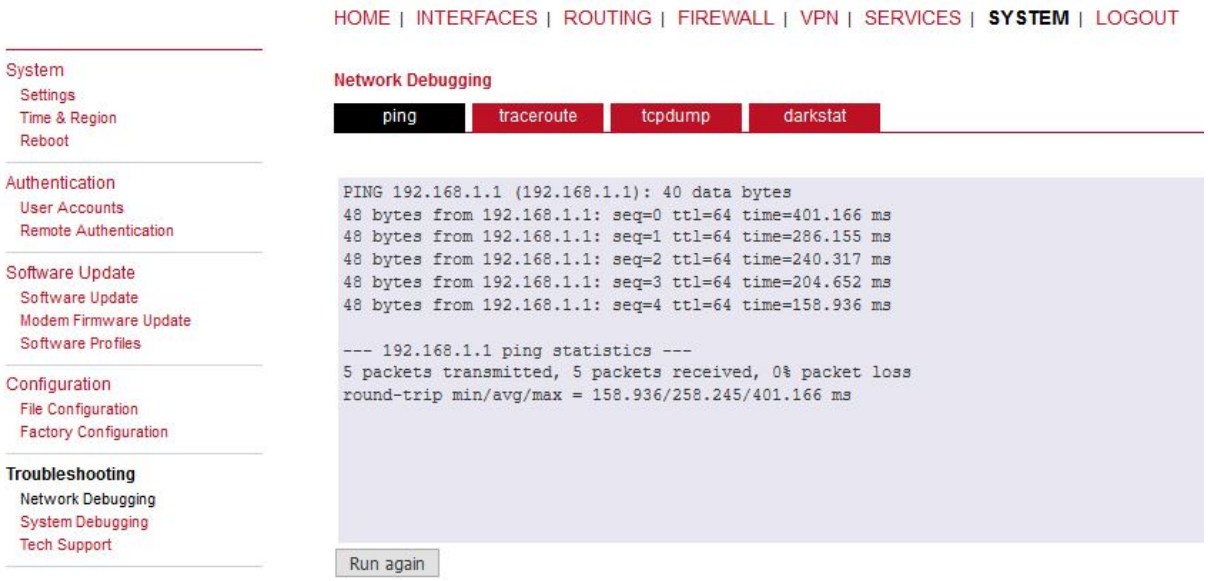


Fig. 4.15: Ping accessibility test

It is not visible if it really utilizes IPsec or just L2TP. For such a purpose, capture the WWAN traffic and open the file in Wireshark application.

Start tcpdump, excluding management ports.

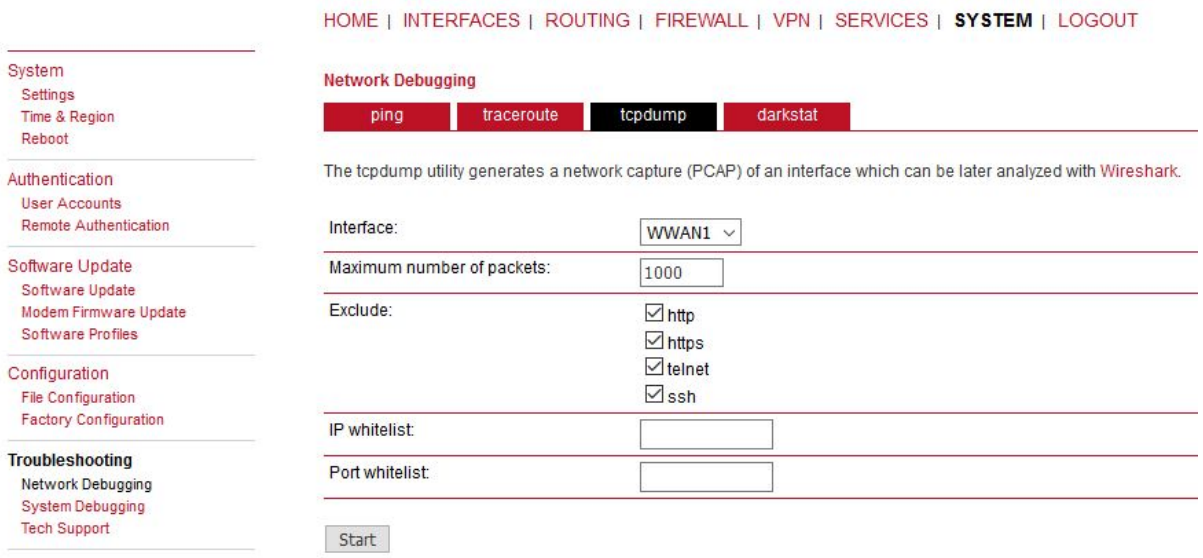


Fig. 4.16: Tcpdump capture

Click on the start button. Then, run the PING command in second M!DGE2 unit.

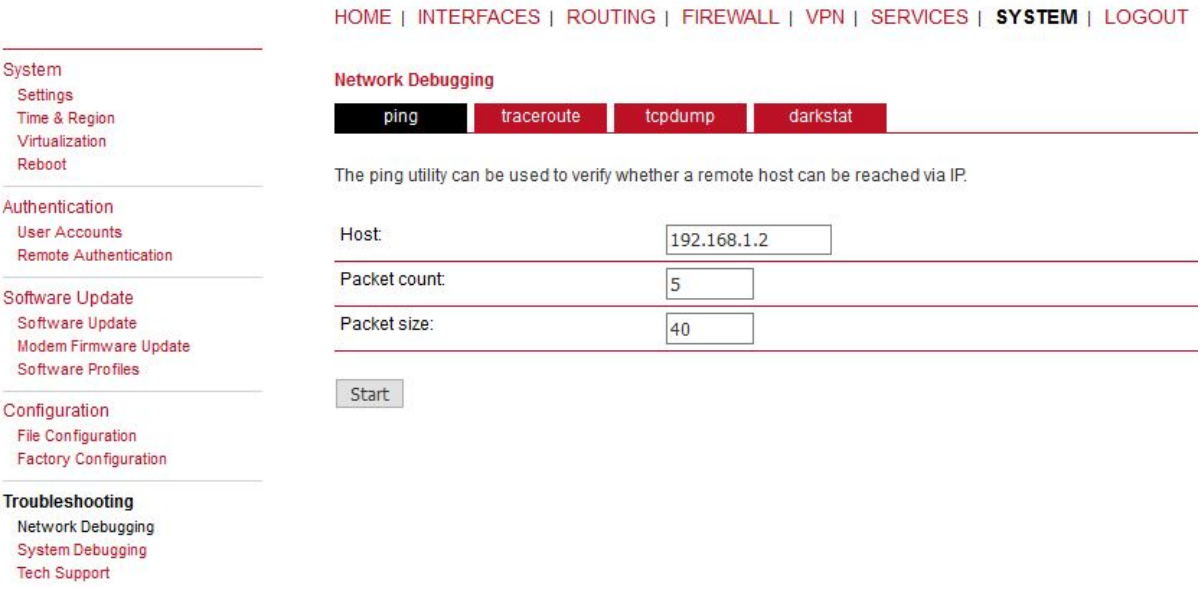


Fig. 4.17: PING to remote unit

After the test finishes, download the tcpdump file. Unzip this file and open the saved file in Windows/Linux application called Wireshark. Check that most of data are ESP (i.e. IPsec encapsulated). If not, check your configuration.

55	13.542262	10.203.3.33	10.203.3.28	ESP	178 ESP (SPI=0xc085a2f2)
56	14.541304	10.203.3.28	10.203.3.33	ESP	178 ESP (SPI=0xc8c2158e)
57	14.542147	10.203.3.33	10.203.3.28	ESP	178 ESP (SPI=0xc085a2f2)
58	14.625292	10.203.3.33	10.203.3.28	ESP	802 ESP (SPI=0xc085a2f2)
59	14.690017	10.203.3.28	10.203.3.33	ESP	162 ESP (SPI=0xc8c2158e)
60	15.113743	10.203.3.28	10.203.3.33	IGRP	466 Request
61	15.114239	10.203.3.28	10.203.3.33	ESP	1058 ESP (SPI=0xc8c2158e)
62	15.116092	10.203.3.33	10.203.3.28	ESP	162 ESP (SPI=0xc085a2f2)
63	15.541366	10.203.3.28	10.203.3.33	ESP	178 ESP (SPI=0xc8c2158e)
64	15.542206	10.203.3.33	10.203.3.28	ESP	178 ESP (SPI=0xc085a2f2)
65	16.620437	10.203.3.33	10.203.3.28	ESP	146 ESP (SPI=0xc085a2f2)
66	16.700364	10.203.3.28	10.203.3.33	ESP	146 ESP (SPI=0xc8c2158e)
67	17.202010	10.203.3.33	10.203.3.28	ESP	802 ESP (SPI=0xc085a2f2)
68	17.351734	10.203.3.28	10.203.3.33	ESP	162 ESP (SPI=0xc8c2158e)

Fig. 4.18: Wireshark ESP/IPsec example output

GRE over IPsec

The very the same principles are used for GRE tunnel over IPsec. Configure IPsec the same way. Configure GRE tunnel for Routing purposes – it is NOT connecting Layer2 devices, but Layer3 (IP). Thus, it requires different LAN subnets at individual sites, e.g. 192.168.1.0/24 and 192.168.2.0/24.

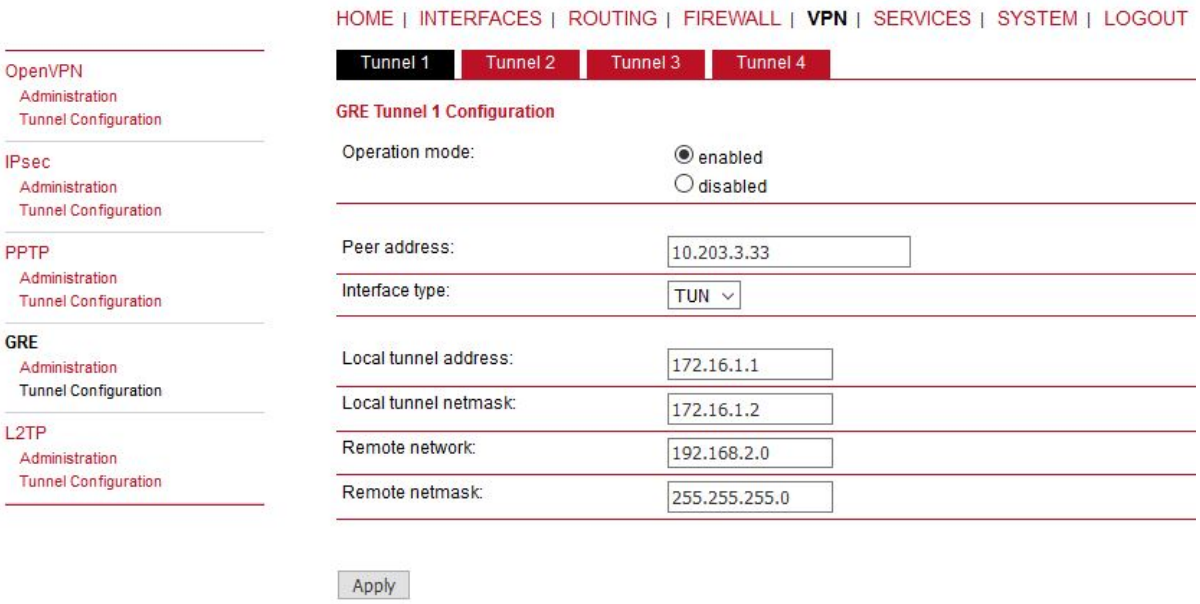


Fig. 4.19: GRE over IPsec example

Do the opposite site the same way, just mirror the parameters. If IPsec is disabled, you should see unencrypted data on WWAN encapsulated to GRE (new network 172.16.1.x). Once IPsec is enabled, you will see ESP data again.

Revision History

Revision 1.0 2017-12-06
First issue

Revision 1.1 2018-02-28
Termination of M!DGE UMTS routers manufacturing

Revision 1.2 2020-02-04
L2TP over IPsec chapter added

Revision 1.3 2021-04-09
Requirements for IP addresses enhanced.