1 Connecting networks via hub and spoke (IPsec VPN)

Document ID: 108412_en_00
Document designation: AH EN MGUARD IPSEC VPN HUB SPOKE

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 *hub and spoke* function which can be used to connected two or more IPsec VPN tunnels via a central mGuard.

1.1 Introduction

The *hub and spoke* function enables network packets that have been received via a VPN tunnel to be forwarded directly in another VPN tunnel.

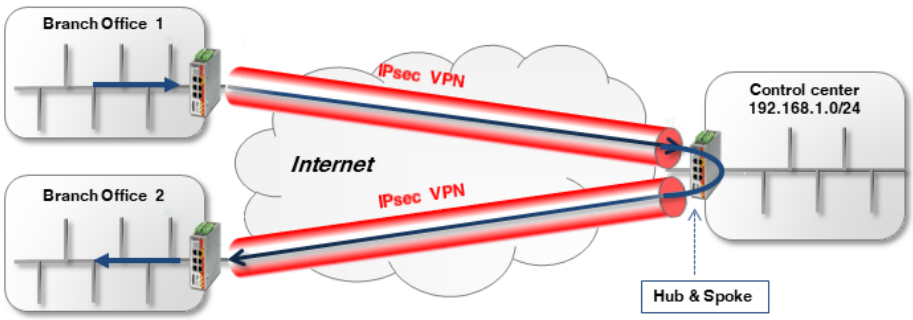
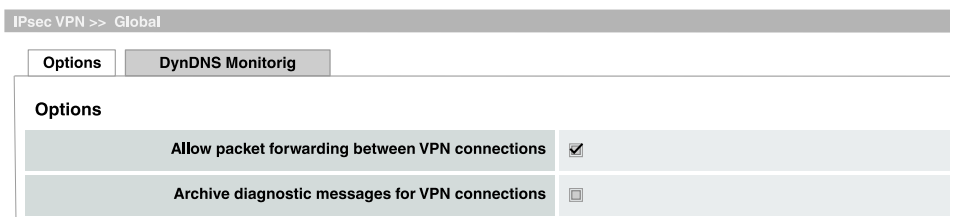


Figure 1-1 *Hub and spoke* via company control center (IPsec VPN)

If several remote locations are connected to the control center and large volumes of data are transmitted, the Internet connection in the control center can become a bottleneck. In such a case, a fully *meshed* network should be used instead of a *hub and spoke* setup.

Along with the activation of *hub and spoke*, the respective networks in the VPN connections must be specified appropriately in order to enable direct routing between the VPN tunnels.



1.2 Connecting branches together via the control center using hub and spoke

Two branches are to communicate with each other via an IPsec VPN connection. The connection is made via the control center, to which both branches have each established a VPN tunnel. The two VPN tunnels are "connected" using the *hub and spoke* function on the mGuard device in the control center (*mGuard 3*).

To enable *routing* from one tunnel to the other, the local network configured in *mGuard 3* must contain all peer networks (e.g. 192.168.0.0/16).

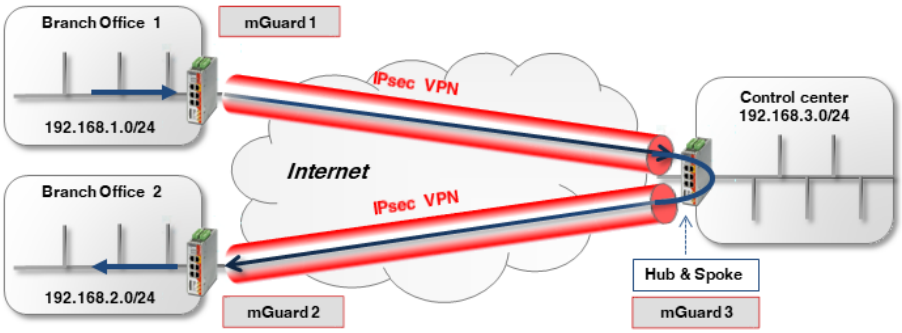


Figure 1-2 *Hub and spoke* via company control center (IPsec VPN)

1.2.1 Configuration

To activate *hub and spoke* on *mGuard 3*, proceed as follows:

1. Log into the web interface of the mGuard device to be configured.
2. Go to **IPsec VPN >> Global** (*Options* tab).
3. Activate the option *Allow packet forwarding between VPN connections*.

The general VPN connection settings are configured under **IPsec VPN >> Connections >> (Edit) >> General** and are described in Section 1 and 1.

The configuration of the respective **transport and tunnel settings** is as follows**:**

mGuard 1 <-> mGuard 3

Seq.	Enabled	Comment	Type	Local	Local NAT	Remote
1	✓	mGuard 1	Tunnel	192.168.1.0/24	No NAT	192.168.0.0/16
2	✓	mGuard 1	Tunnel	192.168.1.0/24	No NAT	10.1.0.0/16

mGuard 2 <-> mGuard 3

Seq.	Enabled	Comment	Type	Local	Local NAT	Remote
1	✓	mGuard 2	Tunnel	192.168.2.0/24	No NAT	192.168.0.0/16
1	✓	mGuard 3	Tunnel	192.168.0.0/16	No NAT	192.168.2.0/24

Hub and spoke, if the local network does not contain all peer networks

What happens if the control center network is not a part of the network **192.168.0.0/16**, but is a part of, e.g. **10.1.0.0/16**?

In this case, the two branches can communicate with each other via the VPN tunnel. However, neither **branch 1** nor **branch 2** have access to the **control center** network, and vice versa.

This problem can be resolved by specifying a second VPN tunnel in each of the configured VPN tunnels which addresses the control center network (see following example for connecting *mGuard 1* to *mGuard 3*).

mGuard 1 <-> mGuard 3

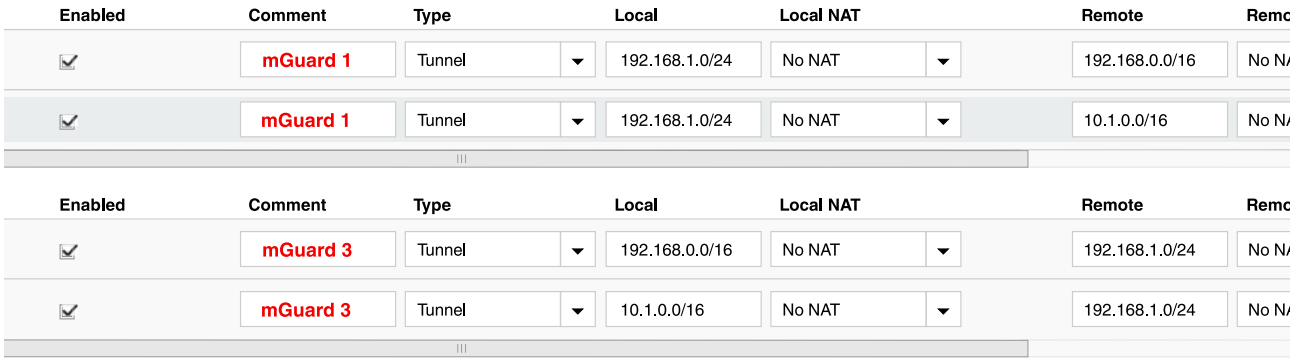


Table 1-1 shows the transport and tunnel settings for all devices (*mGuard 1, 2,* and *3*) in this case:

mGuard 1 <-> mGuard 3 | mGuard 2 <-> mGuard 3

Table 1-1 Transport and tunnel settings with *hub and spoke* (different networks)

VPN connection	Tunnel Settings	Local	Remote
mGuard 1 <---> mGuard 3	mGuard 1	192.168.**1**.0/24	192.168.0.0/16
		192.168.**1**.0/24	10.1.0.0/16
	mGuard 3	192.168.0.0/16	192.168.**1**.0/24
		10.1.0.0/16	192.168.**1**.0/24
mGuard 2 <---> mGuard 3	mGuard 2	192.168.**2**.0/24	192.168.0.0/16
		192.168.**2**.0/24	10.1.0.0/16
	mGuard 3	192.168.0.0/24	192.168.**2**.0/24
		10.1.0.0/16	192.168.**2**.0/24

1.3 Connecting external technicians to production locations via hub and spoke

Two remote maintenance technicians are to be able to access the machines in all production locations (branches) from their laptops via a VPN connection (via VPN Client software or mGuard device). Initially, the VPN connection is via a central mGuard (*mGuard 4*), which establishes a VPN connection with the machine network of the respective production location via *hub and spoke*.

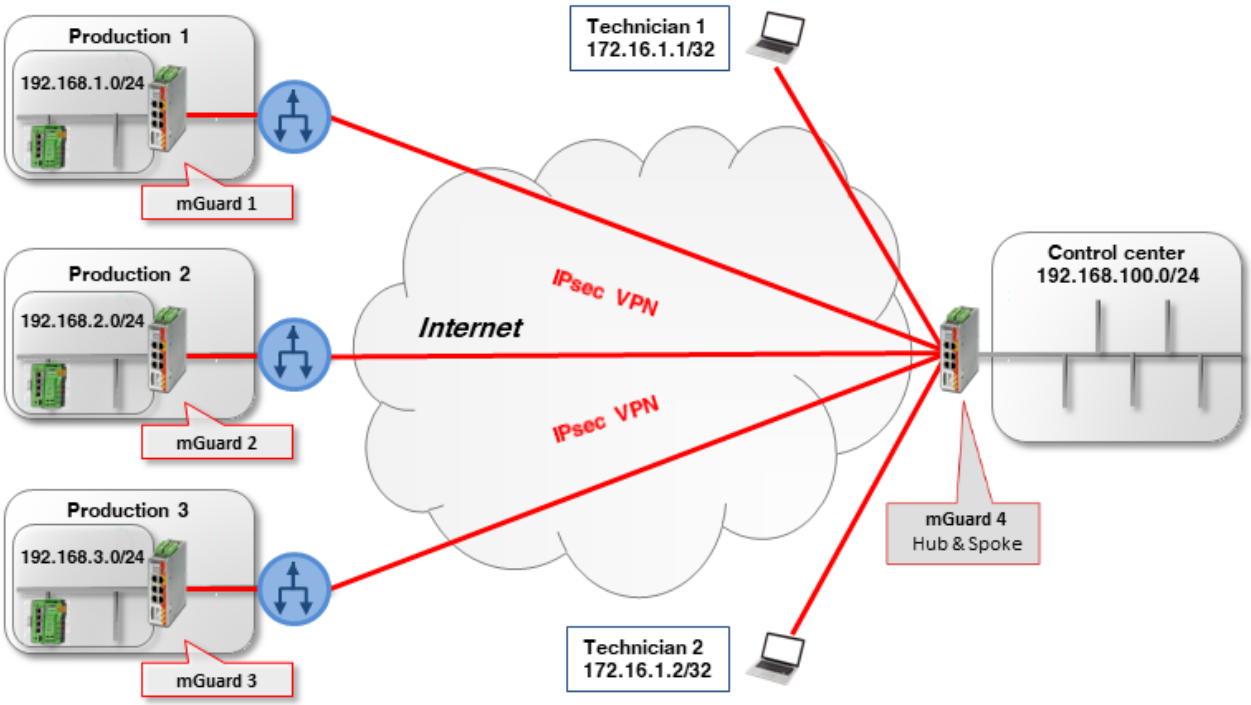


Figure 1-3 Remote maintenance via *hub and spoke* via the company control center (IPsec VPN)

An mGuard device is installed as a router in each of the production locations in order to connect the machine network with the branch network, and to establish a VPN connection to the mGuard device in the company control center.

The technicians use *virtual IP addresses* on their laptops so they are not dependent on the real IP addresses assigned to the laptops:

– Technician 1: 172.16.1.**1**/32
– Technician 2: 172.16.1.**2**/32.

In order access all production locations, the VPN network of the peer specified in each case must contain the machine networks of all three locations (192.168.**1**.0/24, 192.168.**2**.0/24 und 192.168.**3**.0/24): i.e. **192.168.0.0/16**.

The mGuard devices of the branches use the internal networks 192.168.**1**.0/24, 192.168.**2**.0/24 and 192.168.**3**.0/24. Data packets that are sent via the VPN connection from the technicians' laptops to the mGuard devices have one of the two sender IP addresses: 172.16.1.**1**/32 or 172.16.1.**2**/32.

If remote maintenance is not just to be limited to two technicians, a peer VPN network must be specified at the production location mGuard devices via which in principle several technicians can be connected: in this example 172.16.1.0/24.

Example: Access via hub and spoke by two technicians

If the *hub and spoke* function is enabled on the mGuard device in the control center (*mGuard 4*), the tunnel settings for the VPN connections must be configured as follows – taking into consideration the above listed points – (see also the example configuration in Section 1.2.1):

Table 1-2 *Hub and spoke*: Transport and tunnel settings with **different** local networks

VPN connection	Client	Local	<-->	Remote
Technician 1 <–> mGuard 4	Technician 1	172.16.1.1/32	<-->	192.168.0.0/16
	mGuard 4	192.168.0.0/16	<-->	172.16.1.1/32
Technician 2 <–> mGuard 4	Technician 2	172.16.1.2/32	<-->	192.168.0.0/16
	mGuard 4	192.168.0.0/16	<-->	172.16.1.2/32
mGuard 1 <–> mGuard 4	mGuard 1	192.168.1.0/24	<-->	172.16.1.0/24
	mGuard 4	172.16.1.0/24	<-->	192.168.1.0/24
mGuard 2 <–> mGuard 4	mGuard 2	192.168.2.0/24	<-->	172.16.1.0/24
	mGuard 4	172.16.1.0/24	<-->	192.168.2.0/24
mGuard 3 <–> mGuard 4	mGuard 3	192.168.3.0/24	<-->	172.16.1.0/24
	mGuard 4	172.16.1.0/24	<-->	192.168.3.0/24

Example: Access with the same networks in the production locations

What happens when the mGuard devices at the production locations all use the same internal network (e.g. 192.168.**1**.0/24)?

In this case, the mGuard devices in the branches must use *Local 1:1 NAT for IPsec tunnel connections* for the local network (see also Section 1.3, “Connecting locations with the same internal networks to a control center (1:1 NAT)”).

The individual production locations are then accessed via a *Virtual network* and the mGuard device performs a local 1:1 NAT from the *Virtual network* to the local *Real network* (192.168.1.0/24).

In this example, the following *Virtual networks* are used for the production locations:

– Branch 1:172.17.**1**.0/24
– Branch 2: 172.17.**2**.0/24
– Branch 3: 172.17.**3**.0/24.

The technicians must use these virtual networks to access the respective machine. Therefore, the technicians must specify 172.17.0.0/16 as the peer VPN network.

The tunnel settings for this setup are as follows (see Table 1-3 and Figure 1-4).

Table 1-3 *Hub and spoke*: Tunnel settings with the **same** local networks (with local 1:1 NAT)

VPN connection	Client	Local	<-->	Remote
Technician 1 <–> mGuard 4	Technician 1	172.16.1.1/32	<–>	172.17.0.0/16
	mGuard 4	172.17.0.0/16	<–>	172.16.1.1/32
Technician 2 <–> mGuard 4	Technician 2	172.16.1.2/32	<–>	172.17.0.0/16
	mGuard 4	172.17.0.0/16	<–>	172.16.1.2/32
mGuard 1 <–> mGuard 4	mGuard 1	172.17.**1**.0/24	<–>	172.16.1.0/24
		Local 1:1 NAT to 192.168.1.0/24		
	mGuard 4	172.16.1.0/24	<–>	172.17.**1**.0/24
mGuard 2 <–> mGuard 4	mGuard 2	172.17.**2**.0/24	<–>	172.16.1.0/24
		Local 1:1 NAT to 192.168.1.0/24		
	mGuard 4	172.16.1.0/24	<–>	172.17.**2**.0/24
mGuard 3 <–> mGuard 4	mGuard 3	172.17.**3**.0/24	<–>	172.16.1.0/24
		Local 1:1 NAT to 192.168.1.0/24		
	mGuard 4	172.16.1.0/24	<–>	172.17.**3**.0/24

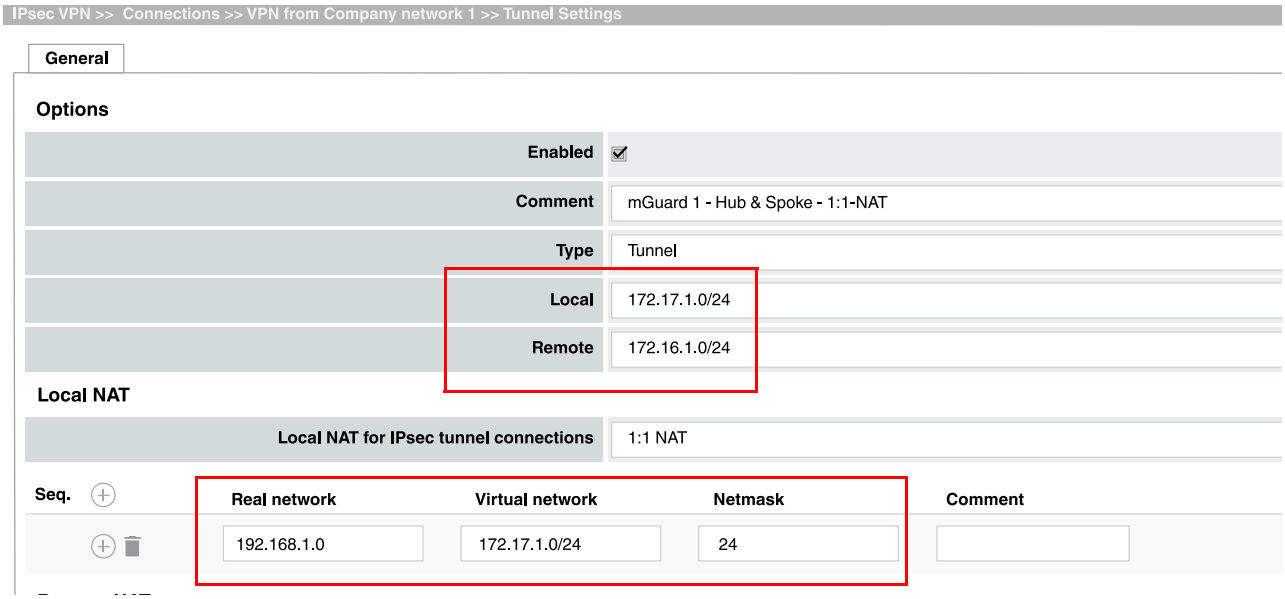


Figure 1-4 *Hub and spoke*: Example *mGuard 1* tunnel settings + local 1:1 NAT