Quick Start

MX530|MX880

with mdex OpenVPN-Device

Release: 2019-02-27 (v.1.0)

This is a supplement to the MX530/MX880 Setup Manual and describes the simple commissioning of the MX530/880 for remote access to a connected terminal device by using the preconfigured mdex fixed.IP+ / public.IP OpenVPN-Device.

Table of contents

1 Preconfiguration

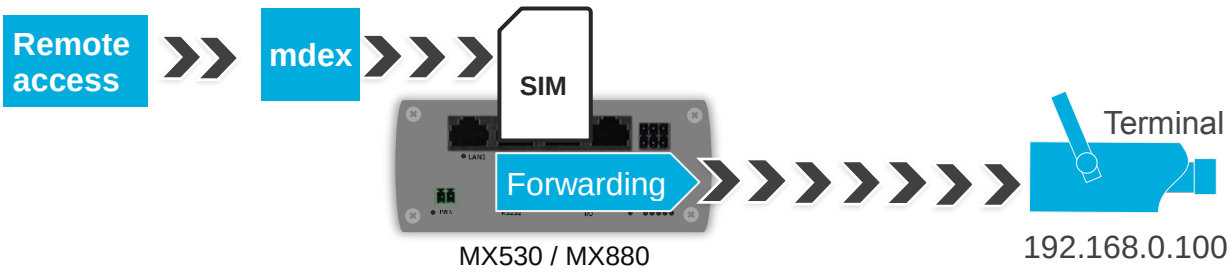
The MX530/MX880 is preconfigured for the ordered mdex fixed.IP+ / public.IP OpenVPN-Device:

OpenVPN Client enabled

- The OpenVPN client of this router is ready for use with your ordered OpenVPN-Device. (The OpenVPN-Device and the IP address are on the additional label.)
- All settings in the router are ready for OpenVPN use. (See also chapter **3.3 Deviations from standard** configuration (Seite 12).)
- Only the mobile settings must be set for the use of your SIM card as described in step 6.

The terminal device can be reached remotely.

- The terminal device obtains the LAN-IP address 192.168.0.100 via DHCP.
- The router forwards all incoming data packets to the 192.168.0.100 address.



Remote access to router web interface

Whether remote access to the MX530/ MX880 web interface is enabled or disabled in the preconfiguration can be found on the MX880 additional lable:

Remote: Disabled
➔ Remote access to the router is disabled and must be enabled if necessary.

Remote: HTTP Port 8080
➔ The router can be reached by remote, f.e. via web.direct port 8080 (mdex fixed.IP+).

Remote: https://xxx.xxx.xxx.xxx:4444
➔ The MX880 remote access is activated and accessible with the specified URL. If no remote access is required, please disable it.

More informations about configuring the MX880 remote access can be found at step 8 (page 8).

Secure login password

When the MX530/880 is preconfigured with a public.IP, the router is preset with an individual alphanumeric login password for accessing the web interface.

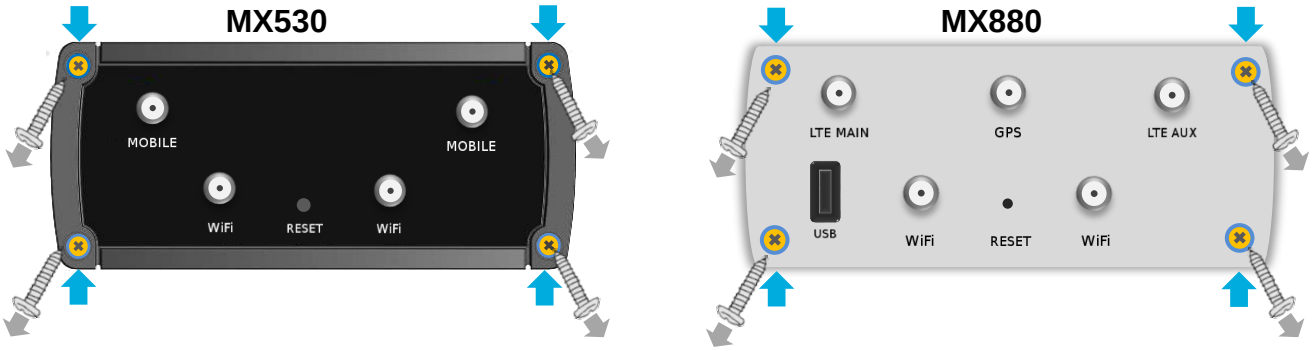
The password can be found on the router's additional label or alternatively in the mdex Management Portal, see step 4 (page 6).

2 Quick start

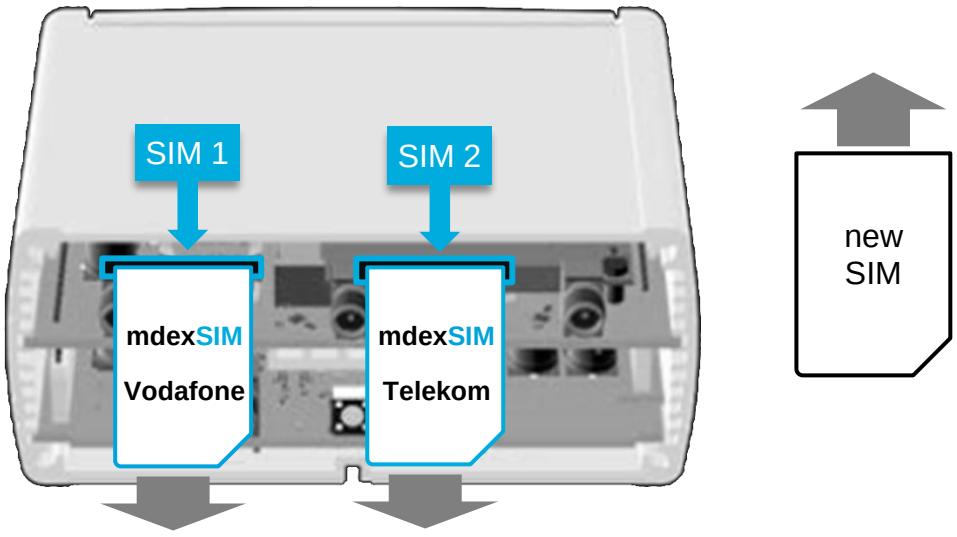
For quick installation please follow the steps below.

Step 1 Insert your SIM-card

1. Unscrew the 4 screws on the back of the router (antenna side) and remove the back cover.



2. Pull out the preinstalled SIM card(s) and insert the new SIM card(s) into the desired SIM card slot (preferably SIM 1).



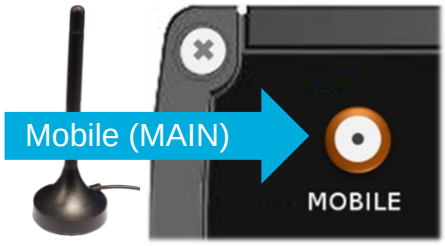
3. Secure the back cover with the four screws.

4. The MX530/MX880's mobile settings must be adjusted to use your SIM card(s), as described at Step 6.

Step 2 Connect mobile antenna(s)

MX530

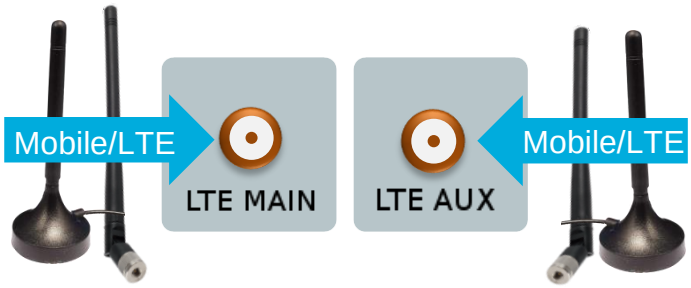
The magnetic base antenna (MOBILE) must be connected to the left **MOBILE** (MAIN) socket.



The other socket, 'MOBILE' (AUX), serves only to connect to another (optional) mobile antenna, e.g. in order to increase the download rate in mobile use.

MX880

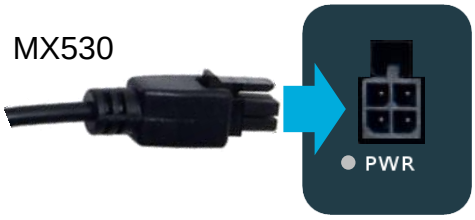
The mobile antenna (Mobile/LTE) with articulated joint or magnetic base antennas must be connected to **LTE MAIN** (main Antenna) and to **LTE AUX** (in order to increase LTE download rate).



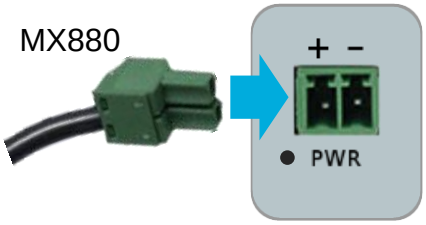
Step 3 Connect the power supply

Plug the router connector of the plug-in power supply into the PWR socket on the router.

MX530



MX880



To use your own power supply, refer to the MX530/880 **Setup Guide** in **Chapter 2.4** "Power Supply".

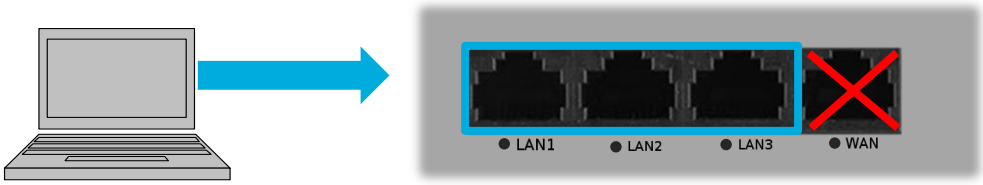
Step 4 Local access to router web interface

1. Set the network card of your PC to 'Obtain an IP address automatically' (DHCP).
   The MX530/MX880 is preconfigured for a dynamic assignment of IP addresses and automatically assigns the IP address **192.168.0.100** to the connected PC.

   ⚠ By default, the MX530/MX880 assigns only one IP address (192.168.0.100) to a connected network device!

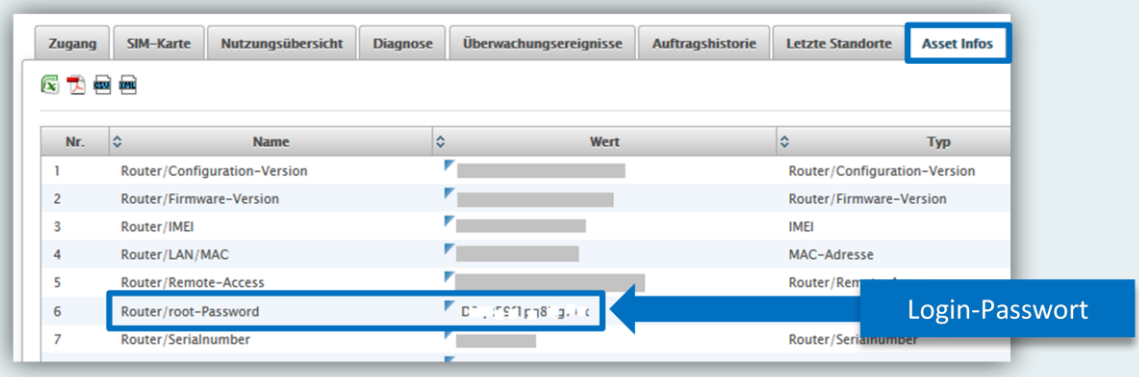
   - If another network device is connected that already has the IP address 192.168.0.100, remove this device again.
   - The IP address 192.168.0.100 will be **released after 5 minutes** and then assigned to your connected PC. Restarting the MX530/MX880 immediately releases the IP address and then assigns it to your connected PC.
   - Alternatively, you can also set the PC NIC to a fixed IP address from the IP address range 192.168.0.2 to 192.168.0.255 (for example, 192.168.0.20).

2. Plugin the network cable of the PC to a **LAN** socket (LAN1, LAN2 or LAN3) of the MX530/MX880. The WAN socket is not intended for connecting terminal devices!



3. To login the router web interface please use an Internet browser and enter the URL **http://192.168.0.1:8080** (or **https://192.168.0.1**).
   Username: **admin**
   Password: according to additional label or management portal

   ℹ When using a **public.IP**, an alphanumeric login password is preset, which you can find on the additional label or alternatively in the mdex **Management Portal** in the **Asset Infos** from the OpenVPN device:



Step 5 Setup mobile settings

The mobile settings in the MX530/MX880 must be set under **Network → Mobile (SIM)** for the operation of your SIM card(s).

A detailed description of the mobile settings can be found in the MX530/MX880 **Setup Guide** in Chapter "**3.5 SIM Mobile Phone Settings**".

Step 6 Establishing the connection

Mobile connection:

The MX530/MX880 establishes a mobile connection with the installed SIM-card.

As soon as the Status-LED lights up (or flickers), the mobile data connection is established:

green: 4G connection (MX880 only) **orange**: 3G connection **red**: 2G connection

The signal strength of the mobile network is displayed with .
The connection status is also displayed at **Status → Network** in the **Mobile** tab.

For more information about the status display and signal strength, refer to the **MX530/MX880 Setup Guide** at Section "**Connection Status and Signal Strength"**.

OpenVPN connection:

As soon as a mobile connection is established, the preconfigured OpenVPN client of the MX530/MX880 establishes an OpenVPN connection to mdex.
The current connection status is displayed at **Status → Network** in the **OpenVPN** tab.

Step 7 Login password

Especially when using a public.IP and the MX530/MX880 remote access is activated according to **step 8**, a secure login password must be set in the MX530/MX880.

You can either leave the default secure password or you can set your own secure password.

Enter new Login-Password

1. Set your own (secure) password at **System → Admin Settings**.
2. Click on the button **Save** to save the new password.
   The router is now accessed locally and remotely with the new login password.

Step 8 Remote access to router web interface

For a remote access to the MX530/MX880 router web interface, the remote access must be enabled in the router.

The remote preconfiguration of the MX530/MX880 is printed on the additional label:

`Remote: Disabled`
➔ Remote access to the router is **disabled** and must be enabled if necessary.

`Remote: HTTP Port 8080`
➔ Remote access is **enabled.** (mdex fixed.IP+.)

- The remote access is possible by web.direct Port 8080.
- Alternatively, when using an optional mdex control center (OpenVPN tunnel) with the URL http://fixed.IP:8080.

`Remote: https://xxx.xxx.xxx.xxx:4444`
➔ Remote access is **enabled.** (mdex public.IP.)

- Wenn generell kein Fernzugriff erforderlich ist, deaktivieren Sie bitte die Option **Enable remote HTTPS access**.

Edit remote access (enable / disable)

1. Click on **Services** → **HTTP/SSH**
2. Enable at **Web Access Control** the needed remote HTTP(s) access:

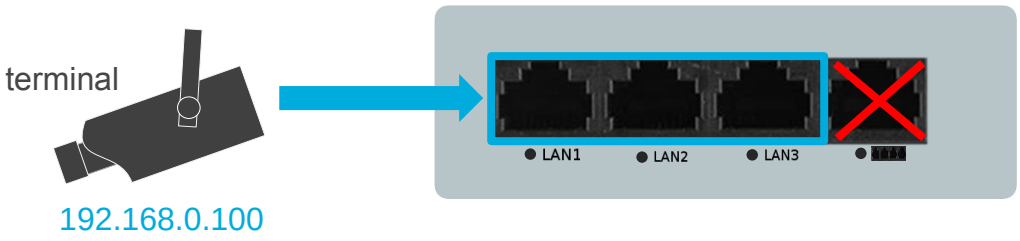
Enable remote HTTP access	Enables HTTP remote access to the web interface with the set HTTP port. (When using a fixed.IP+, HTTP port 8080 is recommended.)
HTTP Port	
Enable remote HTTPS access	Enables HTTPS remote access to the web interface with the set HTTPS port.
HTTPS Port	For security and compatibility reasons we recommend using HTTPS port 4444 when using a public.IP. The router can be reached via **https://xxx.xxx.xxx.xxx:4444** (xxx= your public.IP) from the Internet. Conflicts with remote access to other connected terminal devices via HTTPS port 443 are then avoided.
Source zone	In case of using a ‚fixed.IP / public.IP via OpenVPN', the source zone must be set to **VPN**!

3. Click on **Save**.

Step 9a Connecting a terminal via 'host forwarding'

With the preset 'host forwarding' (DMZ configuration) the connected terminal device 192.168.0.100 can be reached with the mdex fixed.IP+ / public.IP over all ports and protocols. The entered ports in 'Port Forwarding' according to **Step 9b** and the own ports of the MX530/MX880 (e.g. for remote access) are not forwarded via 'host forwarding'.

1. Remove all connected terminal devices and connect only the desired terminal device to the **LAN1**, **LAN2** or **LAN3** jack of the MX530/MX880.



⚠ For security reasons, the device must be protected against unauthorized access from the Internet with a firewall. More protection is given if only the required ports are forwarded according to **step 9b**.

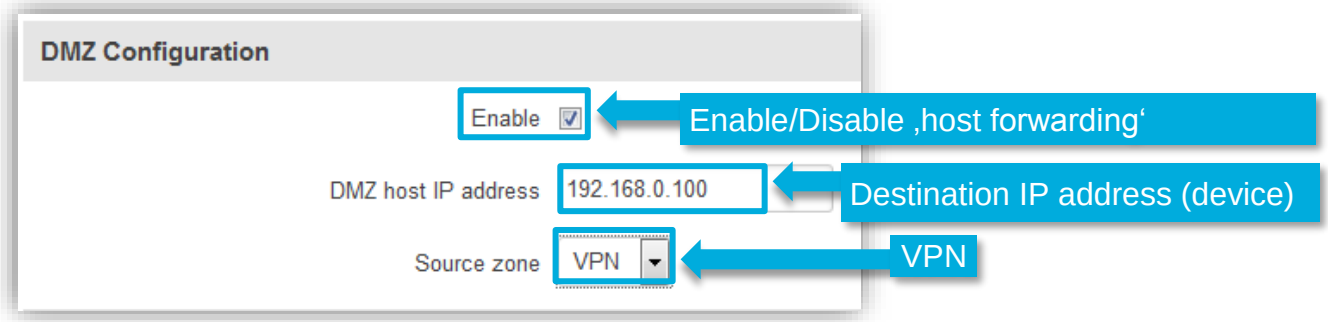
2. Following the instructions of **step 4**, the terminal device automatically obtains the required network addresses from the MX530/MX880 via DHCP.
   IP address: **192.168.0.100** | Gateway: **192.168.0.1** | DNS-Server: **192.168.0.1**
   Alternatively, the network addresses can also be permanently set in the terminal device.

ℹ Further information and individual adjustments can be found in the **MX530/MX880 Setup Guide** at chapter "**2.6 Connecting the terminal devices**".

3. The terminal device can now be reached from the Internet.
   (The active port for remote access in **step 8** is not forwarded to the terminal device.)

Setup 'host forwarding' (edit / disable)

1. Click on **Network → Port Forwarding**.
2. The ‚host forwarding' is set at **DMZ Configuration**:



3. Click on **Save**.

Step 9b Connecting terminals via 'port forwarding'

Port forwarding is suitable for the following applications:

- If several connected terminal devices should be reached by remote.
- To increase security, so that the connected terminal devices can only be reached only via the required ports from the Internet. (especially in case of using a public.IP!)

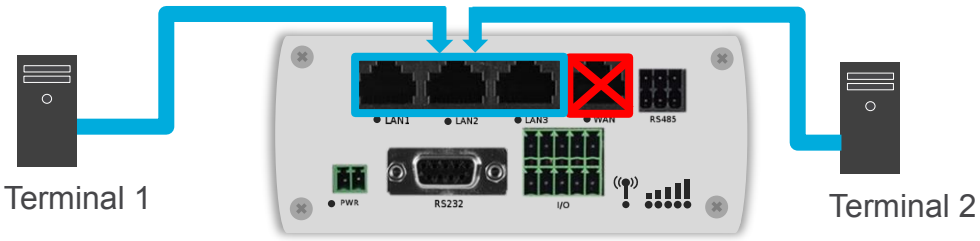
The 'host forwarding' according to **Step 9a** works parallel to the 'port forwarding'. All unregistered ports in 'Port Forwarding' are forwarded to the IP address of the 'Host Forwarding'.

Add Port Forwarding rules

1. Click on **Network** → **Port Forwarding**.
2. At **DMZ Configuration** the checkbox 'Enable' should be removed. Otherwise all unregistered ports will be forwarded to the terminal device with this IP address!
3. Setup the required ports to the IP addresses (terminal devices) with **New Port Forwarding Rule**.

Name:	Enter the name oft this forwarding rule.
Protocol:	Choose the protocol TCP/UDP of this forwarding.
External port(s):	Enter the incoming port. It´s possible to enter several subsequent ports (for example: 2000-2200).
Internal IP:	Ziel-IP-Adresse des Endgeräts eingeben.
Internal port(s):	Enter the internal port of the terminal device. It´s possible to enter several subsequent ports (for example: 2000-2200).
Source Zone:	For ‚fixed.IP/public.IP via OpenVPN' must be set **VPN**.
Add:	This forwarding rule will be added tot he router.

4. Save the setting with **Save** and add further port forwarding if necessary
5. Connect your terminal device(s) at the ports **LAN1**, **LAN2** oder **LAN3**.



6. Set the IP address, Gateway and DNS server in the network settings of the terminal device(s): IP addess: **192.168.0.xxx** | Gateway: **192.168.0.1** | DNS-Server: **192.168.0.1**

> ⚠ Please note that the MX530/880 DHCP server automatically assigns the IP address **192.168.0.100** to a connected terminal device by default.

> ⓘ When connecting several terminal devices, the DHCP server can always assign the same IP address to certain terminal device, see **MX530/MX880 Setup Guide** → Chapter "**2.6 Connecting the terminal devices**".

7. The connected terminal devices are now accessible via the enabled ports from the Internet. (The active remote access according to **Step 8** is not forwarded to the terminal device.)

3 Appendix

3.1 Further functions / adaptations

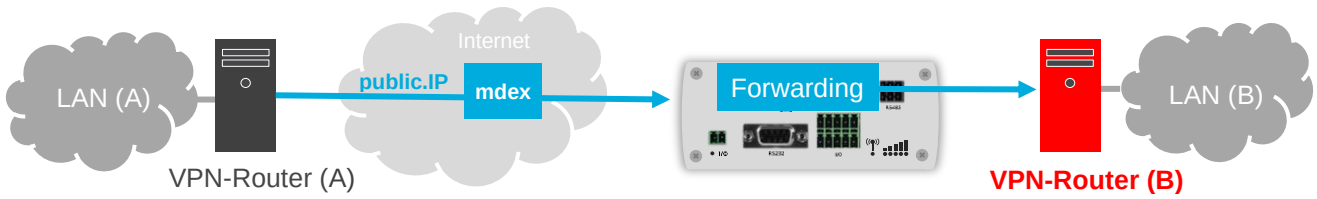
For further functions and adaptations of the MX530/MX880 (e.g. change LAN IP address, adapt DHCP server, activate WLAN, etc.), please refer to the enclosed MX530/MX880 **Setup Guide** or our support page **https://wiki.mdex.de**.

Please note that the preconfiguration described in the general instructions from the MX530/MX880 router differs from this preconfiguration with OpenVPN according to **3.3 Deviations from standard** configuration (page 12).

3.2 IPsec connection to a VPN-Router (public.IP)

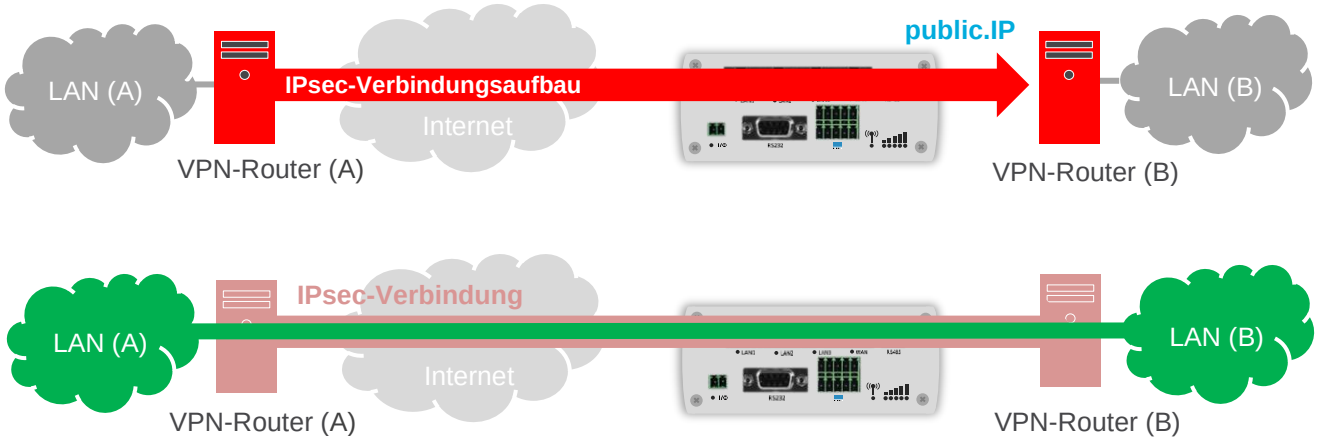
Setup steps for establishing an IPsec connection to a (own) **VPN router (B)** connected to the MX530/MX880 when using an mdex **public.IP** via OpenVPN.

1. Connect the **VPN-Router (B)** according to **Step 9a** or **Step 9b** to the MX530/MX880.



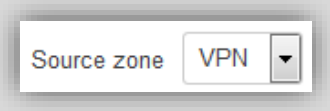
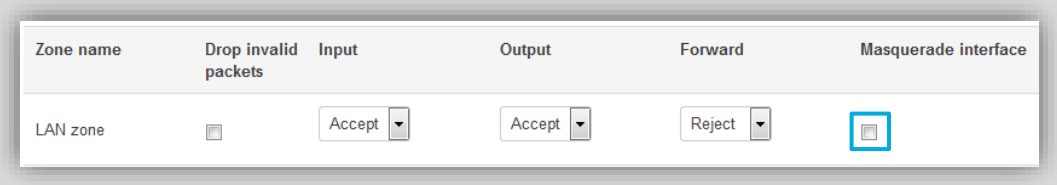
2. Enable the **NAT Traversal** (NAT-T) option in all IPsec clients. Otherwise an IPsec connection setup is usually not possible.
   (For all further settings required for an IPsec connection, please refer to the instructions of the IPsec routers or IPsec clients you are using.)

3. The **VPN router (A)** can now use the public.IP to establish an IPsec connection to the **VPN router (B)** so that **LAN (A)** and **LAN (B)** are securely connected:



3.3 Deviations from standard configuration

Below you will find the different settings of this preconfigured MX530/MX880 with OpenVPN to the original standard configuration.

1.	**OpenVPN Client**	The OpenVPN client is configured and activated with the respective role 'mdex fixed.IP+' or 'mdex public.IP'. The respective mdex OpenVPN access data (username and password) are set. (The required OpenVPN access data can be found in the mdex Management Portal.)
2.	**Ping check**	At **Services Ping/periodic Reboot** is set for **Hosts to ping** the server '172.21.0.1'. (For monitoring the OpenVPN-connection.)
3.	**Source zone set to ‚VPN‘**	The **Source zone** is set to **VPN** for the following menu items: At Network → Port Forwarding At Services → HTTP/SSH 
4.	**Remote access**	Only when using a **public.IP** is at **Services → HTTP/SSH** the parameter 'Enable remote HTTP access' disabled. For security and compatibility reasons is ‘Enable remote HTTPS access’ maybe enabled and set to HTTPS port 4444.
5.	**Masquerade (LAN zone) disabled**	Only when using a **public.IP** is for compatibility reasons at **Network → Firewall** the LAN zone for the 'Masquerade interface' disabled. 
6.	**Secure Password**	Only when using a **public.IP** is a secure login password (administrator password) set at **System → Admin Settings**.

3.4 Reset to preconfiguration settings

With these steps you can reset the MX530/MX880 to the preconfiguration settings.

1. Start the MX530/MX880 (switch on power supply).
2. Press the **RESET** button with a pointed object, leave it pressed for about 10 seconds, then release it again.

   ⚠ All router configuration settings will be reset to factory default settings now!

3. After approx. 1-2 minutes the router web interface can be reached again by URL **http://192.168.0.1:8080** or **https://192.168.0.1**. (Username: admin | Password: admin01).
4. Adjust the configuration of the MX530/MX880 according to chapter **3.3 Deviations from standard** configuration.
5. Reboot the MX530/MX880. The router is now back in its default state for using the mdex fixed.IP+ / public.IP via OpenVPN.