1 IPsec-VPN – Grundfunktionen

Dokument-ID: 108413_de_00

Dokument-Bezeichnung: AH DE MGUARD IPSEC VPN OVERVIEW

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 werden generelle Anwendungsmöglichkeiten und die Grundfunktion von IPsec-VPN-Verbindungen beschrieben.

1.1 Einleitung

Datenpakete werden üblicherweise ungeschützt über das Internet versendet und gewährleisten daher nicht die grundlegenden Sicherheitsanforderungen:

– Verschlüsselung (Vertraulichkeit der Daten)
– Authentifizierung (Nachweis der Identität des Absenders)
– Integrität (Sicherstellung, dass die Datenpakete nicht verändert wurden).

Ein *Virtual Private Network* (VPN) ist ein Kommunikationskanal, der mittels Verschlüsselung und Authentifizierung die gesendeten Daten bei der Übertragung über ein öffentliches Medium (z. B. das Internet) in diesem Sinne schützt.

Das heute am häufigsten eingesetzte VPN-Protokoll ist *Internet Protocol Security* (IPsec). Die meisten VPN-Geräte und -Clients sind IPsec-konform. IPsec ist skalierbar und kann sowohl in kleinen Anwendungen als auch auf großen VPN-Gateways mit mehr als 1000 VPN-Verbindungen eingesetzt werden.

IPsec unterstützt Transportverbindungen, mit denen zwei einzelne Hosts verbunden werden, sowie Tunnelverbindungen, mit denen zwei Netzwerke verbunden werden.

1.1.1 Aufbau von ISAKMP-SA und IPsec-SA

Eine VPN-Verbindung wird in zwei Phasen aufgebaut: Phase I (ISAKMP-SA – Schlüsselaustausch) und Phase II (IPsec-SA – Datenaustausch). SA steht für *Security Association*.

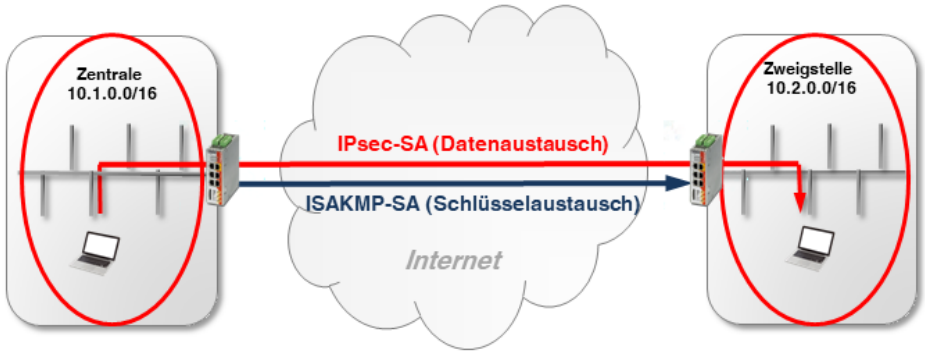

Bild 1-1 Aufbau einer IPsec-Verbindung (ISAKMP-SA und IPsec-SA)

Phase I (ISAKMP-SA):

ISAKMP-SA ist eine sichere Verbindung (*Security Assoziation*) zwischen zwei VPN-Gegenstellen, über die in einem ersten Schritt der sichere Austausch von Schlüsseln (*Keys*) für die VPN-Verschlüsselung vereinbart wird.

Beide VPN-Gegenstellen verhandeln dazu den Verschlüsselungs- und Hash-Algorithmus für Phase I und authentifizieren sich gegenseitig mittels *Pre-Shared Keys* (PSK) oder X.509-Zertifikaten (siehe Kapitel 1.3).

Anschließend einigen sich beide Gegenstellen auf einen Schlüssel (*Key*), um den Datenaustausch der Phase II zu verschlüsseln.

Phase II (IPsec-SA):

Die IPsec-SA ist eine sichere Verbindung (*Security Assoziation*), über die die internen Netzwerke der VPN-Gegenstellen miteinander verbunden werden und Daten austauschen.

Beide Gegenstellen verhandeln dazu den Verschlüsselungs- und Hash-Algorithmus für Phase II und tauschen Informationen über die zu verbindenden Netzwerke aus.

1.1.2 Konfiguration von IPsec-VPN-Verbindungen

Die Konfiguration von IPsec-VPN-Verbindungen zwischen einem mGuard-Gerät und einer VPN-Gegenstelle erfolgt im Menü **IPsec VPN >> Verbindungen** (siehe auch mGuard-Firmwarehandbuch). Eine VPN-Verbindung wird in der Regel von einem Gerät *initiiert*, während das Gerät der Gegenstelle auf die Verbindungsanfrage des Initiators *wartet*.

Die Konfiguration der VPN-Verbindung erfolgt auf den folgenden Registerkarten:

- **Registerkarte „Allgemein“**
- **Registerkarte „Authentifizierung“**
- **Registerkarte „Firewall“**
- **Registerkarte „IKE-Optionen“**

1.2 Registerkarte „Allgemein“

Die Einstellungen auf der Registerkarte „Allgemein“ sind abhängig von der Netzwerkumgebung, in der die VPN-Verbindung aufgebaut wird (z. B. Netzwerkmodus *Stealth, Router, PPPoE*) und von den VPN-Eigenschaften, die verwendet werden sollen (z. B. *1:1-NAT für lokale Netzwerke* oder *Hub & Spoke*). Siehe auch Kapitel 1 und 1.

1.2.1 Beispiel

Zwischen **Firmennetzwerk 1** (192.168.1.0/24) und **Firmennetzwerk 2** (192.168.2.0/24) soll ein verschlüsselter IPsec-VPN-Tunnel aufgebaut werden. Die VPN-Verbindung wird von *mGuard 1* initiiert. Beide Geräte werden im Netzwerkmodus *Router* betrieben.

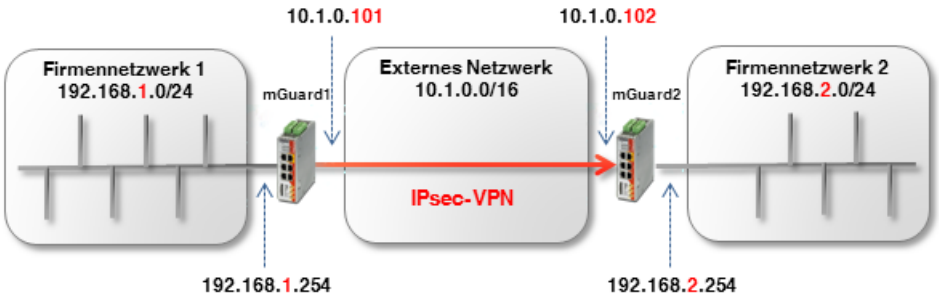

Bild 1-2 Zwei Netzwerke über IPsec-VPN verbinden

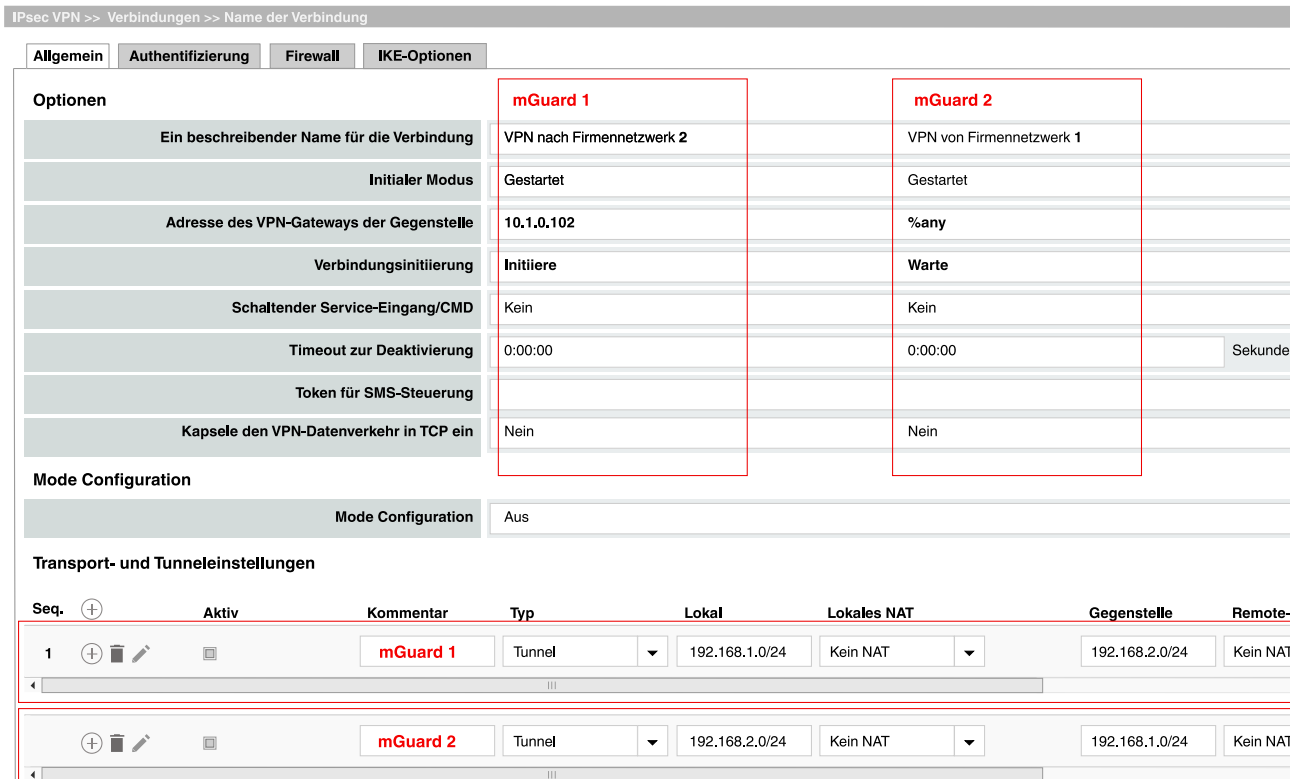

Bild 1-3 Menü: IPsec VPN >> Verbindungen >> (Edit) >> Allgemein

1.3 Registerkarte „Authentifizierung“

Die gegenseitige Authentifizierung der beiden VPN-Gegenstellen kann auf zwei Arten erfolgen:

– X.509-Zertifikate
– Pre-Shared Key (PSK)

Pre-Shared Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec-Implementierungen unterstützt. Dabei authentifizieren sich beide Seiten der VPN-Verbindung über das gleiche Passwort (PSK). Der PSK besteht aus einer alphanumerischen Zeichenfolge. Das PSK-Verfahren kann im sicheren *Main Mode* oder im unsicheren *Aggressive Mode* eingesetzt werden (siehe auch mGuard-Firmwarehandbuch, Abschnitt „IPsec VPN >> Verbindungen >> Authentifizierung“).

X.509-Zertifikate

Dieses Verfahren wird von den meisten IPsec-Implementierungen unterstützt. Dabei besitzt jeder VPN-Teilnehmer einen privaten (geheimen) Schlüssel sowie einen öffentlichen Schlüssel in Form eines X.509-Zertifikats, welches weitere Informationen über seinen Eigentümer und eine Zertifizierungsstelle (*Certificate Authority, CA*) enthält (siehe auch mGuard-Firmwarehandbuch, Abschnitt „IPsec VPN >> Verbindungen >> Authentifizierung“).

Welches Verfahren sollte verwendet werden?

Die Verwendung von Zertifikaten gilt allgemein als sicherer und kann in allen Netzwerk-Szenarien angewandt werden. Die Erstellung eines Zertifikats erfordert allerdings einen gewissen Aufwand und eine genaue Planung.

Die Verwendung von PSK im *Main Mode* gilt mit einem ausreichend komplexem Passwort ebenfalls als relativ sicher. PSK ist allerdings in manchen Netzwerkumgebungen nicht oder nur umständlich einsetzbar:

– PSK im sicheren *Main Mode* kann nicht verwendet werden, wenn die VPN-Verbindung über ein oder mehrere Gateways mit aktivierter *Network Address Translation* (NAT) hergestellt wird. Das heißt, PSK kann nur verwendet werden, wenn beide Geräte an das gleiche externe Netzwerk oder direkt an das Internet angeschlossen sind. Andernfalls würde dies den unsicheren *Aggressive Mode* erfordern.
– Bei Verwendung von PSK muss die externe (oder öffentliche) IP-Adresse des VPN-Gateways der Gegenstelle bei jedem Standort in der VPN-Konfiguration eingetragen werden. Der allgemeine Eintrag *%any* kann nicht auf der antwortenden Seite verwendet werden. Dafür wäre der unsichere *Aggressive Mode* notwendig.

1.3.1 Beispiel: X.509-Zertifikaten erstellen

Ein Zertifikat ist wie eine eindeutige ID und muss deshalb für jedes Gerät eindeutig sein. X.509-Zertifikate können entweder von einer kommerziellen Zertifizierungsstelle (z. B. *VeriSign*), oder einem Microsoft CA-Server bezogen werden oder mit Software-Tools wie z. B. *OpenSSL* oder *XCA* erstellt werden (siehe auch Anwenderhinweise „X.509-Zertifikate mit OpenSSL/XCA erstellen“.

Bei der Erstellung eines Zertifikats müssen zunächst die Parameter angegeben werden, mit denen die Zugehörigkeit des Zertifikats eindeutig bestimmt werden kann (*Common Name, Organization, Organization Unit* etc.).

Als nächstes wird ein Schlüsselpaar erzeugt: Ein privater Schlüssel und ein entsprechender öffentlicher Schlüssel. Der private Schlüssel *muss* sorgfältig geschützt werden, während der öffentliche Schlüssel veröffentlicht werden kann.

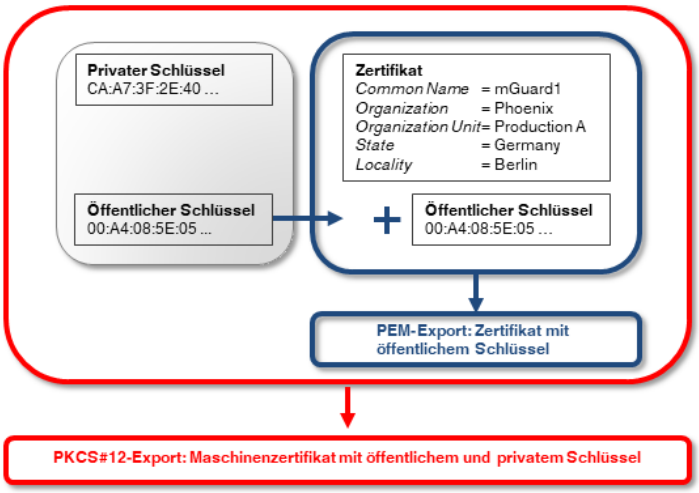

Bild 1-4 PEM- und PKCS#12-Exporte von X.509-Zertifikaten mit öffentlichem bzw. öffentlichem und privatem Schlüssel

1.3.2 Beispiel: X.509-Zertifikate verwenden

In einer VPN-Verbindung muss festgelegt werden,

– wie sich das mGuard-Gerät bei der Gegenstelle authentisiert und
– wie das mGuard-Gerät die entfernte Gegenstelle authentifiziert.

Erfolgt die Autorisierung mittels X.509-Zertifikaten, kann die VPN-Verbindung nur aufgebaut werden, wenn der private Schlüssel auf der einen Seite mit dem öffentlichen Schlüssel auf der anderen Seite „korrespondiert“ (siehe auch Kapitel 1.3, „Maschinenzertifikate (PKCS) importieren“).

Die erstellten Zertifikate müssen dafür in zwei unterschiedliche Formate exportiert und in die entsprechenden Geräte importiert werden:

1. **PEM-Format:**
   Das Zertifikat im PEM-Format enthält nur den öffentlichen Schlüssel. Es muss in jedes Gerät importiert werden, das eine VPN-Verbindung zu dem Gerät aufbauen will, zu dem das Zertifikat (PKCS#12-Export = *Maschinenzertifikat*) gehört (siehe Bild 1-5).
2. **PKCS#12 Format:**
   Das Zertifikat im PKCS#12-Format enthält sowohl den öffentlichen als auch den zugehörigen (korrespondierenden) privaten Schlüssel. Es wird als eindeutiges *Maschinenzertifikat* eines bestimmten Geräts nur in dieses importiert (siehe Bild 1-5).

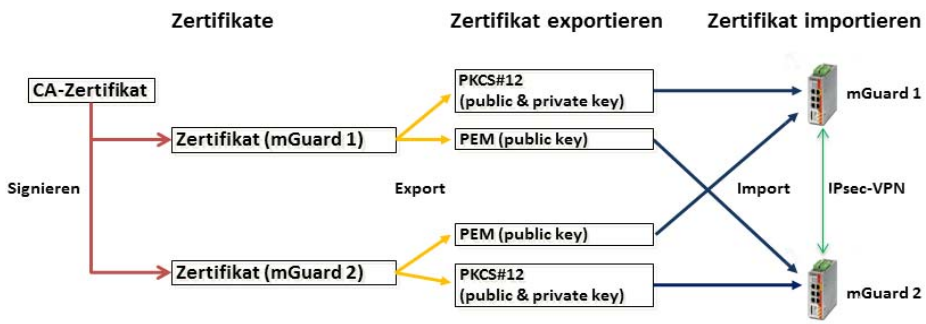

Bild 1-5 Benötigte Zertifikate in einer IPsec-VPN-Verbindung

Tabelle 1-1 Beispiel: Zertifikate in einer IPsec-VPN-Verbindung

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*

mGuard-Geräte unterstützen auch die sogenannte CA-Authentifizierung. Mit dieser Funktion wird die Gegenstelle durch das CA-Zertifikat authentifiziert, mit dem das Zertifikat der Gegenstelle (Remote-Zertifikat) signiert wurde. Eine Authentifizierung durch das Remote-Zertifikat selbst ist dann nicht notwendig. Diese Funktion wird hauptsächlich in VPN-Tunnelgruppen verwendet.

Die Mehrfachnutzung eines Zertifikats (als gerätespezifischer Ausweis) auf unterschiedlichen Geräten ist nicht ratsam und führt in der Regel zu Problemen.

X.509-Zertifikate auf Geräte hochladen und in VPN-Verbindungen verwenden

Die Verwendung von X.509-Zertifikaten auf mGuard-Geräten wird in Kapitel 1, „VPN-Kickstart – Zwei Netzwerke über IPsec-VPN miteinander verbinden“ beschrieben.

1.4 Registerkarte „Firewall“

VPN-spezifische Firewall-Regeln können bei der Konfiguration der VPN-Verbindung angegeben werden. Die VPN-Firewall erlaubt es, den Zugriff über den VPN-Tunnel einzuschränken. Sie kann bei Bedarf konfiguriert werden. In der werkseitigen Voreinstellung werden alle eingehenden und ausgehenden Verbindungen angenommen.

(Siehe auch mGuard-Firmwarehandbuch, Abschnitt „IPsec VPN >> Verbindungen >> Firewall“).

1.4.1 Beispiel

Zwischen **Firmennetzwerk 1** (192.168.1.0/24) und **Firmennetzwerk 2** (192.168.2.0/24) soll ein verschlüsselter IPsec-VPN-Tunnel aufgebaut werden.

Zwei Clients aus Firmennetzwerk 1 sollen auf zwei Steuerungen im Firmennetzwerk 2 zugreifen dürfen. Allen anderen Clients ist der Zugriff auf Firmennetzwerk 2 untersagt. Aus Firmennetzwerk 2 sind alle Verbindung zu Firmennetzwerk 1 untersagt.

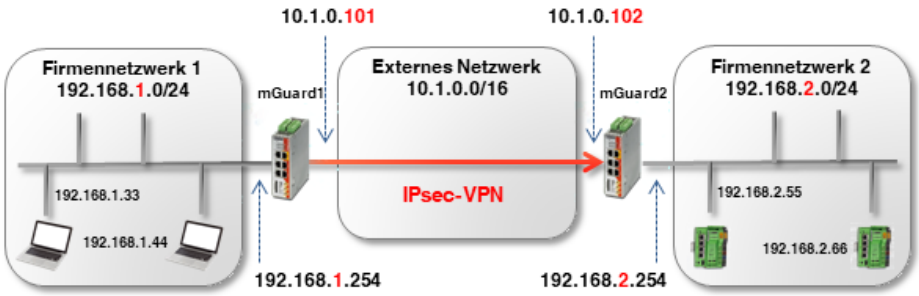

Bild 1-6 VPN-Verbindung zwischen zwei Netzwerken mit Firewall

Die Firewall-Einstellungen können prinzipiell auf *mGuard 1* oder *2* oder auf beiden Geräten konfiguriert werden. In diesem Beispiel wird die Firewall von *mGuard 1* konfiguriert. Die Verwendung von Firewall-Regelsätzen ist ebenfalls möglich (siehe auch Kapitel 1).

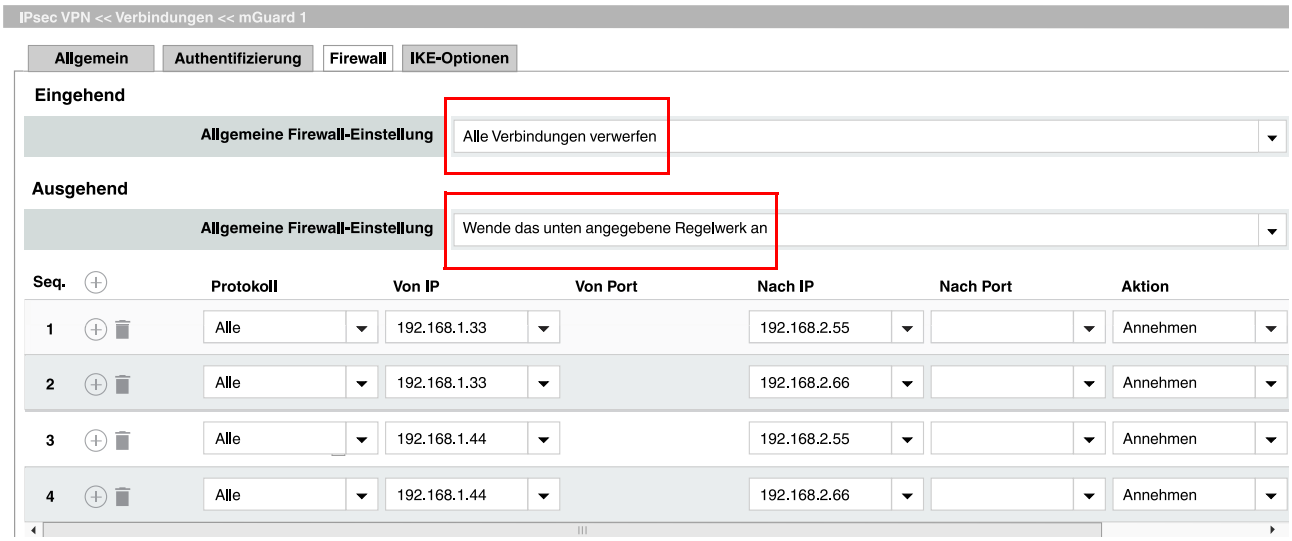

Bild 1-7 *mGuard 1*: IPsec VPN >> Verbindungen >> (Edit) >> Firewall

1.5 Registerkarte „IKE-Optionen“

Internet Key Exchange (IKE) bezeichnet ein Protokoll, das zur Verwaltung und zum Austausch der beteiligten Schlüssel innerhalb des IPsec-Protokols verwendet.

Die IKE-Optionen spezifizieren

– die Verschlüsselungs- und Hash-Algorithmen, die für die ISAKMP-SA und IPsec-SA verwendet werden sollen,
– die Lebensdauer der SAs und
– die Parameter für die Dead Peer Detection (DPD).

Es sollten falls möglich immer die stärksten bzw. sichersten Verschlüsselung und/oder Hash-Algorithmen verwendet werden. Ansonsten können die Standardeinstellungen grundsätzlich übernommen werden. (siehe auch mGuard-Firmwarehandbuch, Abschnitt „IPsec VPN >> Verbindungen >> IKE-Optionen“).

Für Hinweise zur sicheren Verschlüsselung, siehe mGuard-Firmwarehandbuch (Abschnitt „Sichere Verschlüsselung“).

1.6 mGuard hinter einem NAT-Router

Wenn die VPN-Verbindung über ein oder mehrere Gateways hergestellt wird, auf denen *Network Address Translation* (NAT) aktiviert ist,

1. müssen zur sicheren Authentifizierung X.509-Zertifikate verwendet werden. *Pre-Shared Keys* (PSK) können nur im unsicheren *Aggressive Mode* verwendet werden,
2. kann nur eins der mGuard-Geräte die VPN-Verbindung *initiieren*. Das andere Gerät muss auf die Verbindung *warten*,
3. muss auf dem antwortenden mGuard die *Adresse des VPN-Gateways der Gegenstelle* mit *%any* angegeben werden, auch wenn der NAT-Router der Gegenstelle eine statische öffentliche IP-Adresse besitzt,
4. muss beachtet werden, dass die VPN-Verbindung über die UDP-Ports 500 und 4500 aufgebaut wird.

Die in den folgenden Beispielen gezeigten Netzwerk- und NAT-Einstellungen sind zu beachten.

1.6.1 VPN-Initiator hinter NAT-Router

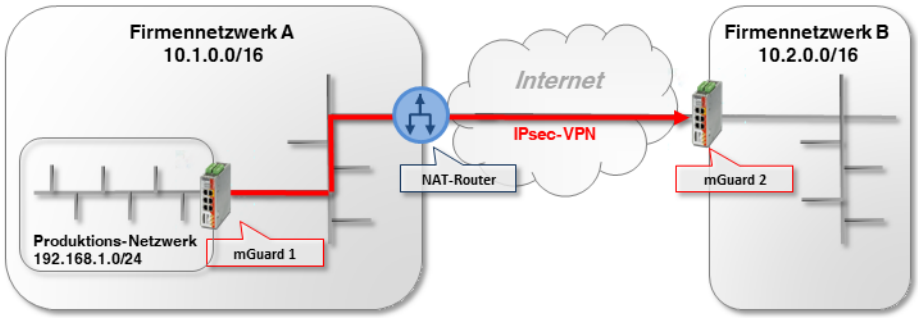

Bild 1-8 VPN-Initiator hinter NAT-Router

mGuard 1 (*Initiator*) initiiert die VPN-Verbindung zu *mGuard 2* (*Responder*).

Die Firewall des NAT-Routers muss ausgehende UDP-Pakete zu den Ports 500 und 4500 zulassen. Können dieses Ports aus bestimmten Gründen nicht geöffnet werden, können TCP-Kapselung (*TCP Encapsulation*) oder die Funktion *Path Finder* verwendet werden, um die VPN-Verbindung aufzubauen (siehe Kapitel 1.7).

1.6.2 VPN-Responder hinter NAT-Router

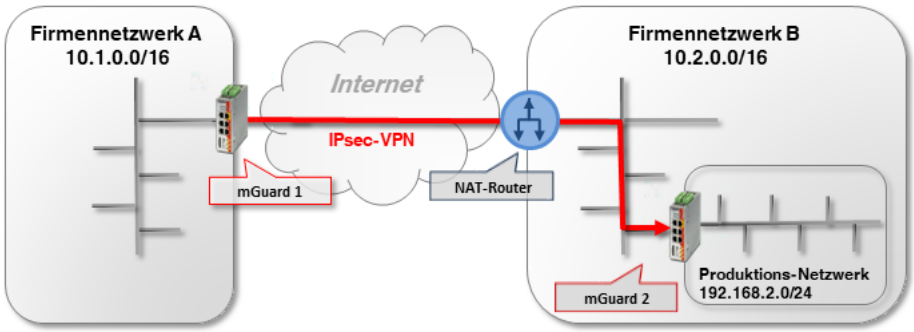

Bild 1-9 VPN-Responder hinter NAT-Router

mGuard 1 (*Initiator*) initiiert die VPN-Verbindung zu *mGuard 2* (*Responder*).

Auf dem NAT-Router muss die Port-Weiterleitung für die UDP-Ports 500 und 4500 zur externen IP-Adresse (WAN-Port) von *mGuard 2* konfiguriert werden. (Falls es sich um ein mGuard-Gerät handelt unter **Netzwerk >> NAT >> IP- und Port-Weiterleitung**.)

Aufgrund der erforderlichen Port-Weiterleitung auf dem NAT-Router für die UDP-Ports 500 und 4500 können keine weiteren VPN-Verbindungen zum NAT-Router selbst aufgebaut werden (terminieren). (Dies wäre möglich mittels TCP-Kapselung/Path-Finder-Funktion.) Auch VPN-Verbindungen zu weiteren mGuard-Geräten im Fimennetzwerk B können nicht aufgebaut werden.

Soll dies der Fall sein, müsste *mGuard 2* die VPN-Verbindung zu *mGuard 1* initiieren. Eine Port-Weiterleitung auf dem NAT-Router müsste dann nicht konfiguriert werden.

1.6.3 VPN-Initiator und -Responder hinter NAT-Router

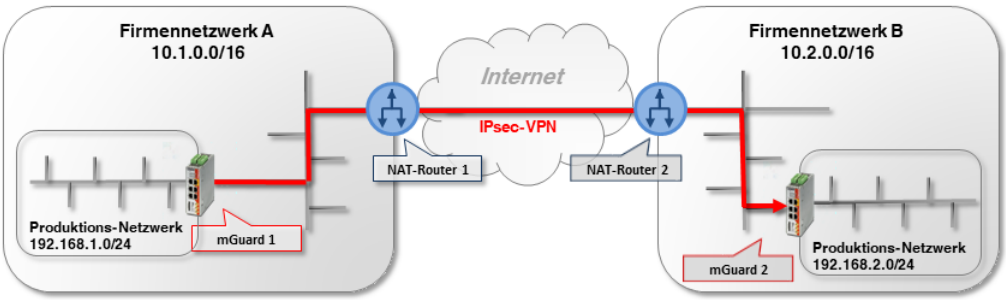

Bild 1-10 VPN-Initiator und VPN-Responder hinter NAT-Router

mGuard 1 (*Initiator*) initiiert die VPN-Verbindung zu *mGuard 2* (*Responder*).

Die Firewall des NAT-Routers 1 muss ausgehende UDP-Pakete zu den Ports 500 und 4500 zulassen.

Auf NAT-Router 2 muss die Port-Weiterleitung für die UDP-Ports 500 und 4500 zur externen IP-Adresse (WAN-Port) von *mGuard 2* konfiguriert werden.

1.7 TCP-Kapselung

Um eine IPsec-VPN-Verbindung aufzubauen, müssen die UDP-Ports 500 und 4500 in einer ausgehenden Firewall geöffnet sein. Sind diese Ports gesperrt, besteht die Möglichkeit, die VPN-Verbindung mittels TCP-Kapselung (*TCP Encapsulation*) oder der Funktion *Path Finder* über einen erlaubten TCP-Port aufzubauen.

Dazu werden die UDP-Pakete in TCP-Pakete verpackt (eingekapselt) und an einen TCP-Port gesendet, der in den Firewall-Einstellungen des NAT-Routers für ausgehende TCP-Pakete erlaubt ist (z. B. Port 80 oder 8080).

TCP-Kapselung kann auch zum Aufbau der VPN-Verbindung verwendet werden, wenn der Zugriff auf das Internet nur über einen Proxy-Server beim Kunden möglich ist. In diesem Fall müssen die Parameter für den Zugriff im Proxy-Server konfiguriert werden (Menü **Netzwerk >> Proxy-Einstellungen**).

1.7.1 Beispiel

Eine Kunde möchte über eine VPN-Verbindung auf einen Server der Herstellerfirma zugreifen. Die Kundenfirewall sperrt allerdings die UDP-Ports 500 und 4500 für ausgehende Verbindungen.

TCP-Verbindungen über den TCP-Port 80 sind dagegen erlaubt. Die VPN-Verbindung soll daher mittels TCP-Kapselung über den TCP-Port 80 aufgebaut werden. (Die Konfiguration von VPN-Verbindungen wird in Kapitel 1 und 1 ausführlich beschrieben.)

Für die sichere Authentifizierung müssen Zertifikate verwendet werden, da die VPN-Verbindung über einen NAT-Router aufgebaut wird. Soll eine Authentifizierung mittels *Pre-Shared Key* erfolgen, muss der unsichere *Aggressive Mode* verwendet werden (siehe Kapitel 1.3).

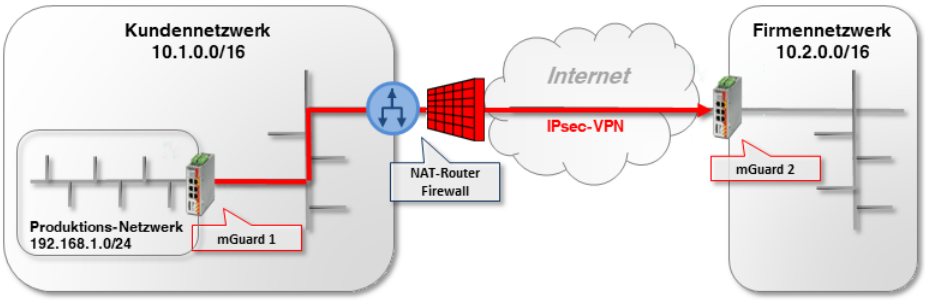

Bild 1-11 VPN-Initiator hinter NAT-Router und Firewall

mGuard 1 (*Initiator*) initiiert die VPN-Verbindung zu *mGuard 2* (*Responder*). Normalerweise würde eine VPN-Verbindung mittels NAT über die UDP-Ports 500 und 4500 aufgebaut. Diese sind jedoch durch die Kunden-Firewall des NAT-Routers gesperrt.

Auch die verschlüsselten ESP-Pakete werden durch NAT-T in UDP-Pakete eingehüllt. Sie wären ebenfalls von einer Sperrung der UDP-Ports 500 und 4500 betroffen.

1.7.2 Einstellungen mGuard 2 (Responder)

Um dem *VPN-Responder* mitzuteilen, auf welchem Port das Gerät auf gekapselte VPN-Verbindungen horchen soll, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 2* an.
2. Gehen Sie zu **IPsec VPN >> Global** (Registerkarte *Optionen*).
3. In Sektion **TCP-Kapselung**: Aktivieren Sie die Option **Horche auf eingehende VPN-Verbindungen, die eingekapselt sind**. Dadurch wird der IPsec-TCP-Server auf dem Gerät gestartet.
4. Tragen Sie in diesem Beispiel bei **TCP-Port, auf dem zu horchen ist** den Port *80* ein. Dieser Port muss beim *VPN-Initiator* (*mGuard 1*) ebenfalls für die TCP-Kapselung eingetragen sein (siehe Kapitel 1.7.3).

Wählen Sie nicht den TCP-Port 443, da über diesen bereits standardmäßig via HTTPS-Fernzugriff auf das *Web-based Management* des Geräts zugegriffen wird.

Wenn die TCP-Kapselung ebenfalls Port 443 verwendet, ist der HTTPS-Fernzugriff auf die Weboberfläche nicht mehr möglich.

Geben Sie entweder einen anderen TCP-Port für den Fernzugriff an (Menü **Verwaltung >> Web-Einstellungen**, Registerkarte *Zugriff*), z. B. Port 4443 oder wählen Sie einen anderen TCP-Port für die TCP-Kapselung.

1.7.3 Einstellungen mGuard 1 (Initiator)

Um dem *VPN-Initiator* mitzuteilen, auf welchem Port das Gerät der Gegenstelle (*VPN-Responder*) auf gekapselte VPN-Verbindungen horcht, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an.
2. Gehen Sie zu **IPsec VPN >> Verbindungen**.
3. Klicken Sie auf das Icon ⊕, um eine neue VPN-Verbindung hinzuzufügen.
4. Geben Sie der Verbindung einen eindeutigen Namen und klicken Sie auf das Icon ✎, um die Verbindung zu bearbeiten.
5. Tragen Sie als **Adresse des VPN-Gateways der Gegenstelle** entweder den DynDNS-Namen oder die öffentliche IP-Adresse der Gegenstelle (*mguard 2*) ein (z. B. *mGuard2.dyndns.org* oder 77.245.32.78).
6. Wählen Sie bei **Verbindungsinitiierung** *Initiate* aus.
7. Wählen Sie bei **Kapsele den VPN-Datenverkehr in TCP ein** TCP-Kapselung.
8. Tragen Sie in diesem Beispiel bei **TCP-Port des Servers, welcher die gekapselte Verbindung annimmt** den Port *80* ein. Dieser Port muss beim *VPN-Responder* (*mGuard 2*) ebenfalls für die TCP-Kapselung eingetragen (siehe Kapitel 1.7.2).

1.8 VPN-Verbindungen mittels URL starten/stoppen oder analysieren

Es ist möglich, eine auf dem mGuard-Gerät konfigurierte VPN-Verbindung mithilfe des Kommandozeilenbefehls *curl* zu starten oder zu stoppen bzw. deren Verbindungsstatus abzufragen:

https://<user>:<password>@<mGuard IP>/nph-vpn.cgi?name=<name>&cmd=[up|down|status]

<user>: Folgende Benutzer können verwendet werden: *admin*, *root* und *user*.

<name>: Name der VPN-Verbindung, wie sie im Menü **IPsec VPN >> Verbindungen** angezeigt wird.

Die Verwendung des Kommandozeilen-Tools **wget** funktioniert nur im Zusammenspiel mit **mGuard-Firmwareversionen < 8.4.0**. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden.

Das Benutzer-Passwort und der Name, auf den sich eine Aktion bezieht, dürfen ausschließlich folgende Zeichen enthalten:

- Buchstaben: A – Z, a – z
- Ziffern: 0 – 9
- Zeichen: - . _ ~

Andere Sonderzeichen, z. B. das Leerzeichen oder das Fragezeichen, müssen entsprechend codiert werden (siehe auch mGuard-Firmwarehandbuch).

1.8.1 Beispiele

Das mGuard-Gerät, auf dem z. B. die VPN-Verbindung „*Athen*“ konfiguriert ist, ist unter der IP-Adresse 192.168.1.1 erreichbar.

1. VPN-Verbindung „*Athen*“ starten:

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up“

2. VPN-Verbindung „*Athen*“ stoppen:

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=down"

curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=down“

3. Status der VPN-Verbindung „*Athen*“ abfragen:

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=status"

curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=status“

Die Option ***--no-check-certificate*** (*wget*) bzw. **--insecure** (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuard-Geräts nicht weiter geprüft wird.

1.9 VPN-Verbindung mittels Taster oder Schalter starten oder stoppen

An manche mGuard-Geräte können Servicekontakte (I/Os) angeschlossen werden:

TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G,
FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD RS,
FL MGUARD GT/GT

Der Anschluss der Servicekontakte wird im Anwenderhandbuch zu den Geräten beschrieben (siehe Guard-Hardwarehandbuch – UM DE MGUARD DEVICES).

Eingang (CMD I1, I2 und I3)

An die Eingänge können Taster oder Ein-/Aus-Schalter (z. B. ein Schlüsselschalter) angeschlossen werden. Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich.

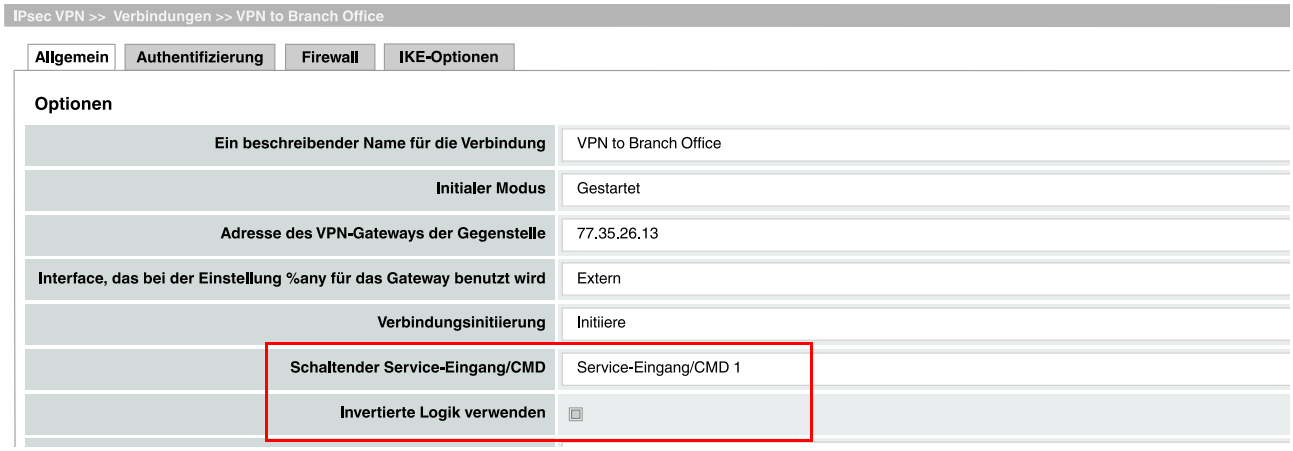

Bild 1-12 IPsec VPN >> Verbindungen: Der VPN-Verbindung wird ein Service-Eingang zugeordnet, über den sie per Taster oder Ein-/Aus-Schalter gestartet oder gestoppt werden kann.

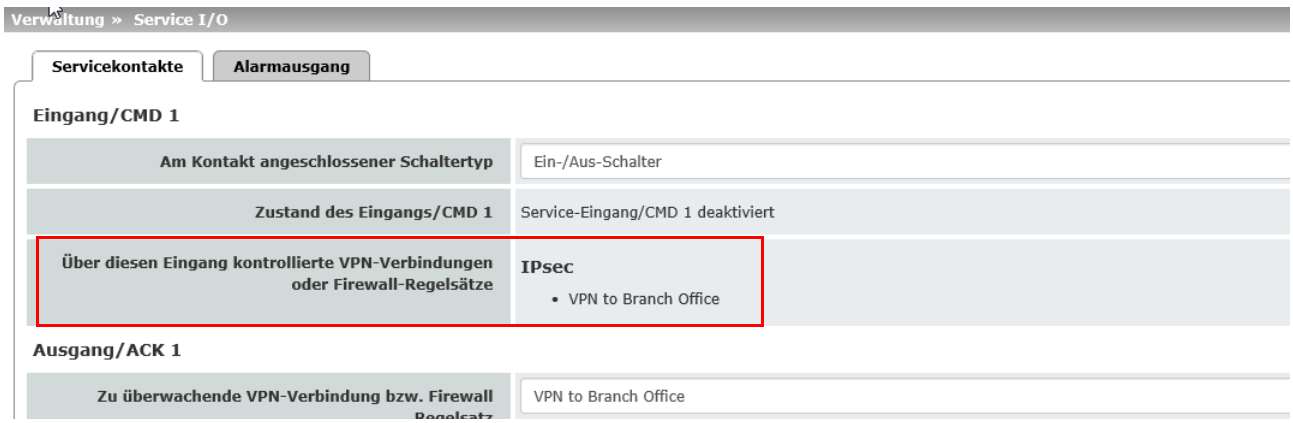

Bild 1-13 Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen oder Firewall-Regelsätze über einen Service-Eingang geschaltet werden.

Meldekontakt (Meldeausgang) ACK 1/2 (O1, O2)

Sie können einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über den Meldeausgang ACK 1 oder 2 bzw. LEDs angezeigt werden.