1 Using NAT in VPN connections

Document ID: 108411_en_00
Document designation: AH EN MGUARD IPSEC VPN NAT

Make sure you always use the latest documentation.
This is available to download at phoenixcontact.net/products.

Contents of this document

This document describes the configuration of IPsec VPN connections using 1:1 NAT and IP masquerading.

1.1 Introduction

A VPN connection can normally only be established between different networks (e.g. network A: 192.168.**1**.0/24 <-> network B: 192.168.**2**.0/24).

If the same internal networks (e.g. 192.168.**1**.0/24) are used at two locations, the following problems can arise:

1. If the locations are connected via a VPN tunnel, this would lead to routing problems. It would not be clear which network should receive the packets that are sent to IP addresses of the internal network which is the same on both sides.
   This problem can be avoided by using of **1:1 NAT** (see Section 1.2).
2. If several locations with partially identical internal networks are connected to a central location via a VPN tunnel, this would also lead to routing problems. This problem can be avoided by using **1:1 NAT** or partially avoided by using **IP masquerading** (see Section 1.3 and 1.5).

1.1.1 1:1 NAT

1:1 NAT means that the **network part** of an IP address is assigned to another network and the **host part** remains unchanged (e.g. **192.168.1**.**102**/24 <-> **192.168.2**.**102**/24). The network part is defined via the subnet mask.

Here, a *Real network* (e.g. the internal network) is assigned to a *Virtual network* in order to circumvent existing network overlapping. The VPN tunnels are then established via *Virtual* instead of *Real networks*.

1.1.2 IP masquerading

IP Masquerading is a special type of NAT. It must be enabled on gateways that connect private networks to the Internet in order to be able to access the Internet.

When accessing a website from an internal network, the gateway (NAT router) replaces the private IP address of the sender (e.g. 192.168.1.100) with its own public IP address (e.g. 77.245.32.78). The destination web server therefore knows which public address it should reply to.

This then replaces the reply of the web server to the NAT router (77.245.32.78) with the IP address of the original sender (192.168.1.100) and forwards it to the client in the internal network.

IP masquerading is only used in one direction, e.g. from the internal to an external network or the Internet. A client in the internal network (e.g. 192.168.1.100) could then access destinations in the external network or on websites in the Internet, but would not be accessible via its private IP address from the external network or the Internet.

IP masquerading in VPN connections

IP masquerading in VPN networks provides the same functionality, however within a VPN connection.

If data packets are sent to a remote network via the VPN tunnel, the mGuard device replaces the IP address of the sender with a specific, unique IP address and reverses the masquerading upon receipt of the answer from the remote network.

The great advantage here is that the entire real (local) network is *masked* by a single IP address.

If several VPN connections end at a central VPN gateway, this function reduces the necessary address space for the VPN connections and makes VPN configuration clearer.

1.2 Connecting locations with the same internal networks (1:1 NAT)

1.2.1 Example

Two locations with the same internal network (192.168.1.0/24) are to be connected via a VPN tunnel. For this, **local NAT for IPsec tunnel connections (1:1 NAT)** must be used on both mGuard devices.

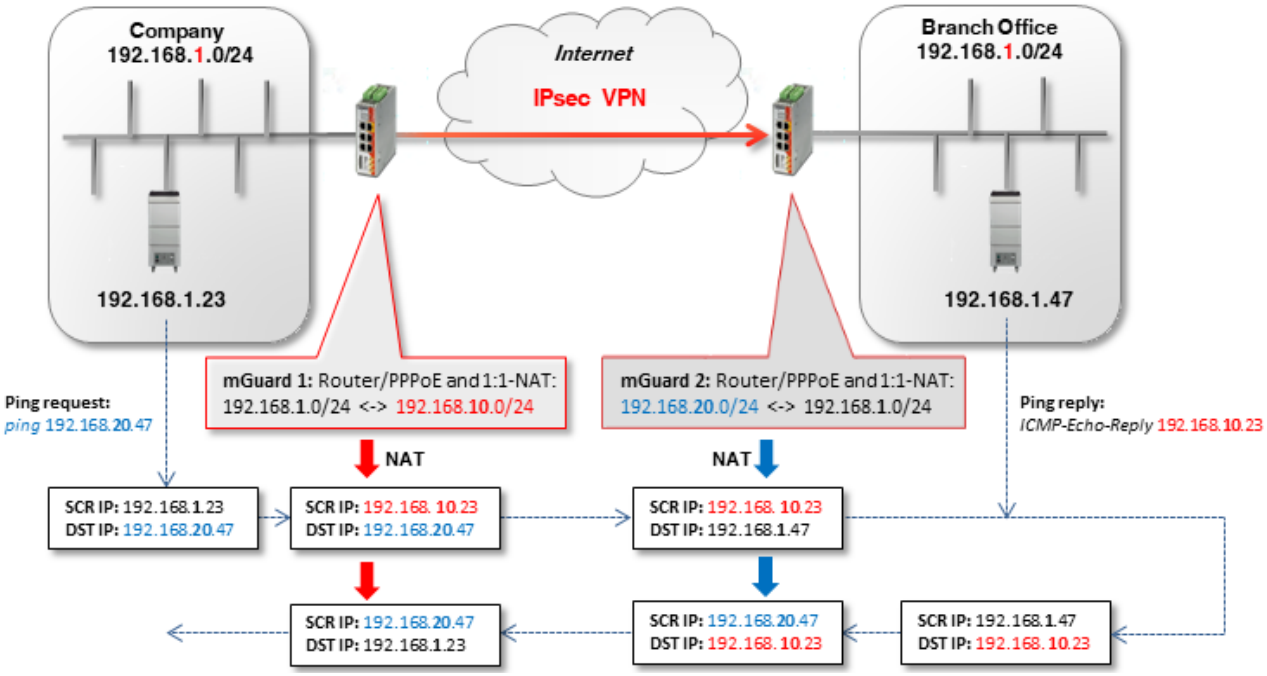


Figure 1-1 Same internal networks: ping request via a VPN tunnel using local 1:1 NAT

- **mGuard 1** performs 1:1-NAT: 192.168.**1**.0/24 <-> 192.168.**10**.0/24.
  The network part is rewritten and the host part is retained. The clients can therefore be reached in the company network via the VPN tunnel in the *Virtual network* 192.168.**10**.0/24.
- **mGuard 2** also performs 1:1-NAT: 192.168.**1**.0/24 <-> 192.168.**20**.0/24.
  The clients in the branch network can be reached via the VPN tunnel in the *Virtual network* 192.168.**20**.0/24.

1.2.2 Configuring the VPN connection

The VPN tunnel must be established between *Virtual networks*. For this, a local 1:1 NAT is performed on both devices.

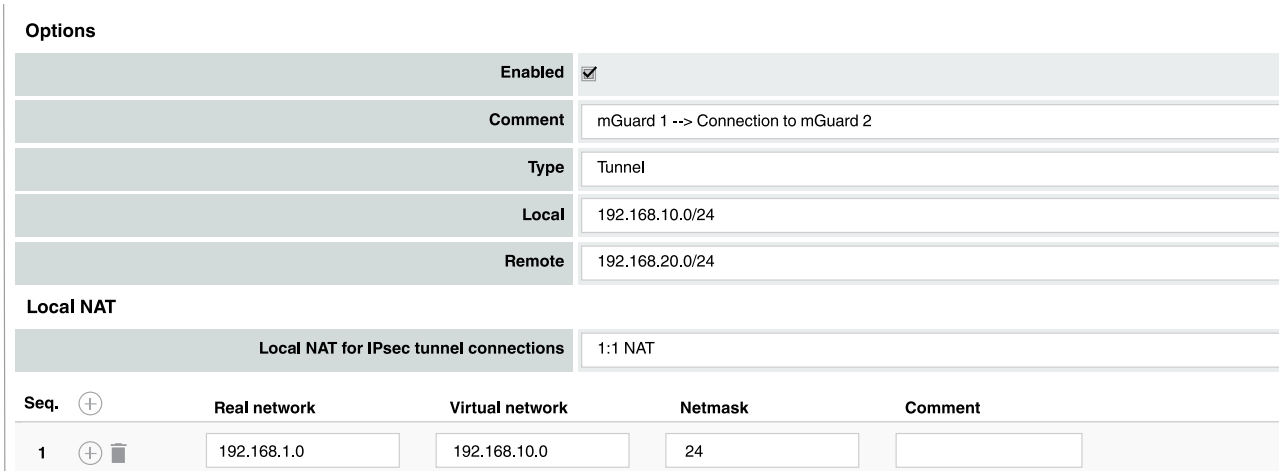


Figure 1-2 **mGuard 1**: IPsec VPN >> General (tunnel setting with 1:1 NAT)

To configure the VPN connection of the mGuard devices, proceed as follows:

1. Go to **IPsec VPN >> Connections**.
2. Click on the ⊕ icon to add a new VPN connection.
3. Give the connection a unique name and click on the ✎ icon.
4. Under **Transport and tunnel settings**, click on the icon ✎.
5. Configure the VPN connection in accordance with Table 1-1 and Figure 1-2.

Table 1-1 Configuring the VPN connection

Section	Parameter	Company / mGuard 1	Branch / mGuard 2
IPsec VPN >> Connections >> (Edit) >> General			
Options	**A descriptive name for the connection**	VPN to the branch	VPN from the company
	Address of the remote site's VPN gateway	77.245.32.78	%any
	Interface to use for gateway setting %any	-----	External
	Connection startup	Initiate	Wait
Transport and tunnel settings >> (Edit) >> General			
Transport and tunnel settings	**Type**	Tunnel	Tunnel
	Local	192.168.**10**.0/24	192.168.**20**.0/24
	Remote	192.168.**20**.0/24	192.168.**10**.0/24
Local NAT	**Local NAT for IPsec tunnel connections**	1:1 NAT	1:1 NAT
	Real network	192.168.**1**.0	192.168.**1**.0
	Virtual network	192.168.**10**.0	192.168.**20**.0
	Netmask	24	24

Result

– Packets to the company network in the internal network of *mGuard 1* must be sent to the *Virtual network* 192.168.**10**.0/24.
– Packets to the branch network in the internal network of *mGuard 2* must be sent to the *Virtual network* 192.168.**20**.0/24.

1.3 Connecting locations with the same internal networks to a control center (1:1 NAT)

1.3.1 Example

Two locations that use the same internal network (192.168.1.0/24) are to be connected simultaneously to the company control center via a VPN tunnel. For this, **local NAT for IPsec tunnel connections (1:1 NAT)** must be used on both mGuard devices.

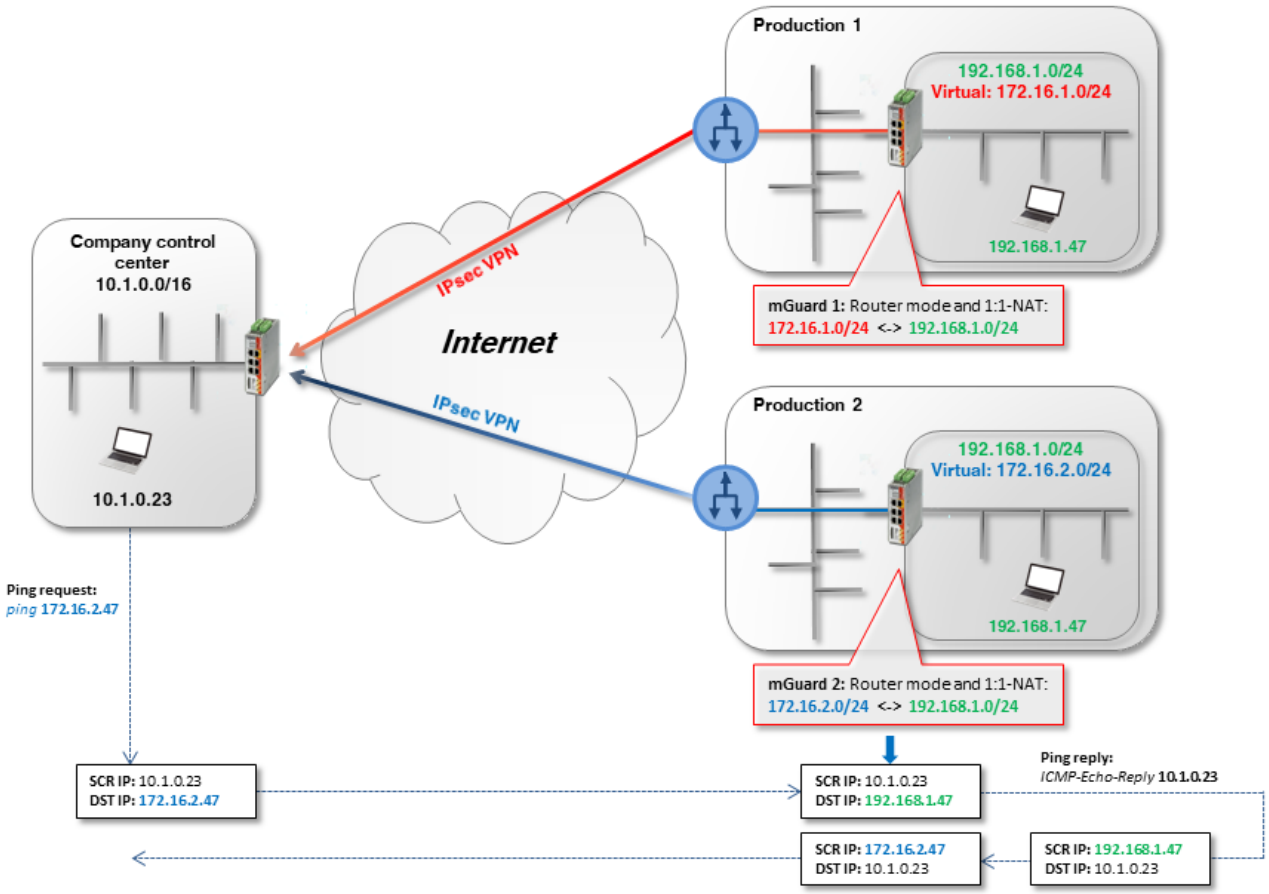


Figure 1-3 (Example *mGuard 2*) The same internal networks: ping request (to production 2) from the company control center via the VPN tunnel using local 1:1 NAT

- **mGuard 1** performs 1:1-NAT: 192.168.1.0/24 <-> 172.16.**1**.0/24).
  The clients in its internal network (**production 1**) can be reached via the VPN tunnel in the *Virtual network* 172.16.**1**.0/24.
- **mGuard 2** performs 1:1-NAT (192.168.1.0/24 <-> 172.16.**2**.0/24).
  The clients in its internal network (**production 2**) can be reached via the VPN tunnel in the *Virtual network* 172.16.**2**.0/24.

Configuring VPN connection

Two VPN connections must be configured on the mGuard device of the control center and a local 1:1 NAT must be performed on each. Here, the *Virtual network* of mGuard **1** or **2** must be specified in the tunnel settings as the peer (172.16.**1**.0/24 or 172.16.**2**.0/24).

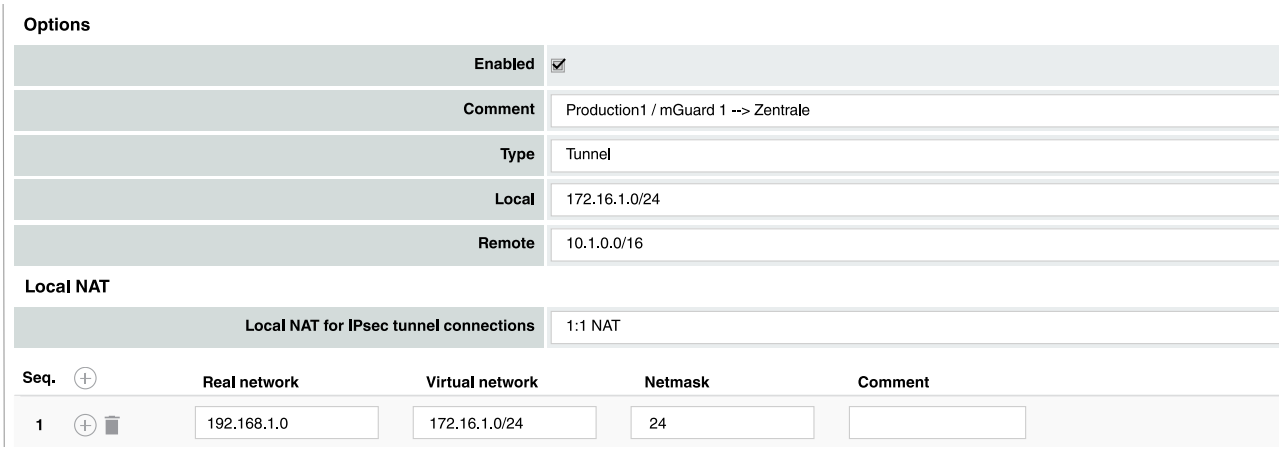


Figure 1-4 **mGuard 1**: IPsec VPN >> General (tunnel settings with 1:1-NAT)

To configure the VPN connection of the mGuard devices, proceed as follows:

1. Go to **IPsec VPN >> Connections**.
2. Click on the ⊕ icon to add a new VPN connection.
3. Give the connection a unique name and click on the ✎ icon.
4. Under **Transport and tunnel settings**, click on the icon ✎.
5. Configure the VPN connection in accordance with Table 1-2 and Figure 1-3.

Table 1-2 Configuring the VPN connection

Section	Parameter	Production mGuard 1	Production mGuard 2	Control center
IPsec VPN >> Connections >> (Edit) >> General				
Options	**A descriptive name for the connection**	VPN to control center	VPN to control center	To production (**1** or **2**)
	Address of the remote site's VPN gateway	77.245.32.78	77.245.32.78	%any
	Interface to use for gateway setting %any	-----	-----	External
	Connection startup	Initiate	Initiate	Wait
Transport and tunnel settings >> (Edit) >> General				
Transport and tunnel settings	**Type**	Tunnel	Tunnel	Tunnel
	Local	172.16.**1**.0/24	172.16.**2**.0/24	10.1.0.0/16
	Remote	10.1.0.0/16	10.1.0.0/16	172.16.**1**.0/24 or 172.16.**2**.0/24
Local NAT (Only mGuard 1 or 2)	**Local NAT for IPsec tunnel connections**	1:1 NAT	1:1 NAT	
	Real network	192.168.**1**.0	192.168.**1**.0	
	Virtual network	172.16.**1**.0/24	172.16.**2**.0/24	
	Netmask	24	24	

Result

Packets to the network **production 1** (in the internal network of *mGuard 1*) or **production 2** (in the internal network of *mGuard 2*) must be sent to the *Virtual network* 172.10.**1**.0/24 or 172.16.**2**.0/24.

1.4 Connecting locations with the same internal networks to a control center (masquerading)

The control center is to be connected to several external locations (production) using a central VPN gateway via VPN tunnel. Some of the external locations use the same internal networks or the same internal network as the control center.

1.4.1 Example 1: Transmission in one direction (IP masquerading)

IP masquerading can be used if the data is only to be transmitted in one direction – from the machine controllers to the control center.

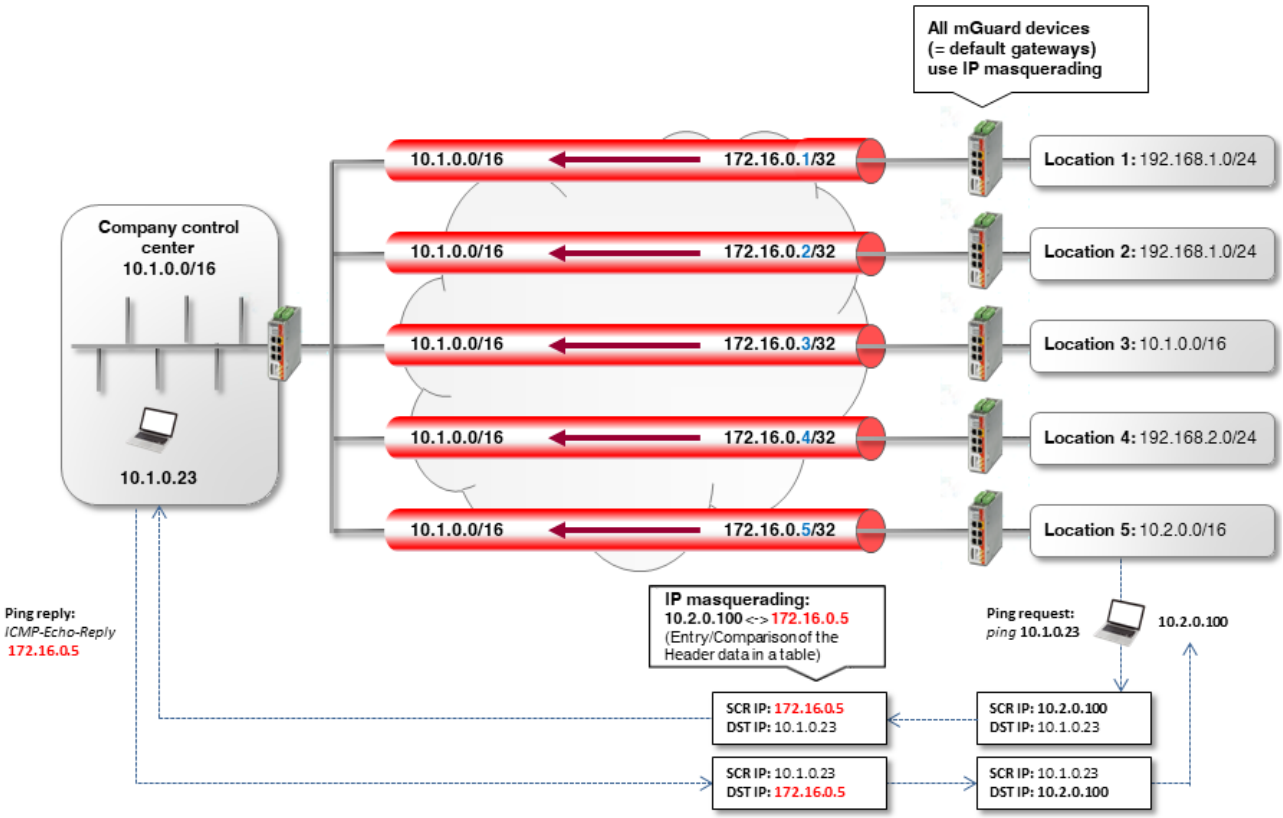


Figure 1-5 **Transmission in just one direction (IP masquerading)**: clients (e.g. PLCs) in the external networks can send data to the control center via VPN. However, the control center **cannot** access the clients. The respective mGuard device is the default gateway of the internal client.

Configuring VPN connection

To be able to establish connections with the control center from all locations, IP masquerading must be used at every location. In this case, the IP address used for masquerading can simply be increased at each location.

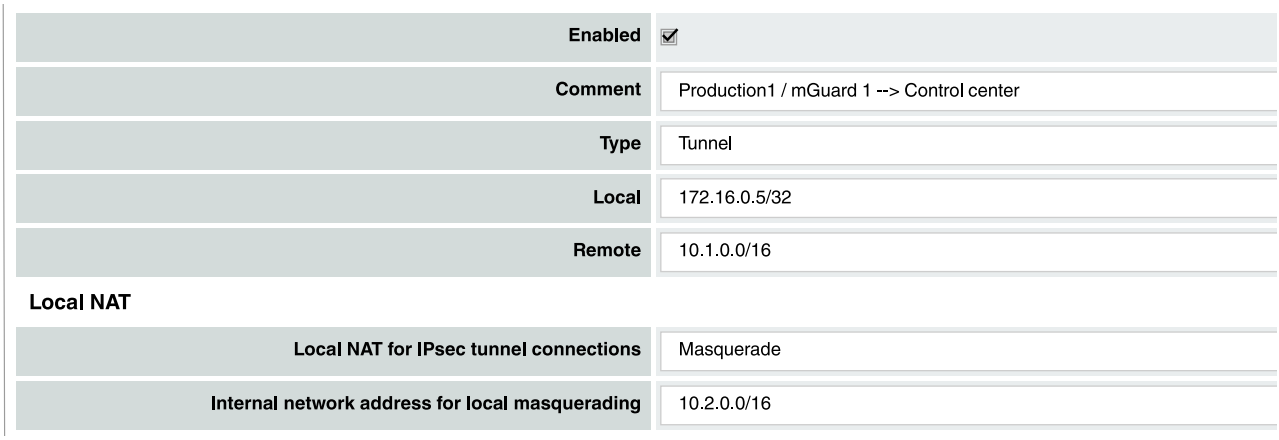


Figure 1-6 Configuration example *Location 5* (tunnel settings with IP masquerading)

Table 1-3 Configuring VPN connection

Section	Parameter	Control center	Location 5
IPsec VPN >> Connections >> (Edit) >> General			
Options	**A descriptive name for the connection**	VPN from Location 5	VPN to control center
	Address of the remote site's VPN gateway	%any	77.245.32.78
	Interface to use for gateway setting %any	External	-----
	Connection startup	Wait	Initiate
Transport and tunnel settings >> (Edit) >> General			
Transport and tunnel settings	**Type**	Tunnel	Tunnel
	Local	10.1.0.0/16	172.16.0.5/32
	Remote	172.16.0.5/32	10.1.0.0/16
Local NAT	**Local NAT for IPsec tunnel connections**	No NAT	Masquerade
	Internal network address for local masquerading	-----	10.2.0.0/16

Result

The clients in the network of the control center can be reached via their real IP addresses.

Advantages

Configuring VPNs is uncomplicated and easy to understand. The address space for the peers is reduced.

Disadvantages

The VPN connections can only be used in one direction. In the above example, only the locations can access the control center.

1.4.2 Example 2: Transmission in both directions (1:1 NAT)

If data is to be transmitted in both directions, local 1:1 NAT must be used (see also Section 1.3).

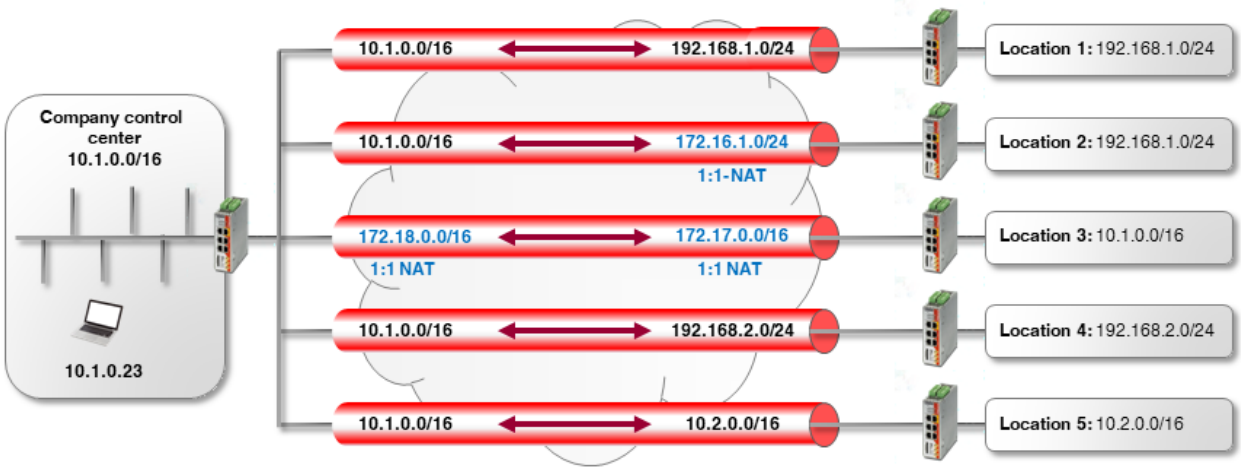


Figure 1-7 **Transmission in both directions (local 1:1 NAT):** the clients (e.g. PLCs) in the external networks can access the control center network via the VPN network, and vice versa.

1. **Location 1**: both locations have different internal networks, which means that the VPN tunnel can be established between networks 10.1.0.0/16 and 192.168.1.0/24.
2. **Location 2**: the internal network of *Location 2* (192.168.1.0/24) is already used for the VPN connection to *Location 1*.

   In order to be able to access the internal network of Location 2 via VPN, 1:1 NAT must be used at the VPN gateway. The VPN tunnel will be established between the Real *network* 10.1.0.0/16 and the *Virtual network* 172.16.1.0/24 (see also Section 1.3).
3. **Location 3**: both networks have the same internal network 10.1.0.0/16.

   In order to establish a VPN connection between the two networks, 1:1 NAT must be used at both VPN gateways. The VPN tunnel will be established between the *Virtual networks* 172.18.0.0/16 and 172.17.0.0/16 (see also Section 1.2).
4. **Locations 4 and 5**: both locations have internal networks that are not used by other VPN connections. Therefore, neither 1:1 NAT nor IP masquerading needs to be used to be able to access the other network in each case.

NOTE: Do not use *Virtual networks* that are already used for other VPN connections.

Configuring VPN connection

The connections are configured along the same lines as Section 1.3.

Advantages

The VPN connections can be used in both directions. The locations can be reached by the control center via the VPN connections, and vice versa.

Disadvantages

Each VPN connection has to be configured separately, depending on which internal network configuration the participating peers use.

Configuration becomes increasingly complex as the number of remote locations increases – which can easily lead to incorrect configurations.

1.5 Using 1:1 NAT for the remote network

The company network is connected to a branch via a VPN connection. The clients (destination systems) in the branch network can be reached via the VPN tunnel.

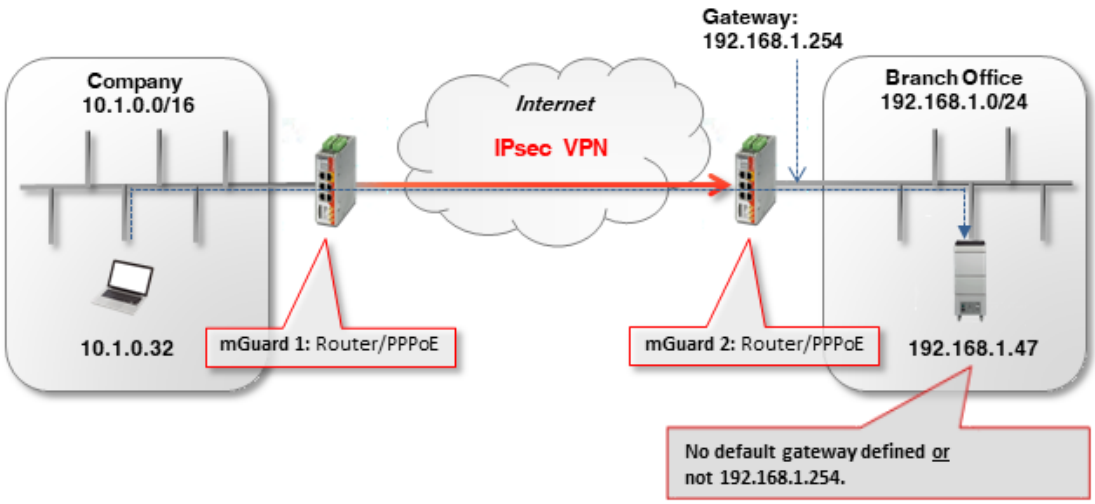
However, there is no default gateway defined on a destination system (e.g. a machine controller which normally only has to be accessed internally), or the defined default gateway is not the mGuard device that makes the VPN tunnel available as the VPN gateway.

The destination system therefore cannot respond to VPN access instances from the company network. If the IP setting of the destination system cannot be changed, the **Remote NAT for IPsec tunnel connections** function can be used to avoid this problem.

1.5.1 Example

The company network (10.1.0.0/16) is not recognized by the destination system (192.168.1.47/24). If the destination (machine controller) receives a packet via VPN tunnel from the company network,

– it will not respond to this at all (if a default gateway has not been defined) or
– it will send the response to its default gateway (and not to the *mGuard 2* VPN gateway).

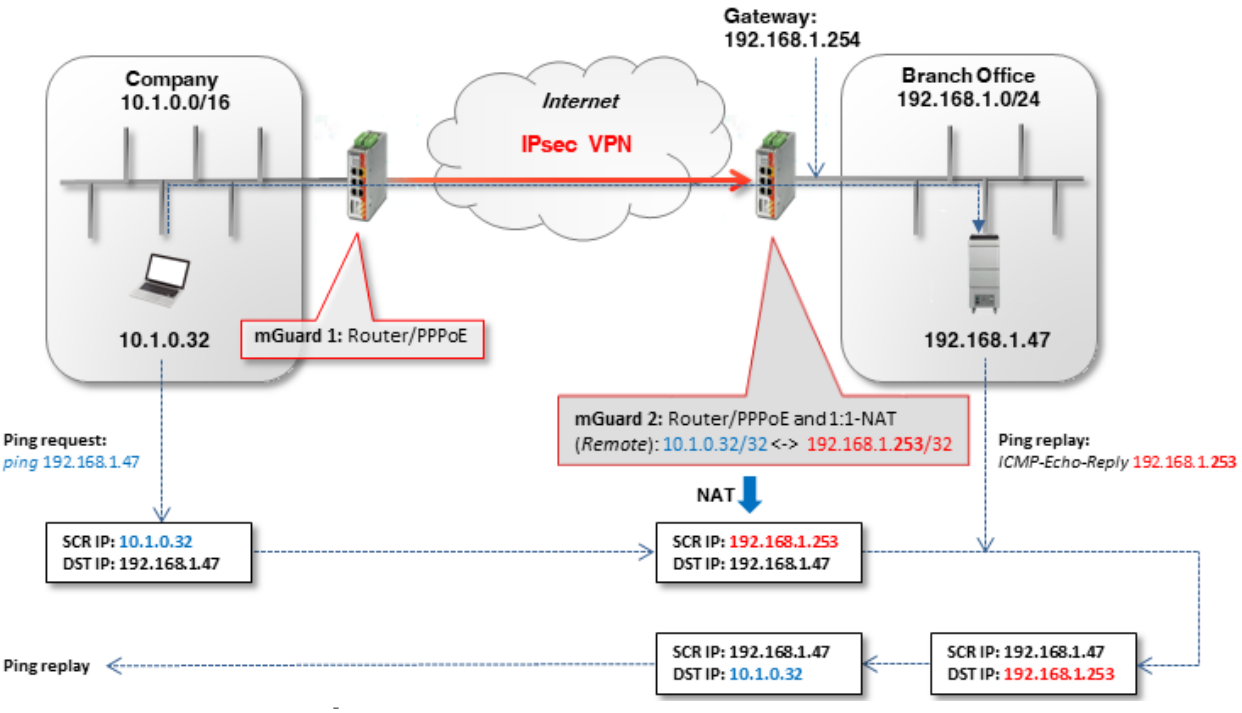


Solution

The **Remote NAT for IPsec tunnel connections** function (*1:1 NAT*) is used in the VPN tunnel settings of *mGuard 2* (branch VPN gateway).

1.5.2 Configuring VPN connection

Remote 1:1 NAT must be used to enable the destination system (e.g. machine controller with IP address 192.168.1.47) to send a response to the "unknown" sender.



Options	
Enabled	☑
Comment	From Company to Branch Office
Type	Tunnel
Local	192.168.1.0/24
Remote	10.1.0.32/32
Local NAT	
Local NAT for IPsec tunnel connections	No NAT
Remote NAT	
Remote NAT for IPsec tunnel connections	1:1 NAT
Network address for remote 1:1 NAT	192.168.1.253

Figure 1-8 **mGuard 2**: IPsec VPN >> General (Tunnel settings with 1:1 NAT)

To configure the VPN connection of the mGuard devices, proceed as follows:

1. Go to **IPsec VPN >> Connections**.
2. Click on the ⊕ icon to add a new VPN connection.
3. Give the connection a unique name and click on the ✎ icon.
4. Under **Transport and tunnel settings**, click on the icon ✎.
5. Configure the VPN connection in accordance with Table 1-4 and Figure 1-8.

Table 1-4 Configuring the VPN connection

Section	Parameter	Company / mGuard 1	Branch / mGuard 2
IPsec VPN >> Connections >> (Edit) >> General			
Options	**A descriptive name for the connection**	VPN to the branch	VPN from the company
	Address of the remote site's VPN gateway	77.245.32.78	%any
	Interface to use for gateway setting %any	-----	External
	Connection startup	Initiate	Wait
Transport and tunnel settings >> (Edit) >> General			
Transport and tunnel settings	**Type**	Tunnel	Tunnel
	Local	**10.1.0.32/32**	192.168.1.0/24
	Remote	192.168.1.0/24	**10.1.0.32/32**
Remote NAT	**Remote NAT for IPsec tunnel connections**	No NAT	1:1 NAT
	Network address for 1:1 NAT in the remote network	-----	192.168.1.**253**

The remote network or the remote IP address is rewritten *(mapped)* to a **free (virtual) IP address** in the internal network of the branch: **10.1.0.32/32 <-> 192.168.1.253**.

A netmask does not need to be specified for the remote network (192.168.1.253). This is automatically adopted by the specified peer network.

The *Virtual network* / IP address must not be used by network clients in the internal network of the branch.

According to the configuration used in the example, only the client 10.1.0.32 in the company network has access to the destination in the branch.

Be careful when selecting the subnet mask for the remote network and specify the network to which the remote network is to be assigned (see "Problem with 1:1 NAT for remote networks").

The ARP proxy of *Guard 2* provides the ARP resolution for the *Virtual network* / IP address. The destination system sends its responses to *mGuard 2*:

- Packets from the company network (10.1.0.0/16) are sent via the VPN gateway (*mGuard 1*) to the real IP address of the destination client in the branch (**192.168.1.47)**.
- *mGuard 2* receives the request, performs a 1:1-NAT for the remote network / IP address (**10.1.0.32/32** <-> **192.168.1.253**) and forwards the request to the destination client (**192.168.1.47**).
- The destination client receives the request and sends its response packet to the virtual sender's IP address (**192.168.1.253**).
- *mGuard 2* receives the response, reverses the 1:1-NAT (**192.168.1.253** <-> **10.1.0.32/32**) and forwards the response to *mGuard 1* or the sender in the company network (**10.1.0.32**).

Problem with 1:1 NAT for remote networks

The subnet mask */24* for the remote network (e.g. 10.1.0.0/24) and a remote 1:1-NAT address (e.g. 192.168.1.0) would not work, because in this case, the ARP proxy of *mGuard 2* would respond to all ARP requests from the internal network of the branch (192.168.1.0 – 192.168.1.255).

Increasing the subnet mask of the remote network would also increase the number of clients in the company network from where the client in the branch can be accessed. However, the number of unused IP addresses in the branch required to assign the source IP address would also increase.

The following table summarizes the relationship between

– the remote subnet mask,
– the clients that can access the destination system,
– the number of necessary unused IP addresses in the internal network.

	Example 1	Example 2	Example 3	Example 4
Specified remote network	10.1.0.0/26	10.1.0.64/26	10.1.0.128/28	10.1.0.32/32
Remote IP addresses that can access the destination system	10.1.0.0 – 10.1.0.63	10.1.0.64 – 10.1.0.127	10.1.0.128 – 10.1.0.143	10.1.0.32
Internal network	192.168.1.0/24			
Network address for remote 1:1 NAT	192.168.1.128/26	192.168.1.192/26	192.168.1.240/28	192.168.1.253/32
Hosts to which the mGuard would respond to ARP requests **(Must not be used in the internal network!)**	192.168.1.128 – 192.168.1.191 **64 hosts**	192.168.1.192 – 192.168.1.255 **64 hosts**	192.168.1.240 – 192.168.1.255 **16 hosts**	192.168.1.253 **1 host**

Additional NAT router

If several clients in the company network are to access the destination system in the branch, a NAT router can be used before the packets are transferred to the VPN tunnel.

For this, the IP address of the NAT router must be specified with subnet mask */32* as the remote network. Only one unused IP address would be necessary.

IP masquerading

If the VPN connection is only to be used in one direction, e.g. from the company network to the branch (remote maintenance), *IP masquerading* can be used on *mGuard 1* in the tunnel instead of an additional NAT router (see also Section 1.4).

In this way, the incoming data packets at *mGuard 2* always have the same source IP address (/32).