

# 1 VPN-Verbindungen mit variierenden Netzwerkmodi konfigurieren



Dokument-ID: 108410\_de\_00

Dokument-Bezeichnung: AH DE MGUARD IPSEC VPN NW MODE

© PHOENIX CONTACT 2018-10-16



Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.

Diese steht unter der Adresse [phoenixcontact.net/products](https://phoenixcontact.net/products) zum Download bereit.

## Inhalt dieses Dokuments

In diesem Dokument wird die Konfiguration von IPsec-VPN-Verbindungen zwischen zwei mGuard-Geräten mit verschiedenen Netzwerkmodi (*Router*, *Stealth*) beschrieben.

Die Beispiele zeigen die Konfiguration unter **IPsec VPN >> Verbindungen >> (Edit) >> Allgemein**.

|     |                                                        |    |
|-----|--------------------------------------------------------|----|
| 1.1 | Einleitung.....                                        | 1  |
| 1.2 | VPN-Transportverbindung (Stealth <-> Stealth) .....    | 2  |
| 1.3 | VPN-Tunnelverbindung (Router <-> Router) .....         | 4  |
| 1.4 | VPN-Tunnelverbindung (Single Stealth <-> Router) ..... | 8  |
| 1.5 | VPN-Tunnelverbindung (Multi Stealth <-> Router) .....  | 10 |

## 1.1 Einleitung

Die Konfiguration von VPN-Verbindungen erfolgt über das Menü **IPsec VPN >> Verbindungen** auf vier Registerkarten.

Die Konfiguration auf den Registerkarten *Authentifizierung*, *Firewall* und *IKE-Optionen* ist dabei unabhängig von den allgemeinen Netzwerkeigenschaften des mGuard-Geräts, wie **Netzwerkmodus** (z. B. *Stealth*, *Router*, *Router/PPPoE*) oder **VPN-Funktion** (z. B. *1:1 NAT* für das lokale Netzwerk, *Hub & Spoke*).

Auf der Registerkarte *Allgemein* haben diese Eigenschaften jedoch Auswirkungen auf die Tunneleinstellungen, weshalb in den folgenden Beispielen verschiedene Einstellungen auf der Registerkarte *Allgemein* betrachtet werden.

## 1.2 VPN-Transportverbindung (Stealth <-> Stealth)

### 1.2.1 Einleitung

Im Gegensatz zu einer VPN-Tunnelverbindung, die zwei Netzwerke verbindet, wird eine VPN-Transportverbindung dazu verwendet, zwei einzelne Clients (Hosts) miteinander zu verbinden.

Würde die VPN-Transportverbindung zwischen zwei mGuard-Geräten im Netzwerkmodus *Router* verwendet, ist ein Zugriff auf alle Clients im internen Netzwerk der Geräte über die VPN-Verbindung nicht möglich.

Die Verwendung einer Transportverbindung ist daher nur sinnvoll, wenn die mGuard-Geräte im *Single-Stealth-Modus* betrieben werden (z. B. um den Datentransfer zwischen zwei Clients zu sichern oder um zu Wartungszwecken über eine gesicherte Verbindung auf einen Client zuzugreifen). Die Geräte müssen sich im gleichen Netz befinden.



Eine Transportverbindung kann nicht verwendet werden, wenn die Verbindung über einen oder mehrere Gateways hergestellt wird, bei denen Network Address Translation (NAT) aktiviert ist.

### 1.2.2 Beispiel

Zwei Clients (Hosts) im gleichen Netzwerk sollen über eine IPsec-VPN-Verbindung miteinander verbunden werden, um einen permanenten verschlüsselten Datenaustausch zu gewährleisten. Bild 1-1 zeigt die Netzwerkkonfiguration der beteiligten Clients.

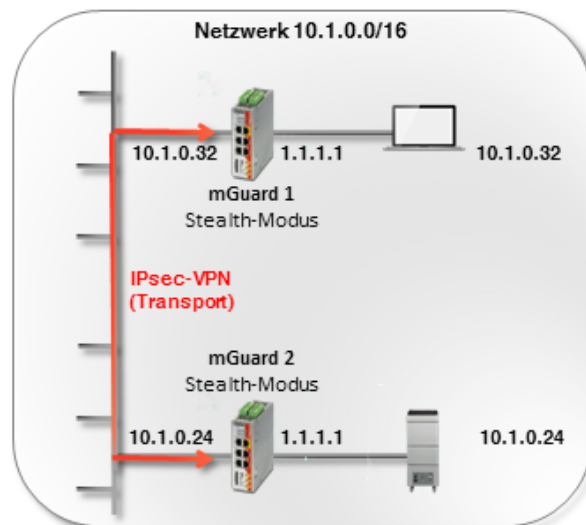


Bild 1-1 VPN-Transportverbindung im Netzwerkmodus *Stealth*

Die VPN-Verbindung (Typ *Transport*) wird dazu über zwei, den jeweiligen Clients vorgeschaltete, mGuard-Geräte im Netzwerkmodus *Stealth (Automatisch)* aufgebaut und bereitgestellt.

Die beiden mGuard-Geräte übernehmen im *Stealth-Modus (Automatisch)* jeweils die IP- und MAC-Adresse ihres internen Clients ( *mGuard 1* die 10.1.0.32 und *mGuard 2*: 10.1.0.24).

### 1.2.3 VPN-Verbindung konfigurieren

Bild 1-2 zeigt die Konfiguration der mGuard-Geräte (zur besseren Übersicht in einer Abbildung). Die Transport- und Tunneleinstellungen sind auf beiden Geräten gleich.

IPsec VPN >> Verbindungen >> VPN to 10.1.0.24

Allgemein    Authentifizierung    Firewall    IKE-Optionen

| Optionen                                   | mGuard 1         | mGuard 2           |
|--------------------------------------------|------------------|--------------------|
| Ein beschreibender Name für die Verbindung | VPN to 10.1.0.24 | VPN from 10.1.0.32 |
| Initialer Modus                            | Gestartet        | Gestartet          |
| Adresse des VPN-Gateways der Gegenstelle   | 10.1.0.24        | 10.1.0.32          |
| Verbindungsinitiiierung                    | Initiiere        | Warte              |
| Schaltender Service-Eingang/CMD            | Kein             | Kein               |
| Timeout zur Deaktivierung                  | 0:00:00          | 0:00:00            |
| Token für SMS-Steuerung                    |                  |                    |
| Kapsel den VPN-Datenverkehr in TCP ein     | Nein             | Nein               |

Mode Configuration

Mode Configuration    Aus    Aus

Transport- und Tunneleinstellungen

| Seq. | Aktiv                               | Kommentar | Typ       | Lokal | Lokales NAT | Gegenstelle | Remote-NAT |
|------|-------------------------------------|-----------|-----------|-------|-------------|-------------|------------|
| 1    | <input checked="" type="checkbox"/> |           | Transport |       |             |             |            |

Bild 1-2 VPN-Verbindung (Typ: *Transport*): Stealth-Modus <-> Stealth-Modus

Um die VPN-Verbindung der mGuard-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon , um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon , um die Verbindung zu bearbeiten.
4. Konfigurieren Sie die VPN-Verbindung gemäß Bild 1-2 bzw. Tabelle 1-1.

Tabelle 1-1 VPN-Verbindung konfigurieren (IPsec VPN >> Verbindungen >> (Edit) >> Allgemein)

| Sektion                            | Parameter                                  | mGuard 1         | mGuard 2           |
|------------------------------------|--------------------------------------------|------------------|--------------------|
| Optionen                           | Ein beschreibender Name für die Verbindung | VPN to 10.1.0.24 | VPN from 10.1.0.32 |
|                                    | Adresse des VPN-Gateways der Gegenstelle   | 10.1.0.24        | 10.1.0.32          |
|                                    | Verbindungsinitiiierung                    | Initiiere        | Warte              |
| Transport- und Tunneleinstellungen | Typ                                        | Transport        | Transport          |

#### Ergebnis

Die Kommunikation der beiden Clients, die jeweils über ein mGuard-Gerät im Netzwerkmodus *Stealth* an das Netzwerk angeschlossen sind, erfolgt verschlüsselt über die zwischen den mGuard-Geräten aufgebaute IPsec-VPN-Verbindung (Typ *Transport*).

Eine *Transportverbindung* verbindet immer nur zwei einzelne Clients (Hosts) und keine Netzwerke wie die *Tunnelverbindung*.

## 1.3 VPN-Tunnelverbindung (Router <-> Router)

### 1.3.1 Einleitung

Im Gegensatz zu einer VPN-Transportverbindung, die zwei einzelne Hosts miteinander verbindet, wird eine VPN-Tunnelverbindung dazu verwendet, zwei Netzwerke zu verbinden.

### 1.3.2 Beispiel

Zwischen **Firmennetzwerk 1** (192.168.1.0/24) und **Firmennetzwerk 2** (192.168.2.0/24) soll unter Verwendung zweier mGuard-Geräte ein IPsec-VPN-Tunnel aufgebaut werden.



Ein VPN-Tunnel kann nur zwischen verschiedenen Netzwerken aufgebaut werden. Wenn zwei Standorte das gleiche interne Netzwerk haben, muss die Funktion VPN 1:1 NAT für das lokale Netzwerk (siehe Kapitel 1, „NAT in VPN-Verbindungen verwenden“) verwendet werden.

Die VPN-Verbindung wird dabei von *mGuard 1* initiiert. *mGuard 2* wartet auf die Verbindung. Beide mGuard-Geräte werden im Netzwerkmodus *Router (Statisch)* betrieben.

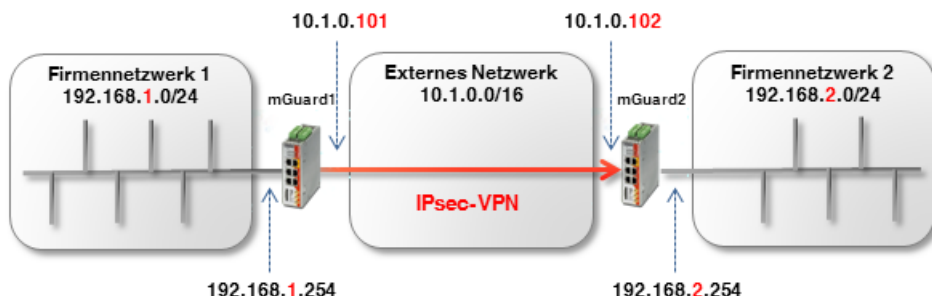


Bild 1-3 Zwei Netzwerke über IPsec-VPN verbinden

Die Netzwerkeinstellungen der Interfaces beider mGuard-Geräte werden im Menü **Netzwerk >> Interfaces** vorgenommen (Registerkarten: *Allgemein*, *Extern*, *Intern*). Beide Geräte werden im Netzwerkmodus *Router (Statisch)* betrieben.

Tabelle 1-2 Netzwerkkonfiguration der Interfaces

| Parameter                 | mGuard 1      | mGuard 2      |
|---------------------------|---------------|---------------|
| <b>Externe IP-Adresse</b> | 10.1.0.101    | 10.1.0.102    |
| Netzmaske                 | 255.255.0.0   | 255.255.0.0   |
| Standard-Gateway          | 10.1.0.254    | 10.1.0.254    |
| <b>Interne IP-Adresse</b> | 192.168.1.254 | 192.168.2.254 |
| Netzmaske                 | 255.255.255.0 | 255.255.255.0 |

Die Clients in den internen Netzwerken sollen als Standard-Gateway jeweils die interne IP-Adresse des zugehörigen mGuard-Geräts verwenden.

### Optionaler Aufbau im Router-Modus PPPoE

Der Aufbau eines VPN-Tunnels zwischen zwei mGuard-Geräten im Router-Modus *PPPoE* über das Internet erfolgt im Prinzip ähnlich (siehe Bild 1-4). In diesem Fall ist das Externe Netzwerk das Internet. Die Geräte erhalten ihre dynamisch vergebenen öffentlichen (externen) IP-Adressen vom Internet Service Provider (ISP).

Um unter diesen Umständen eine statische Namensauflösung zu ermöglichen, müssen die Geräte ihre aktuellen IP-Adressen jeweils unter einem festen Namen bei einem DynDNS-Anbieter registrieren.

Das initiiierende mGuard-Gerät (*mGuard 1*) muss dann auf den DynDNS-Namen des antwortenden mGuard-Geräts verweisen (z. B. *mGuard2.dyndns.org*), um eine VPN-Verbindung aufzubauen.



Aktivieren Sie in diesem Fall die **DynDNS-Überwachung (IPsec VPN >> Global >> DynDNS-Überwachung)** in der VPN-Verbindung des initiiierenden Geräts (*mGuard 1*). Andernfalls weiß das Gerät nicht, wenn sich die IP-Adresse der Gegenstelle geändert hat und der Aufbau der VPN-Verbindung schlägt fehl.

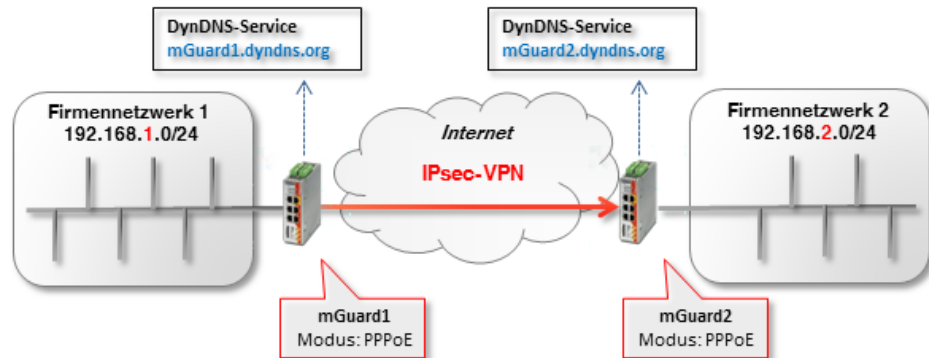


Bild 1-4

Zwei Netzwerke über IPsec-VPN verbinden (*Router/PPPoE* <-> *Router/PPPoE*). Festlegung der Hostnamen für die mGuard-Geräte mittels DynDNS. (Da die Initiierung der VPN-Verbindung durch *mGuard 1* erfolgt, benötigt dieser in diesem Beispiel prinzipiell keine DynDNS-Adresse.)

### 1.3.3 VPN-Verbindung konfigurieren

Konfigurieren Sie die VPN-Verbindung gemäß Bild 1-5 und 1-6 bzw. Tabelle 1-3.

Psec VPN >> Verbindungen >> Name der Verbindung

**Allgemein** Authentifizierung Firewall IKE-Optionen

**Optionen**

|                                            |                           |  |  |  |                     |
|--------------------------------------------|---------------------------|--|--|--|---------------------|
| Ein beschreibender Name für die Verbindung | VPN nach Firmennetzwerk 2 |  |  |  |                     |
| Initialer Modus                            | Gestartet                 |  |  |  |                     |
| Adresse des VPN-Gateways der Gegenstelle   | 10.1.0.102                |  |  |  |                     |
| Verbindungsinitiation                      | Initiiere                 |  |  |  |                     |
| Schaltender Service-Eingang/CMD            | Kein                      |  |  |  |                     |
| Timeout zur Deaktivierung                  | 0:00:00                   |  |  |  | Sekunden (hh:mm:ss) |
| Token für SMS-Steuerung                    |                           |  |  |  |                     |
| Kapsel den VPN-Datenverkehr in TCP ein     | Nein                      |  |  |  |                     |

**Mode Configuration**

Mode Configuration Aus

**Transport- und Tunneleinstellungen**

| Seq. | + | - | Aktiv                    | Kommentar | Typ    | Lokal          | Lokales NAT | Gegenstelle    | Remote-NAT |
|------|---|---|--------------------------|-----------|--------|----------------|-------------|----------------|------------|
| 1    | + | - | <input type="checkbox"/> |           | Tunnel | 192.168.1.0/24 | Kein NAT    | 192.168.2.0/24 | Kein NAT   |

Bild 1-5 mGuard 1 (Initiator): Konfiguration der VPN-Verbindung

Psec VPN >> Verbindungen >> VPN von Firmennetzwerk 1

**Allgemein** Authentifizierung Firewall IKE-Optionen

**Optionen**

|                                                                      |                          |  |  |  |                     |
|----------------------------------------------------------------------|--------------------------|--|--|--|---------------------|
| Ein beschreibender Name für die Verbindung                           | VPN von Firmennetzwerk 1 |  |  |  |                     |
| Initialer Modus                                                      | Gestartet                |  |  |  |                     |
| Adresse des VPN-Gateways der Gegenstelle                             | %any                     |  |  |  |                     |
| Interface, das bei der Einstellung %any für das Gateway benutzt wird | Extern                   |  |  |  |                     |
| Verbindungsinitiation                                                | Warte                    |  |  |  |                     |
| Schaltender Service-Eingang/CMD                                      | Kein                     |  |  |  |                     |
| Timeout zur Deaktivierung                                            | 0:00:00                  |  |  |  | Sekunden (hh:mm:ss) |
| Token für SMS-Steuerung                                              |                          |  |  |  |                     |
| Kapsel den VPN-Datenverkehr in TCP ein                               | Nein                     |  |  |  |                     |

**Mode Configuration**

Mode Configuration Aus

**Transport- und Tunneleinstellungen**

| Seq. | + | - | Aktiv                               | Kommentar | Typ    | Lokal          | Lokales NAT | Gegenstelle    | Remote-NAT |
|------|---|---|-------------------------------------|-----------|--------|----------------|-------------|----------------|------------|
| 1    | + | - | <input checked="" type="checkbox"/> |           | Tunnel | 192.168.2.0/24 | Kein NAT    | 192.168.1.0/24 | Kein NAT   |

Bild 1-6 mGuard 2 (Responder): Konfiguration der VPN-Verbindung

## VPN-Verbindungen mit variierenden Netzwerkmodi konfigurieren

Um die VPN-Verbindung der mGuard-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon , um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon , um die Verbindung zu bearbeiten.
4. Konfigurieren Sie die VPN-Verbindung gemäß Bild 1-5 und 1-6 bzw. Tabelle 1-3.

Tabelle 1-3 VPN-Verbindung konfigurieren (IPsec VPN >> Verbindungen >> (Edit) >> Allgemein)

| Sektion                            | Parameter                                                            | mGuard 1                  | mGuard 2                 |
|------------------------------------|----------------------------------------------------------------------|---------------------------|--------------------------|
| Optionen                           | Ein beschreibender Name für die Verbindung                           | VPN nach Firmennetzwerk 2 | VPN von Firmennetzwerk 1 |
|                                    | Adresse des VPN-Gateways der Gegenstelle                             | 10.1.0.102                | %any                     |
|                                    | Interface, das bei der Einstellung %any für das Gateway benutzt wird | (Feld nicht sichtbar)     | Extern                   |
|                                    | Verbindungsinitiierung                                               | Initiiere                 | Warte                    |
| Transport- und Tunneleinstellungen | Typ                                                                  | Tunnel                    | Tunnel                   |
|                                    | Lokal                                                                | 192.168.1.0/24            | 192.168.2.0/24           |
|                                    | Gegenstelle                                                          | 192.168.2.0/24            | 192.168.1.0/24           |

### Ergebnis

Die beiden Netzwerke sind über einen IPsec-VPN-Tunnel miteinander verbunden. Die Clients können jeweils verschlüsselt mit den Clients des anderen Netzwerks kommunizieren.

Eine *Tunnelverbindung* verbindet immer Netzwerke miteinander (inkl. Netzwerke mit der Subnetzmaske /32) und nicht wie die *Transportverbindung* ausschließlich zwei einzelne Clients (Hosts).

## 1.4 VPN-Tunnelverbindung (Single Stealth <-> Router)

### 1.4.1 Einleitung

Wenn eine VPN-Verbindung zwischen zwei mGuard-Geräten aufgebaut wird, bei denen ein Gerät im *Single-Stealth-Modus* (= *Statisch* oder *Automatisch*) betrieben wird, dann ist es möglich, dass die IP-Adresse des zugeordneten Clients dynamisch über einen DHCP-Server vergeben wird. Ändert sich diese IP-Adresse, ändert sich im *Stealth-Modus* folglich auch die IP-Adresse des mGuard-Geräts.

Damit in diesem Fall nicht die VPN-Konfiguration der mGuard-Geräte geändert werden muss, wird eine *Virtuelle IP-Adresse* verwendet. Das Gerät leitet dann automatisch die über den VPN-Tunnel an diese *Virtuelle IP-Adresse* gesendeten Pakete an die reale IP-Adresse des Clients weiter.

### 1.4.2 Beispiel

Zwischen **Firmennetzwerk 1** (10.1.0.0/16) und **Firmennetzwerk 2** (192.168.2.0/24) soll unter Verwendung zweier mGuard-Geräte ein IPsec-VPN-Tunnel aufgebaut werden.

Ein mGuard-Gerät im *Single-Stealth-Modus* (*Statisch* oder *Automatisch*) soll dazu einen VPN-Tunnel zu einem mGuard-Gerät im Netzwerkmodus *Router* (*Statisch* oder *PPPoE*) aufbauen.

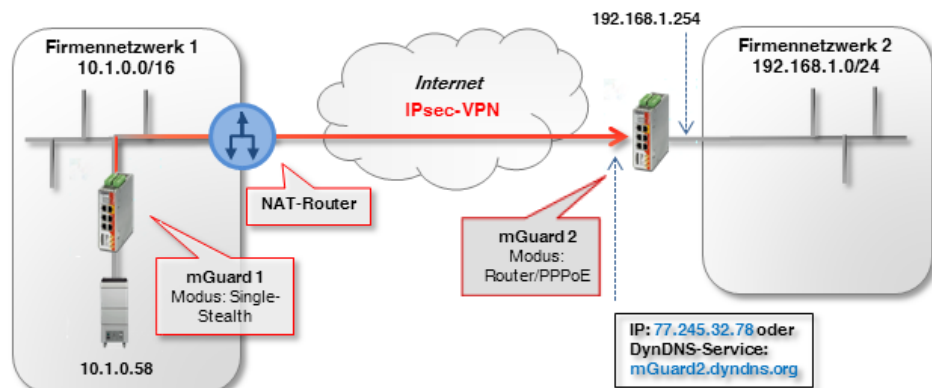


Bild 1-7 Zwei Netzwerke über IPsec-VPN verbinden (*Single-Stealth <-> Router*)

Das antwortende mGuard-Gerät (*mGuard 2*) ist in unserem Beispiel über eine statische öffentliche IP-Adresse aus dem Internet erreichbar.

Ist das mGuard-Gerät über wechselnde (dynamische) IP-Adressen mit dem Internet verbunden, muss es seine aktuelle IP-Adresse unter einem festen Namen bei einem DynDNS-Anbieter registrieren.

Das initiiierende mGuard-Gerät im *Stealth-Modus* (*mGuard 1*) muss dann auf den DynDNS-Namen des antwortenden mGuard-Geräts verweisen (z. B. *mGuard2.dyndns.org*), um eine VPN-Verbindung aufzubauen.



Aktivieren Sie in diesem Fall die **DynDNS-Überwachung (IPsec VPN >> Global >> DynDNS-Überwachung)** in der VPN-Verbindung des initiiierenden Geräts (*mGuard 1*). Andernfalls weiß das Gerät nicht, wenn sich die IP-Adresse der Gegenstelle geändert hat und der Aufbau der VPN-Verbindung schlägt fehl.

### 1.4.3 VPN-Verbindung konfigurieren

Der Aufbau des VPN-Tunnels wird von *mGuard 1* initiiert. Im *Stealth-Modus (Automatisch)* nimmt *mGuard 1* die IP- und MAC-Adresse seines zugehörigen Clients an (10.1.0.58). Im *Stealth-Modus (Statisch)* werden die IP-Adressen statisch eingetragen.

Der antwortende *mGuard 2* im *Router-Modus (PPPoE)* ist unter der statischen öffentlichen (externen) IP-Adresse (77.245.32.78) über das Internet erreichbar. Mit seiner internen IP-Adresse (192.168.1.254) fungiert das Gerät als Standard-Gateway im Netzwerk 192.168.1.0/24 für die angeschlossenen Clients.

Erhält der Client seine IP-Einstellungen von einem DHCP-Server, kann sich seine IP-Adresse prinzipiell ändern. Damit ein konfigurierter VPN-Tunnel auch bei einer dynamischen Änderung der IP-Adresse weiter aufgebaut werden kann, *muss* in den Einstellungen eine *Virtuelle IP-Adresse* angegeben werden, die dann von einer Gegenstelle als Endpunkt des VPN-Tunnels verwendet wird.

#### Transport- und Tunneleinstellungen

|                 | Seq. |                                                                                                                                                                                                                                                       | Aktiv                               | Kommentar | Typ    | Lokal          | Gegenstelle    | Virtuelle IP |
|-----------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-----------|--------|----------------|----------------|--------------|
| <b>mGuard 1</b> | 1    |    | <input checked="" type="checkbox"/> |           | Tunnel | 172.16.1.1/32  | 192.168.1.0/24 | 172.16.1.1   |
| <b>mGuard 2</b> | 1    |    | <input checked="" type="checkbox"/> |           | Tunnel | 192.168.1.0/24 | 172.16.1.1/32  |              |

Soll in unserem Beispiel durch einen VPN-Tunnel aus dem Firmennetzwerk 2 auf den Client im Firmennetzwerk 1 (10.1.0.58) zugegriffen werden, *muss* der Zugriff auf die Virtuelle IP-Adresse erfolgen (z. B. 172.16.1.1/32).

*mGuard 1* würde dann automatisch ein 1:1-NAT von der *Virtuellen IP-Adresse* (172.16.1.1/32) auf die reale IP-Adresse des Clients (10.1.0.58/32) durchführen.

Um die VPN-Verbindung der *mGuard*-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon , um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon , um die Verbindung zu bearbeiten.
4. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 1-4.

Tabelle 1-4 VPN-Verbindung konfigurieren (IPsec VPN >> Verbindungen >> (Edit) >> Allgemein)

| Sektion                            | Parameter                                                            | mGuard 1 (Stealth)        | mGuard 2                 |
|------------------------------------|----------------------------------------------------------------------|---------------------------|--------------------------|
| Optionen                           | Ein beschreibender Name für die Verbindung                           | VPN nach Firmennetzwerk 2 | VPN von Firmennetzwerk 1 |
|                                    | Adresse des VPN-Gateways der Gegenstelle                             | 77.245.32.78              | %any                     |
|                                    | Interface, das bei der Einstellung %any für das Gateway benutzt wird | -----                     | Extern                   |
|                                    | Verbindungsinitiierung                                               | Initiiere                 | Warte                    |
| Transport- und Tunneleinstellungen | Typ                                                                  | Tunnel                    | Tunnel                   |
|                                    | Lokal                                                                | 172.16.1.1/32             | 192.168.1.0/24           |
|                                    | Gegenstelle                                                          | 192.168.1.0/24            | 172.16.1.1/32            |
|                                    | Virtuelle IP                                                         | 172.16.1.1                | -----                    |

## 1.5 VPN-Tunnelverbindung (Multi Stealth <-> Router)

### 1.5.1 Einleitung

Anders als im *Single-Stealth-Modus* (*Automatisch* oder *Statisch*) können mehr als ein Rechner an das LAN-Interface des mGuard-Geräts angeschlossen und somit mehrere IP-Adressen am LAN-Interface verwendet werden.

### 1.5.2 Beispiel

Zwischen **Firmennetzwerk 1** (10.1.0.0/16) und **Firmennetzwerk 2** (192.168.2.0/24) soll unter Verwendung zweier mGuard-Geräte ein IPsec-VPN-Tunnel aufgebaut werden.

Ein mGuard-Gerät im Netzwerkmodus *Stealth* (*Mehrere Clients*) soll dazu einen VPN-Tunnel zu einem mGuard-Gerät im Netzwerkmodus *Router* (*Statisch* oder *PPPoE*) aufbauen. Die Clients hinter dem mGuard-Gerät im Firmennetzwerk 1 (*mGuard 1*) sollen über eine VPN-Tunnel erreichbar sein.

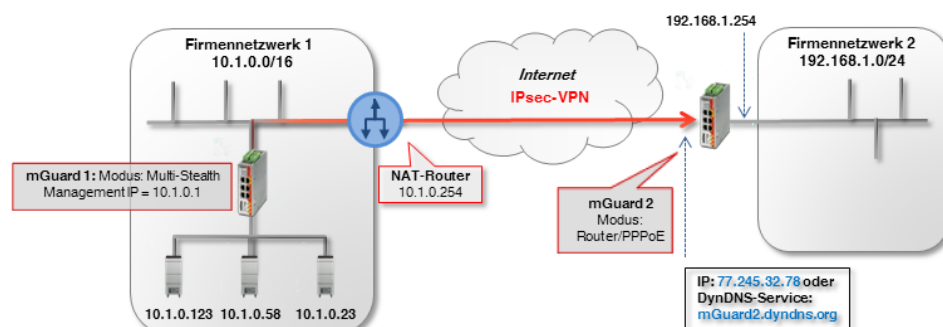


Bild 1-8 Zwei Netzwerke über IPsec-VPN verbinden (Multi-Stealth <-> Router)

Das antwortende mGuard-Gerät (*mGuard 2*) ist in unserem Beispiel über eine statische öffentliche IP-Adresse aus dem Internet erreichbar.

Ist das mGuard-Gerät über wechselnde (dynamische) IP-Adressen mit dem Internet verbunden, muss es seine aktuelle IP-Adresse unter einem festen Namen bei einem DynDNS-Anbieter registrieren (siehe Kapitel 1.4.1).

Die Netzwerkeinstellungen der Interfaces beider mGuard-Geräte werden im Menü **Netzwerk >> Interfaces** vorgenommen (Registerkarten: *Allgemein*, *Stealth*, *Intern*).

Tabelle 1-5 Netzwerkkonfiguration der Interfaces

| Parameter                            | mGuard 1 (Multi-Stealth) | mGuard 2 (Router) |
|--------------------------------------|--------------------------|-------------------|
| <b>Stealth-Management IP-Adresse</b> | 10.1.0.1                 | -----             |
| Netzmaske                            | 255.255.0.0              | -----             |
| Standard-Gateway                     | 10.1.0.254               | -----             |
| <b>Interne IP-Adresse</b>            | -----                    | 192.168.1.254     |
| Netzmaske                            | -----                    | 255.255.255.0     |

### 1.5.3 VPN-Verbindung konfigurieren

Die VPN-Verbindung wird von *mGuard 1* initiiert. Um die VPN-Funktion im Stealth-Modus (*Mehrere Clients*) nutzen zu können, muss dem Gerät eine *Management-IP-Adresse* zugewiesen werden. Diese IP muss zu dem Netzwerk gehören, in dem sich das mGuard-Gerät befindet. Sie darf von keinem anderen Gerät im Netzwerk verwendet werden.

Das wartende Gerät *mGuard 2* hat die statische öffentliche IP-Adresse 77.245.32.78.

#### Transport- und Tunneleinstellungen

|                 | Seq. |                                                                                                                                                                                                                                                       | Aktiv                               | Kommentar | Typ    | Lokal          | Gegenstelle    |
|-----------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-----------|--------|----------------|----------------|
| <b>mGuard 1</b> | 1    |    | <input checked="" type="checkbox"/> |           | Tunnel | 10.1.0.0/16    | 192.168.1.0/24 |
| <b>mGuard 2</b> | 1    |    | <input checked="" type="checkbox"/> |           | Tunnel | 192.168.1.0/24 | 10.1.0.0/16    |

Um die VPN-Verbindung der mGuard-Geräte zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie zu **IPsec VPN >> Verbindungen**.
2. Klicken Sie auf das Icon , um eine neue VPN-Verbindung hinzuzufügen.
3. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon , um die Verbindung zu bearbeiten.
4. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 1-6.

Tabelle 1-6 VPN-Verbindung konfigurieren (*IPsec VPN >> Verbindungen >> (Edit) >> Allgemein*)

| Sektion                            | Parameter                                                            | mGuard 1 (Stealth)        | mGuard 2                 |
|------------------------------------|----------------------------------------------------------------------|---------------------------|--------------------------|
| Optionen                           | Ein beschreibender Name für die Verbindung                           | VPN nach Firmennetzwerk 2 | VPN von Firmennetzwerk 1 |
|                                    | Adresse des VPN-Gateways der Gegenstelle                             | 77.245.32.78              | %any                     |
|                                    | Interface, das bei der Einstellung %any für das Gateway benutzt wird | -----                     | Extern                   |
|                                    | Verbindungsinitiierung                                               | Initiiere                 | Warte                    |
| Transport- und Tunneleinstellungen | Typ                                                                  | Tunnel                    | Tunnel                   |
|                                    | Lokal                                                                | 10.1.0.0/16               | 192.168.1.0/24           |
|                                    | Gegenstelle                                                          | 192.168.1.0/24            | 10.1.0.0/16              |

