1 VPN-Kickstart – Zwei Netzwerke über IPsec-VPN miteinander verbinden

Dokument-ID: 108404_de_00

Dokument-Bezeichnung: AH DE MGUARD VPN KICKSTART

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 Konfiguration einer IPsec-VPN-Verbindung zwischen zwei Netzwerken beschrieben.

1.1 Einleitung

Mittels IPsec-VPN können Netzwerke über einen verschlüsselten VPN-Tunnel miteinander verbunden werden.

1.1.1 Beispiel

Zwischen **Firmennetzwerk 1** (192.168.1.0/24) und **Firmennetzwerk 2** (192.168.2.0/24) soll unter Verwendung zweier mGuard-Geräte ein verschlüsselter IPsec-VPN-Tunnel 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. Der VPN-Tunnel wird aufgebaut, wenn das *wartende* mGuard-Gerät der Gegenstelle (*mGuard 2*) erreichbar ist. Beide mGuard-Geräte werden im Netzwerkmodus *Router* betrieben.

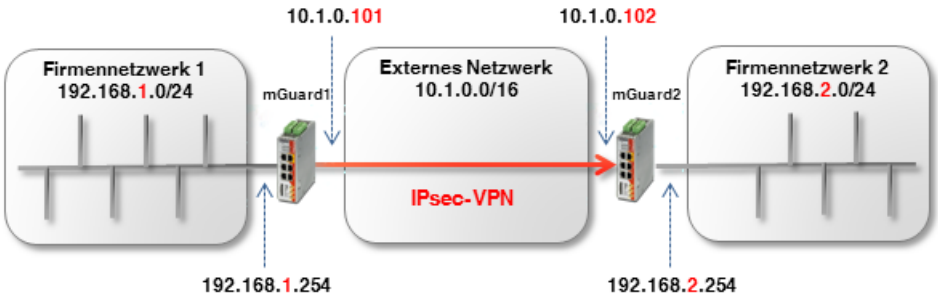


Bild 1-1 Zwei Netzwerke über IPsec-VPN verbinden

Optional: 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 1-2). In diesem Fall ist das Externe Netzwerk das Internet. Die Geräte erhalten ihre externen IP-Einstellungen vom Internet Service Provider (ISP). Eine statische Namensauflösung bei dynamisch vergebenen IP-Adressen wird dann mithilfe eines DynDNS-Services möglich.

Hat das antwortende (wartende) mGuard-Gerät (*mGuard 2*) eine dynamische öffentliche IP-Adresse, muss dieser mGuard seine externe IP-Adresse unter einem frei wählbaren Namen bei einem DynDNS-Dienst registrieren (z. B. *mGuard2.dyndns.org*). Das initiierende mGuard-Gerät (*mGuard 1*) muss auf diesen Namen verweisen, um die VPN-Verbindung aufzubauen.

Aktivieren Sie in diesem Fall die **DynDNS-Überwachung** (**IPsec VPN >> Global >> DynDNS-Überwachung**) in der VPN-Verbindung des initiierenden 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.

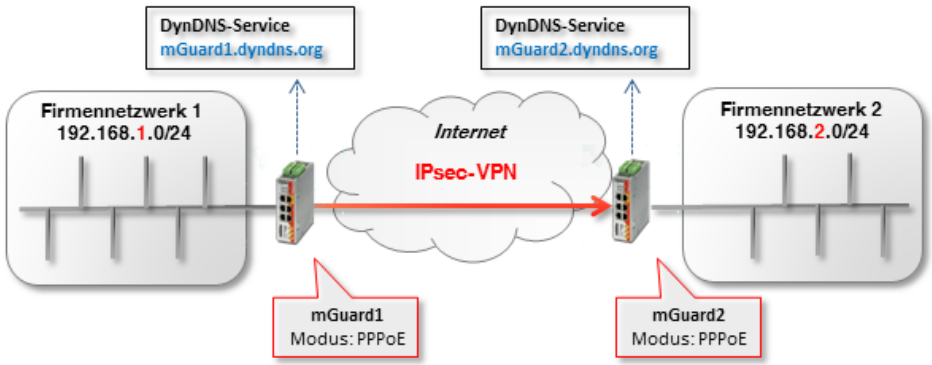


Bild 1-2 Festlegung der Hostnamen für die mGuard-Geräte mittels DynDNS. Da die Initiierung der VPN-Verbindung durch *mGuard 1* erfolgt, benötigt dieser keine DynDNS-Adresse.

1.1.2 Voraussetzung

1. Zwei mGuard-Geräte mit aktueller Firmware (z. B. Version 8.6.1 oder höher),
2. Eine vorhandene Netzwerkverbindung (IP-Verbindung) zwischen den mGuard-Geräten (z. B. über Internet, WAN oder LAN).

3. Eine interne und eine externe IP-Adresse für jedes mGuard-Gerät.
4. In der Firewall geöffnete UDP-Ports 500 und 4500 auf beiden Seiten der IPsec-VPN-Verbindung.
5. (Optional) einen Hostnamen für jedes mGuard-Gerät, z. B. via DynDNS (z. B. *mGuard1.dyndns.org* und *mGuard2.dyndns.org*).

1.1.3 Vorgehen

1. X.509-Zertifikate und Schlüssel erzeugen
2. X.509-Zertifikate und Schlüssel importieren
3. Tunneleinstellungen der IPsec-VPN-Verbindung konfigurieren
4. IPsec-VPN-Verbindungsaufbau testen

1.2 Maschinenzertifikate (X.509-Zertifikate) erzeugen

Zertifikate, die für eine sichere Authentifizierung von mGuard-Geräten benötigt werden, können zum einen von einer kommerziellen Zertifizierungsstelle ausgestellt werden. Zum Erstellen von selbst-signierten Zertifikaten können Programme wie *XCA*, *OpenSSL* oder *Microsoft Certification Authority (CA) Server* verwendet werden.

Selbst-signierte Zertifikate sind nicht durch eine offizielle CA beglaubigt und deshalb nur unter bestimmten Voraussetzungen einsetzbar.

Das Erzeugen von selbst-signierten Zertifikaten mittels OpenSSL oder XCA wird in den Anwenderhinweisen „X.509-Zertifikate mit OpenSSL/XCA erstellen“ beschrieben.

Folgende Zertifikate werden für die Authentisierung einer IPsec-VPN-Verbindung zwischen zwei mGuard-Geräten benötigt. (In unserem Beispiel werden als *CommonName* in den Zertifikaten die eindeutigen Namen *mGuard 1* und *mGuard 2* verwendet.)

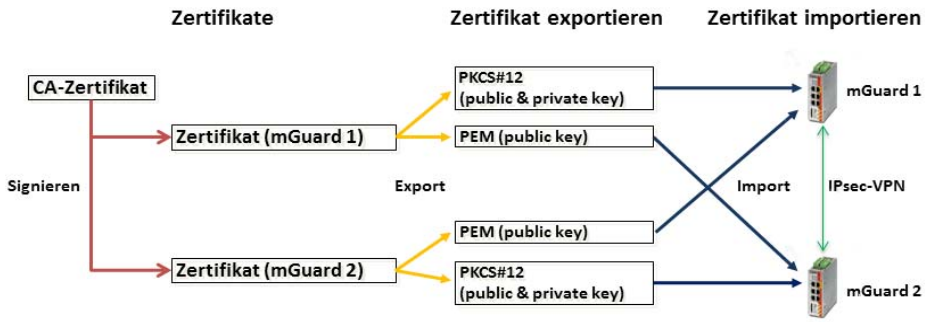
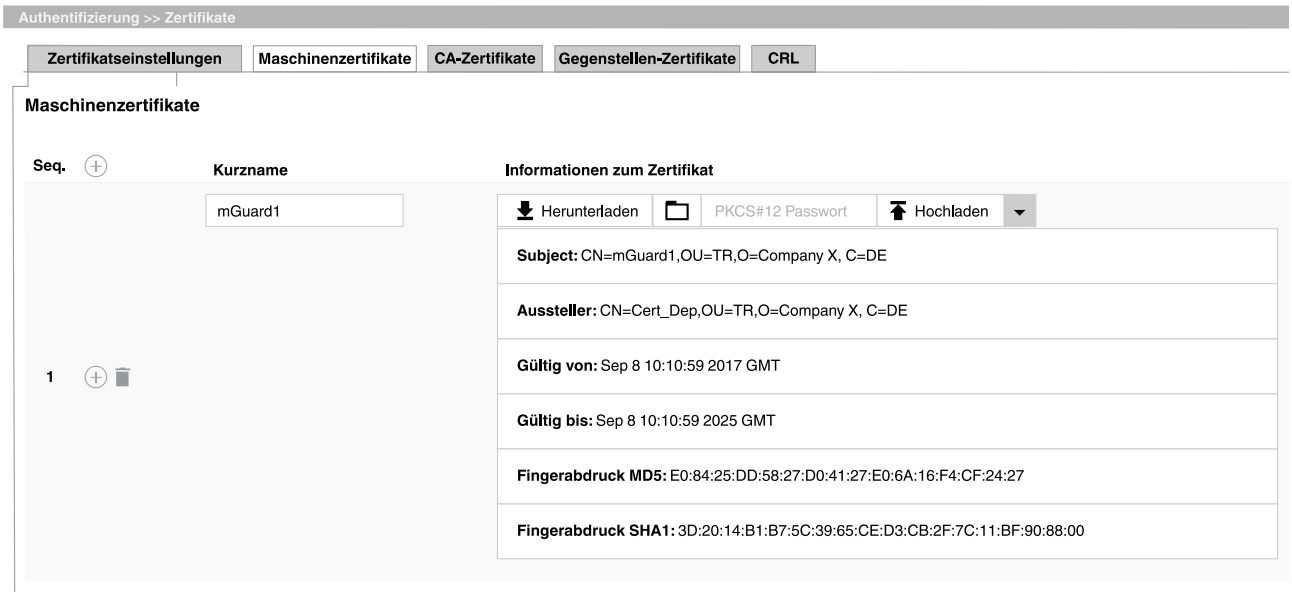


Bild 1-3 Beteiligte Zertifikate in einer IPsec-VPN-Verbindung

Tabelle 1-1 Benötigte Zertifikate

Gerät	Maschinenzertifikat (beinhaltet auch den privaten Schlüssel)	Client-Zertifikat (beinhaltet nur den öffentlichen Schlüssel)
mGuard 1	*mGuard1.p12*	*mGuard1.pem*
mGuard 2	*mGuard2.p12*	*mGuard2.pem*

1.3 Maschinenzertifikate (PKCS) importieren



Um X.509-Maschinenzertifikate (inkl. privatem Schlüssel) in Ihre mGuard-Geräte zu importieren, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (z. B. https://192.168.1.254).
2. Gehen Sie zu **Authentifizierung >> Zertifikate** (Registerkarte *Maschinenzertifikate*).
3. Klicken Sie auf das Icon ⊕, um ein neues Maschinenzertifikat hinzuzufügen.
4. Klicken Sie auf das Icon 🗀, um die Zertifikatsdatei auf dem Installationsrechner auszuwählen.
5. Wählen Sie die zuvor erstellte Datei *mGuard1.p12* aus.
6. Geben Sie das bei der Erzeugung des Zertifikats vergebene PKCS#12-Passwort an.
7. Geben Sie dem Zertifikat einen eindeutigen Kurznamen. Wenn Sie das Feld freilassen, wird automatisch der *CommonName (CN)* des Zertifikats verwendet.
8. Klicken Sie auf die Schaltfläche **Hochladen**, um das Zertifikat zu importieren.
9. Klicken Sie auf das Icon 🖫 „*Übernehmen*“, um den Import abzuschließen.

Führen Sie den Vorgang erneut für das Gerät *mGuard2* durch, und importieren Sie das Maschinenzertifikat mit dem Dateinamen *mGuard2.p12.*

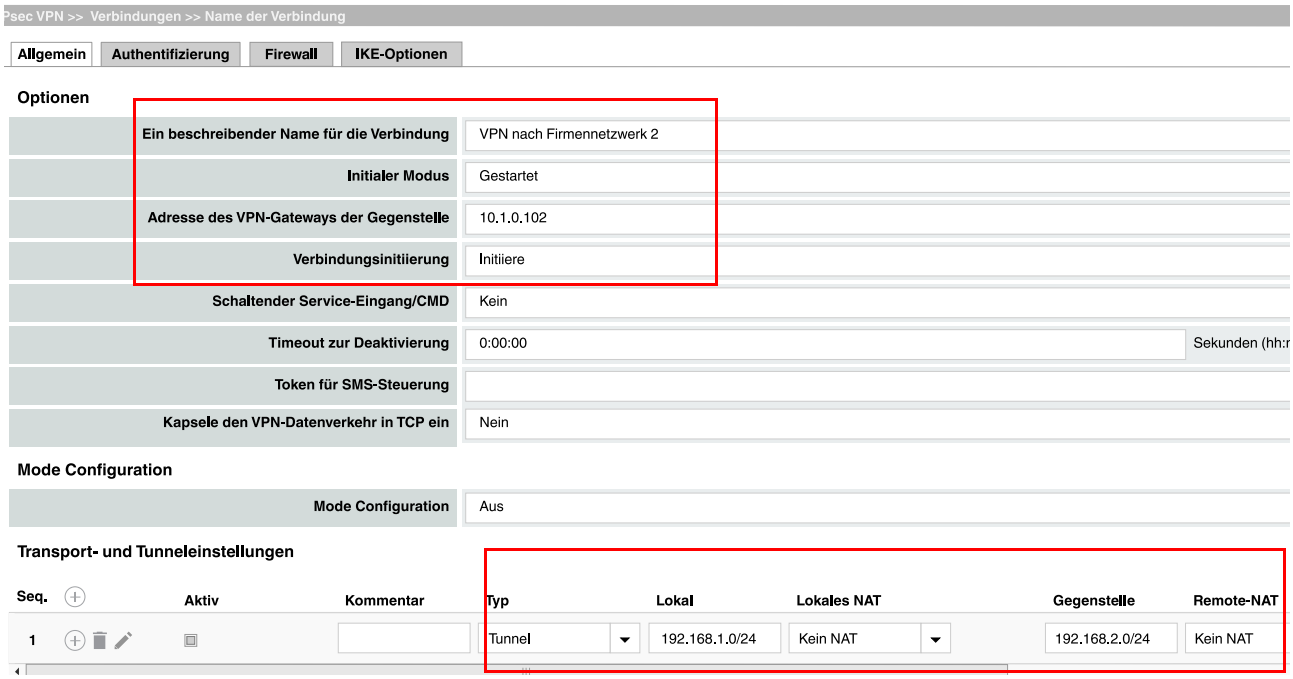
1.4 VPN-Verbindung mGuard1 anlegen

1.4.1 Voraussetzung

Um die IPsec-VPN-Verbindung zu konfigurieren, müssen folgende Grundeinstellungen vorgenommen werden:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (z. B. https://192.168.1.254).
2. Gehen Sie zu **IPsec VPN >> Global** (Registerkarte *Optionen*).
3. In Sektion **IP-Fragmentierung**: Aktivieren Sie die Option *IKE-Fragmentierung* und stellen Sie bei *MTU für IPsec* aus Kompatibilitätsgründen sicherheitshalber einen Wert von 1414 oder niedriger ein.

1.4.2 VPN-Verbindung konfigurieren



Um die VPN-Verbindung 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.

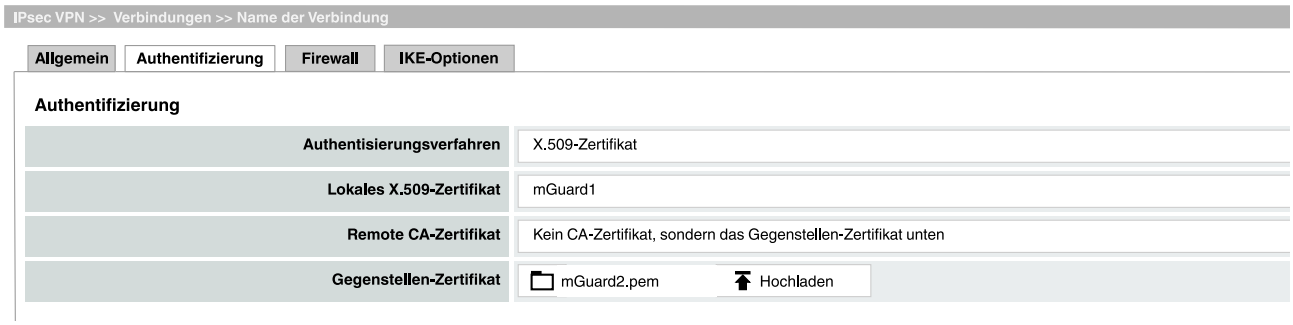
Sektion „Optionen“

1. Tragen Sie als **Adresse des VPN-Gateways der Gegenstelle** entweder den DynDNS-Namen oder die externe IP-Adresse der Gegenstelle (*mguard2*) ein (*mGuard2.dyndns.org* oder 10.1.0.102).
2. Wählen Sie bei **Verbindungsinitiierung** *Initiiere* aus.

Sektion „Transport- und Tunneleinstellungen“

1. Tragen Sie die Adresse des Netzwerks, das über das interne Interface von *mGuard1* erreichbar sein soll, in das Feld **Lokal** ein (192.168.**1**.0/24).
2. Tragen Sie die Adresse des Netzwerks, das über das interne Interface von *mguard2* erreichbar sein soll, in das Feld **Gegenstelle** ein (192.168.**2**.0/24).
3. Klicken Sie auf das Icon „*Übernehmen*“, um den Vorgang abzuschließen.

1.4.3 Authentifizierung der VPN-Verbindung konfigurieren



Um eine gegenseitige Authentifizierung der beiden Gegenstellen beim Aufbau der VPN-Verbindung zu konfigurieren, gehen Sie wie folgt vor:

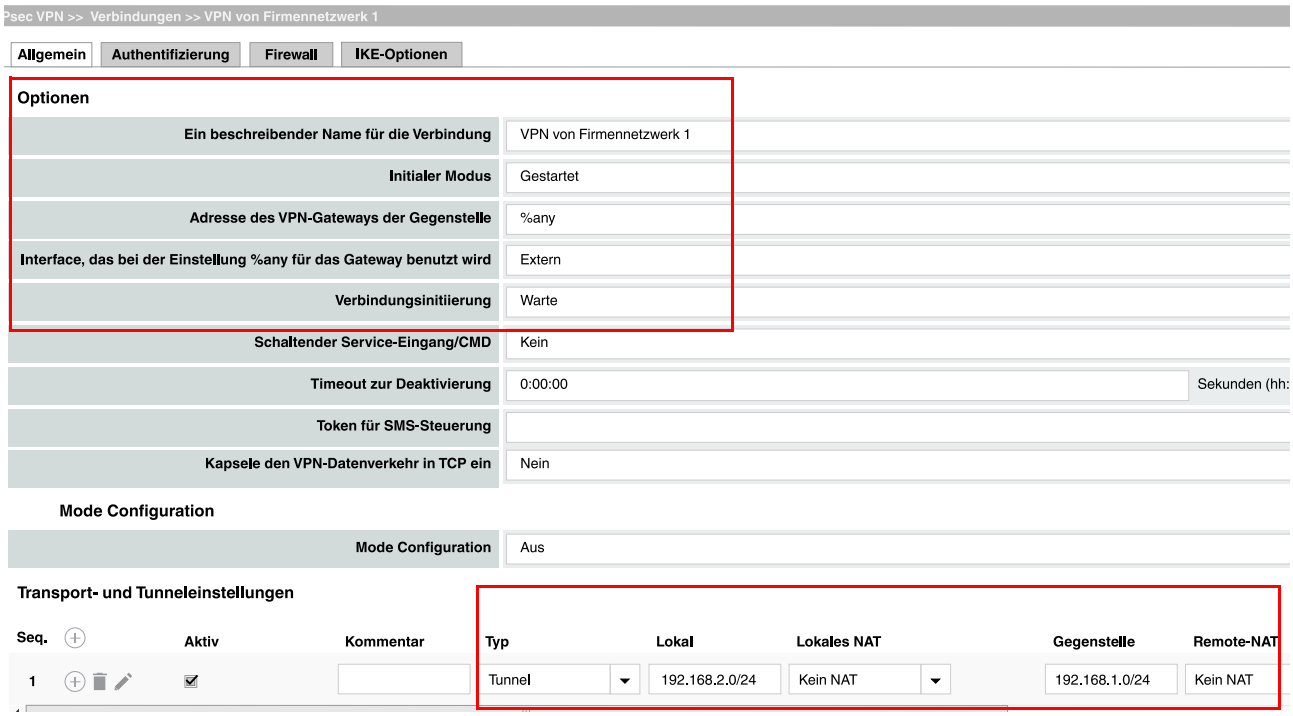
1. Gehen Sie zu **IPsec VPN >> Verbindungen** (Registerkarte *Authentifizierung*)
2. Wählen Sie unter **Lokales X.509-Zertifikat** das Zertifikat aus, das Sie zuvor als Maschinenzertifikat für *mGuard1* in das Gerät importiert haben (*mGuard1*).
3. Wählen Sie unter **Remote CA-Zertifikat** die Option *Kein CA-Zertifikat, sondern das Gegenstellen-Zertifikat unten*.
4. Importieren Sie unter **Gegenstellen-Zertifikat** das Client-Zertifikat von *mGuard2*.
   Klicken Sie dazu auf das Icon und wählen Sie das auf dem Konfigurationsrechner gespeicherte Zertifikat (*mGuard2.pem*) aus. Klicken Sie anschließend auf die Schaltfläche **Hochladen**.
5. Klicken Sie auf das Icon „*Übernehmen*“, um den Vorgang abzuschließen.

1.5 VPN-Verbindung mGuard2 anlegen

1.5.1 Voraussetzung

Es gelten die gleichen Voraussetzungen wie bei mGuard1 (siehe „Voraussetzung“ auf Seite 6).

1.5.2 VPN-Verbindung konfigurieren



Führen Sie die oben beschriebenen Konfigurationsschritte (*mguard1*) nun für die VPN-Gegenstelle (*mGuard2*) durch. Beachten Sie folgende Unterschiede:

IPsec VPN >> Verbindungen (Registerkarte *Allgemein*)

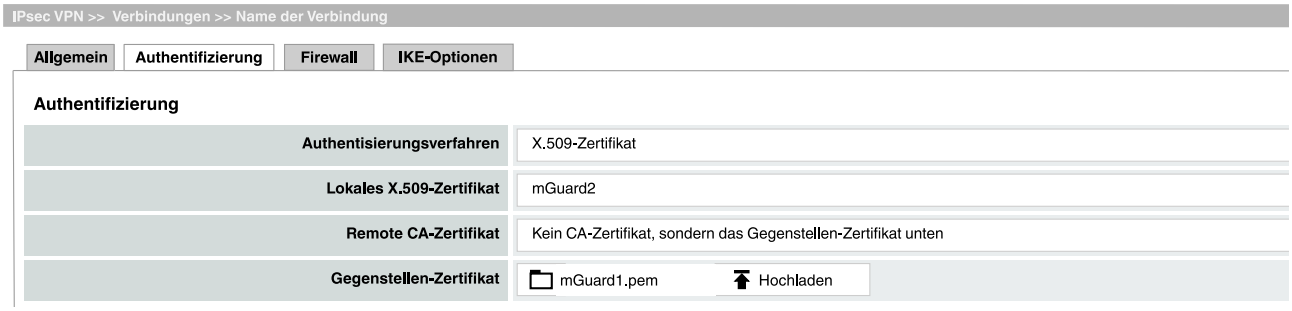
Sektion „Optionen“

1. Tragen Sie als **Adresse des VPN-Gateways der Gegenstelle** *%any* ein.
2. Tragen Sie bei **Interface, das bei der Einstellung %any für das Gateway benutzt wird** *Extern* ein.
3. Wählen Sie bei **Verbindungsinitiierung** *Warte* aus.

Sektion „Transport- und Tunneleinstellungen“

1. Tragen Sie die Adresse des Netzwerks, das über das interne Interface von *mGuard2* erreichbar sein soll in das Feld **Lokal** ein (192.168.**2**.0/24).
2. Tragen Sie die Adresse des Netzwerks, das über das interne Interface von *mGuard1* erreichbar sein soll in das Feld **Gegenstelle** ein (192.168.**1**.0/24).
3. Klicken Sie auf das Icon „*Übernehmen*“, um den Vorgang abzuschließen.

1.5.3 Authentifizierung der VPN-Verbindung konfigurieren



Führen Sie die oben beschriebenen Konfigurationsschritte (*mguard1*) nun für die VPN-Gegenstelle (*mGuard2*) durch. Beachten Sie folgende Unterschiede:

IPsec VPN >> Verbindungen (Registerkarte *Authentifizierung*)

1. Wählen Sie unter **Lokales Zertifikat** das Zertifikat aus, das Sie zuvor als Maschinenzertifikat für *mGuard2* in das Gerät importiert haben (*mGuard2*).
2. Wählen Sie unter **Remote CA-Zertifikat** die Option *Kein CA-Zertifikat, sondern das Gegenstellen-Zertifikat unten*.
3. Importieren Sie unter **Gegenstellen-Zertifikat** das Client-Zertifikat von *mGuard1*.

   Klicken Sie dazu auf das Icon und wählen Sie das auf dem Konfigurationsrechner gespeicherte Zertifikat (*mGuard1.pem*) aus. Klicken Sie anschließend auf die Schaltfläche **Hochladen**.
4. Klicken Sie auf das Icon „*Übernehmen*“, um den Vorgang abzuschließen.

1.6 VPN-Verbindung testen

1.6.1 Voraussetzung

– Schließen Sie die beiden konfigurierten mGuard-Geräte in den entsprechenden Netzwerkumgebungen an.
– Optional: Sorgen Sie dafür, dass eine Verbindung ins Internet hergestellt werden kann (UDP-Ports 500 und 4500 müssen geöffnet sein).

1.6.2 Vorgehen

1. Melden Sie sich auf der Weboberfläche von *mGuard1* oder *mGuard2* an (z. B. https://192.168.1.254).
2. Gehen Sie zu **IPsec VPN >> IPsec-Status**.
3. Prüfen Sie auf der Statusseite, ob beide Geräte (*mGuard1* und *mGuard2*) untereinander eine VPN-Verbindung aufgebaut haben.

   Es muss sowohl eine ISAKMP- als auch eine IPsec SA-Verbindung aufgebaut sein.
4. Überprüfen Sie die sichere VPN-Verbindung, indem Sie entweder die jeweilige VPN-Gegenstelle anpingen oder aber den Zugriff auf eine Gegenstelle (z. B. Webserver, Steuerung, Rechner) im Remote-Netz testen.