1 Netzwerke mittels Hub & Spoke (IPsec VPN) verbinden

Dokument-ID: 108412_de_00
Dokument-Bezeichnung: AH DE MGUARD IPSEC VPN HUB SPOKE

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird die Funktion *Hub & Spoke* beschrieben, mit der über einen zentralen mGuard zwei oder mehr IPsec-VPN-Tunnel miteinander verbunden werden.

1.1 Einleitung 1
1.2 Zweigstellen über Zentrale mittels Hub & Spoke miteinander verbinden 2
1.3 Externe Techniker mittels Hub & Spoke mit Produktionsstandorten verbinden 4

1.1 Einleitung

Die Funktion *Hub & Spoke* ermöglicht die direkte Weiterleitung von Netzwerkpaketen, die über einen VPN-Tunnel empfangen werden, in einen anderen VPN-Tunnel.

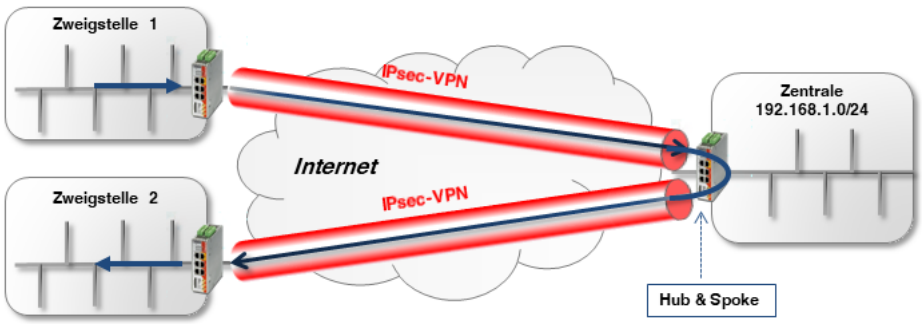

Bild 1-1 *Hub & Spoke* über Firmenzentrale (IPsec VPN)

Wenn viele Remote-Standorte mit der Zentrale verbunden sind und große Datenmengen gesendet werden, kann die Internetverbindung in der Zentrale zum Flaschenhals werden. In einem solchen Fall sollte statt *Hub & Spoke* besser ein vollständiges vermaschtes (engl. *mesh*) Netzwerk verwendet werden.

Neben der Aktivierung von *Hub & Spoke* müssen die jeweiligen Netzwerke in den VPN-Verbindungen entsprechend angegeben werden, um das direkte Routing zwischen den VPN-Tunneln zu ermöglichen.

1.2 Zweigstellen über Zentrale mittels Hub & Spoke miteinander verbinden

Zwei Zweigstellen sollen über eine IPsec-VPN-Verbindung miteinander kommunizieren. Die Verbindung erfolgt über die Firmenzentrale, zu der beide Zweigstellen jeweils einen VPN-Tunnel aufgebaut haben. Auf dem mGuard-Gerät der Zentrale (*mGuard 3*) werden die beiden VPN-Tunnel mittels *Hub & Spoke* miteinander „verbunden“.

Um das *Routing* von einem Tunnel in den anderen zu ermöglichen, muss das konfigurierte lokale Netzwerk von *mGuard 3* alle Gegenstellen-Netze enthalten (z. B. 192.168.0.0/16).

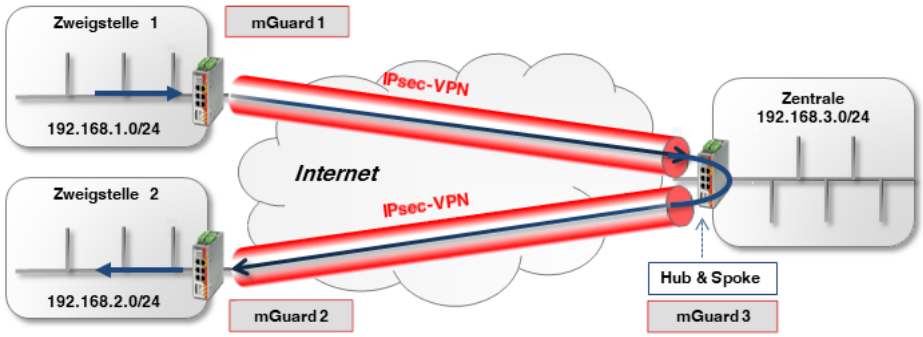

Bild 1-2 *Hub & Spoke* über Firmenzentrale (IPsec VPN)

1.2.1 Konfiguration

Um *Hub & Spoke* auf *mGuard 3* zu aktivieren, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des zu konfigurierenden mGuard-Geräts an.
2. Gehen Sie zu **IPsec VPN >> Global** (Registerkarte *Optionen*).
3. Aktivieren Sie die Option *Erlaube Paketweiterleitung zwischen VPN-Verbindungen*.

Die allgemeine Konfiguration von VPN-Verbindungen erfolgt unter **IPsec VPN >> Verbindungen >> (Edit) >> Allgemein** und wird in Kapitel 1 und 1 beschrieben.

Die Konfiguration der jeweiligen **Transport- und Tunneleinstellungen** sieht wie folgt aus:

mGuard 1 <-> mGuard 3

Seq.	Aktiv	Kommentar	Typ	Lokal	Lokales NAT	Gegenstelle
1	☑	mGuard 1	Tunnel	192.168.1.0/24	Kein NAT	192.168.0.0/16
	☑	mGuard 3	Tunnel	192.168.0.0/16	Kein NAT	192.168.1.0/24

mGuard 2 <-> mGuard 3

Seq.	Aktiv	Kommentar	Typ	Lokal	Lokales NAT	Gegenstelle
1	☑	mGuard 2	Tunnel	192.168.2.0/24	Kein NAT	192.168.0.0/16
	☑	mGuard 3	Tunnel	192.168.0.0/16	Kein NAT	192.168.2.0/24

Hub & Spoke, wenn das lokale Netz nicht alle Gegenstellen-Netze enthält

Was passiert, wenn das Netzwerk der Zentrale nicht Teil des Netzwerks **192.168.0.0/16** ist, sondern z. B. von **10.1.0.0/16**?

In diesem Fall könnten zwar die beiden Zweigstellen über die VPN-Tunnel miteinander kommunizieren. Aber weder **Zweigstelle 1** und **2** hätten Zugriff auf das Netzwerk der **Zentrale** und umgekehrt.

Das Problem ließe sich lösen, indem in jeder konfigurierten VPN-Verbindung ein zweiter VPN-Tunnel angegeben wird, der das Netz der Zentrale adressiert (siehe folgendes Beispiel für die Verbindung von *mGuard 1* zu *mGuard 3*).

mGuard 1 <-> mGuard 3

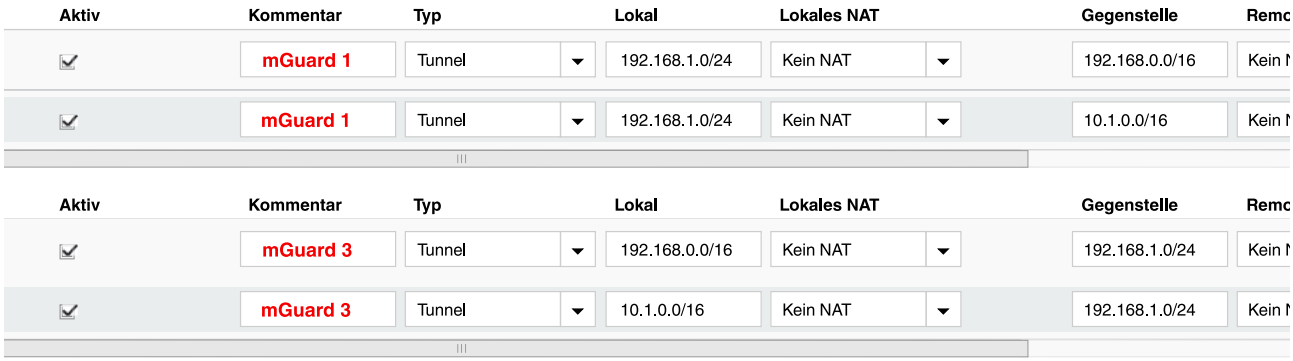

Tabelle 1-1 zeigt für diesen Fall die Transport- und Tunneleinstellungen für alle Geräte (*mGuard 1, 2* und *3*):

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

Tabelle 1-1 Transport- und Tunneleinstellungen bei *Hub & Spoke* (unterschiedliche Netze)

VPN-Verbindung	Tunneleinstellungen	Lokal	Gegenstelle
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 Externe Techniker mittels Hub & Spoke mit Produktionsstandorten verbinden

Zwei Fernwartungs-Techniker sollten von ihren Laptops aus über eine VPN-Verbindung auf die Maschinen aller Produktionsstandorte (Zweigstellen) zugreifen können (per Software-VPN-Client oder per mGuard-Gerät). Die VPN-Verbindung erfolgt dabei zunächst über einen zentralen mGuard (*mguard 4*) der via *Hub & Spoke* eine VPN-Verbindung ins Maschinennetzwerk des jeweiligen Produktionsstandorts herstellt.

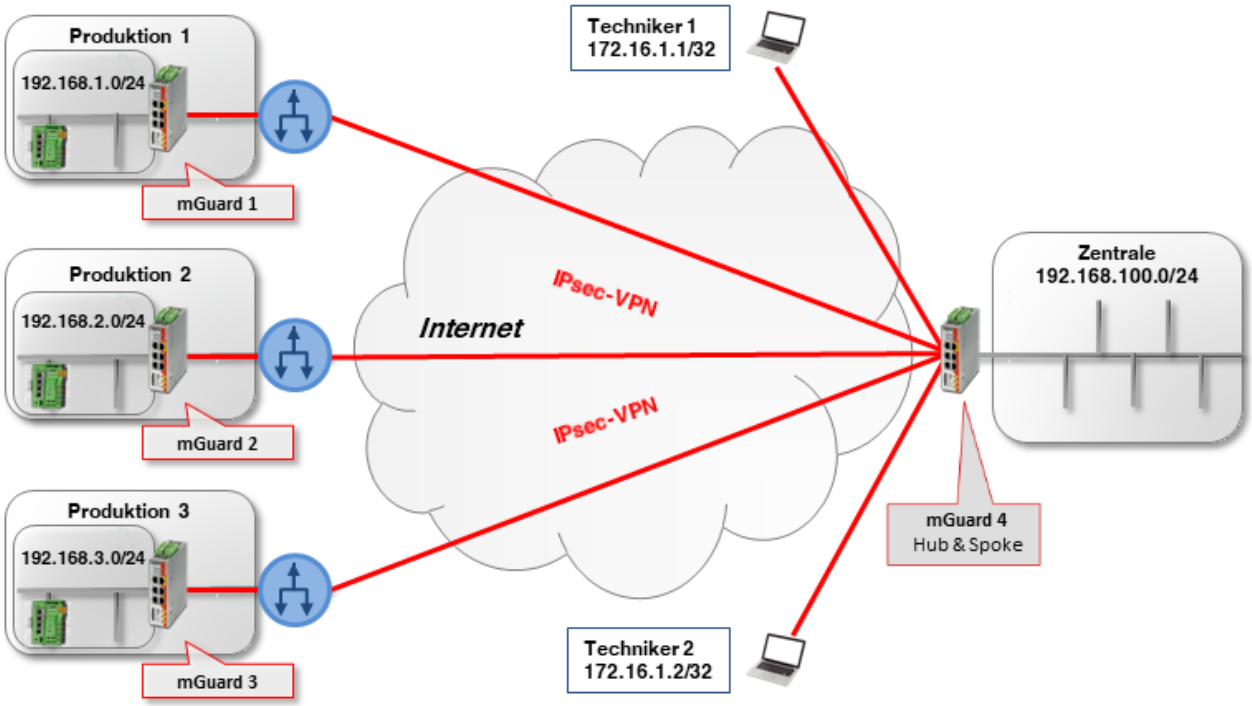

Bild 1-3 Fernwartung via *Hub & Spoke* über die Firmenzentrale (IPsec VPN)

In den Produktionsstandorten wird jeweils ein mGuard-Gerät als Router eingesetzt, um das Maschinennetzwerk mit dem Zweigstellennetzwerk zu verbinden und die VPN-Verbindung zum mGuard-Gerät der Firmenzentrale aufzubauen.

Die Techniker verwenden auf ihren Laptops *Virtuelle IP-Adressen*, um nicht von den realen, den Laptops aktuell zugewiesenen, IP-Adressen abhängig zu sein:

– Techniker 1: 172.16.1.**1**/32,
– Techniker 2: die 172.16.1.**2**/32.

Um Zugriff auf alle Produktionsstandorte zu erhalten, muss das jeweils angegebene VPN-Netzwerk der Gegenstelle die Maschinennetzwerke aller drei Standorte (192.168.**1**.0/24, 192.168.**2**.0/24 und 192.168.**3**.0/24) enthalten: in diesem Beispiel also die **192.168.0.0/16**.

Die mGuard-Geräte der Zweigstellen verwenden die internen Netze 192.168.**1**.0/24, 192.168.**2**.0/24 und 192.168.**3**.0/24. Datenpakete, die über die VPN-Verbindung von den Laptops der Technikern zu den mGuard-Geräten gelangen, besitzen eine der beiden Absender-IP-Adressen: 172.16.1.**1**/32 oder 172.16.1.**2**/32.

Wenn die Fernwartung nicht nur auf zwei Techniker beschränkt werden soll, muss auf den mGuard-Geräten der Produktionsstandorte ein VPN-Netzwerk der Gegenstelle angegeben werden, über das prinzipiell mehrere Techniker angebunden werden können: in diesem Beispiel 172.16.1.0/24.

Beispiel: Zugriff via Hub & Spoke durch zwei Techniker

Wenn die Funktion *Hub & Spoke* auf dem mGuard-Gerät der Zentrale (*mGuard 4*) aktiviert ist, müssen – unter Berücksichtigung der oben genannten Punkte – die Tunneleinstellungen für die VPN-Verbindungen wie folgt konfiguriert werden (vergleiche auch die Beispiel-Konfiguration in Kapitel 1.2.1):

Tabelle 1-2 *Hub & Spoke*: Transport- und Tunneleinstellungen bei **unterschiedlichen** lokalen Netzwerken

VPN-Verbindung	Client	Lokal	<-->	Gegenstelle
Techniker 1 <–> mGuard 4	Techniker 1	172.16.1.1/32	<-->	192.168.0.0/16
	mGuard 4	192.168.0.0/16	<-->	172.16.1.1/32
Techniker 2 <–> mGuard 4	Techniker 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

Beispiel: Zugriff bei gleichen Netzwerke in den Produktionsstandorten

Was passiert, wenn die mGuard-Geräte der Produktionsstandorte alle das gleiche interne Netzwerk verwenden (z. B. 192.168.**1**.0/24)?

In diesem Fall muss *Lokales 1:1 NAT-für IPsec-Tunnelverbindungen* für das lokale Netzwerk auf den mGuard-Geräten der Zweigstellen verwendet werden (siehe auch Kapitel 1.3, „Standorte mit gleichen internen Netzen mit Zentrale verbinden (1:1-NAT)“).

Der Zugriff auf die einzelnen Produktionsstandorte erfolgt dann über ein *Virtuelles Netzwerk* und das mGuard-Gerät führt ein lokales 1:1-NAT vom *Virtuellen Netzwerk* zum lokalen *Realen Netzwerk* durch (192.168.1.0/24).

In diesem Beispiel werden folgende *Virtuelle Netzwerke* für die Produktionsstandorte verwendet:

– Zweigstelle 1:172.17.**1**.0/24,
– Zweigstelle 2: 172.17.**2**.0/24,
– Zweigstelle 3: 172.17.**3**.0/24.

Die Techniker müssen diese virtuellen Netzwerke nutzen, um Zugriff auf die entsprechende Maschine zu erhalten. Daher müssen die Techniker 172.17.0.0/16 als Gegenstellen-VPN-Netzwerk angeben.

Die Tunneleinstellungen für dieses Setup sehen wie folgt aus (siehe Tabelle 1-3 und Bild 1-4).

Tabelle 1-3 *Hub & Spoke*: Tunneleinstellungen bei **gleichen** lokalen Netzwerken (mit lokalem 1:1-NAT)

VPN-Verbindung	Client	Lokal	<-->	Gegenstelle
Techniker 1 <–> mGuard 4	Techniker 1	172.16.1.1/32	<–>	172.17.0.0/16
	mGuard 4	172.17.0.0/16	<–>	172.16.1.1/32
Techniker 2 <–> mGuard 4	Techniker 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
		Lokales 1:1-NAT nach 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
		Lokales 1:1-NAT nach 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
		Lokales 1:1-NAT nach 192.168.1.0/24		
	mGuard 4	172.16.1.0/24	<–>	172.17.**3**.0/24

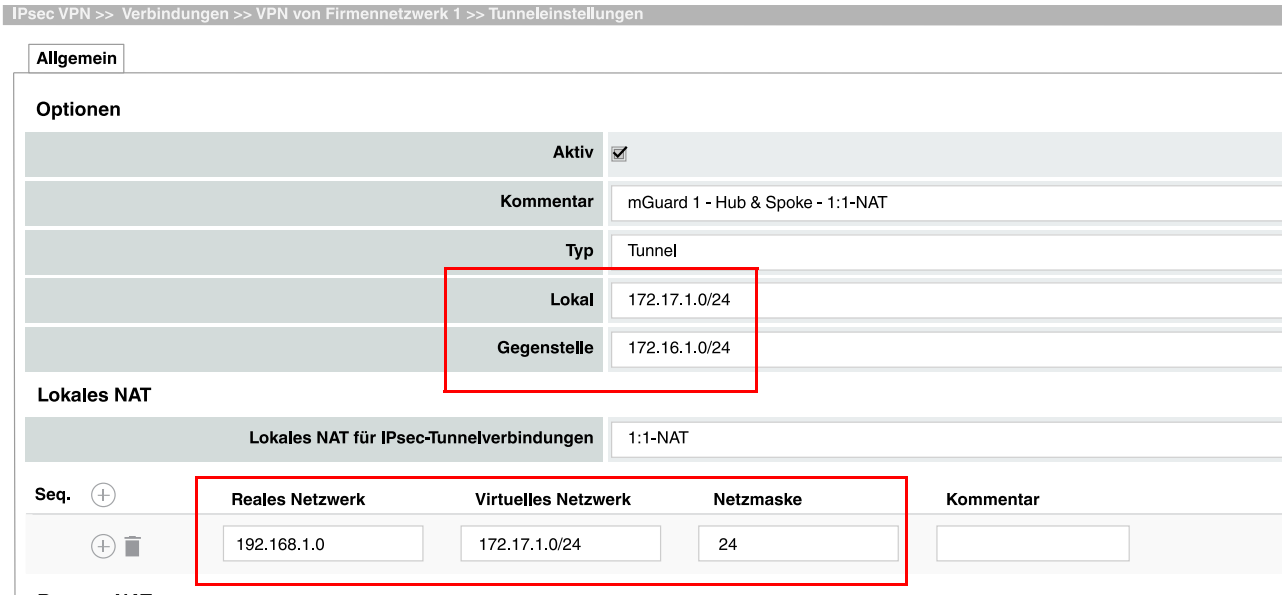

Bild 1-4 *Hub & Spoke*: Beispiel *mGuard 1* – Tunneleinstellungen + lokales 1:1-NAT