1 Configuring VPN connections with various network modes

Document ID: 108410_en_00
Document designation: AH EN MGUARD IPSEC VPN NW MODE
© PHOENIX CONTACT 2018-10-16

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 between two mGuard devices with different network modes (*Router*, *Stealth*).

The examples show the configuration under **IPsec VPN >> Connections >> (*Edit*) >> General**.

1.1 Introduction

VPN connections are configured via the menu **IPsec VPN >> Connections** in four tabs.

Configuration in the *Authentication, Firewall* and *IKE Options* tabs is carried out independenty of the general network properties of the mGuard device, such as **network mode** (e.g. *Stealth*, *Router*, *Router/PPPoE*) or **VPN function** (e.g. *1: 1 NAT* for the local network, *hub and spoke*).

In the *General* tab, however, these properties have an effect on the tunnel settings; various properties in the *General* tab will therefore be considered in the following examples.

1.2 VPN transport connection (Stealth <-> Stealth)

1.2.1 Introduction

In contrast to a VPN tunnel connection that connects two networks, a VPN transport connection is used to link two individual clients (hosts).

If the VPN transport connection is used between two mGuard devices in the *Router* network mode, it is not possible to access all clients in the internal network of the devices via the VPN connection.

Using a transport connection is therefore only meaningful if the mGuard devices are operated in the *Single Stealth mode* (e.g. to secure data transfer between two clients or to access a client via a secure connection for maintenance purposes). The devices must be in the same network.

A transport connection cannot be used if the connection is established via one or more gateways in which Network Address Translation (NAT) is enabled.

1.2.2 Example

Two clients (hosts) in the same network are to be connected via an IPsec VPN connection in order to ensure permanent encrypted data exchange. Figure 1-1 shows the network configuration of the participating clients.

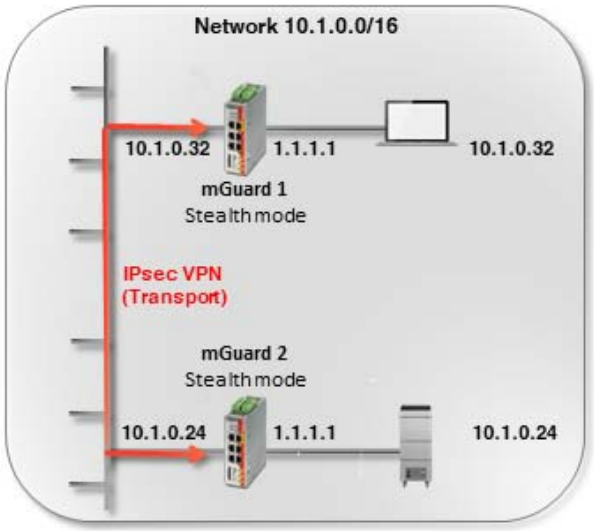


Figure 1-1 VPN transport connection in the *Stealth* network mode

The VPN connection (type: *transport*) is established and made available via two mGuard devices in the *Stealth* (*Automatic*) network mode connected upstream of the respective clients.

In *Stealth mode* (*Automatic*), the two mGuard devices adopt the IP and MAC address of their respective internal clients (*mGuard 1* adopts 10.1.0.32 and *mGuard 2*: 10.1.0.24).

1.2.3 Configuring the VPN connection

Figure 1-2 shows the configuration of the mGuard devices (in illustrated form for the sake of clarity). The transport and tunnel settings are the same on both devices.

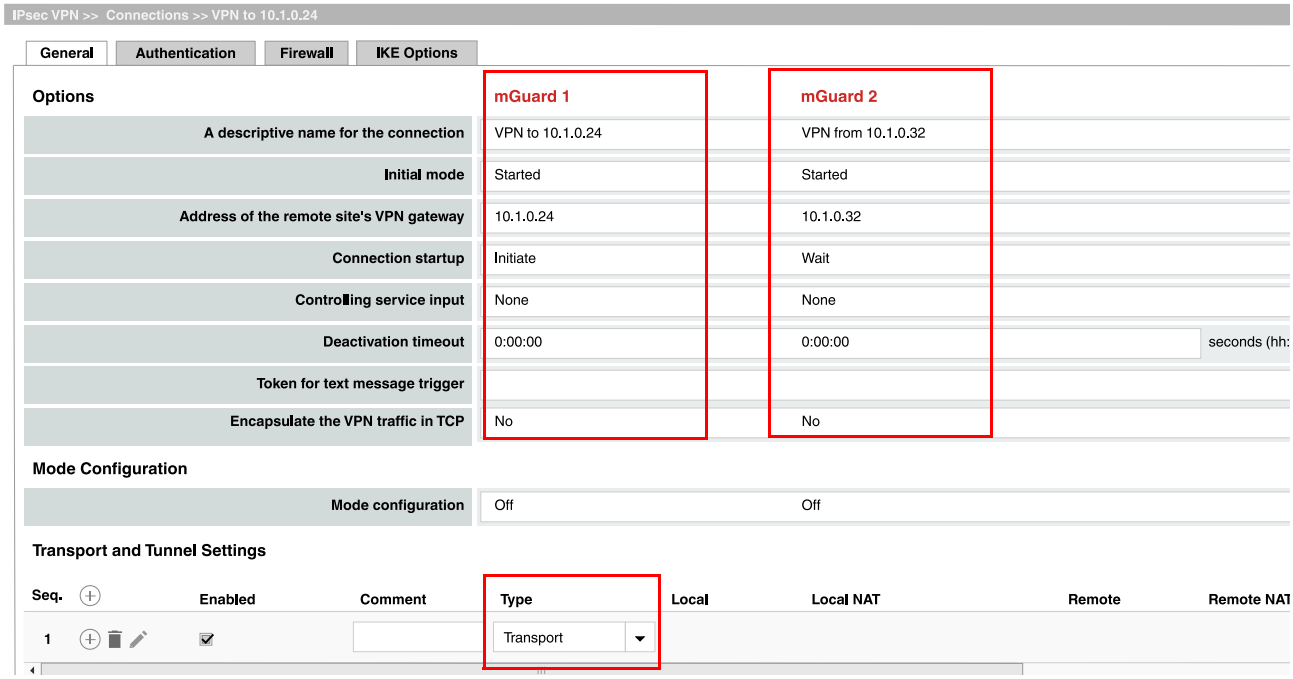


Figure 1-2 VPN connection (type: *transport*): Stealth mode <-> Stealth mode

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. Specify a unique name for the connection and click on the ✎ icon to edit the connection.
4. Configure the VPN connection in accordance with Figure 1-2 or Table 1-1.

Table 1-1 Configuring VPN connection (*IPsec VPN* >> *Connections* >> *(Edit)* >> *General*)

Section	Parameter	mGuard 1	mGuard 2
Options	**A descriptive name for the connection**	VPN to 10.1.0.24	VPN from 10.1.0.32
	Address of the remote site's VPN gateway	10.1.0.24	10.1.0.32
	Connection startup	Initiate	Wait
Transport and tunnel settings	**Type**	Transport	Transport

Result

The two clients, each of which are connected to the network via an mGuard device in the *Stealth* network mode, communicate via the encrypted IPsec VPN connection established between the mGuard devices (type: *transport*).

A *transport connection* only ever connects two individual clients (hosts), not networks – as is the case with a *tunnel connection*.

1.3 VPN tunnel connection (Router <-> Router)

1.3.1 Introduction

In contrast to a VPN transport connection that connects two individual hosts, a VPN tunnel connection is used to connect two networks.

1.3.2 Example

An IPsec VPN tunnel is to be established between **company network 1** (192.168.1.0/24) and **company network 2** (192.168.2.0/24) using two mGuard devices.

A VPN tunnel can only be established between different networks. If two locations have the same internal network, the VPN 1:1 NAT function has to be used for the local network (see “Using NAT in VPN connections” on page 1).

In this case *mGuard 1* initiates the VPN connection. *mGuard 2* waits for the connection. Both mGuard devices are operated in the *Router* (*static*) network mode.

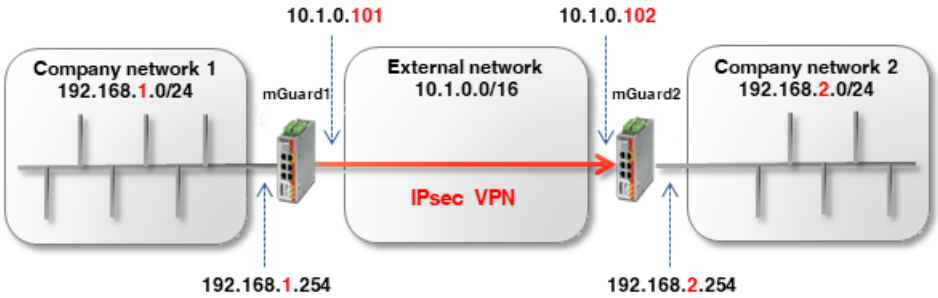


Figure 1-3 Connecting two networks via IPsec VPN

The network settings of the interfaces of the two mGuard devices are configured in the menu **Network >> Interfaces** (tabs: *General*, *External*, *Internal*). Both devices are operated in the *Router* (*static*) network mode.

Table 1-2 Network configuration of the interfaces

Parameter	mGuard 1	mGuard 2
External IP address	10.1.0.101	10.1.0.102
Netmask	255.255.0.0	255.255.0.0
Default gateway	10.1.0.254	10.1.0.254
Internal IP address	192.168.1.254	192.168.2.254
Netmask	255.255.255.0	255.255.255.0

The clients in the internal networks are to use the internal IP address of the respective mGuard device as the default gateway.

Optional setup in the PPPoE router mode

Establishing a VPN tunnel between two mGuard devices in the *PPPoE* router mode via the Internet is similar in principle (see Figure 1-4). In this case, the Internet is the external network. The devices receive their dynamically assigned public (external) IP addresses from the Internet Service Provider (ISP).

In order to enable static name resolution under these circumstances, the devices must register their current IP addresses under a fixed name with a DynDNS provider.

The initiating mGuard device (*mGuard 1*) must then provide a reference to the DynDNS name of the responding mGuard device (e.g. *mGuard2.dyndns.org*) in order to establish a VPN connection.

In this case, activate **DynDNS Monitoring** (**IPsec VPN >> Global >> DynDNS Monitoring**) in the VPN connection of the initiating device (*mGuard 1*). Otherwise, the device will not know when the IP address of the remote peer has changed and the VPN connection will not be established.

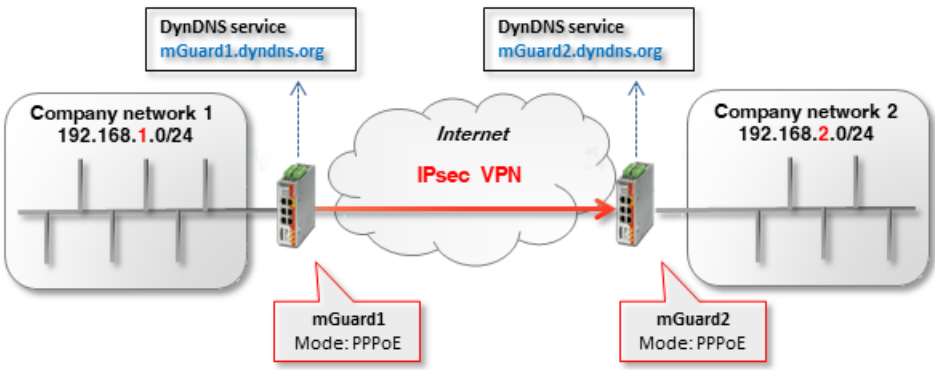


Figure 1-4 Connecting two networks via IPsec VPN (*Router/PPPoE* <-> *Router/PPPoE*). The host names for the mGuard devices are determined using DynDNS. (Because in this example the VPN connection is initiated by *mGuard 1*, in principle it does not need a DynDNS address.)

1.3.3 Configuring the VPN connection

Configure the VPN connection in accordance with Figure 1-5 and 1-6 or Table 1-3.

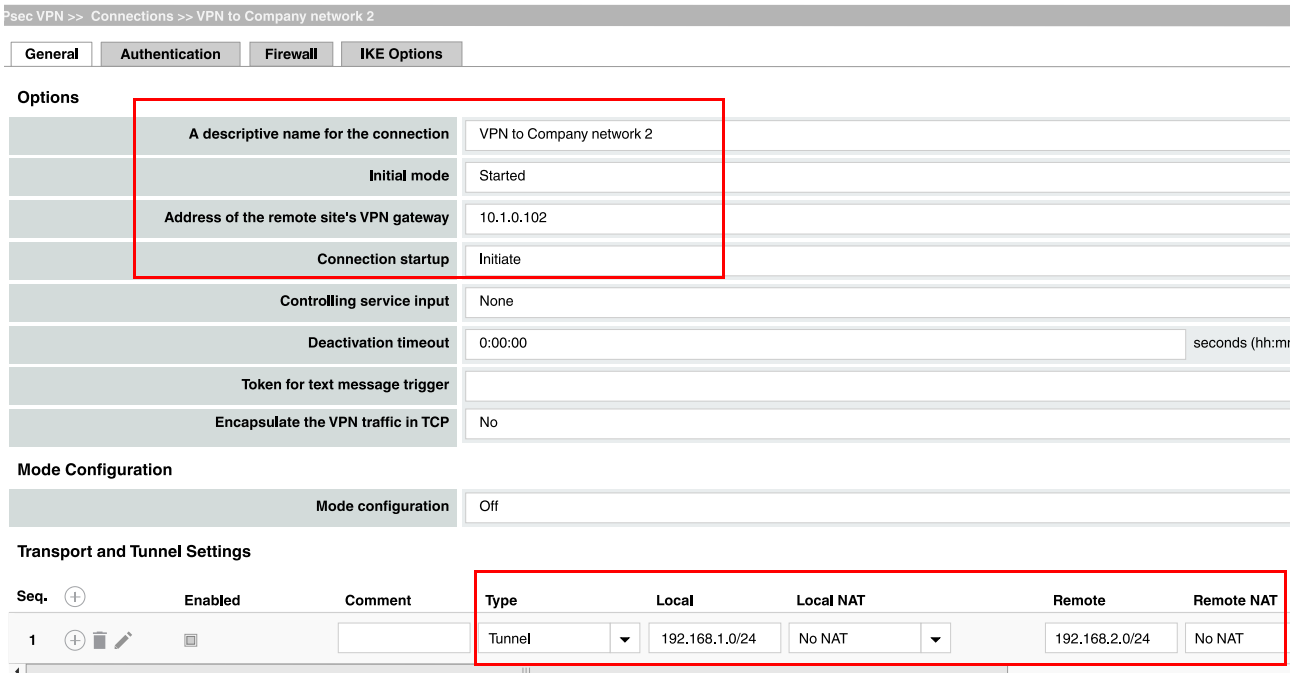


Figure 1-5 *mGuard 1* (*initiator*): VPN connection configuration

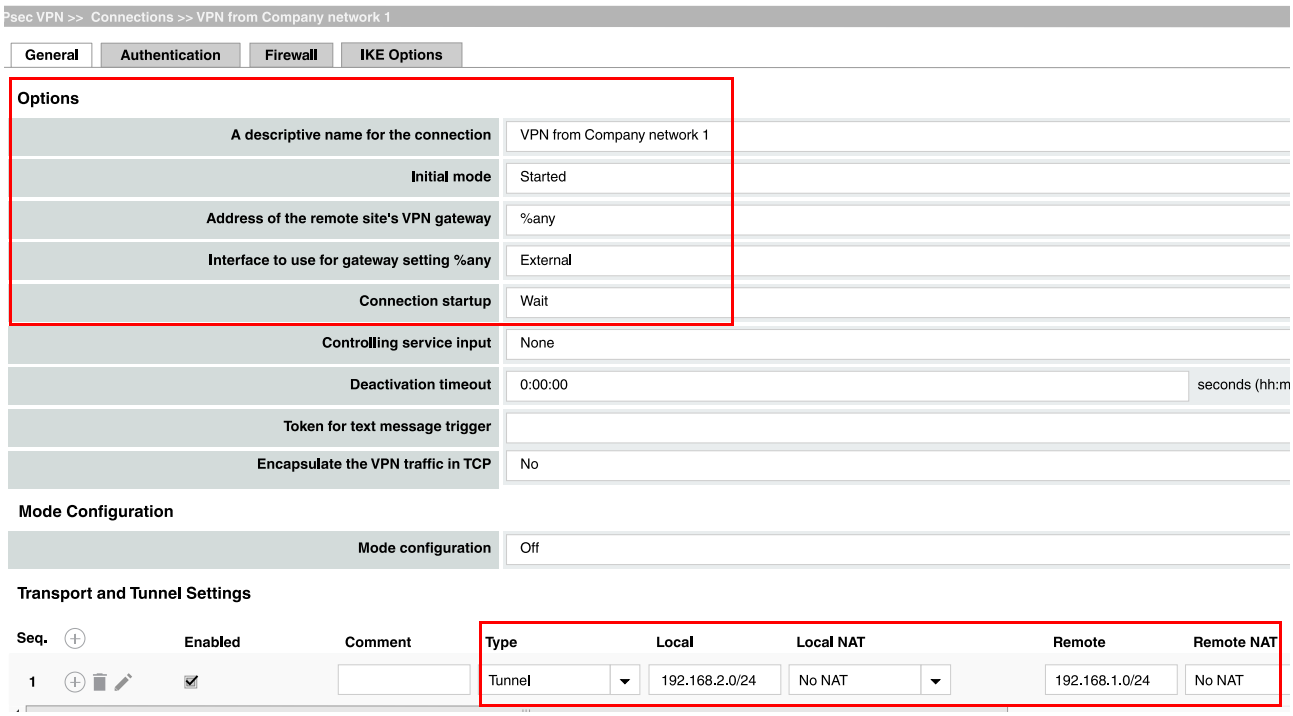


Figure 1-6 *mGuard 2* (*responder*): VPN connection configuration

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. Specify a unique name for the connection and click on the ✎ icon to edit the connection.
4. Configure the VPN connection in accordance with Figure 1-5 and 1-6 or Table 1-3.

Table 1-3 Configuring VPN connection (*IPsec VPN* >> *Connections* >> *(Edit)* >> *General*)

Section	Parameter	mGuard 1	mGuard 2
Options	**A descriptive name for the connection**	VPN to company network 2	VPN from company network 1
	Address of the remote site's VPN gateway	10.1.0.102	%any
	Interface to use for gateway setting %any	(field not visible)	External
	Connection startup	Initiate	Wait
Transport and tunnel settings	**Type**	Tunnel	Tunnel
	Local	192.168.1.0/24	192.168.2.0/24
	Remote	192.168.2.0/24	192.168.1.0/24

Result

The two networks are connected via an IPsec VPN tunnel. Communication between each client and clients of the other network can be encrypted.

A *tunnel connection* always connects networks (incl. networks with the subnet mask /32), and not just two individual clients (hosts) – as is the case with *transport connections*.

1.4 VPN tunnel connection (Single Stealth <-> Router)

1.4.1 Introduction

If a VPN connection is established between two mGuard devices one of which is operated in *Single Stealth mode* (= *static* or *automatic*), it is possible that the IP address of the assigned client is controlled dynamically via a DHCP server. If this IP address is changed, the IP address of the mGuard device also changes in *Stealth mode*.

A *virtual IP address* is used in this case so the VPN configuration of the mGuard devices does not have to be changed. The device then automatically forwards the packets that are sent to this *virtual IP address* via the VPN tunnel to the real IP address of the client.

1.4.2 Example

An IPsec VPN tunnel is to be established between **company network 1** (10.1.0.0/16) and **company network 2** (192.168.2.0/24) using two mGuard devices.

Here, an mGuard device in *Single Stealth mode* (*static* or *automatic*) is to establish a VPN tunnel to an mGuard device in the *Router* network mode (*static* or *PPPoE*).

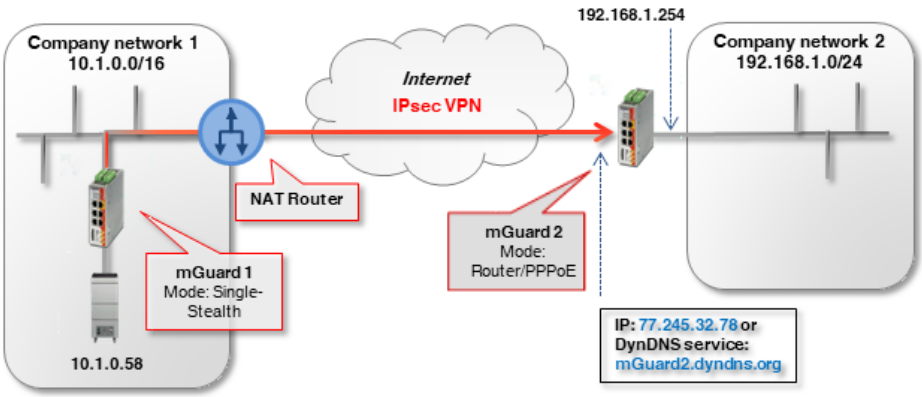


Figure 1-7 Connecting two networks via IPsec VPN (*Single Stealth <-> Router*)

In this example, the responding mGuard device (*mGuard 2*) can be reached from the Internet via a static public IP address.

If the mGuard device is connected to the Internet via changing (dynamic) IP addresses, its current IP address must be registered with a DynDNS provider under a fixed name.

The initiating mGuard device (*mGuard 1*) in *Stealth mode* must then provide a reference to the DynDNS name of the responding mGuard device (e.g. *mGuard2.dyndns.org*) in order to establish a VPN connection.

In this case, activate **DynDNS Monitoring** (**IPsec VPN >> Global >> DynDNS Monitoring**) in the VPN connection of the initiating device (*mGuard 1*). Otherwise, the device will not know when the IP address of the remote peer has changed and the VPN connection will not be established.

1.4.3 Configuring the VPN connection

The *mGuard 1* device initiates the VPN tunnel. In the *Stealth mode* (*automatic*), *mGuard 1* adopts the IP and MAC address of its respective client (10.1.0.58). In *Stealth mode* (*static*), the IP address are entered as fixed addresses.

The responding *mGuard 2* in *Router mode* (*PPPoE*) can be reached via the static public (external) IP address (77.245.32.78) via the Internet. With its internal IP address (192.168.1.254), the device acts as the default gateway for the connected clients in the network 192.168.1.0/24.

If the client receives its IP settings from a DHCP server, it can, in principle, change its IP address. In order for a configured VPN tunnel to continue to be established even with a dynamic change of IP address, a *virtual IP address must* be specified in the settings which is then used by a peer as the endpoint of the VPN tunnel.

If in our example the client in company network 1 (10.1.0.58) is to be accessed from company network 2 via a VPN tunnel, it *must* be accessed via the virtual address (e.g. 172.16.1.1/32).

mGuard 1 would then automatically perform a 1:1 NAT from the *virtual IP address* (172.16.1.1/32) to the real IP address of the client (10.1.0.58/32).

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. Specify a unique name for the connection and click on the ✎ icon to edit the connection.
4. Configure the VPN connection in accordance with Table 1-4.

Table 1-4 Configuring VPN connection (*IPsec VPN >> Connections >> (Edit) >> General*)

Section	Parameter	mGuard 1 (Stealth)	mGuard 2
Options	**A descriptive name for the connection**	VPN to company network 2	VPN from company network 1
	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	**Type**	Tunnel	Tunnel
	Local	172.16.1.1/32	192.168.1.0/24
	Remote	192.168.1.0/24	172.16.1.1/32
	Virtual IP	172.16.1.1	-----

1.5 VPN tunnel connection (Multi Stealth <-> Router)

1.5.1 Introduction

In *Multi Stealth mode*, in contrast to *Single Stealth mode* (*automatic* or *static*), more than one computer can be connected to the LAN interface of the mGuard device, and therefore several IP addresses can be used at the LAN interface.

1.5.2 Example

An IPsec VPN tunnel is to be established between **company network 1** (10.1.0.0/16) and **company network 2** (192.168.2.0/24) using two mGuard devices.

Here, an mGuard device in the *Stealth* (*multiple clients*) network mode is to establish a VPN tunnel to an mGuard device in the *Router* network mode (*static* or *PPPoE*). The clients behind the mGuard device in company network 1 (*mGuard 1*) should be accessible via a VPN tunnel.

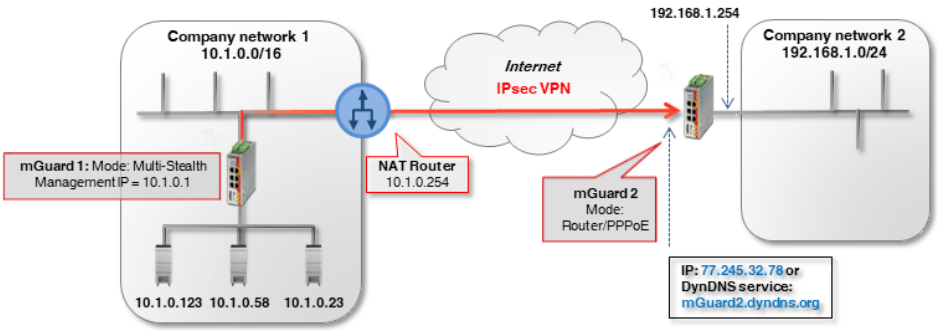


Figure 1-8 Connecting two networks via IPsec VPN (Multi Stealth <-> Router)

In this example, the responding mGuard device (*mGuard 2*) can be reached from the Internet via a static public IP address.

If the mGuard device is connected to the Internet via changing (dynamic) IP addresses, its current IP address must be registered with a DynDNS provider under a fixed name (see Section 1.4.1).

The network settings of the interfaces of the two mGuard devices are configured in the menu **Network >> Interfaces** (tabs: *General*, *Stealth*, *Internal*).

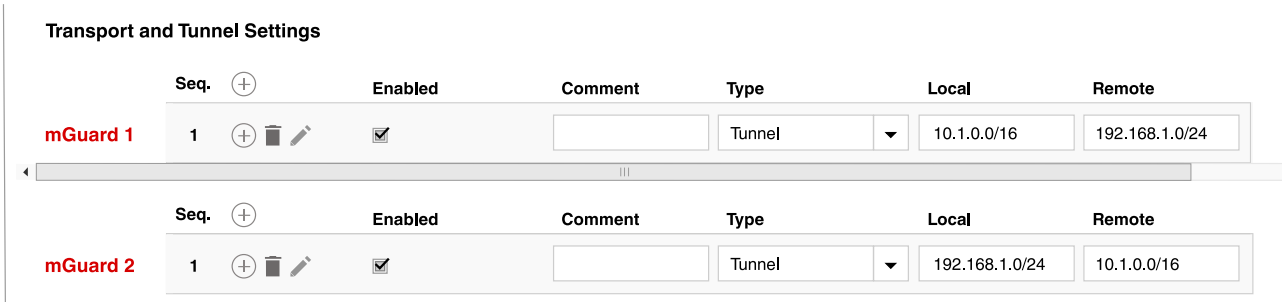
Table 1-5 Network configuration of the interfaces

Parameter	mGuard 1 (Multi Stealth)	mGuard 2 (Router)
Stealth Management IP Address	10.1.0.1	-----
Netmask	255.255.0.0	-----
Default gateway	10.1.0.254	-----
Internal IP address	-----	192.168.1.254
Netmask	-----	255.255.255.0

1.5.3 Configuring the VPN connection

The VPN connection is initiated by *mGuard 1*. To be able to use the VPN function in Stealth mode (*multiple clients*), a *Management IP address* must be assigned to the device. This IP address must belong to the same network as the mGuard device. It may not be used by any other device in the network.

The waiting device *mGuard 2* has the static public IP address 77.245.32.78.



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. Specify a unique name for the connection and click on the ✎ icon to edit the connection.
4. Configure the VPN connection in accordance with Table 1-6.

Table 1-6 Configuring VPN connection (*IPsec VPN >> Connections >> (Edit) >> General*)

Section	Parameter	mGuard 1 (Stealth)	mGuard 2
Options	**A descriptive name for the connection**	VPN to company network 2	VPN from company network 1
	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	**Type**	Tunnel	Tunnel
	Local	10.1.0.0/16	192.168.1.0/24
	Remote	192.168.1.0/24	10.1.0.0/16