1 VPN Kickstart – Connecting two networks together via IPsec VPN

Document ID: 108404_en_00

Document designation: AH EN MGUARD VPN KICKSTART

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 an IPsec VPN connection between two networks.

1.1 Introduction

Using IPsec VPN, networks can be connected together via an encrypted VPN tunnel.

1.1.1 Example

Using two mGuard devices, an encrypted 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).

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 the VPN connection is initiated by *mGuard 1*. The VPN tunnel is established once the *waiting* mGuard device of the peer (*mGuard 2*) is available. Both mGuard devices are operated in the *Router* network mode.

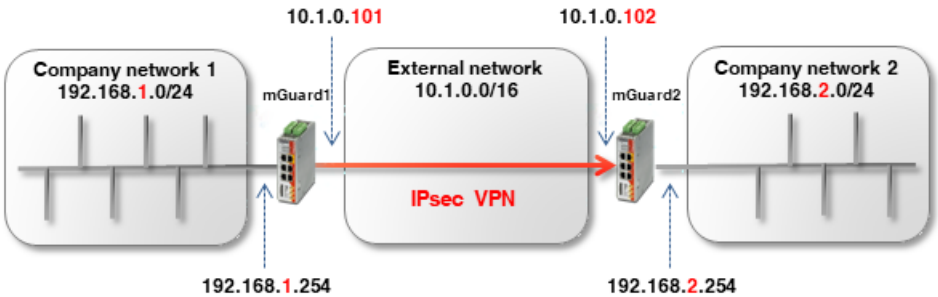


Figure 1-1 Connecting two networks via IPsec VPN

Optional: router mode PPPoE

Establishing a VPN tunnel between two mGuard devices in the *PPPoE* router mode via the Internet is similar in principle (see Figure 1-2). In this case, the Internet is the external network. The devices receive their external IP settings from the Internet Service Provider (ISP). Static name resolution with dynamically assigned IP addresses is then possible with the aid of a DynDNS service.

If the responding (waiting) mGuard device (*mGuard 2*) has a dynamic public IP address, this mGuard must register its external IP address with a DynDNS service (e.g. *mGuard2.dyndns.org*) using a freely selectable name. The initiating mGuard device (*mGuard 1*) must provide a reference to this name in order to establish the 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 peer has changed and the VPN connection will not be established.

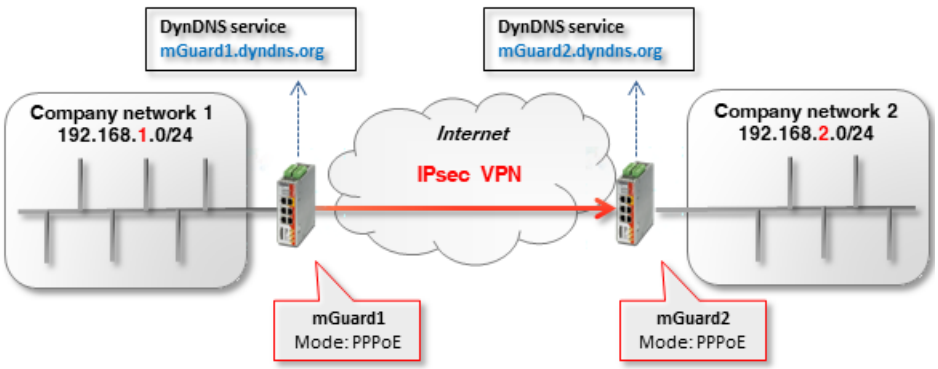


Figure 1-2 Determination of the host names for the mGuard devices using DynDNS. Because the VPN connection is initiated via *mGuard 1*, this does not need a DynDNS address.

1.1.2 Prerequisite

1. Two mGuard devices with the latest firmware (e.g. version 8.6.1 or higher).
2. An existing network connection (IP connection) between the mGuard devices (e.g. via Internet, WAN or LAN).
3. An internal and an external IP address for each mGuard device.
4. UDP ports 500 and 4500 open in the firewall on both sides of the IPsec VPN connection.
5. (Optional) a host name for each mGuard device, e.g. via DynDNS (e.g. *mGuard1.dyndns.org* and *mGuard2.dyndns.org*).

1.1.3 Procedure

1. Generate X.509 certificates and keys
2. Import X.509 certificates and keys
3. Configure IPsec VPN connection tunnel settings
4. Test IPsec VPN connection setup

1.2 Generating machine certificates (X.509 certificates)

Certificates that are necessary for secure authentication of mGuard devices can be obtained from a commercial certification authority. Programs such as *XCA*, *OpenSSL* and *Microsoft Certification Authority (CA) Server* can be used for creating self-signed certificates.

Self-signed certificates are not accredited by an official certification authority, and can therefore only be used under certain circumstances.

The application notes "Creating X.509 certificates with OpenSSL/XCA" describe how to generate self-signed certificates using OpenSSL and XCA.

The following certificates are necessary for the authentication of an IPsec VPN connection between two mGuard devices. (In our example, the unique names *mGuard 1* and *mGuard 2* are used as the *common names* in the certificates.)

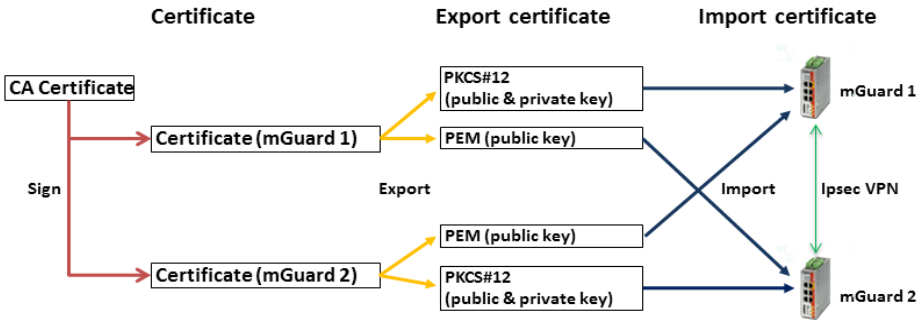
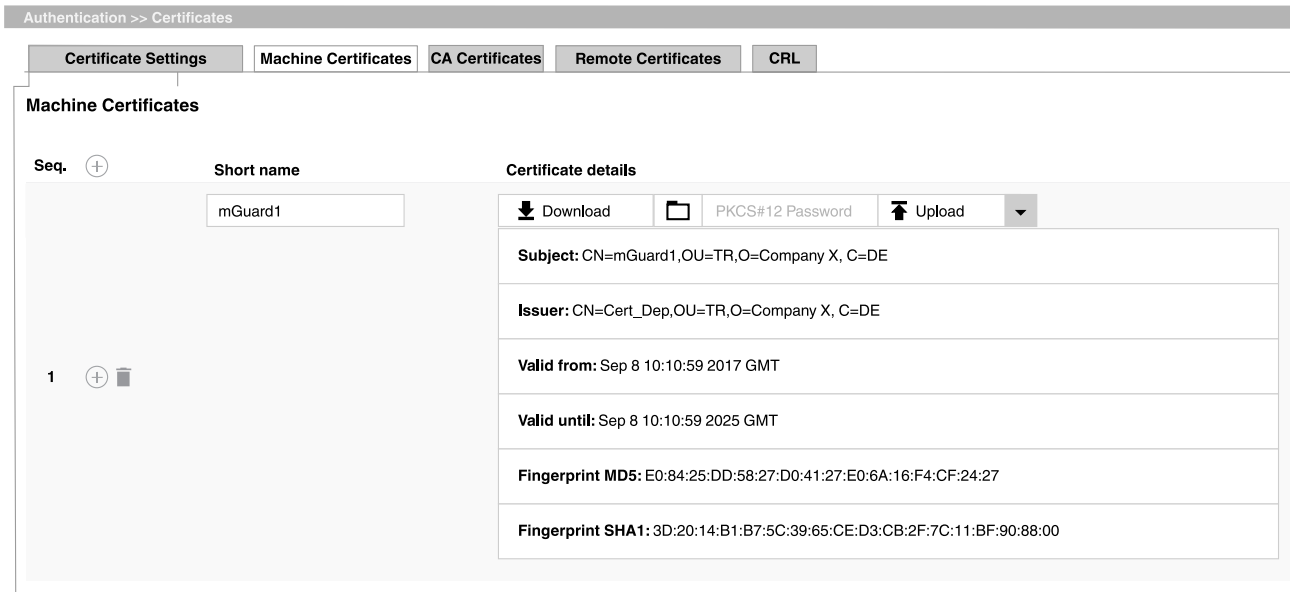


Figure 1-3 Participating certificates in an IPsec VPN connection

Table 1-1 Necessary certificates

Device	Machine certificate (also contains the private key)	Client certificate (only contains the public key)
mGuard 1	*mGuard1.p12*	*mGuard1.pem*
mGuard 2	*mGuard2.p12*	*mGuard2.pem*

1.3 Importing machine certificates (PKCS)



To import X.509 machine certificates (incl. private key) into your mGuard devices, proceed as follows:

1. Log into the *mGuard 1* web interface (e.g. https://192.168.1.254).
2. Go to **Authentication >> Certificates** (*Machine certificates* tab).
3. Click on the ⊕ icon to add a new machine certificate.
4. Click on the 🗀 icon to select the certificate file on the installation computer.
5. Select the previously created file *mGuard1.p12.*
6. Enter the PCKS#12 password issued when generating the certificate.
7. Give the certificate a unique short name. If you leave this field empty, the *common name (CN)* of the certificate is used automatically.
8. Click on the **Upload** button to import the certificate.
9. Click on the "*Save*" icon 🖫 to complete the import.

Repeat the procedure for the device *mGuard2*, and import the machine certificate with the file name *mGuard2.p12.*

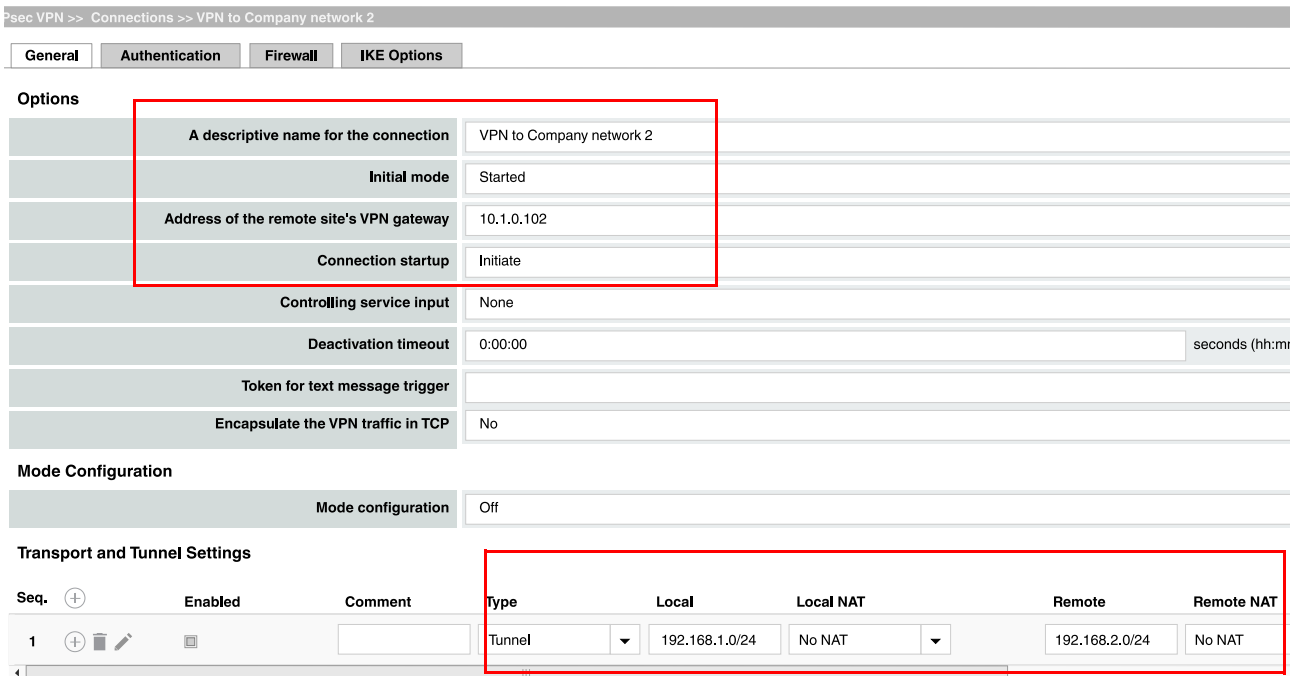
1.4 Creating the mGuard1 VPN connection

1.4.1 Prerequisite

To configure the IPsec VPN connection, the following basic settings must be made:

1. Log into the *mGuard 1* web interface (e.g. https://192.168.1.254).
2. Go to **IPsec VPN >> Global** (*Options* tab).
3. In the section **IP Fragmentation**: activate the option *IKE fragmentation* and as a precaution set a value of 1414 or less *for IPsec* under *MTU* for compatibility reasons.

1.4.2 Configuring the VPN connection



To configure the VPN connection, 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.

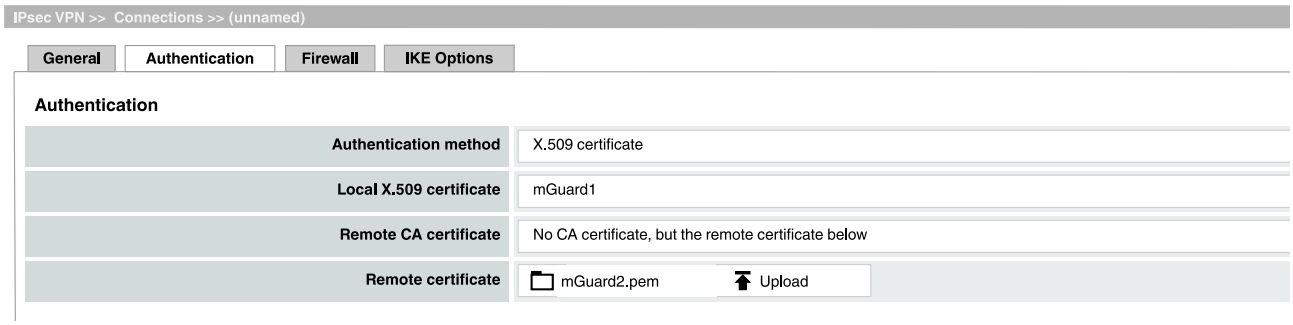
Section "Options"

1. Enter either the DynDNS name or the external IP address of the peer (*mGuard 2*) (*mGuard2.dyndns.org* or 10.1.0.102) as the **Address of the remote site's VPN gateway**.
2. Select *Initiate* in the **Connection startup** field.

Section "Transport and Tunnel Settings"

1. Enter the address of the network that is to be accessible via the *mGuard1* internal interface in the field **Local** (192.168.**1**.0/24).
2. Enter the address of the network that is to be accessible via the *mGuard2* internal interface in the field **Remote** (192.168.**2**.0/24).
3. Click on the "*Save*" icon to complete the procedure.

1.4.3 Configuring authentication of the VPN connection



To configure mutual authentication of the two peers when setting up the VPN connection, proceed as follows:

1. Go to **IPsec VPN >> Connections** (*Authentication* tab)
2. In the **Local X.509 certificate** field, select the certificate (*mGuard1*) that you previously imported into the device as the machine certificate for *mGuard1*.
3. In the **Remote CA certificate** field, select the option *No CA certificate and select the remote certificate below instead*.
4. In the **Remote certificate** field, import the *mGuard2* client certificate.

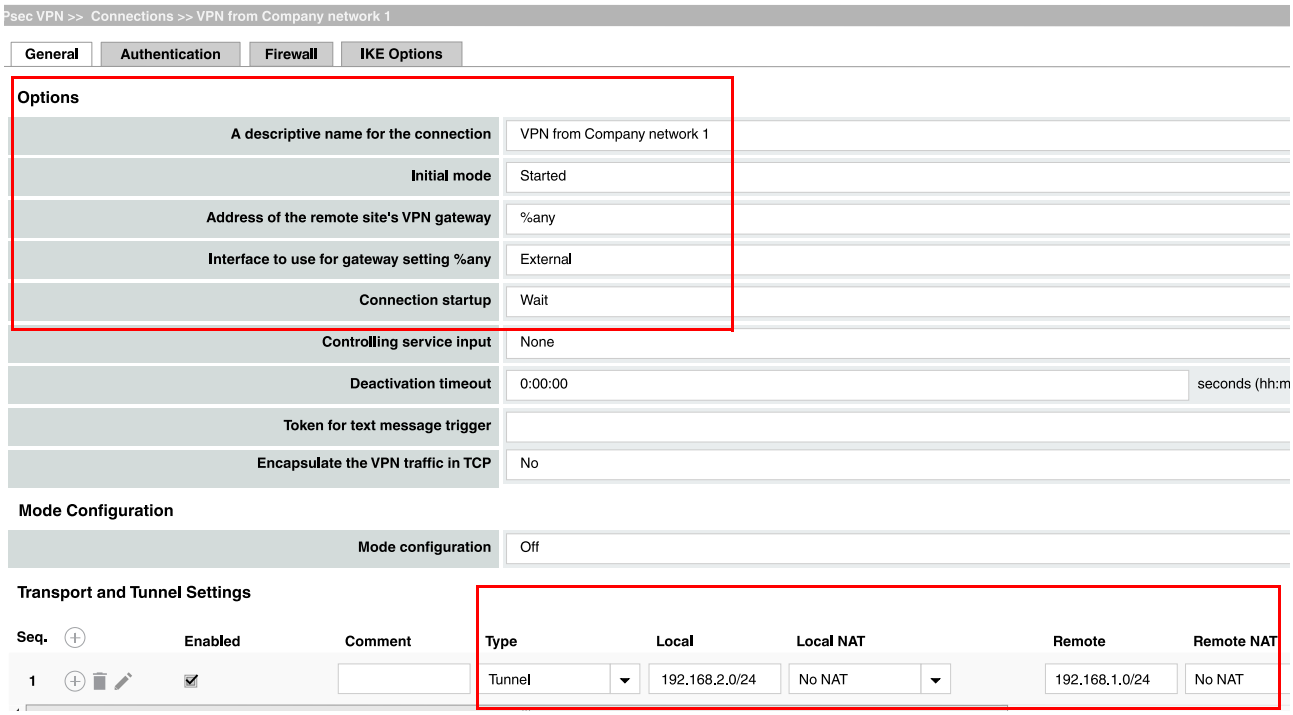
   To do so, click on the icon and select the certificate (*mGuard2.pem*) saved onto the configuration computer. Then click on the **Upload** button.
5. Click on the "*Save*" icon to complete the procedure.

1.5 Creating the mGuard2 VPN connection

1.5.1 Prerequisite

The same prerequisites apply here as to mGuard 1 (see “Prerequisite” on page 5).

1.5.2 Configuring the VPN connection



Repeat the configuration steps described above (*mGuard1*) for the VPN peer (*mGuard2*). Note the following differences:

IPsec VPN >> Connections (*General* tab)

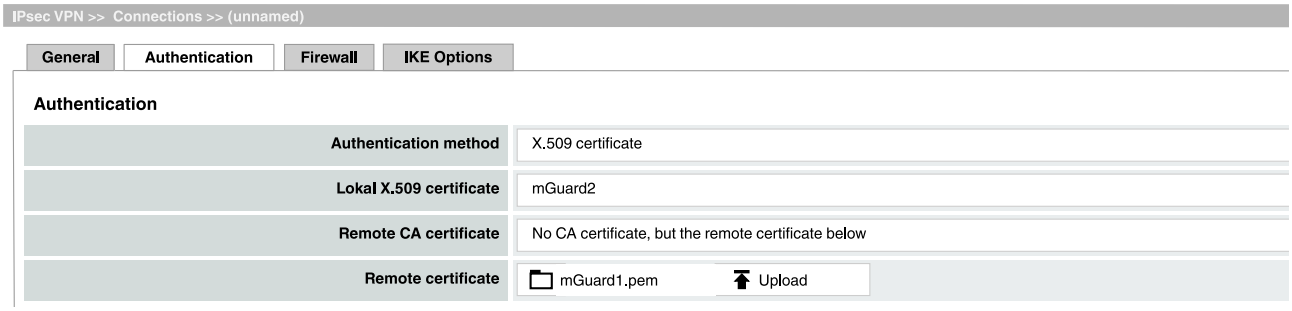
Section "Options"

1. Enter *%any as* **Address of the remote site’s VPN gateway**.
2. Enter *External u*nder **Interface to use for gateway setting %any**.
3. Select *Wait* in the **Connection startup** field.

Section "Transport and Tunnel Settings"

1. Enter the address of the network that is to be accessible via the *mGuard2* internal interface in the field **Local** (192.168.**2**.0/24).
2. Enter the address of the network that is to be accessible via the *mGuard1* internal interface in the field **Remote** (192.168.**1**.0/24).
3. Click on the "*Save*" icon to complete the procedure.

1.5.3 Configuring authentication of the VPN connection



Repeat the configuration steps described above (*mGuard1*) for the VPN peer (*mGuard2*). Note the following differences:

IPsec VPN >> Connections (*Authentication* tab)

1. In the **Local X.509 certificate** field, select the certificate (*mGuard2*) that you previously imported into the device as the machine certificate for *mGuard2*.
2. In the **Remote CA certificate** field, select the option *No CA certificate and select the remote certificate below instead*.
3. In the **Remote certificate** field, import the *mGuard1* client certificate.
   To do so, click on the icon and select the certificate (*mGuard1.pem*) saved onto the configuration computer. Then click on the **Upload** button.
4. Click on the "*Save*" icon to complete the procedure.

1.6 Testing the VPN connection

1.6.1 Prerequisite

– Connect the two configured mGuard devices into the corresponding network environments.
– Optional: ensure that a connection to the Internet can be established (UDP ports 500 and 4500 must be open).

1.6.2 Procedure

1. Log into the *mGuard 1* or *mGuard 2* web interface (e.g. https://192.168.1.254).
2. Go to **IPsec VPN >> IPsec Status**.
3. On the status page, check whether a VPN connection between the two devices (*mGuard1* and *mGuard2*) exists.

   Both an ISAKMP and an IPsec SA connection must have been established.
4. Check the secure VPN connection by either pinging the respective VPN peer or by testing access to a peer (e.g. web server, controller, computer) in the remote network.