mGuard-Konfigurationsbeispiele

Konfigurationsbeispiele

AH DE MGUARD CONFIG

PHOENIX CONTACT
INSPIRING INNOVATIONS

Konfigurationsbeispiele

mGuard-Konfigurationsbeispiele

AH DE MGUARD CONFIG, Revision 01 2019-03-01

Dieses Handbuch ist gültig für mGuard-Security-Appliances.

108392_de_01

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Inhaltsverzeichnis

1 Sicherheitshinweise

Lesen Sie dieses Handbuch sorgfältig und bewahren Sie es für späteres Nachschlagen auf.

1.1 Kennzeichnung der Warnhinweise

Dieses Symbol mit dem Signalwort **ACHTUNG** warnt vor Handlungen, die zu einem Sachschaden oder einer Fehlfunktion führen können.

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

- Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.
- Qualifizierte Anwendungsprogrammierer und Software-Ingenieure. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.

1.3 Hinweis zur Verwendung von Anwenderhinweisen

Die zur Verfügung gestellten Anwenderhinweise sind ein kostenloser Service von Phoenix Contact. Bei den dargestellten Beispielen und Lösungswegen handelt es sich nicht um kundenspezifische Lösungen, sondern um allgemeine Hilfestellungen bei typischen Anwendungsszenarien. Die Anwenderhinweise sind grundsätzlich unverbindlich und erheben keinen Anspruch auf Vollständigkeit.

Eine Qualitätsprüfung der Anwenderhinweise findet statt, ist jedoch nicht mit der Qualitätskontrolle kostenpflichtiger Produkte vergleichbar. Fehler, Funktions- und Leistungsmängel können nicht ausgeschlossen werden.

Zur Vermeidung von Fehlfunktionen/Fehlkonfigurationen und damit einhergehenden Schäden liegt die sachgemäße und sichere Verwendung des Produkts/der Software allein in der Verantwortung des Kunden und muss innerhalb der geltenden Vorschriften erfolgen.

Die beschriebenen Beispiele müssen vom Kunden auf ihre Funktion überprüft und an die individuellen, kundenspezifischen Anforderungen der Anlage bzw. des Einsatzszenarios angepasst werden.

Die IP-Einstellungen in den Anwenderhinweisen wurden beispielhaft gewählt. In einer echten Netzwerkumgebung müssen diese IP-Einstellungen grundsätzlich angepasst werden, um möglich Adresskonflikte zu vermeiden.

Die Angaben in den Anwenderhinweisen werden regelmäßig überprüft. Sollten Korrekturen notwendig sein, werden diese in der jeweils nachfolgenden Revision enthalten sein. Eine Benachrichtigung von Nutzern findet nicht statt.

2 Zusätzliche interne/externe Routen anlegen

Dokument-ID: 108409_de_00
Dokument-Bezeichnung: AH DE MGUARD ADDITIONAL INT ROUTES

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 Verwendung von zusätzlichen internen Routen beschrieben, um den Zugriff von einem Netzwerk auf ein anderes zu ermöglichen.

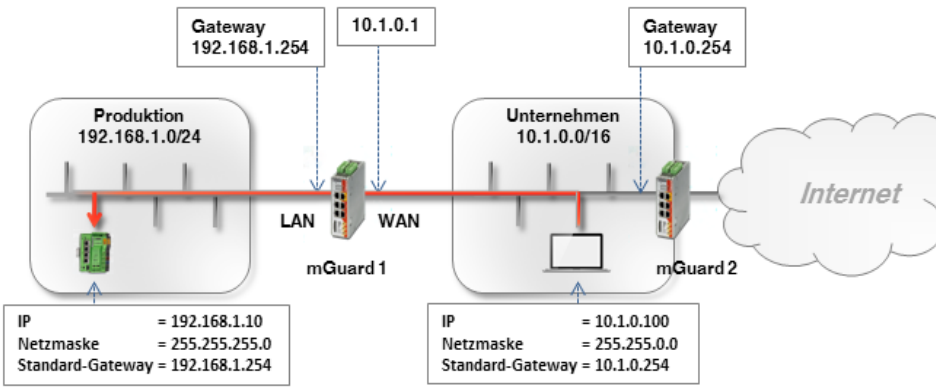
Die Verwendung von zusätzlichen externen Routen erfolgt analog und wird nicht eigens beschrieben.

2.1 Einleitung

Wenn Pakete im internen Netzwerk des Gateways (*mGuard 2*) an eine IP-Adresse in einem anderen Netzwerk (Extern oder DMZ) verschickt werden sollen, muss das Gateway wissen, über welchen Router bzw. über welches Gateway es diese Pakete weiterleiten muss. Dazu können im Gateway (*mGuard 2*) *Zusätzliche interne Routen* eingetragen werden. (Weitere Optionen werden in den Kapiteln 4 und 5 beschrieben.)

2.2 Beispiel

Aus dem Unternehmensnetzwerk soll auf das Webinterface einer Maschinensteuerung (SPS) im Produktionsnetzwerk zugegriffen werden.



Der Büro-Computer (10.1.0.100) und die SPS (192.168.1.10) befinden sich nicht im gleichen Netzwerk. Der Büro-Computer sendet Pakete, die an die SPS gerichtet sind, grundsätzlich an sein Standard-Gateway (*mGuard 2*: 10.1.0.254).

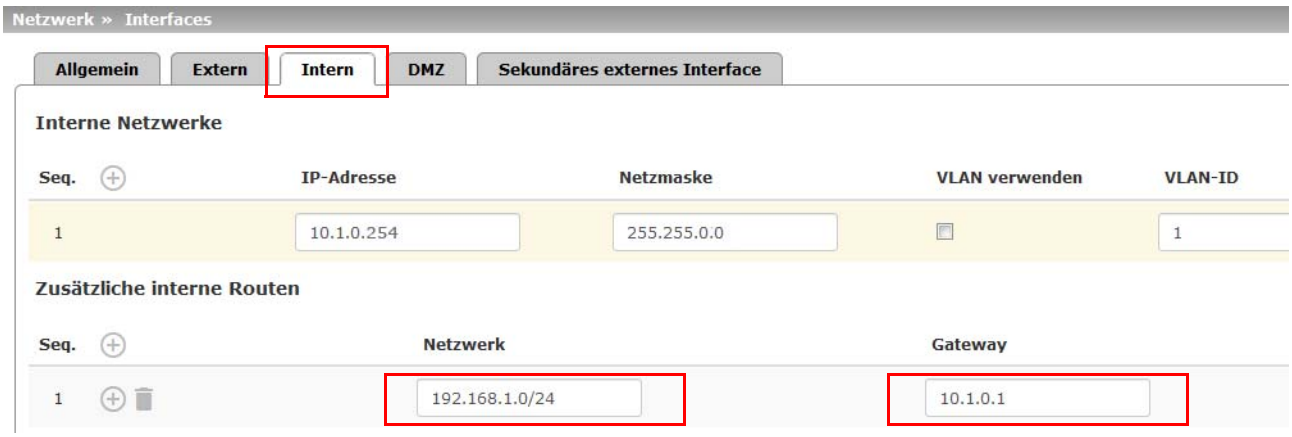
Dieses Gateway muss nun wissen, wohin es die Pakete weiterleiten soll. Das erfolgt über das Hinzufügen von zusätzlichen internen Routen.

Auf dem Standard-Gateway (*mGuard 2*: 10.1.0.254) des Büro-Computers muss eine zusätzliche Route konfiguriert werden, die *mGuard 1* (10.1.0.1) als Gateway und das Produktionsnetzwerk (192.168.1.0/24) als Zielnetzwerk angibt. *mGuard 1* fungiert als Router, der die beiden Netzwerke miteinander verbindet.

2.3 Vorgehen

Wenn das Standard-Gateway im Unternehmensnetzwerk ein mGuard-Gerät (*mGuard 2* im Netzwerkmodus *Router*) ist, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des Standard-Gateways (*mGuard 2*) im Unternehmensnetzwerk an (LAN-Interface unter 10.1.0.254).
2. Gehen Sie zu **Netzwerk >> Interfaces >> Intern**.
3. Legen Sie eine **Zusätzliche Interne Route** zum Produktionsnetzwerk an (Netzwerk: 192.168.1.0/24 über Gateway 10.1.0.1):



4. Clients im Unternehmensnetzwerk senden Pakete, die an das Netzwerk 192.168.1.0/24 gerichtet sind, über ihr Standard-Gateway (*mGuard 2*) an *mGuard 1*.

Ergebnis

Clients aus dem Unternehmensnetzwerk können die SPS im Produktionsnetzwerk über ihre reale IP-Adresse erreichen:

- Webbrowser: http://192.168.1.10
- Ping: 192.168.1.10

Die Eingangsregeln der Firewall von *mGuard 1* müssen entsprechende Anfragen erlauben.

Vorteile

- Die SPS kann direkt über ihre reale IP-Adresse erreicht werden.
- Die Netzwerkkonfiguration des Büro-Computers und anderer Clients im Unternehmensnetzwerk muss nicht geändert werden.

Nachteile

- Auf dem Gateway müssen zusätzliche Routen konfiguriert werden.

3 Network Address Translation (1:1-NAT) verwenden

Dokument-ID: 108407_de_00
Dokument-Bezeichnung: AH DE MGUARD NAT

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 grundsätzliche Verwendung von 1:1-NAT beschrieben. Der Zugriff aus einem externen Netzwerk auf zwei interne Netzwerke sowie der Zugriff aus einem internen auf ein externes Netzwerk werden beschrieben.

3.1 Einleitung

Mithilfe von NAT (*Network Address Translation*) werden die Adressinformationen in Datenpaketen durch andere ersetzt bzw. umgeschrieben, um verschiedene Netze miteinander zu verbinden.

mGuard-Geräte unterstützen die NAT-Verfahren *IP-Maskierung* und *1:1-NAT*. Die Verwendung von NAT in VPN-Verbindungen ist ebenfalls möglich (siehe Kapitel 13).

IP-Maskierung

Beim Aktivieren von IP-Maskierung (*IP-Masquerading*) maskiert das mGuard-Gerät die IP-Adressen von Absendern, z. B. aus dem Produktionsnetzwerk (= *Internes Netzwerk*), mit seiner eigenen externen IP-Adresse.

1:1-NAT

1:1-NAT bildet IP-Adressen eines *Realen Netzwerks* auf IP-Adressen eines *Virtuellen Netzwerks* ab. Geräte im *Realen Netzwerk* können somit direkt über die ihnen zugeordneten (*mapped*) IP-Adressen aus dem *Virtuellen Netzwerk* erreicht werden.

Abhängig von der angegebenen Netzmaske in der 1:1-NAT-Konfiguration können das gesamte *Reale Netzwerk* oder Subnetze davon auf das *Virtuelle Netzwerk* abgebildet werden.

3.2 Wichtige Hinweise zur Verwendung von NAT

1:1-NAT wird im Netzwerkmodus *Stealth* nicht unterstützt.

Die unter *„Virtuelles Netzwerk“* angegebenen IP-Adressen müssen frei sein. Sie dürfen nicht für andere Geräte vergeben sein, weil sonst im „*Virtuellen Netzwerk*“ ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer IP-Adresse aus dem angegebenen „*Virtuellen Netzwerk*“ gar kein Gerät im „*Realen Netzwerk*" existiert.

Beim 1:1-NAT wird der *Netzwerk-Teil* einer IP-Adresse umgeschrieben (*mapped*) und der *Host-Teil* in der Regel unverändert beibehalten. Der Netzwerkteil der IP-Adresse wird durch die angegebene Netzmaske vorgegeben.

Die gleiche Netzmaske, die vom *Virtuellen Netzwerk* verwendet wird, darf nicht gleichzeitig zur Abbildung des *Realen Netzwerks* auf den virtuellen Standort verwendet werden. In diesem Fall würde der mGuard auf alle ARP-Anfragen des *Virtuellen Netzwerks* antworten und es damit unbenutzbar machen.

Die angegebene Netzmaske muss kleiner sein als diejenige, die vom *Virtuellen Netzwerk* verwendet wird.

Soll der Zugriff beschränkt werden, müssen entsprechende Firewall-Regeln erstellt werden.

3.3 Beispiel 1: Mapping von IP-Adressen (1:1-NAT)

3.3.1 Aus dem Unternehmensnetzwerk soll auf einzelne Geräte im Produktionsnetzwerk zugegriffen werden

Einzelne Geräte in zwei Produktionsnetzwerken (mit der gleichen Netzwerkeinstellung) sollen aus dem Unternehmensnetzwerk über 1:1-NAT erreichbar sein.

Die *reale* IP-Adresse eines Clients im Produktionsnetzwerk wird dazu auf eine *virtuelle* IP-Adresse im Unternehmensnetzwerk umgeschrieben (*gemappt*). Über diese *virtuelle* IP-Adresse kann direkt auf den zugeordneten Client im Produktionsnetzwerk zugegriffen werden.

(Soll der Zugriff beschränkt werden, müssen entsprechende Firewall-Regeln erstellt werden.)

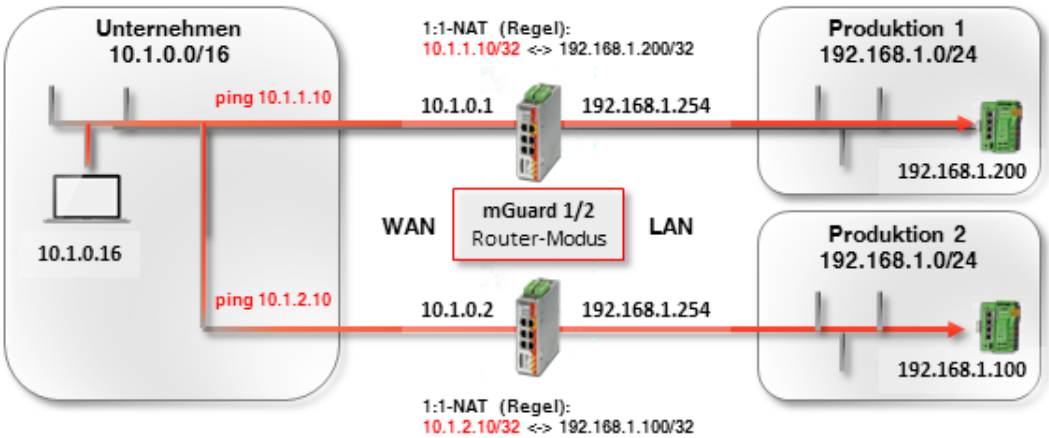


Bild 3-1 1:1-NAT-Regel: Aus dem Unternehmensnetzwerk auf einzelne IP-Adressen im Produktionsnetzwerk zugreifen

Der ARP-*Daemon* auf dem mGuard-Gerät wird auf ARP-Anfragen, die an die zugeordneten IP-Adressen des *Virtuellen Netzwerks* gerichtet sind, antworten. Daher müssen keine IP-Änderungen im *Virtuellen Netzwerk* vorgenommen werden.

Tabelle 3-1 Beispiel-Regeln für 1:1-NAT mit der Netzmasken 32 (Mapping von IP-Adressen)

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
192.168.1.200	10.1.1.10	**32**	192.168.1.200 <-> 10.1.1.10

3.3.2 Einstellung auf dem mGuard-Gerät

Um Geräte in Produktionsnetzwerken aus dem Unternehmensnetzwerk mithilfe von 1:1-NAT erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 3-2.

Bild 3-2 *mGuard 1*: Produktion 1 erreichen (IP-Adressen)

1. Melden Sie sich auf der Weboberfläche von *mGuard 2* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 3-4.

Bild 3-3 *mGuard 2*: Produktion 2 erreichen (IP-Adressen)

Ergebnis

Netzwerkpakte aus dem Unternehmensnetzwerk an die *virtuelle* IP-Adresse 10.1.1.10 werden über *mGuard 1* an die *reale* IP-Adresse 192.168.1.200 im Produktionsnetzwerk 1 geleitet.

Netzwerkpakte aus dem Unternehmensnetzwerk an die *virtuelle* IP-Adresse 10.1.2.10 werden über *mGuard 2* an die *reale* IP-Adresse 192.168.1.100 im Produktionsnetzwerk 2 geleitet.

3.4 Beispiel 2: Mapping von Netzwerken (1:1-NAT)

3.4.1 Aus dem Unternehmensnetzwerk soll auf das gesamte Produktionsnetzwerk zugegriffen werden

Zwei Produktionsnetzwerke mit der gleichen Netzwerkeinstellung sollen aus dem Unternehmensnetzwerk über 1:1-NAT erreicht werden.

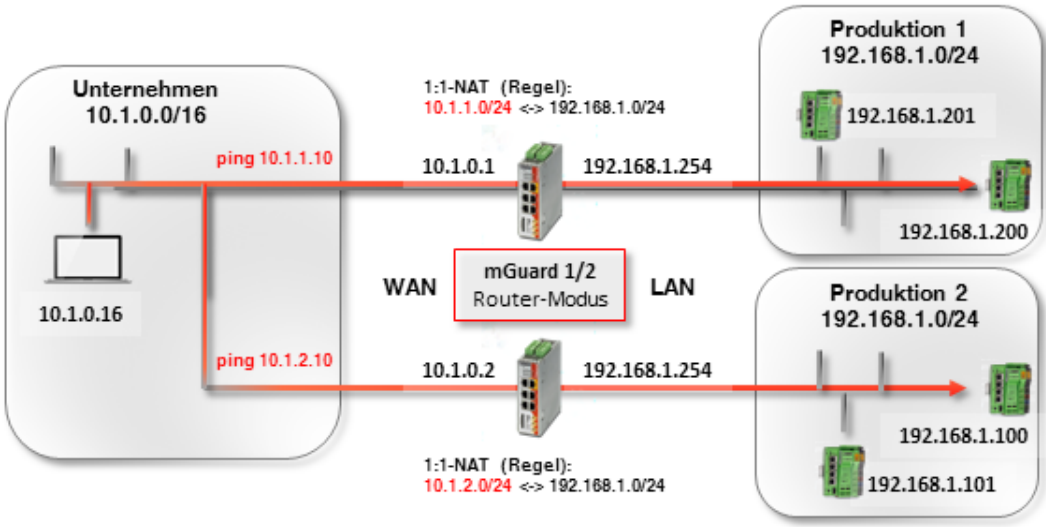


Bild 3-4 1:1-NAT-Regel: Aus dem Unternehmensnetzwerk auf das gesamte Produktionsnetzwerk zugreifen

Die beiden mGuard-Geräte verfügen über externe IP-Adressen, die zum externen Unternehmensnetzwerk gehören (10.1.0.1 und 10.1.0.2).

Aus dem Unternehmensnetzwerk soll mittels 1:1-NAT über das *virtuelle* Netzwerk **10.1.1.0/24** auf die Systeme des **Produktionsstandortes 1** und über das *virtuelle* Netzwerk **10.1.2.0/24** auf die Systeme des **Produktionsstandortes 2** zugegriffen werden.

Kein *realer* Client im Unternehmensnetzwerk darf eine IP-Adresse aus den *virtuellen* Netzwerken verwendet.

Tabelle 3-2 Beispiel-Regeln für 1:1-NAT mit unterschiedlichen Netzmasken und resultierende Zuordnungen

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
192.168.1.0	10.1.0.0	**24**	192.168.1.0 <-> 10.1.0.0 192.168.1.1 <-> 10.1.0.1 … 192.168.1.254 <-> 10.1.0.254 192.168.1.255 <-> 10.1.0.255

Der jeweilige ARP-Daemon auf den beiden mGuard-Routern stellt sicher, dass Clients im externen Netzwerk wissen, wohin sie Pakete senden sollen, die an die Netzwerke 10.1.1.0/24 und 10.1.2.0/24 adressiert sind.

3.4.2 Einstellung auf dem mGuard-Gerät

Um die Produktionsnetzwerke aus dem Unternehmensnetzwerk mithilfe von 1:1-NAT erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 3-5.

Bild 3-5 *mGuard 1*: Produktion 1 erreichen (Netzwerke)

1. Melden Sie sich auf der Weboberfläche von *mGuard 2* an.
2. Gehen Sie zu **Netzwerk >> NAT**.
3. Konfigurieren Sie die 1:1-NAT-Regeln gemäß Bild 3-6.

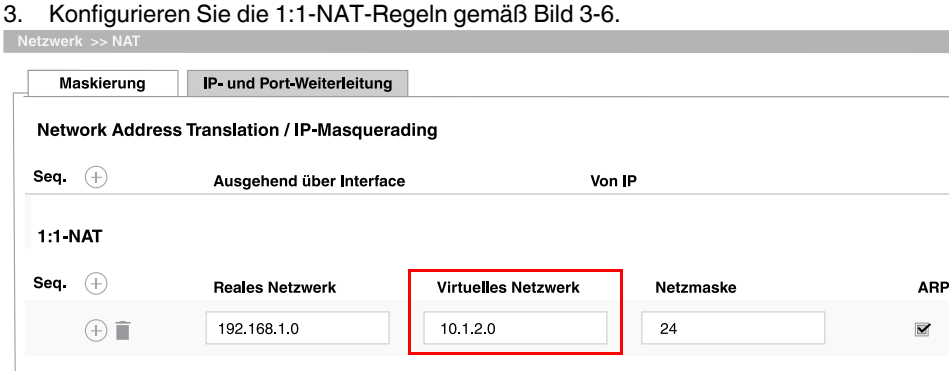


Bild 3-6 *mGuard 2*: Produktion 2 erreichen (Netzwerke)

Ergebnis

Auf den Client 192.168.1.200 der Produktionsstandortes 1 kann aus dem externen Netzwerk über die IP-Adresse 10.1.1.200 zugegriffen werden. Der Client 192.168.1.201 ist über die IP-Adresse 10.1.1.201 erreichbar.

Auf den Client 192.168.1.10 der Produktionsstandortes 2 kann aus dem externen Netzwerk über die IP-Adresse 10.1.2.10 auf den Client 192.168.1.11 mit der IP-Adresse 10.1.2.11 usw. zugegriffen werden.

Clients des Produktionsstandorts 2 können prinzipiell auch von Produktionsstandort 1 aus über ihre *virtuellen* IP-Adressen (10.1.2.0/24) erreicht werden und umgekehrt.

4 Interne Netzwerke erreichen (Zusätzliche Routen | IP-/Port-Weiterleitung | 1:1-NAT)

Dokument-ID: 108406_de_00

Dokument-Bezeichnung: AH DE MGUARD NETWORK SEGMENT 1

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 Verwendung des mGuard-Geräts als Router beschrieben, der zwei Netzwerke (internes und externes Netzwerk) miteinander verbindet. Das interne Netzwerk soll aus dem externen erreicht werden.

Beschrieben werden die folgenden Verfahren:

– Option 1: Zusätzliche interne Routen
– Option 2: IP- und Port-Weiterleitung
– Option 3: Network Address Translation (1:1-NAT)

4.1 Einleitung

Im Netzwerkmodus „Router“ (*Router-Modus*) kann ein mGuard-Gerät dazu eingesetzt werden, zwei Netzwerke miteinander zu verbinden. Die Sicherheitsfunktionen Firewall und VPN (lizenzabhängig) stehen dabei ebenfalls zur Verfügung.

Bei einigen Modellen kann optional eine Demilitarisierte Zone (DMZ) über das zusätzliche DMZ-Interface angebunden werden.

4.1.1 Beispiel

Das Produktionsnetzwerk (= *Internes Netzwerk*) und das Unternehmensnetzwerk (= *Externes Netzwerk*) sind über einen mGuard-Router miteinander verbunden.

Aus dem Unternehmensnetzwerk soll auf das Web-Interface einer Maschinensteuerung (SPS) im Produktionsnetzwerk zugegriffen werden. Eine Ping-Anfrage an die Steuerung soll ebenfalls von dieser beantwortet werden.

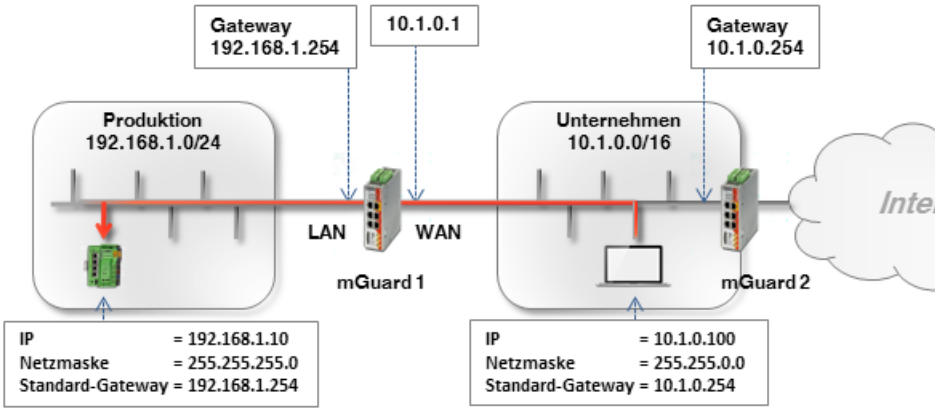


Bild 4-1 Netzwerkeinstellungen der Clients und mGuard-Router

Das Ziel, die beiden Netzwerke miteinander zu verbinden, kann auf unterschiedlichen Wegen erreicht werden:

– Option 1: Zusätzliche interne Routen
– Option 2: IP- und Port-Weiterleitung
– Option 3: Network Address Translation (1:1-NAT)

4.1.2 Vorgehen

1. WAN- und LAN-Interface des Routers (*mGuard 1*) konfigurieren
2. Firewall-Regeln konfigurieren
3. Netzwerkeinstellungen gemäß Option 1, 2 oder 3 konfigurieren

4.2 Netzwerkeinstellungen des mGuard-Routers

Um den Netzwerkverkehr zwischen den beiden Netzwerken zu ermöglichen, müssen in allen Optionen das externe (= WAN-Port) und das internes Interface (= LAN-Port) des Routers *mGuard 1* konfiguriert und mit mindestens einer IP-Adresse versehen werden.

Stellen Sie sicher, dass die Clients im Produktions- und Unternehmensnetzwerk ihrem Netzwerk entsprechend konfiguriert sind.

Die Clients im Produktionsnetzwerk (SPS) müssen als Standard-Gateway die interne IP-Adresse des *mGuard 1* konfiguriert haben (192.168.1.254).

Die Clients im Unternehmensnetzwerk müssen als Standard-Gateway die interne IP-Adresse des *mGuard 2* konfiguriert haben (10.1.0.254).

Um *mGuard 1* als Router zwischen dem Unternehmensnetzwerk (WAN)10.1.0.0/16 und dem Produktionsnetzwerk (LAN) 192.168.1.0.0/24 einzusetzen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (192.168.1.254).
2. Gehen Sie zu **Netzwerk >> Interfaces**.
3. Registerkarte *Allgemein*: Wählen Sie den **Netzwerk-Modus** *Router* und den **Router-Modus** *Statisch*.
4. Registerkarte *Intern*: Wählen Sie als Interne IP-Adresse 192.168.1.254 (Netzmaske 255.255.255.0).
5. Registerkarte *Extern*: Wählen Sie als Externe IP-Adresse 10.1.0.1 (Netzmaske 255.255.0.0).

Bild 4-2 Internes Interface

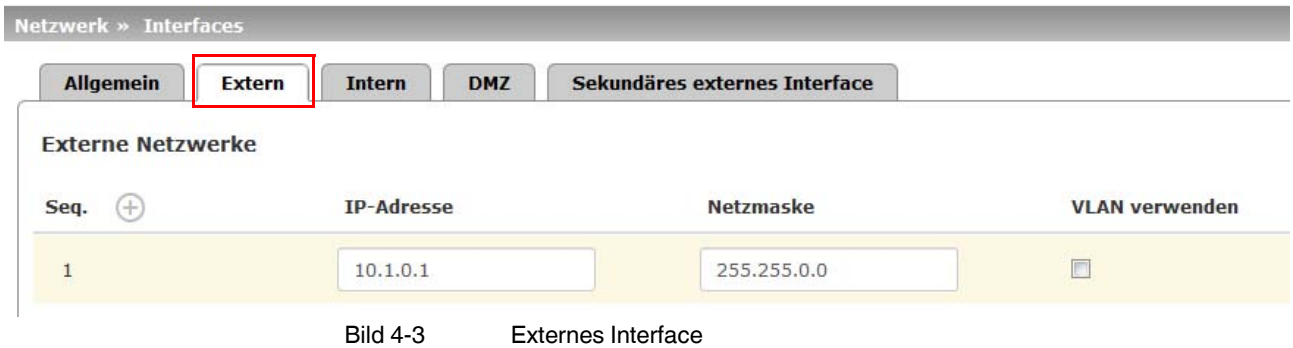


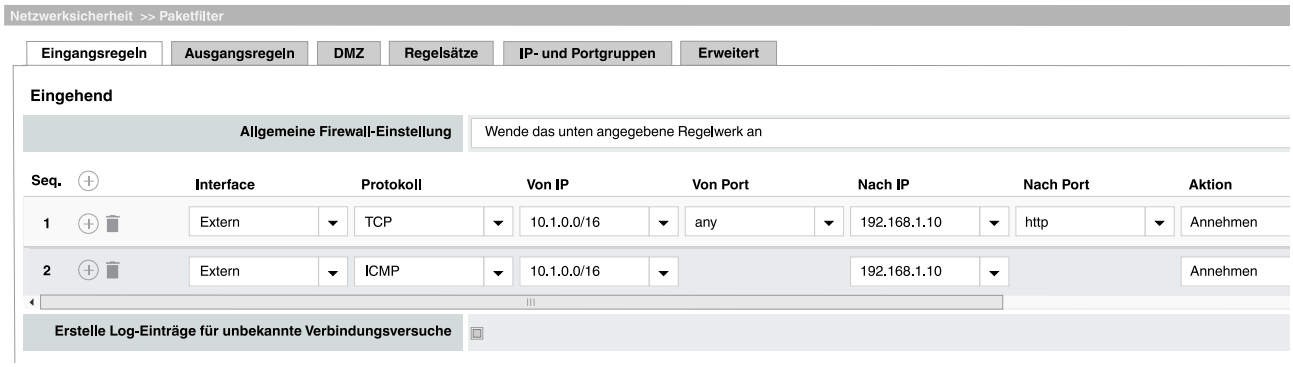
Bild 4-3 Externes Interface

4.3 Firewall-Regeln konfigurieren

mGuard 1 soll so konfiguriert werden, dass er den HTTP-Zugriff auf das Webinterface der SPS (192.168.1.10) aus dem Unternehmensnetzwerk (= Externes Netzwerk: 10.1.0.0/16) ermöglicht. Abgesehen davon soll es auch möglich sein, die Steuerung zu "*pingen*" (ICMP-Anfrage).

Gehen Sie wie folgt vor:

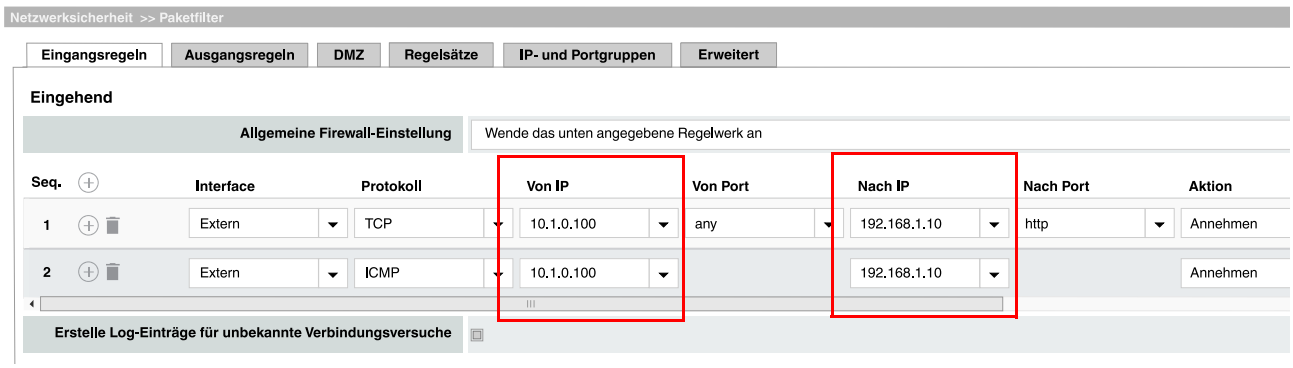
1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (192.168.1.254).
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Eingangsregeln**.
3. Wählen Sie bei **Allgemeine Firewall-Einstellung** „*Wende das unten angegebene Regelwerk an*“.
4. Legen Sie zwei Firewall-Regeln wie folgt an:



Ergebnis

Die Firewall-Regeln erlauben eingehende TCP-Pakete an den HTTP-Port sowie eingehende ICMP-Pakete aus dem Unternehmensnetzwerk an die IP-Adresse der SPS. Alle anderen Pakete werden von der Firewall verworfen.

Die Felder **Von IP** und **Nach IP** können auch dazu verwendet werden, die Erlaubnis auf einzelne Clients zu beschränken (z. B. von **10.1.0.100** auf **192.168.1.10**).



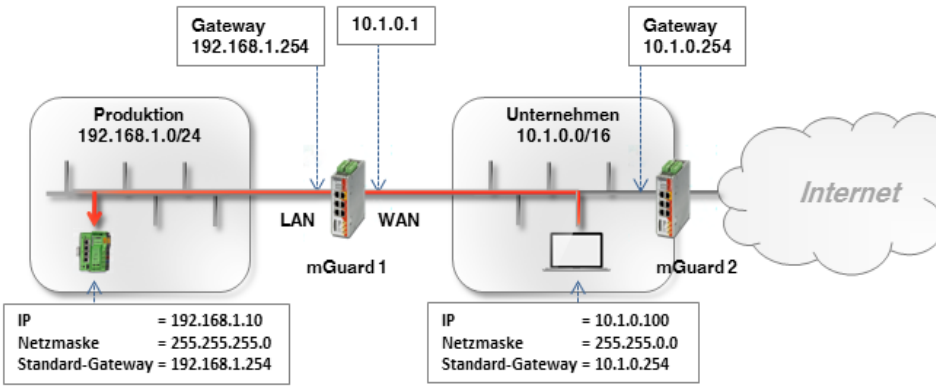
4.4 Netzwerkeinstellungen gemäß Option 1, 2 und 3

4.4.1 Option 1: Zusätzliche interne Routen auf dem Gateway

Der Büro-Computer (10.1.0.100) und die SPS (192.168.1.10) befinden sich nicht im gleichen Netzwerk. Der Büro-Computer sendet Pakete, die an die SPS gerichtet sind, grundsätzlich an sein Standard-Gateway (*mGuard 2*: 10.1.0.254).

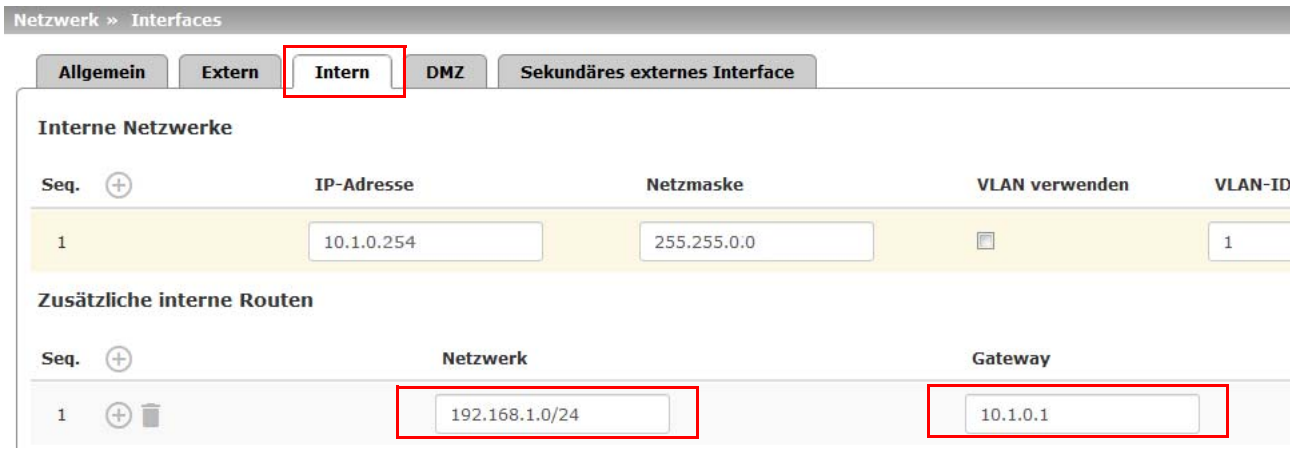
Dieses Gateway muss nun wissen, wohin es die Pakete weiterleiten soll. Das erfolgt über das Hinzufügen von zusätzlichen internen Routen:

Auf dem Standard-Gateway (10.1.0.254) des Büro-Computers muss eine zusätzliche Route konfiguriert werden, die *mGuard 1* (10.1.0.1) als Gateway und das Produktionsnetzwerk (192.168.1.0/24) als Zielnetzwerk angibt. *mGuard 1* fungiert als Router, der die beiden Netzwerke miteinander verbindet.



Wenn das Standard-Gateway im Unternehmensnetzwerk ein mGuard-Gerät (hier *mGuard 2*) ist, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des Standard-Gateways (*mGuard 2*) im Unternehmensnetzwerk an (LAN-Interface unter 10.1.0.254).
2. Gehen Sie zu **Netzwerk >> Interfaces >> Intern**.
3. Legen Sie eine **Zusätzliche Interne Route** zum Produktionsnetzwerk an (Netzwerk: 192.168.1.0/24 über Gateway 10.1.0.1):



4. Clients im Unternehmensnetzwerk (z. B. der Büro-Computer) senden Pakete, die an das Netzwerk 192.168.1.0/24 gerichtet sind, über das Standard-Gateway (*mGuard 2*) an *mGuard 1*

Ergebnis

Clients aus dem Unternehmensnetzwerk können nun die SPS im Produktionsnetzwerk über ihre reale IP-Adresse erreichen:

– Webbrowser: http://192.168.1.10
– Ping: 192.168.1.10

Vorteile

– Die SPS kann direkt über ihre reale IP-Adresse erreicht werden.
– Die Netzwerkkonfiguration des Büro-Computers und anderer Clients im Unternehmensnetzwerk muss nicht geändert werden.

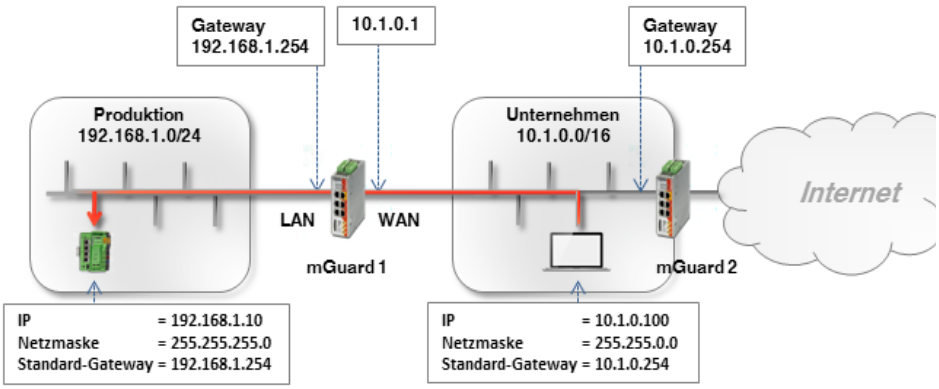
Nachteile

– Auf dem Gateway müssen zusätzliche Routen konfiguriert werden.

4.4.2 Option 2: IP- und Port-Weiterleitung

Bei der IP- und Port-Weiterleitung wird die IP-Adresse und Port-Nummer im Header eingehender Datenpakete so umgeschrieben, dass Datenpakete an die externe IP-Adresse von *mGuard 1* an eine beliebige IP-Adresse und/oder Port-Nummer im internen Netzwerk weitergeleitet werden.

Die SPS (192.168.1.10) befindet sich nicht in dem Netzwerk, in dem sich der anfragende Büro-Computer befindet (10.1.0.100).



Netzwerkpakete an *mGuard 1* aus dem Unternehmensnetzwerk (WAN), die an seine externe IP-Adresse gerichtet sind, werden so umgeschrieben, dass sie an die IP-Adresse der SPS im Produktionsnetzwerk (LAN) weitergeleitet werden. Neben der IP-Adresse kann der Port, an den das Paket adressiert ist, ebenfalls in einen beliebigen Port umgeschrieben werden.

IP- und Port-Weiterleitung kann nur für die Netzwerkprotokolle TCP, UDP und GRE angewendet werden. ICMP wird nicht unterstützt. Ein *Ping* auf die SPS ist daher mit dieser Option nicht möglich.

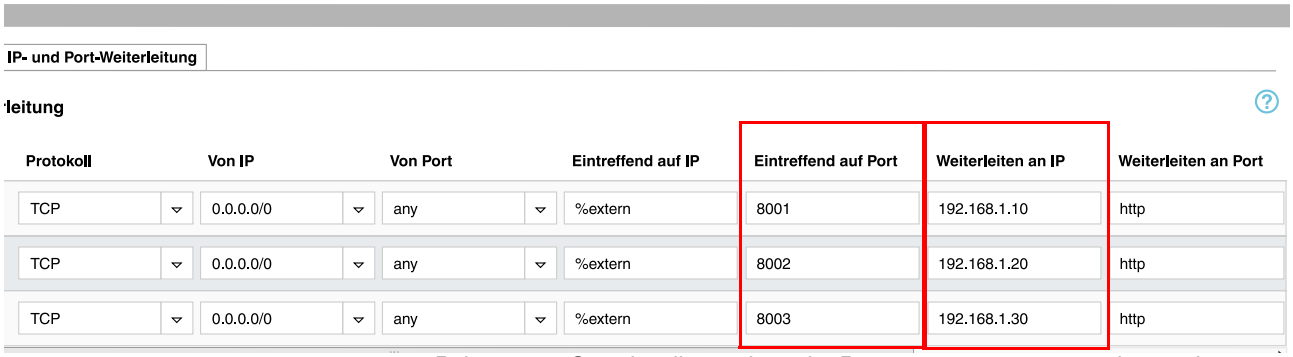
ACHTUNG: Trifft eine Regel zur IP- und Portweiterleitung auf ein Paket zu, wird dieses sofort an das angegebene Ziel weitergeleitet. Eventuell vorhandene Firewall-Regeln, die unter **Netzwerksicherheit >> Paketfilter** konfiguriert wurden, werden nicht mehr berücksichtigt.

Gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des *mGuard 1* an (LAN-Interface unter 192.168.1.254).
2. Gehen Sie zu **Netzwerk >> NAT >> IP- und Port-Weiterleitung**.
3. Legen Sie eine Regel mit folgender Konfiguration an:

4. **Optional**:
   – Mit den Angaben *Von IP* und *Von Port* kann die Regel auf bestimmte Absenderadressen (z. B. ein bestimmter Rechner im Unternehmensnetzwerk: 10.1.0.100) oder Netzwerke sowie bestimmte Ports beschränkt werden.

   – Im Feld *Eintreffend auf IP* könnte auch die externe IP-Adresse des mGuards angegeben werden.
     Wird die Variable **%extern** bei der Verwendung von mehreren statischen IP-Adressen für die WAN-Schnittstelle verwendet, bezieht sich die Angabe nur auf die erste IP-Adresse der Liste.
     Die Variable **%extern** muss verwendet werden, wenn ein dynamischer Wechsel der externen IP-Adresse des mGuards erfolgen kann, so dass eine bestimmte externe IP-Adresse nicht angegeben werden kann.
   – In unserem Beispiel werden nur Anfragen an Port 80 (*http*) an die Zieladresse und den Zielport weitergeleitet.
   – Um mithilfe von IP- und Port-Weiterleitung mehrere Clients im Zielnetzwerk zu erreichen, könnte die folgende Konfiguration verwendet werden:



   Pakete an *mGuard 1*, die an einen der Ports. 8001 – 8003 gesendet werden, werden nun an Port 80 (*http*) der jeweils entsprechenden IP-Adressen (z. B. 192.168.1.10) weitergeleitet.

Ergebnis

Alle oder (optional) nur bestimmte Clients aus dem Unternehmensnetzwerk können die SPS im Produktionsnetzwerk über die folgende IP-Adresse erreichen:

– Webbrowser: http://10.1.0.1 (= mGuard-Gerät)
– *Ping*: nicht möglich!

Vorteile

– Einfach zu konfigurieren für eine kleine Anzahl von Zielen.

Nachteile

– Nur Port-basierte Protokolle (UDP/TCP) können weitergeleitet werden (kein *Ping*).

- Der Zugriff auf den Ziel-Client (SPS) erfolgt über die externe IP des mGuard-Geräts und nicht über seine reale IP-Adresse
- Wenn mehrere Clients (Maschinensteuerungen) im Produktionsnetzwerk auf dem gleichen Port erreicht werden sollen, muss eine Art Mapping-Tabelle gepflegt werden, um zu wissen, welcher Port für den Zugriff auf einen bestimmten Client verwendet werden muss (z. B. http://10.1.0.1:8001 für 192.168.1.10 oder http://10.1.0.1:8002 für 192.168.1.20). Dies kann leicht zur Verwirrung führen.

Für mehr Informationen siehe auch mGuard-Firmwarehandbuch.

4.4.3 Option 3: 1:1-NAT

Bei 1:1-NAT wird ein **Reales Netzwerk** (z. B. das internen Produktionsnetzwerk) durch den mGuard in einem **Virtuellen Netzwerk** abgebildet. (Das virtuelle Netzwerk ist in unserem Beispiel ein Teil des externen Unternehmensnetzwerks.)

Der mGuard ordnet also IP-Adressen des Realen Netzwerks bestimmten IP-Adressen des Virtuellen Netzwerks zu. Werden Pakete an diese virtuellen IP-Adressen gesendet, leitet der mGuard diese an die realen IP-Adressen weiter.

Bei den realen und virtuellen Netzwerken kann es sich je nach Anwendungsfall um LAN-, WAN- oder DMZ-Netzwerke handeln.

Abhängig von der angegebenen Subnetzmaske in der 1:1 NAT-Konfiguration können auch Subnetze des **Realen Netzwerks** im **Virtuellen Netzwerk** abgebildet werden.

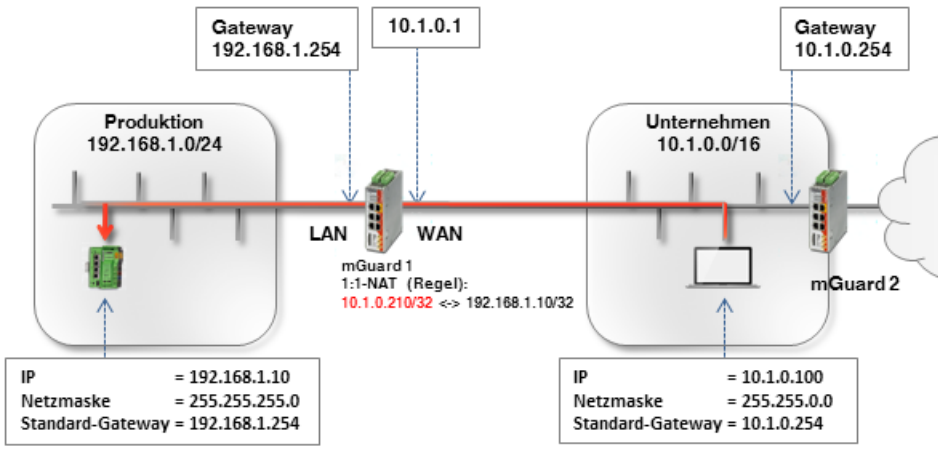
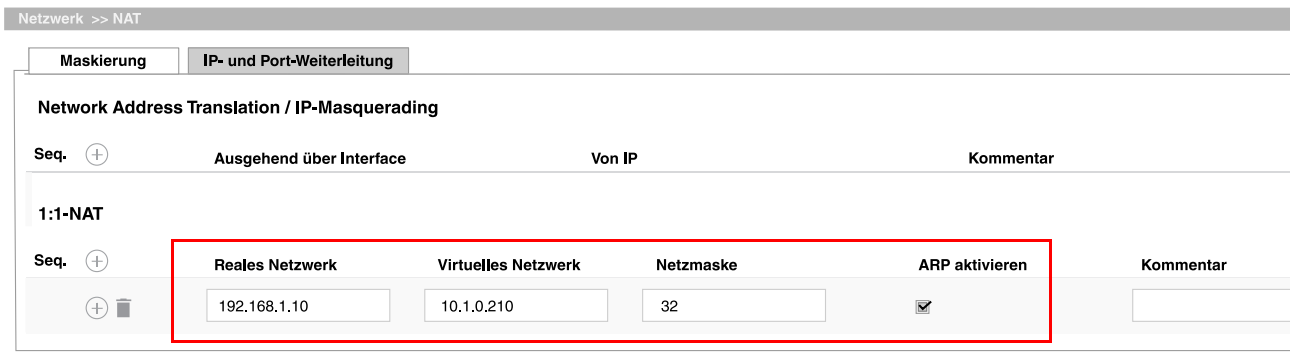


Tabelle 4-1 Beispiel-Regeln für 1:1-NAT mit unterschiedlichen Netzmasken und resultierende Zuordnungen

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
192.168.1.10	10.1.0.210	**32**	192.168.1.10 <-> 10.1.0.210

Um die SPS für alle Clients im Unternehmensnetzwerk erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des *mGuard 1* an (LAN-Interface unter 192.168.1.254).
2. Gehen Sie zu **Netzwerk >> NAT >> Maskierung**.
3. Legen Sie in der Sektion 1:1-NAT eine Regel mit folgender Konfiguration an:



4. Pakete, die im Unternehmensnetzwerk an die IP-Adresse 10.1.0.210 gesendet werden, werden nun an IP-Adresse 192.168.1.10 weitergeleitet.

ACHTUNG: Die unter *Virtuelles Netzwerk* angegebenen IP-Adressen müssen frei sein. Sie dürfen nicht für andere Geräte vergeben oder gar in Benutzung sein, weil sonst im virtuellen Netzwerk ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer oder mehreren IP-Adressen aus dem angegebenen *Virtuellen Netzwerk* gar kein Gerät im *Realen Netzwerk* existiert.

Ergebnis

Die SPS kann aus dem Unternehmensnetzwerk über die folgende IP-Adresse erreicht werden:

– Webbrowser: http://10.1.0.210
– Ping: 10.1.0.210

Vorteile

– Im Produktionsnetzwerk müssen keine Änderungen vorgenommen werden.
– Jeder Client im Produktionsnetzwerk ist über eine *virtuelle* IP-Adresse des Unternehmensnetzwerks erreichbar.
– Der Zugriff auf die SPS kann über Protokolle und Ports gemäß den festgelegten Regeln der eingehenden Firewall erfolgen.
– Die Anbindung weiterer Netzwerk-Segmente (z. B. verschiedene Produktionseinheiten) an das Unternehmensnetzwerk, ist über jeweils eigene mGuard-Geräte möglich. Diese Netzwerke könnten teilweise oder alle die gleichen internen Netzwerkeinstellungen verwenden (z. B. 192.168.1.0.0/24).

  Allgemein formuliert: Wenn z. B. das (virtuelle) externe Netzwerk eine Subnetzmaske von 16 hat und die Systeme in diesem Netzwerk nur IP-Adressen aus dem Bereich 10.1.0.1 – 10.1.0.254 verwenden, können die Netzwerke 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24 zur Abbildung der (realen) internen Netzwerke auf IP-Adressen des (virtuellen) externen Netzwerks verwendet werden.

Nachteile

Eine ausreichende Anzahl unbenutzter IP-Adressen aus dem virtuellen Netzwerk ist erforderlich, um das Mapping durchzuführen.

5 Externe Netzwerke erreichen (IP-Masquerading | 1:1-NAT)

Dokument-ID: 108408_de_01
Dokument-Bezeichnung: AH DE MGUARD NETWORK SEGMENT 2

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 Verwendung des mGuard-Geräts als Router beschrieben, der zwei Netzwerke (internes und externes Netzwerk) miteinander verbindet. Das externe Netzwerk soll aus dem internen erreicht werden.

Beschrieben werden die folgenden Verfahren:

– Option 1: NAT– Maskierung (IP-Masquerading)
– Option 2: NAT – 1:1-NAT

5.1 Einleitung

Im Netzwerkmodus „Router“ (*Router-Modus*) kann ein mGuard-Gerät dazu eingesetzt werden, zwei Netzwerke miteinander zu verbinden. Die Sicherheitsfunktionen Firewall und VPN (lizenzabhängig) stehen dabei ebenfalls zur Verfügung.

Bei einigen Modellen kann optional eine Demilitarisierte Zone (DMZ) über das zusätzliche DMZ-Interface angebunden werden.

5.1.1 Beispiel

Das Produktionsnetzwerk (= *Internes Netzwerk*) und das Unternehmensnetzwerk (= *Externes Netzwerk*) sind über einen mGuard-Router miteinander verbunden.

Aus dem Produktionsnetzwerk soll auf einen Server im Unternehmensnetzwerk zugegriffen werden.

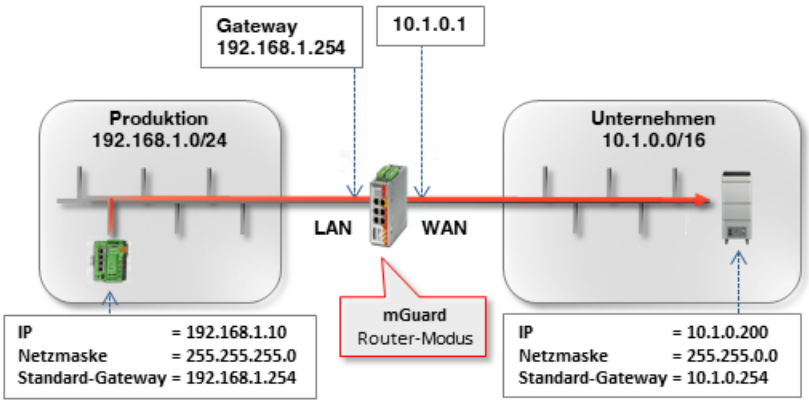


Bild 5-1 Netzwerkeinstellungen der Clients und mGuard-Router

Das Ziel, die beiden Netzwerke miteinander zu verbinden, kann auf unterschiedlichen Wegen erreicht werden:

– Option 1: **Maskierung / IP-Masquerading**
– Option 2: **1:1-NAT**

5.1.2 Vorgehen

1. WAN- und LAN-Interface des Routers (*mGuard 1*) konfigurieren
2. Firewall-Regeln konfigurieren
3. Netzwerkeinstellungen gemäß Option 1 oder 2 konfigurieren

5.2 Netzwerkeinstellungen des mGuard-Routers

Um den Netzwerkverkehr zwischen den beiden Netzwerken zu ermöglichen, müssen in allen Optionen das externe (= WAN-Port) und das internes Interface (= LAN-Port) des Routers *mGuard 1* konfiguriert und mit mindestens einer IP-Adresse versehen werden.

Stellen Sie sicher, dass die Clients im Produktions- und Unternehmensnetzwerk ihrem Netzwerk entsprechend konfiguriert sind.

Die Clients im Produktionsnetzwerk (SPS) müssen als Standard-Gateway die interne IP-Adresse des *mGuard 1* konfiguriert haben (192.168.1.254).

Die Clients im Unternehmensnetzwerk müssen als Standard-Gateway die interne IP-Adresse des *mGuard 2* konfiguriert haben (10.1.0.254).

Um *mGuard 1* als Router zwischen dem Unternehmensnetzwerk (WAN)10.1.0.0/16 und dem Produktionsnetzwerk (LAN) 192.168.1.0/24 einzusetzen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (192.168.1.254).
2. Gehen Sie zu **Netzwerk >> Interfaces**.
3. Registerkarte *Allgemein*: Wählen Sie den **Netzwerk-Modus** *Router* und den **Router-Modus** *Statisch*.
4. Registerkarte *Intern*: Wählen Sie als Interne IP-Adresse 192.168.1.254.
5. Registerkarte *Extern*: Wählen Sie als Externe IP-Adresse 10.1.0.1.

Bild 5-2 Internes Interface

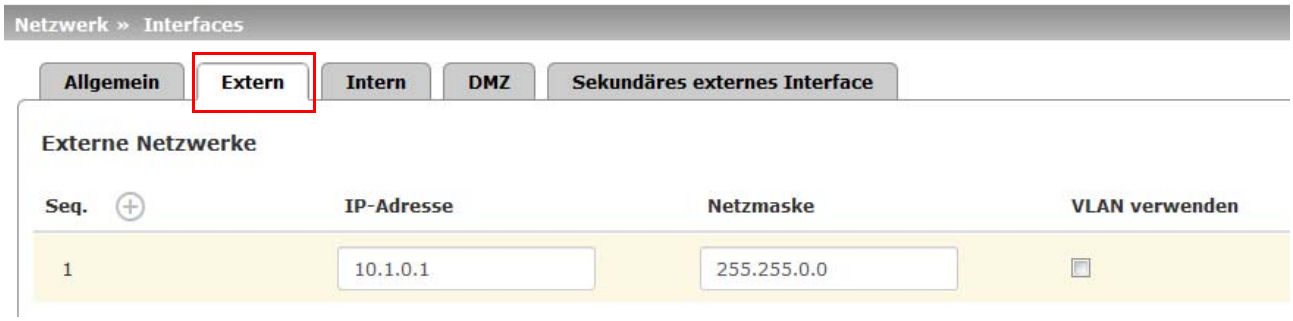


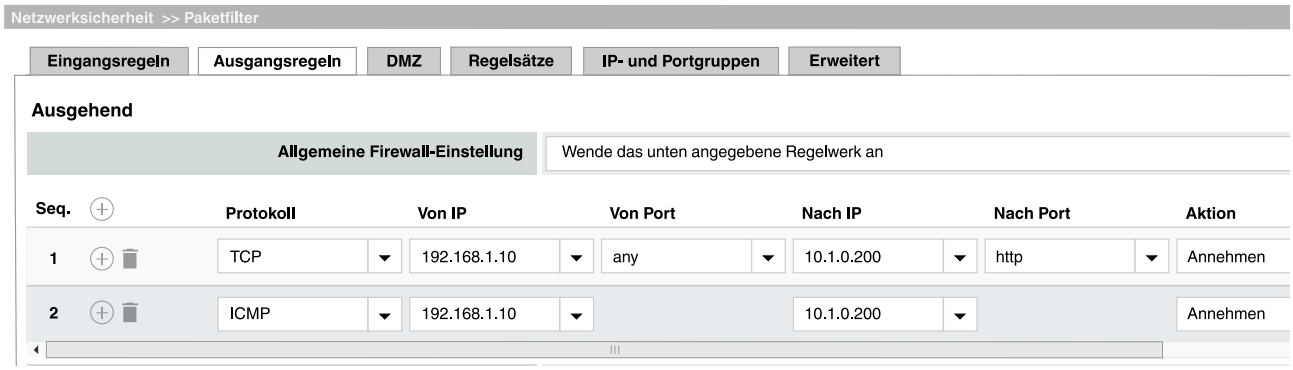
Bild 5-3 Externes Interface

5.3 Firewall-Regeln konfigurieren

mGuard 1 soll so konfiguriert werden, dass er ausschließlich den Zugriff eines bestimmten Clients aus dem Produktionsnetzwerk (192.168.1.10) auf den Webserver (10.1.0.200) im Unternehmensnetzwerk erlaubt. Abgesehen davon soll es auch möglich sein, den Webserver zu "*pingen*" (ICMP-Anfrage).

Gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche von *mGuard 1* an (192.168.1.254).
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Ausgangsregeln**.
3. Wählen Sie bei **Allgemeine Firewall-Einstellung** „*Wende das unten angegebene Regelwerk an*“.
4. Legen Sie zwei Firewall-Regeln wie folgt an:



Ergebnis

Die Firewall-Regeln erlauben ausgehende TCP-Pakete an den HTTP-Port sowie ausgehende ICMP-Pakete. Alle anderen Pakete werden von der Firewall verworfen. Die Felder **Von IP** und **Nach IP** geben an, von welcher IP-Adresse (Client) auf welche IP-Adresse (Server) zugegriffen werden kann.

5.4 Netzwerkeinstellungen gemäß Option 1 und 2

5.4.1 Option 1: Maskierung / IP-Masquerading

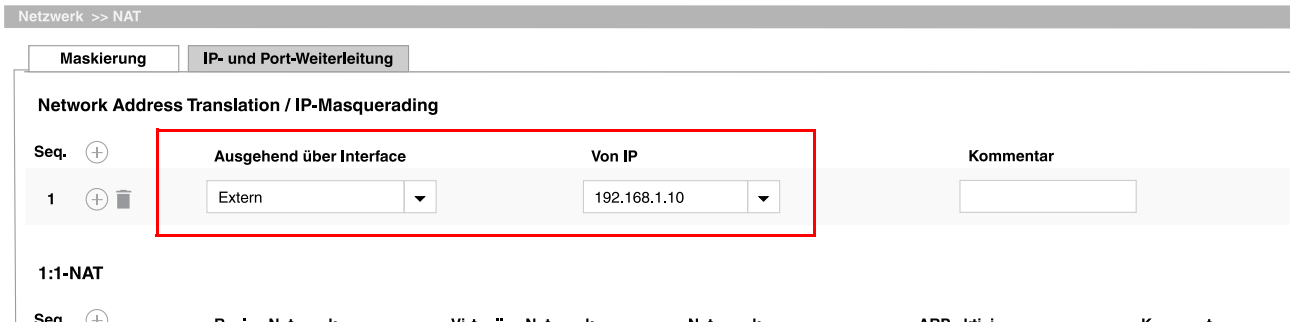
Das mGuard-Gerät maskiert die IP-Adressen von Absendern aus dem Produktionsnetzwerk (= *Internes Netzwerk*) mit seiner eigenen externen IP-Adresse.

Das heißt, der mGuard ersetzt in den Datenpaketen die IP-Adresse des Absenders (192.168.1.10) durch seine externe IP-Adresse (10.1.0.1).

Wenn die Pakete beim Ziel-Server (10.1.0.200) ankommen, befindet sich die IP-Adresse des Absenders (mGuard: 10.1.0.1) im selben Netzwerk und der Server sendet die Antwort direkt an den mGuard zurück. Der mGuard macht die NAT-Änderungen rückgängig und leitet die Antwort an den ursprünglichen Absender (192.168.1.10) weiter.

Um den Server im Unternehmensnetzwerk für den Client aus dem Produktionsnetzwerk erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuards an (LAN-Interface unter 192.168.1.254).
2. Gehen Sie zu **Netzwerk >> NAT >> Maskierung**.
3. Legen Sie in der Sektion *Network Address Translation / IP-Masquerading* eine Regel mit folgender Konfiguration an:



4. **Optional**: Sie können im Feld *Von IP* auch alle IPs angeben (0.0.0.0/0), wenn Sie allen Clients aus dem Produktionsnetzwerk IP-Masquerading ermöglichen wollen. Die Zugriffsbeschränkung müsste dann über die Firewall-Einstellungen geregelt werden.

Ergebnis

Pakete, die vom Client (192.168.1.10) im Produktionsnetzwerk an die IP-Adresse des Servers im Unternehmensnetzwerk (10.1.0.200) gesendet werden, werden vom mGuard-Router auf seine externe IP-Adresse umgeschrieben und weitergeleitet.

Der Server im Unternehmensnetzwerk kann von dem Client unter seiner realen IP-Adresse erreicht werden:

– Webbrowser: http://10.1.0.200
– Ping: 10.1.0.200

Vorteile

– Im Produktionsnetzwerk müssen keine Änderungen vorgenommen werden.
– Jeder Client im Produktionsnetzwerk kann alle Ziele im Unternehmensnetzwerk unter ihren realen IP-Adressen erreichen.
– Der Zugriff auf die Ziele im Unternehmensnetzwerk kann über Protokolle und Ports gemäß festgelegter Firewall-Regeln (Ausgangsregeln) erfolgen.

5.4.2 Option 2: 1:1-NAT

Bei 1:1-NAT wird ein **Reales Netzwerk** (z. B. das externe Unternehmensnetzwerk) durch den mGuard in einem **Virtuellen Netzwerk** abgebildet. (Das *virtuelle Netzwerk* ist in unserem Beispiel ein Teil des internen Produktionsnetzwerks.)

Der mGuard ordnet also IP-Adressen des *Realen Netzwerks* bestimmten IP-Adressen des *Virtuellen Netzwerks* zu. Werden Pakete an diese virtuellen IP-Adressen gesendet, leitet der mGuard diese an die realen IP-Adressen weiter.

Bei den realen und virtuellen Netzwerken kann es sich je nach Anwendungsfall um LAN-, WAN- oder DMZ-Netzwerke handeln.

Abhängig von der angegebenen Subnetzmaske in der 1:1 NAT-Konfiguration können auch Subnetze des **Realen Netzwerks** im **Virtuelle Netzwerk** abgebildet werden.

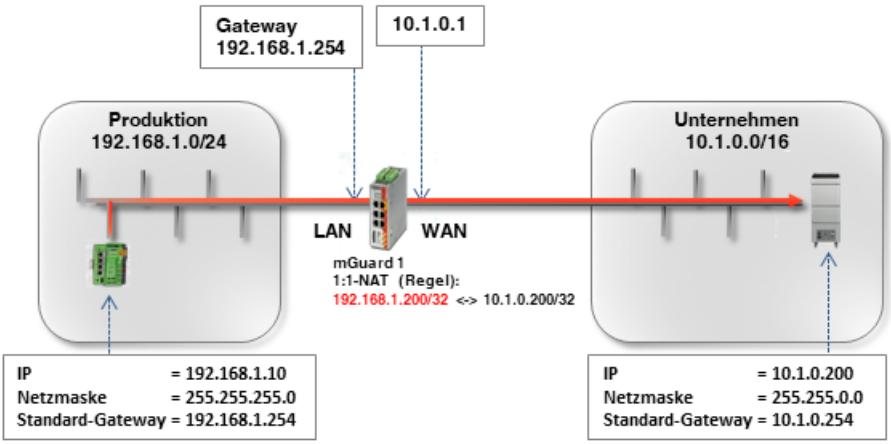
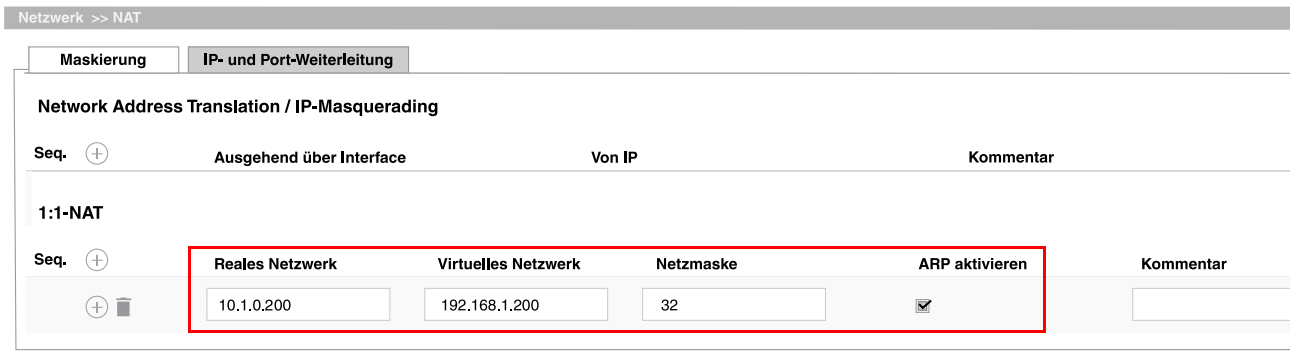


Tabelle 5-1 Beispiel-Regeln für 1:1-NAT mit unterschiedlichen Netzmasken und resultierende Zuordnungen

Reales Netzwerk	Virtuelles Netzwerk	Netzmaske	Zugeordnete IP-Adressen
10.1.0.200	192.168.1.200	**32**	10.1.0.200 <-> 192.168.1.200

Um den Server im Unternehmensnetzwerk für den Client aus dem Produktionsnetzwerk erreichbar zu machen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuards an (LAN-Interface unter 192.168.1.254).
2. Gehen Sie zu **Netzwerk >> NAT >> Maskierung**.
3. Legen Sie in der Sektion *1:1-NAT* eine Regel mit folgender Konfiguration an:



4. Pakete, die im Produktionsnetzwerk an die IP-Adresse 192.168.1.200 gesendet werden, werden nun an IP-Adresse 10.1.0.200 weitergeleitet.

ACHTUNG: Die unter *Virtuelles Netzwerk* angegebenen IP-Adressen müssen frei sein. Sie dürfen nicht für andere Geräte vergeben oder gar in Benutzung sein, weil sonst im virtuellen Netzwerk ein IP-Adressenkonflikt entsteht. Dies gilt selbst dann, wenn zu einer oder mehreren IP-Adressen aus dem angegebenen *Virtuellen Netzwerk* gar kein Gerät im *Realen Netzwerk* existiert.

Ergebnis

Der Server im Unternehmensnetzwerk kann über die folgende IP-Adresse erreicht werden:

– Webbrowser: http://192.168.1.200
– Ping: 192.168.1.200

Vorteile

– Im Unternehmensnetzwerk müssen keine Änderungen vorgenommen werden.
– Jeder Client im Unternehmensnetzwerk ist über eine *virtuelle* IP-Adresse des Produktionsnetzwerks erreichbar.
– Der Zugriff auf die Ziele im Unternehmensnetzwerk kann über Protokolle und Ports gemäß den festgelegten Regeln der eingehenden Firewall erfolgen.

Nachteile

Eine ausreichende Anzahl unbenutzter IP-Adressen aus dem virtuellen Netzwerk ist erforderlich, um das Mapping durchzuführen.

6 Eigenschaften und Anwendungsmöglichkeiten der mGuard-Firewall

Dokument-ID: 108405_de_00
Dokument-Bezeichnung: AH DE MGUARD FIREWALL

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 die grundlegende Funktionsweise der mGuard-Firewall sowie verschiedene Anwendungsmöglichkeiten beschrieben.

6.1 Stateful-Packet-Inspection-Firewall

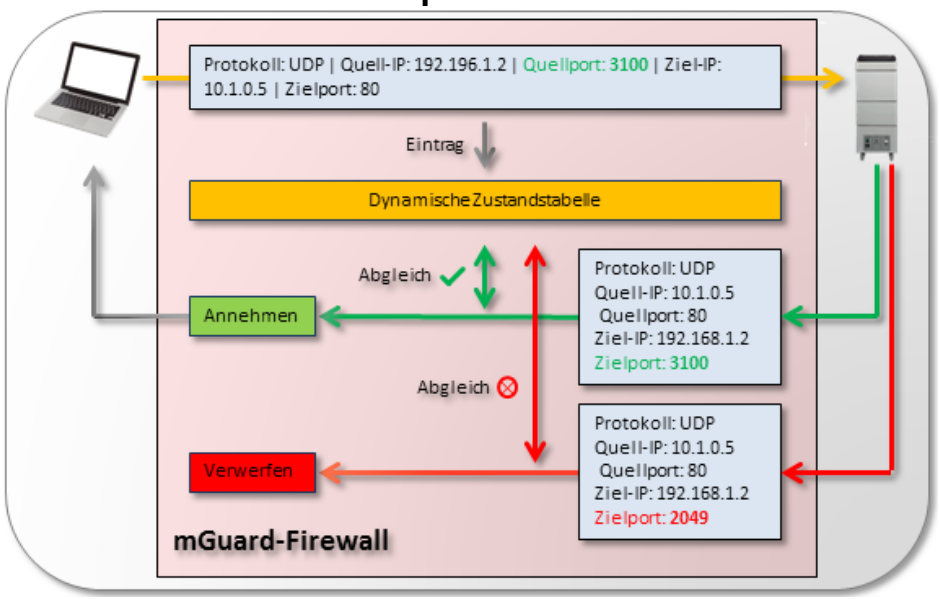


Bild 6-1 Passieren ein- oder ausgehende Pakete die mGuard-Firewall (oranger Pfeil), werden ihre Eigenschaften (z. B. Protokoll, Absender-IP/Port, Ziel-IP/Port) in einer dynamischen Zustandstabelle gespeichert. Die Eigenschaften des zu erwartenden Antwortpakets werden ebenfalls gespeichert, damit auch dieses durch die Firewall gelangt. Antwortpakete werden dann mit den Werten der Zustandstabelle verglichen. Entsprechen die Pakete den dynamisch eingetragenen Werten der Zustandstabelle, werden sie angenommen (grüner Pfeil). Stimmen sie nicht überein, werden die Pakete verworfen (roter Pfeil).

Die mGuard-Firewall funktioniert als dynamischer Paketfilter (*Stateful-Packet-Inspection-Firewall*), der ein- und ausgehende Netzwerkpakete nach konfigurierten Regeln analysiert.

Durch die dynamische Paketfilterung können Antwortpakete die eingehende Firewall automatisch passieren, wenn die Antwortpakete zweifelsfrei der Anfrage zugeordnet werden können, die zuvor die ausgehende Firewall passiert hat.

Die Konfiguration von Eingangsregeln, um Antworten auf ausgehende Anfragen zu akzeptieren, ist deshalb grundsätzlich nicht erforderlich. Tatsächlich könnte eine Eingangsregel so konfiguriert sein, dass sie alle eingehenden Pakete verwirft. Eingehende Antworten auf Anfragen würden trotzdem angenommen.

6.2 Statische Firewall

Mithilfe von statischen Firewall-Regeln werden Zugriffe auf der Grundlage von Netzwerken (IP-Adressen, Protokolle und Ports) geregelt.

Diese Regeln sind statisch und für die ausgewählten Interfaces immer aktiv, nachdem sie angelegt wurden. D. h. bestimmte Geräte/Netzwerke können miteinander kommunizieren.

(**Beispiel**: siehe Kapitel 4.3, „Firewall-Regeln konfigurieren“)

6.3 Dynamisch aktivierte Firewall (über Firewall-Regelsätze)

Firewall-Regeln, die in Firewall-Regelsätzen zusammengefasst sind, können dynamisch aktiviert oder deaktiviert werden. Die Aktivierung/Inaktivierung erfolgt wahlweise über

– die Weboberfläche,
– eine SMS,
– einen Schalter/Taster,
– den Aufbau einer VPN-Verbindung.

Wie bei statischen Firewall-Regeln werden die Zugriffe auf der Grundlage von Netzwerken (IP-Adressen, Protokolle und Ports) geregelt. Die Regeln sind aber nur bei Bedarf aktiv.

(**Beispiel „Firewall-Regelsatz“**: siehe Kapitel 8, „Firewall-Regelsätze verwenden“)

6.4 Benutzerfirewall

Die Benutzerfirewall erlaubt es, benutzerspezifische Firewall-Regeln zu definieren, die nur für angelegte Firewall-Benutzer oder Benutzergruppen gelten. Benutzerfirewall-Regeln haben Vorrang vor an anderer Stelle konfigurierten Firewall-Regeln (z. B. *Eingangsregeln /Ausgangsregeln*) und setzen diese ggf. außer Kraft.

Der Zugriff auf das Ziel wird dabei nicht auf der Grundlage von statisch konfigurierten Firewall-Regeln erlaubt, sondern dynamisch nach Anmeldung des Firewall-Benutzers mittels dem Firewall-Benutzer zugeordneten Benutzerfirewall-Regeln.

Eine Benutzerfirewall-Regel tritt dann in Kraft, wenn sich ein der Regel zugeordneter Firewall-Benutzer über die Weboberfläche des mGuard-Geräts anmelden. Die Authentifizierung erfolgt über die interne Datenbank oder einen RADIUS-Server.

(**Beispiel**: siehe Kapitel 9, „Benutzerfirewall verwenden, um den Zugriff auf ein externes Netzwerk zu erlauben“)

7 Häufige Fehler bei der Erstellung von Firewall-Regeln

Dokument-ID: 108403_de_00
Dokument-Bezeichnung: AH DE MGUARD FIREWALL MISCONFIG

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 häufige Fehler bei der Erstellung von Firewall-Regeln beschrieben (z. B. falsche Reihenfolge, falscher Quellport).

7.1 Einleitung

Die mGuard-Firewall funktioniert als dynamischer Paketfilter, der ein- und ausgehende Netzwerkpakete nach konfigurierten Regeln analysiert (siehe auch Kapitel 6, „Eigenschaften und Anwendungsmöglichkeiten der mGuard-Firewall“).

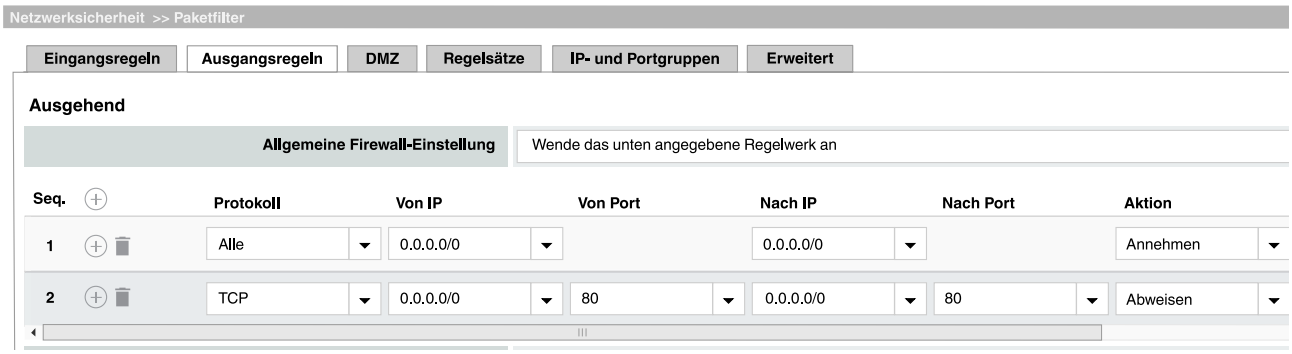
Häufiger Fehler: Entscheidend beim Anlegen von Firewall-Regeln in einer Tabelle ist deren Reihenfolge. Die in der Tabelle angelegten Firewall-Regeln werden nacheinander von oben nach unten geprüft. Wenn eine Regel zutrifft, wird die angegebene Aktion (*Annehmen, Verwerfen* oder *Abweisen)* ausgeführt und die nachfolgenden Regeln werden **nicht mehr** berücksichtigt.

7.1.1 Beispiel

Der Zugriff auf HTTP-Webserver aus dem internen Netzwerk soll mithilfe konfigurierter Firewall-Regeln unterbunden werden (mGuard-Menü: **Netzwerksicherheit >> Paketfilter >> Ausgangsregeln**).

Spezifizierte Ports (*Von Port* und *Nach Port*) werden nur berücksichtigt, wenn das Protokoll auf TCP oder UDP eingestellt ist.

7.2 Falsche Konfiguration



Fehler 1: Falsche Reihenfolge

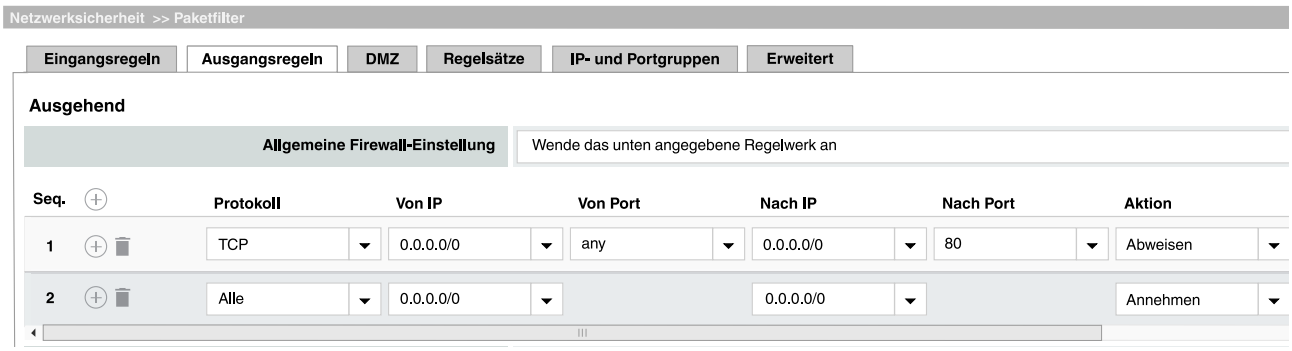
Da die erste Regel in Reihe 1 bereits für alle Paket zutrifft, werden die nachfolgenden Regeln nicht mehr überprüft. Eine ausgehende TCP-Verbindung auf Port 80 wird also nicht abgelehnt.

Fehler 2: Falscher Quellport

HTTP-Anfragen von Webbrowsern verwenden einen variierenden Quellport größer oder gleich 1024. Die Anfragen werden an Port 80 gesendet. Die angelegte Regel in Reihe 2 wird aufgrund des eingetragenen Quellports (*Von Port* = 80), also kleiner 1024, nicht zutreffen.

7.3 Richtige Konfiguration

In der richtigen Konfiguration muss die Reihenfolge der Firewall-Regeln so geändert werden, dass zuerst die Regel, die Zugriffe auf einen Webserver abweist, geprüft wird.



Als Quellport (*Von Port)* kann z. B. *any* angegeben werden, um die Anfragen eines Standard-Webbrowsers zu prüfen. Mit der Angabe des Zielports (*Nach Port* = 80) wird der Zugriff auf einen Webserver abgewiesen.

Wenn die erste Regel **zutrifft**, wird die zweite Regel nicht mehr beachtet. Wenn die erste Regel **nicht zutrifft**, erlaubt die zweite Regel den ausgehenden Datenverkehr.

8 Firewall-Regelsätze verwenden

Dokument-ID: 108402_de_00
Dokument-Bezeichnung: AH DE MGUARD FIREWALL RULESETS 1

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 Verwendung von Firewall-Regelsätzen beschrieben. Das Anlegen von Firewall-Regeln wird dadurch vereinfacht und beschleunigt.

8.1 Einleitung

Einzelne Firewall-Regeln können in Regelsätzen zusammengefasst werden. Diese Regelsätze können anschließend in Firewall-Regeln als Aktion ausgewählt und somit zur Anwendung gebracht werden.

8.1.1 Beispiel

Der externe Zugriff auf drei bestimmte Server im internen Netzwerk über die Netzwerkdienste *ftp*, *telnet* und *https* soll erlaubt werden. Der Zugriff auf alle übrigen Dienste und Netzwerkadressen aus dem externen Netz (WAN) soll verboten werden.

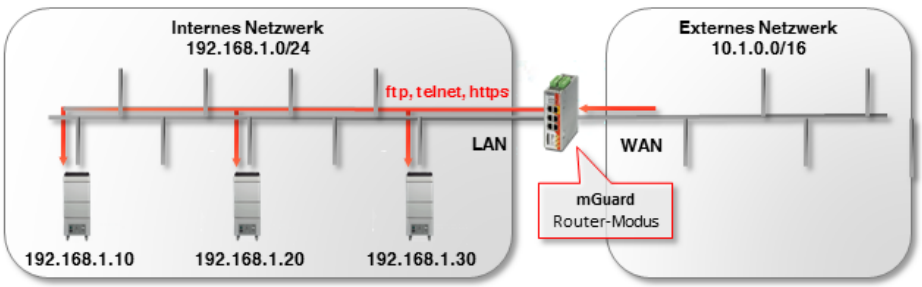


Bild 8-1 Zugriff auf spezielle Dienste auf bestimmten Servern erlauben

Problem

Ohne Regelsätze müssten neun Firewall-Regeln in einer Firewall-Tabelle angelegt werden: jeweils drei für jeden Dienst bzw. jede Server-IP-Adresse.

Lösung

Mithilfe von Regelsätzen können bestimmte Teilregeln, d. h. die Server-IP-Adressen oder die Netzwerkdienste, in Regelsätzen zusammengefasst werden. Diese können dann in Firewall-Tabellen als Aktion ausgewählt werden.

In diesem Beispiel reichen drei Eingangsregeln in der Firewall-Tabelle aus, um ausschließlich den Zugriff auf die drei Server und die drei Netzwerkdienste zu erlauben. Dazu muss **wahlweise** ein Regelsatz „*Server*“ oder ein Regelsatz *Service* angelegt werden (siehe „Beispiel 1 (Regelsatz: „Server“)“ und „Beispiel 2 (Regelsatz „Service“)“).

Bitte beachten Sie: Wenn eine Verbindung, die zu einem Firewall-Regelsatz passt, aufgebaut worden ist und diese Verbindung kontinuierlich Datenverkehr erzeugt, dann kann es sein, dass das Deaktivieren des Firewall-Regelsatzes diese Verbindung nicht wie erwartet unterbricht (siehe mGuard-Firmwarehandbuch).

8.1.2 Vorgehen

Um den Zugriff auf definierte Server und Netzwerkdienste zuzulassen, sind folgende Arbeitsschritte notwendig:

1. Firewall-Regelsatz anlegen.
2. Firewall-Regeln in Firewall-Tabelle anlegen und auf den Regelsatz verweisen.

8.2 Beispiel 1 (Regelsatz: „Server“)

Um den Regelsatz anzulegen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Regelsätze**.
3. Legen Sie einen neuen Regelsatz mit dem Namen *Server* an und klicken Sie auf das Icon *Zeile bearbeiten*.
4. Konfigurieren Sie den Regelsatz gemäß Bild 8-2.

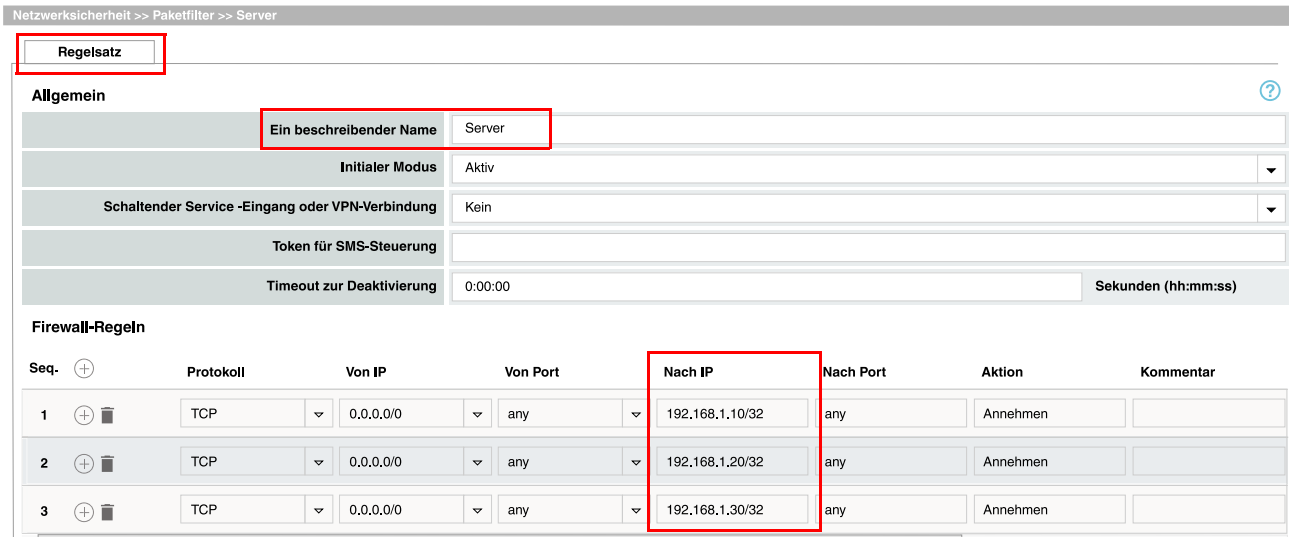


Bild 8-2 Im **Regelsatz** *Server* werden die zugelassenen Ziel-IP-Adressen (Ziel-Server) zusammengefasst.

Um den Regelsatz in einer Firewall-Regel anzuwenden, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Netzwerksicherheit >> Paketfilter >> Eingangsregeln**.
3. Wählen Sie **Wende das unten angegebene Regelwerk an** aus.
4. Legen Sie drei Firewall-Regeln gemäß Bild 8-3 an.

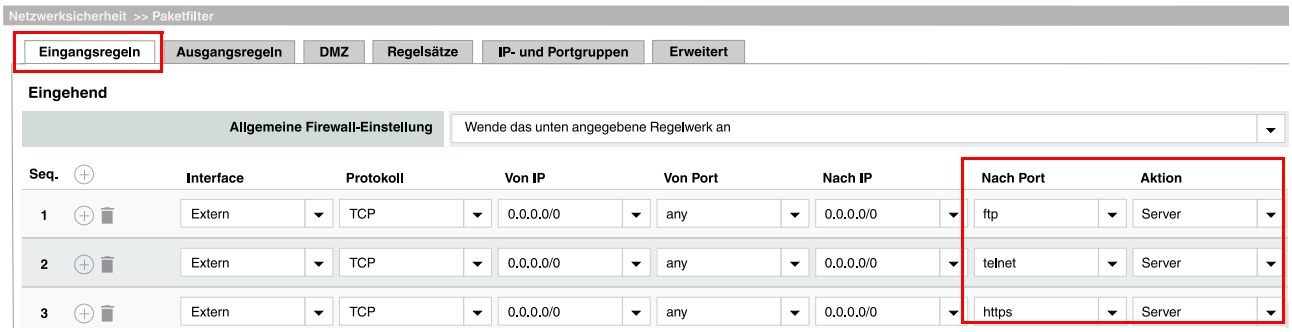


Bild 8-3 In der **Firewall-Tabelle** wird bei Zugriffen auf die angegebenen Netzwerkdienste als Aktion auf den Regelsatz *Server* verwiesen.

Die Firewall-Regeln definieren den Zugriff auf spezifische Netzwerkdienste (*Nach Port*) und verweisen auf den Regelsatz *Server*. In diesem wird der Zugriff auf die Ziele definiert.

8.3 Beispiel 2 (Regelsatz „Service“)

Anstatt die Server-IP-Adressen können Sie auch die Netzwerkdienste in einem Regelsatz zusammenfassen und diesen in den Firewall-Regeln anwenden. Die Einstellungen sind wie folgt (siehe Bild 8-4 und Bild 8-5).

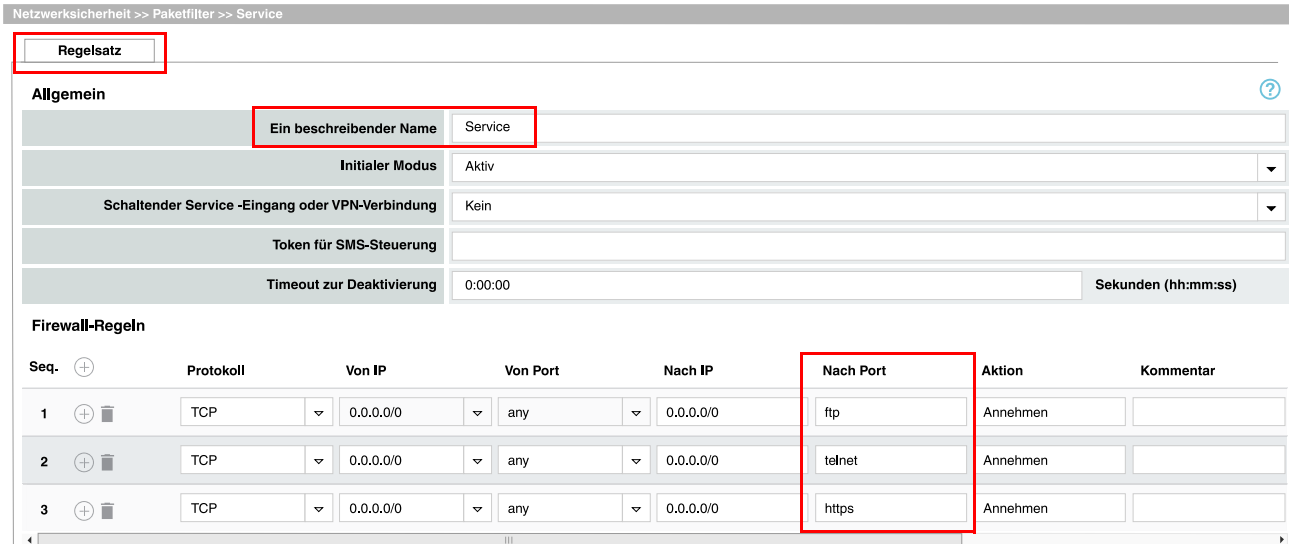


Bild 8-4 Im **Regelsatz** *Service* werden die erlaubten Netzwerkdienste zusammengefasst.

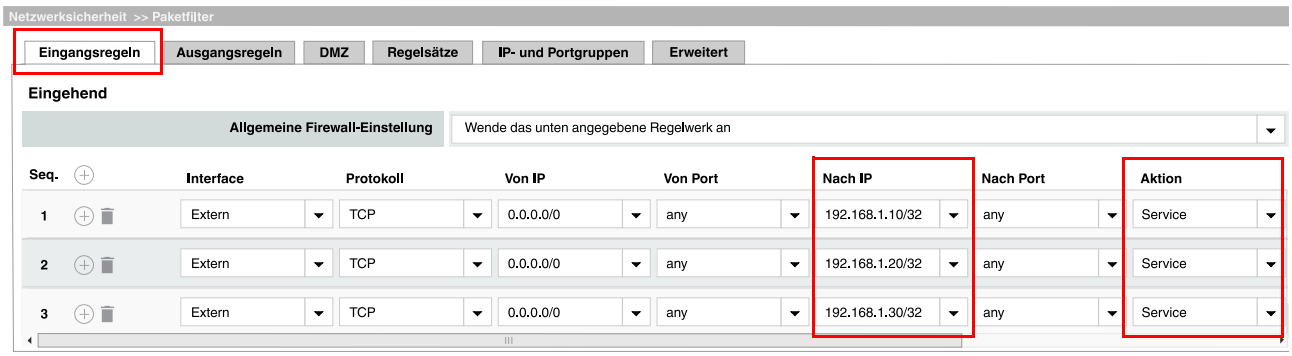


Bild 8-5 In der **Firewall-Tabelle** wird bei Zugriffen auf die angegebenen Ziel-IP-Adressen (Ziel-Server) als Aktion auf den **Regelsatz** *Service* verwiesen.

Die Firewall-Regeln definieren den Zugriff auf spezifische Ziel-IP-Adressen (*Nach IP*) und verweisen auf den Regelsatz *Service*. In diesem wird der Zugriff auf die erlaubten Netzwerkdienste definiert.

9 Benutzerfirewall verwenden, um den Zugriff auf ein externes Netzwerk zu erlauben

Dokument-ID: 108401_de_00

Dokument-Bezeichnung: AH DE MGUARD USERFIREWALL 1

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 beschrieben, wie einem Firewall-Benutzer mithilfe von Benutzerfirewall-Regeln der Zugriff aus dem internen auf ein externes Netzwerk erlaubt wird.

Eine Benutzerfirewall steht auf Geräten der RS2000-Serie und dem mGuard Blade-Controller nicht zur Verfügung.

9.1 Einleitung

Die Benutzerfirewall erlaubt es, benutzerspezifische Firewall-Regeln zu definieren, die nur für angelegte Firewall-Benutzer oder Benutzergruppen gelten.

Benutzerfirewall-Regeln haben Vorrang vor an anderer Stelle konfigurierten Firewall-Regeln (z. B. *Eingangsregeln/Ausgangsregeln*) und setzen diese ggf. außer Kraft.

Der Zugriff auf das Ziel wird dabei nicht auf der Grundlage von statisch konfigurierten Firewall-Regeln erlaubt, sondern dynamisch nach Anmeldung des Firewall-Benutzers mittels dem Firewall-Benutzer zugeordneten Benutzerfirewall-Regeln.

9.1.1 Beispiel

Die Netzwerkanbindung des Produktionsnetzwerks (Intern) an das Unternehmensnetzwerk (Extern) wird in diesem Beispiel mittels NAT (IP-Maskierung) ermöglicht (siehe auch Kapitel 5.4.1, „Option 1: Maskierung / IP-Masquerading“).

Gleichzeitig werden jedoch **alle Zugriffe** aus der Produktion auf das Unternehmensnetzwerk durch eine allgemeine Firewall-Regel (Ausgangsregel) verboten.

Mithilfe der Benutzerfirewall erhalten nun die Firewall-Benutzer *pwerner* und *hpotter* individuellen Zugriff auf Webserver und können somit auf die Webserver im Unternehmensnetzwerk zugreifen.

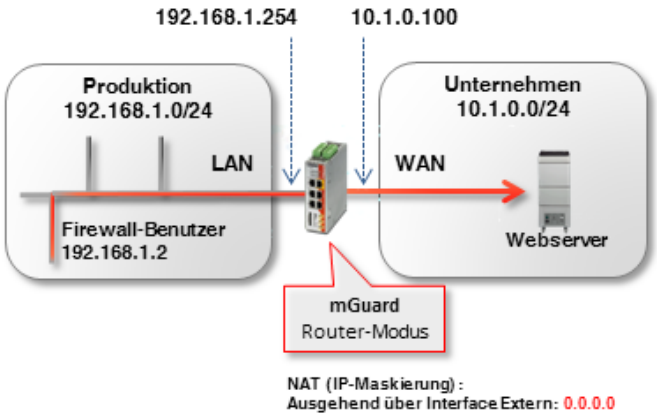


Bild 9-1 Firewall-Benutzer mit Zugriffsrechten auf HTTP(S)-Webserver

9.1.2 Vorgehen

Um den Zugriff auf einen Webserver über Port 80 (http) und 443 (https) für die Firewall-Benutzer *pwerner* und *hpotter* zu erlauben, sind folgende Arbeitsschritte notwendig:

1. Firewall-Benutzer anlegen
2. Benutzerfirewall-Template mit Firewall-Regeln erstellen
3. Benutzerfirewall aktivieren
4. Als Firewall-Benutzer anmelden

9.2 Firewall-Benutzer anlegen

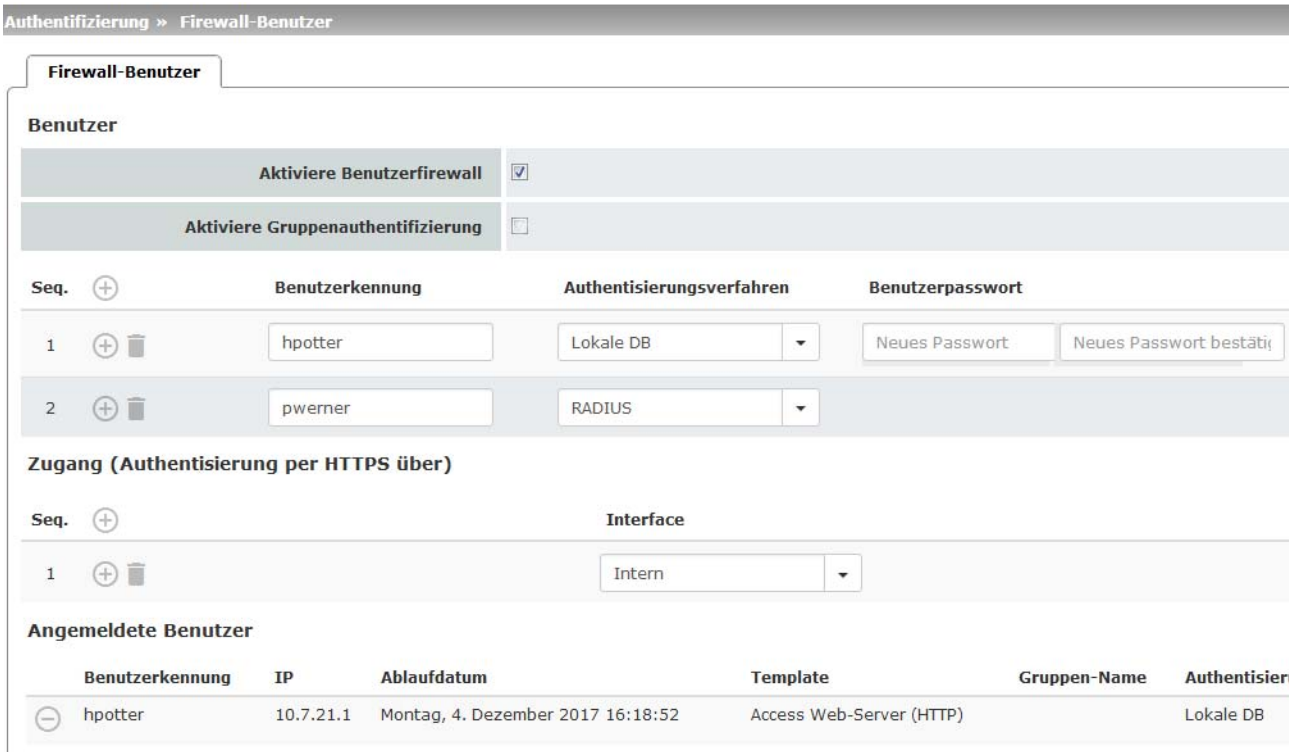


Bild 9-2 Firewall-Benutzer anlegen

Firewall-Benutzer werden unter **Authentifizierung >> Firewall-Benutzer** angelegt. Dort wird ebenfalls festgelegt, ob der Nutzer über einen RADIUS-Server oder ein lokal auf dem mGuard-Gerät konfiguriertes Benutzerpasswort authentifiziert wird.

Die allgemeine Konfiguration zur Verwendung eines RADIUS-Servers durch das mGuard-Gerät erfolgt im Menü **Authentifizierung >> RADIUS**.

Ein Firewall-Benutzer kann einem oder mehreren Benutzerfirewall-Templates zugeordnet werden (siehe „Registerkarte „Template-Benutzer““ auf Seite 47).

Um einen Firewall-Benutzer anzulegen, gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Authentifizierung >> Firewall-Benutzer**.
3. Erstellen Sie die gewünschten Firewall-Benutzer.
4. Geben Sie jeweils das Authentisierungsverfahren für den Benutzer an (Password oder RADIUS-Server).
5. Geben Sie an, über welche Interfaces sich Firewall-Benutzer am mGuard-Gerät anmelden dürfen.

9.3 Benutzerfirewall-Template erstellen

In einem Benutzerfirewall-Template werden Firewall-Regeln erstellt und bereits existierenden Firewall-Benutzern zugewiesen.

Wenn ein Benutzerfirewall-Template oder eine Firewall-Regel eines Templates hinzugefügt, geändert, gelöscht oder deaktiviert wird, sind sofort alle eingeloggten Firewall-Benutzer betroffen.

Bestehende Verbindungen werden unterbrochen. Eine Ausnahme bildet die Änderung von Benutzerfirewall-Regeln, wenn unter **Netzwerksicherheit >> Paketfilter >> Erweitert** die Funktion „Bestehende Verbindungen nach Änderungen an der Firewall zurücksetzen“ deaktiviert ist. In diesem Fall wird eine Netzwerkverbindung, die aufgrund einer vorher erlaubten Regel besteht, nicht unterbrochen.

Wenn ein Firewall-Regelsatz (Template) **deaktiviert** und anschließend **aktiviert** wird, müssen sich betroffene eingeloggte Firewall-Benutzer zunächst ausloggen und dann wieder einloggen, um die Firewall-Regeln aus dem Template erneut für sich zu aktivieren.

Um ein Benutzerfirewall-Template zu erstellen, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Weboberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Netzwerksicherheit >> Benutzerfirewall**.
3. Legen Sie ein neues Template an und klicken Sie auf das Icon *Zeile bearbeiten*.

9.3.1 Registerkarte „Allgemein“

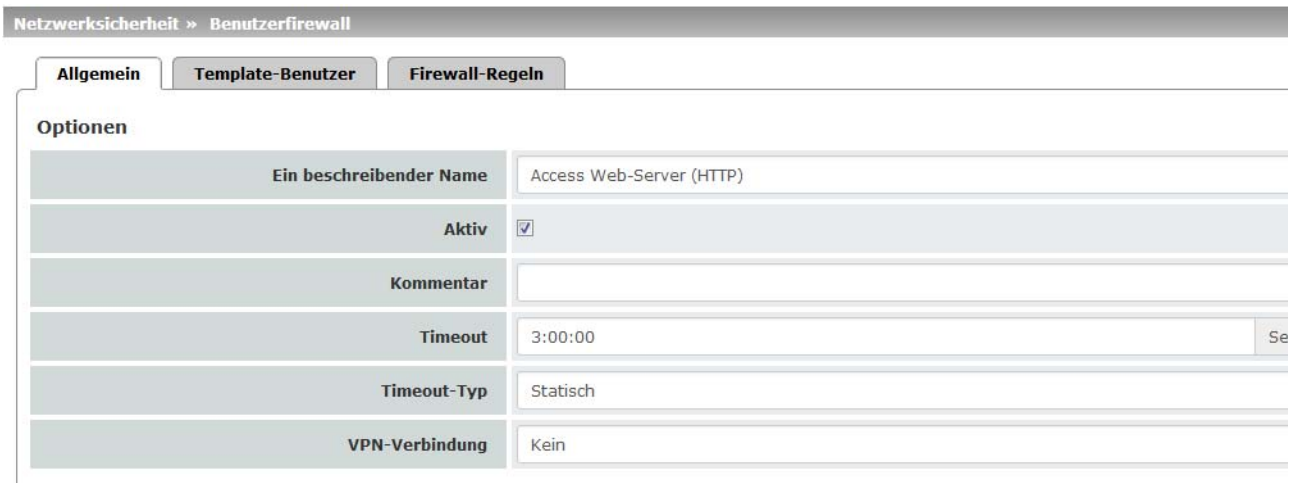


Bild 9-3 Benutzerfirewall-Template erstellen: Registerkarte *Allgemein*

Gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

- Geben Sie dem Benutzerfirewall-Template einen beschreibenden Namen.
- Geben Sie an, wie lange eine Benutzerfirewall-Regel gültig sein soll, nachdem sich ein Firewall-Benutzer angemeldet hat (Timeout-Typ beachten).
- Wenn die Regeln des Benutzerfirewall-Templates ausschließlich in einer bestimmten VPN-Verbindung gültig sein sollen, geben Sie diese an.

9.3.2 Registerkarte „Template-Benutzer“

Bild 9-4 Benutzerfirewall-Template erstellen: Registerkarte *Template-Benutzer*

Gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

- Geben Sie die Namen der Firewall-Benutzer an, für die die Regeln dieses Benutzerfirewall-Templates gelten sollen.

Die angegebenen Benutzer müssen unter **Authentifizierung >> Firewall-Benutzer >> Benutzer** definiert und angelegt werden (siehe „Firewall-Benutzer anlegen“ auf Seite 45).

ACHTUNG: Es wird nicht überprüft, ob die angegebenen Benutzernamen tatsächlich existieren. Achten Sie unbedingt auf die korrekte Schreibweise der Namen.

9.3.3 Registerkarte „Firewall-Regeln“

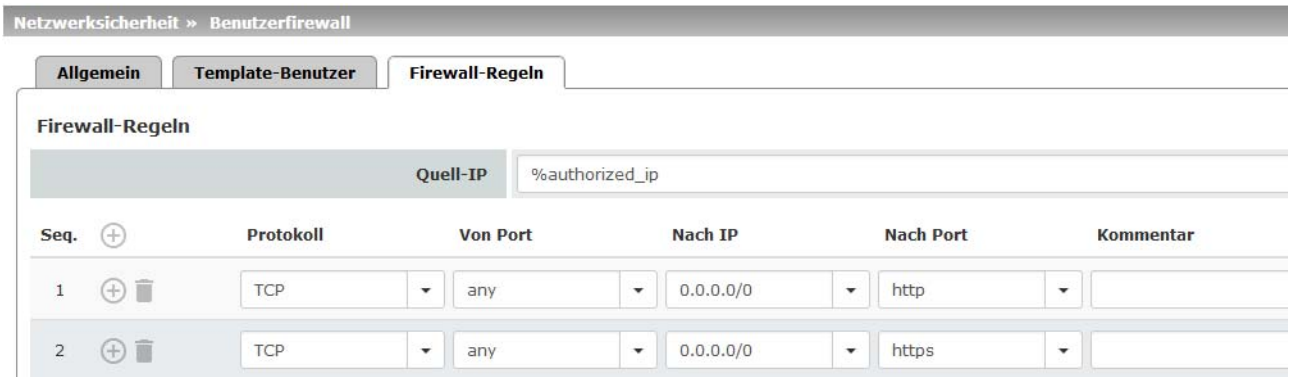


Bild 9-5 Benutzerfirewall-Template erstellen: Registerkarte *Firewall-Regeln*

Das Gerät erkennt automatisch, über welches Interface der Login erfolgt ist und wendet das Benutzerfirewall-Template entsprechend als Eingangs- (Anmeldung aus dem externen Netzwerk) oder Ausgangsregel (Anmeldung aus dem internen Netzwerk) an.

Wenn das Template mit dynamischem Timeout konfiguriert ist, setzen an dieser Stelle zugelassene UDP- und andere Netzwerkpakete (außer ICMP) den dynamischen Timeout auf den Ausgangswert zurück.

Um die Firewall-Regeln des Templates zu konfigurieren, gehen Sie wie folgt vor (siehe auch mGuard-Firmwarehandbuch):

- Geben Sie eine Quell-IP-Adresse an, von der aus Verbindungen zugelassen sind.

Wenn %authorized_ip angegeben ist, werden die Firewall-Regeln auf Datenpakete angewendet, die von der gleichen Quell-IP-Adresse gesendet wurden, von der aus sich der Benutzer angemeldet hat. Datenpakete von anderen IP-Adressen werden verworfen .

Wenn eine IP-Adresse angegeben wird, werden die Firewall-Regeln auf Datenpakete angewendet, die von dieser Quell-IP-Adresse gesendet wurden. Datenpakete von anderen IP-Adressen werden verworfen. Diese Option sollte z. B. verwendet werden, wenn sich ein Administrator am Gerät anmeldet, um die Benutzer-Firewall für einen Techniker zu aktivieren, der auf einem anderen Rechner arbeitet.

- Legen Sie Firewall-Regeln an, um den zugeordneten Firewall-Benutzern den Zugriff entsprechend der angelegten Regeln zu erlauben.

  In diesem Beispiel der Zugriff auf beliebige Webserver über die Netzwerkdienste *http* und *https*.

9.4 Als Firewall-Benutzer anmelden

Ein Firewall-Benutzer muss sich via Webbrowser per HTTPS auf der Weboberfläche des mGuard-Geräts anmelden, um die Firewall-Regeln zu aktivieren. Dies kann sowohl vom internen als auch vom externen Netzwerk aus (oder über VPN, DMZ und Einwahl) erfolgen. Um sich über das externe Netzwerk am Gerät anzumelden, muss der HTTPS-Fernzugriff auf dem mGuard-Gerät aktiviert sein (Menü **Verwaltung >> Web-Einstellungen >> Zugriff**).

Das Gerät erkennt automatisch, über welches Interface der Login erfolgt ist und wendet das Benutzerfirewall-Template entsprechend als *Eingangsregeln* (Anmeldung aus dem externen Netzwerk) oder *Ausgangsregel* (Anmeldung aus dem internen Netzwerk) an.

Um sich als Firewall-Benutzer anzumelden, gehen Sie wie folgt vor:

1. Öffnen Sie das Anmeldefenster auf der Weboberfläche des mGuard-Geräts.
2. Wählen Sie die Zugangsart „Benutzerfirewall“.
3. Geben Sie die Benutzerkennung und das Passwort des Firewall-Benutzers an.
4. Eine erfolgreiche Anmeldung wird im Anmeldefenster angezeigt.

Ergebnis

Alle Verbindungen zu einem HTTP(S)-Webserver über das ausgewählte Protokoll sind nach Anmeldung des Firewall-Benutzers bis zum Ablauf des Timeouts erlaubt.

10 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.

10.1 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.

10.1.1 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*.

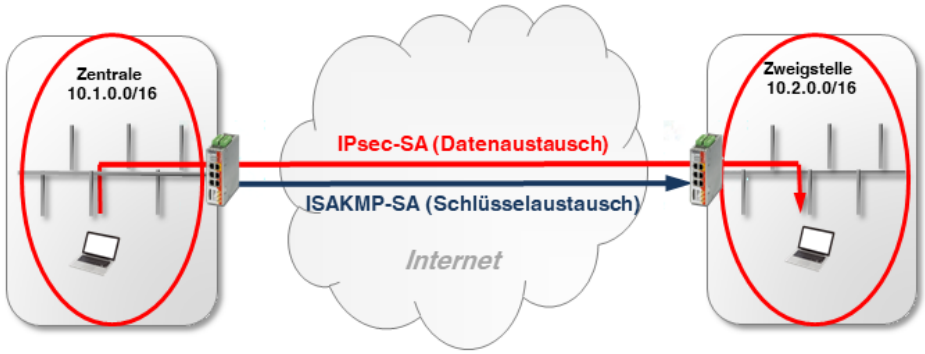


Bild 10-1 Aufbau einer IPsec-Verbindung (ISAKMP-SA und IPsec-SA)

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 10.3).

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.

10.1.2 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“**

10.2 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 11 und 12.

10.2.1 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.

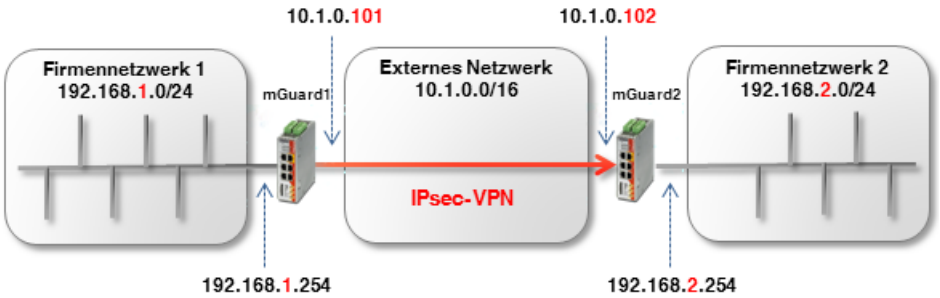


Bild 10-2 Zwei Netzwerke über IPsec-VPN verbinden

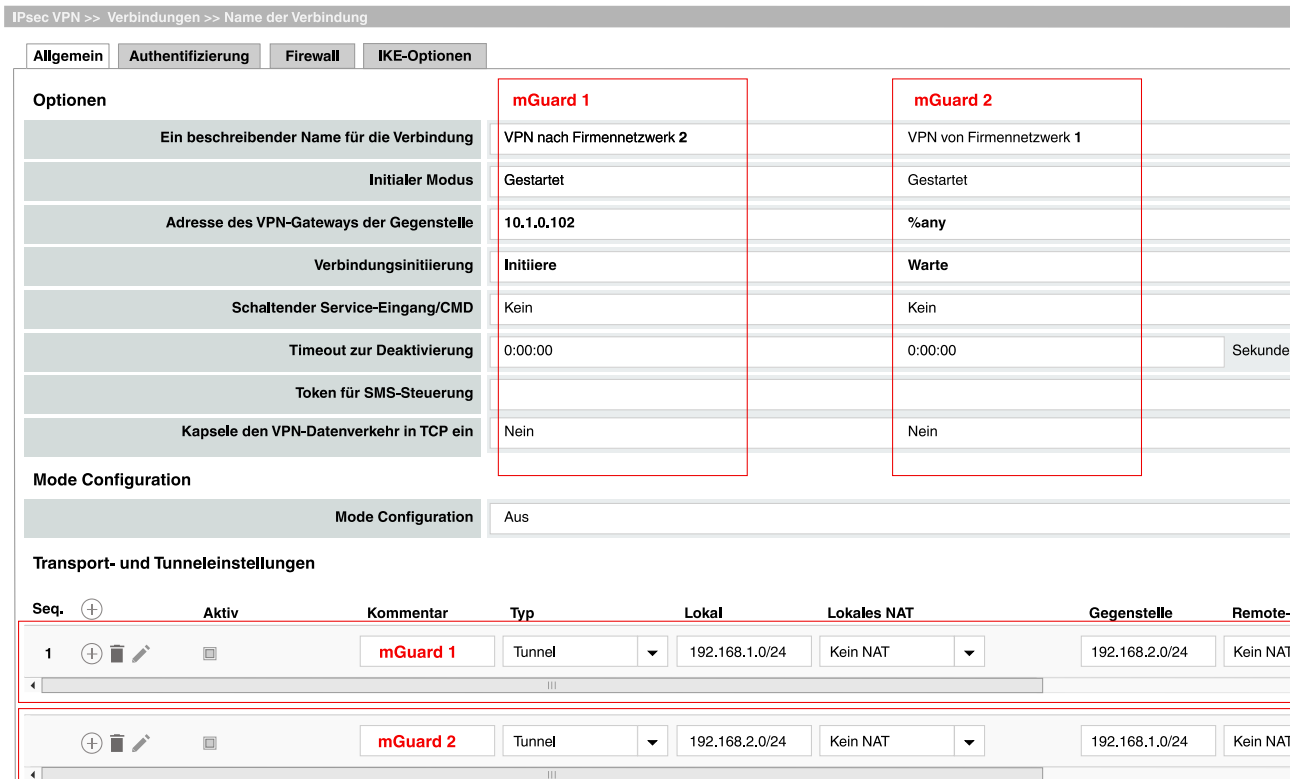


Bild 10-3 Menü: IPsec VPN >> Verbindungen >> (Edit) >> Allgemein

10.3 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.

10.3.1 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.

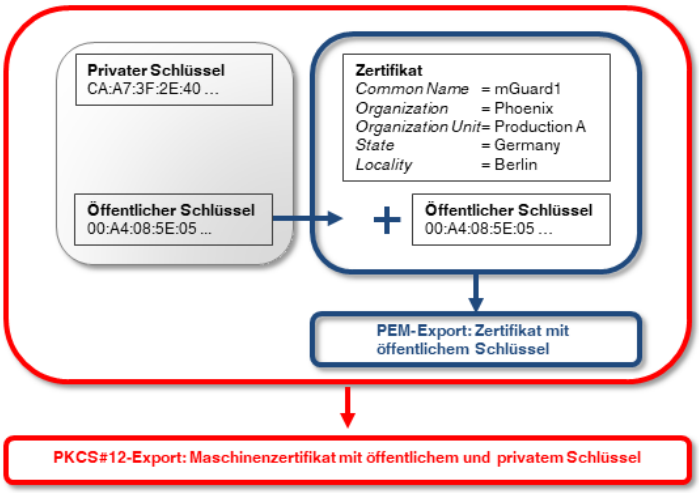


Bild 10-4 PEM- und PKCS#12-Exporte von X.509-Zertifikaten mit öffentlichem bzw. öffentlichem und privatem Schlüssel

10.3.2 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 11.3, „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 10-5).
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 10-5).

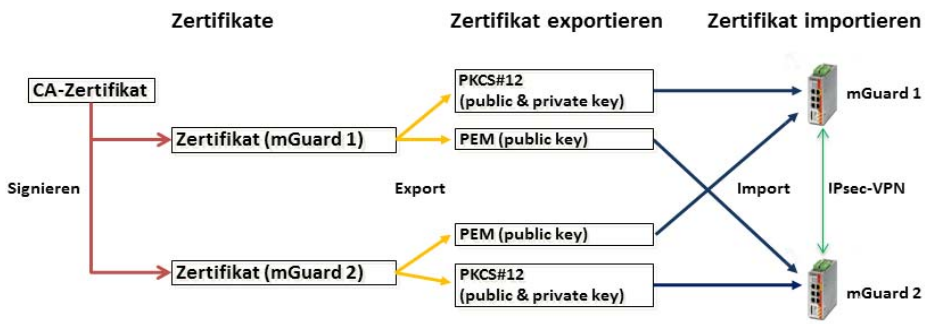


Bild 10-5 Benötigte Zertifikate in einer IPsec-VPN-Verbindung

Tabelle 10-1 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 11, „VPN-Kickstart – Zwei Netzwerke über IPsec-VPN miteinander verbinden“ beschrieben.

10.4 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“).

10.4.1 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.

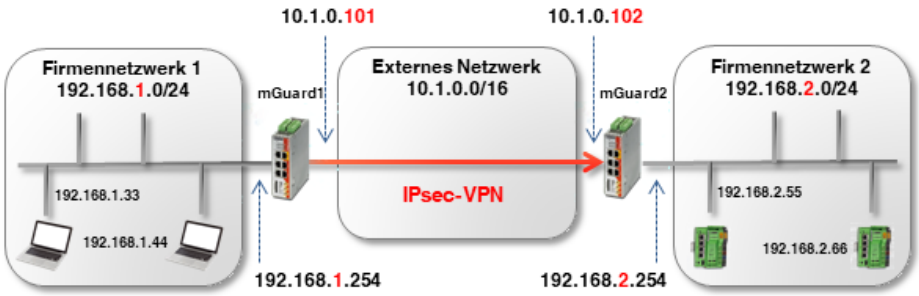


Bild 10-6 VPN-Verbindung zwischen zwei Netzwerken mit Firewall

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 8).

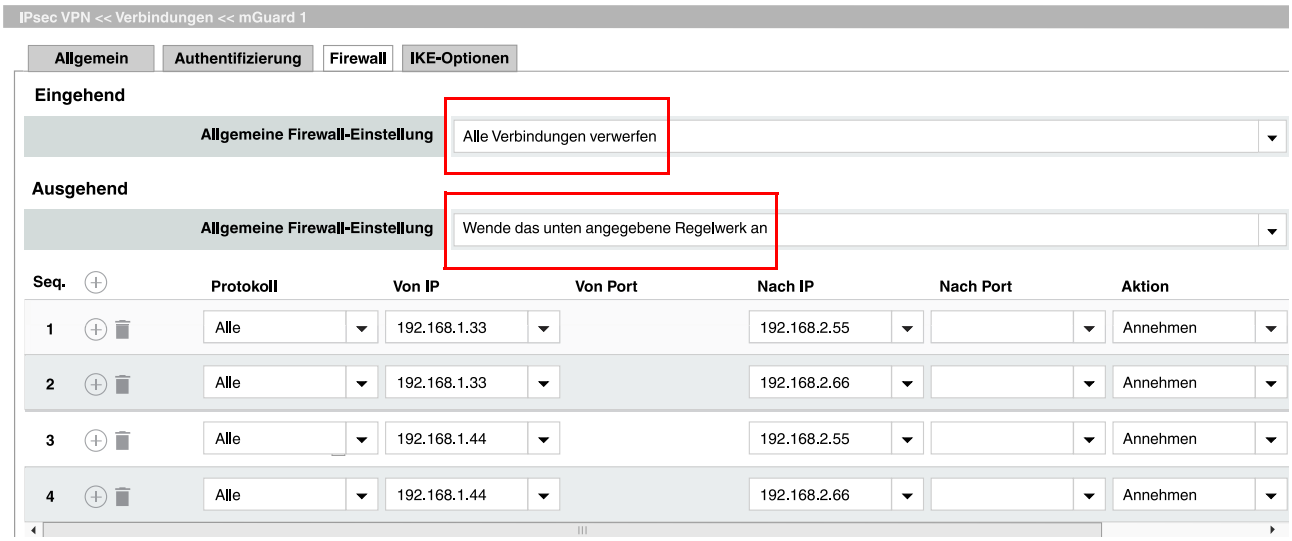


Bild 10-7 *mGuard 1*: IPsec VPN >> Verbindungen >> (Edit) >> Firewall

10.5 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“).

10.6 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.

10.6.1 VPN-Initiator hinter NAT-Router

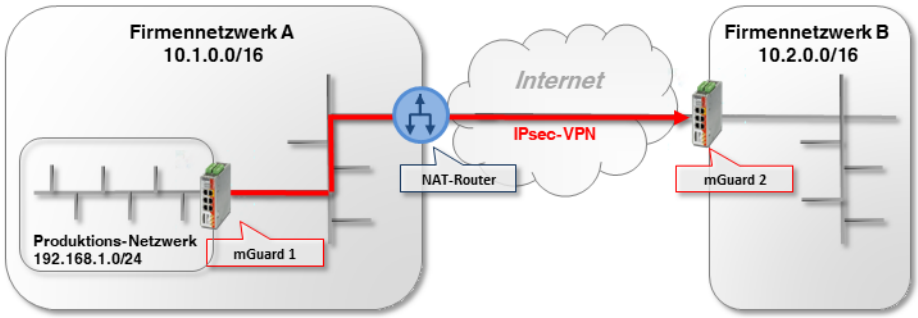


Bild 10-8 VPN-Initiator hinter NAT-Router

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 10.7).

10.6.2 VPN-Responder hinter NAT-Router

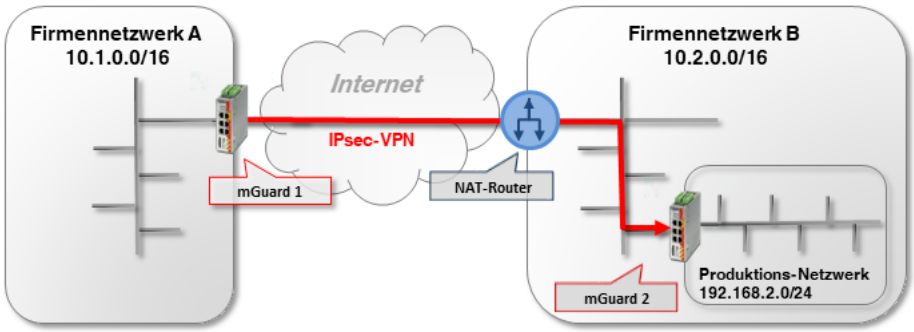


Bild 10-9 VPN-Responder hinter NAT-Router

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.

10.6.3 VPN-Initiator und -Responder hinter NAT-Router

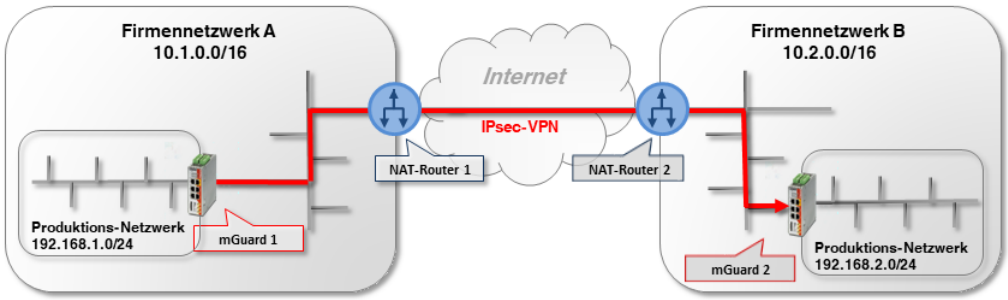


Bild 10-10 VPN-Initiator und VPN-Responder hinter NAT-Router

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.

10.7 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**).

10.7.1 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 11 und 12 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 10.3).

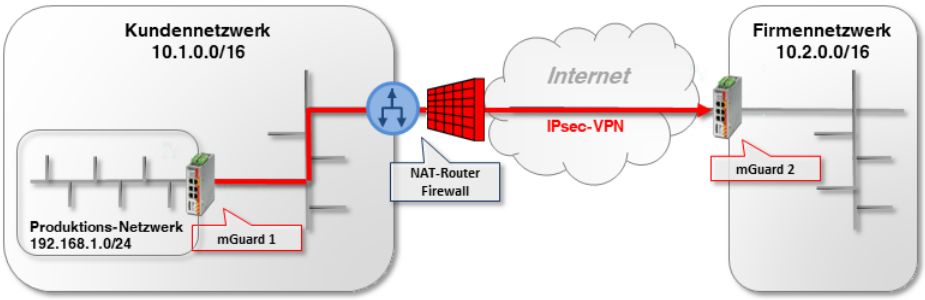


Bild 10-11 VPN-Initiator hinter NAT-Router und Firewall

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.

10.7.2 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 10.7.3).

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.

10.7.3 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 10.7.2).

10.8 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).

10.8.1 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.

10.9 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.

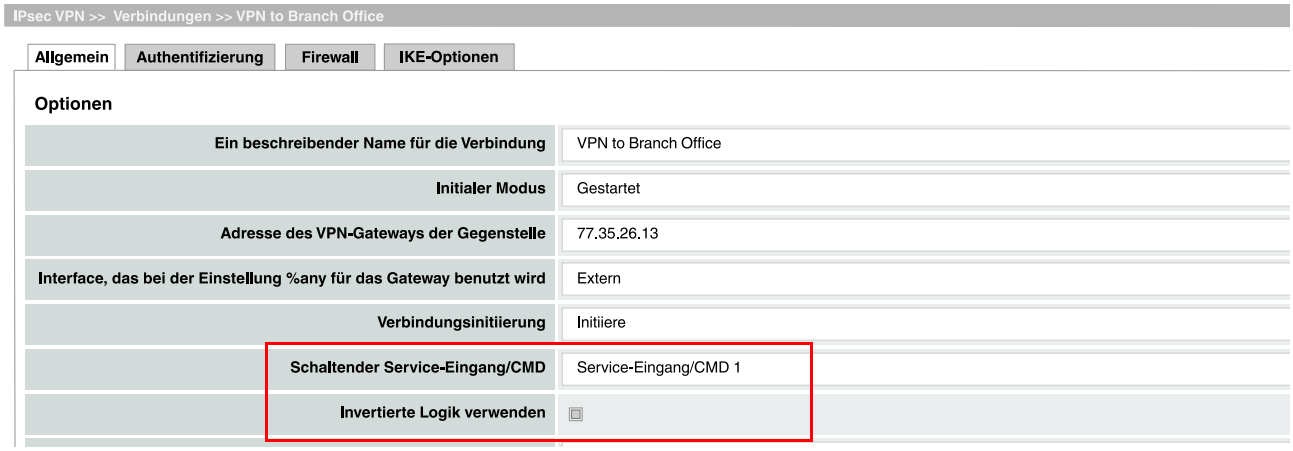


Bild 10-12 IPsec VPN >> Verbindungen: Der VPN-Verbindung wird ein Service-Eingang zugeordnet, über den sie per Taster oder Ein-/Aus-Schalter gestartet oder gestoppt werden kann.

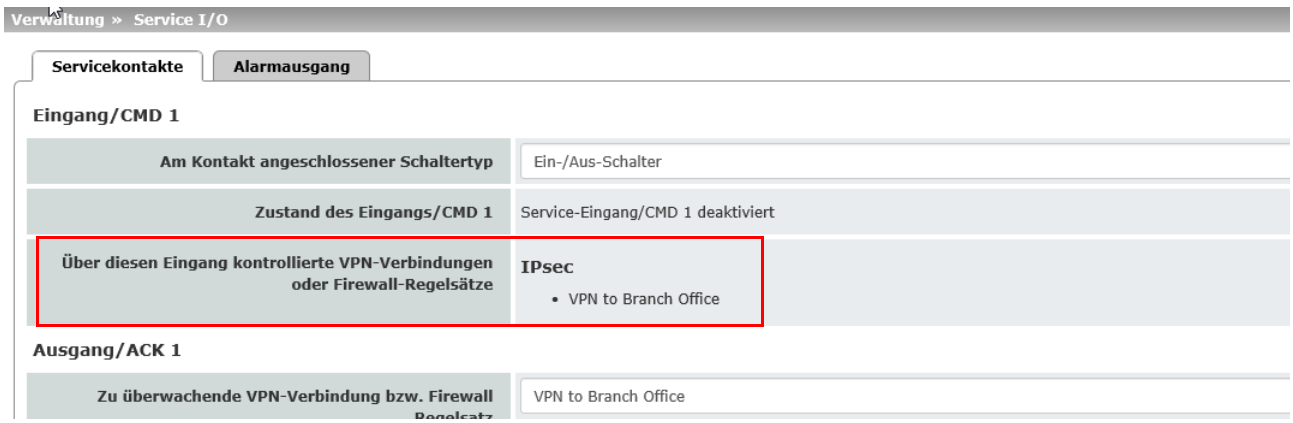


Bild 10-13 Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen oder Firewall-Regelsätze über einen Service-Eingang geschaltet werden.

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.

11 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.

11.1 Einleitung

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

11.1.1 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 13, „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.

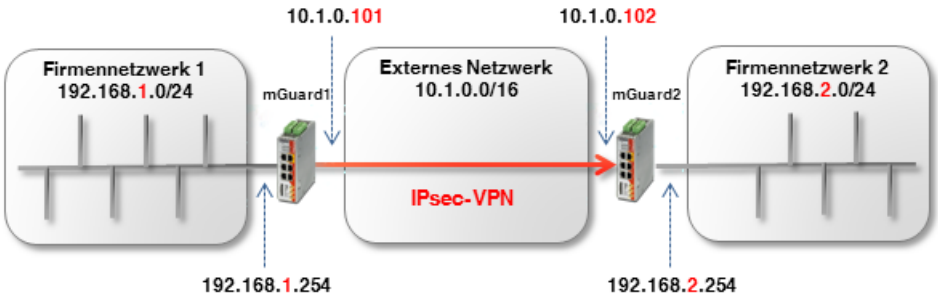


Bild 11-1 Zwei Netzwerke über IPsec-VPN verbinden

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 11-2). 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.

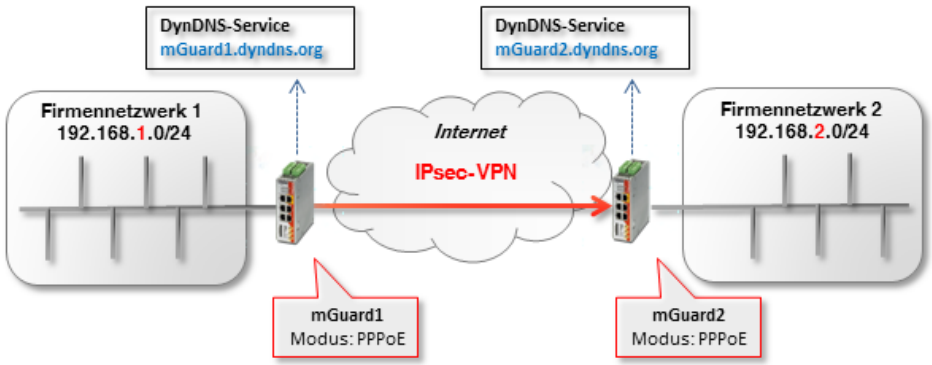


Bild 11-2 Festlegung der Hostnamen für die mGuard-Geräte mittels DynDNS. Da die Initiierung der VPN-Verbindung durch *mGuard 1* erfolgt, benötigt dieser keine DynDNS-Adresse.

11.1.2 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*).

11.1.3 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

11.2 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.)

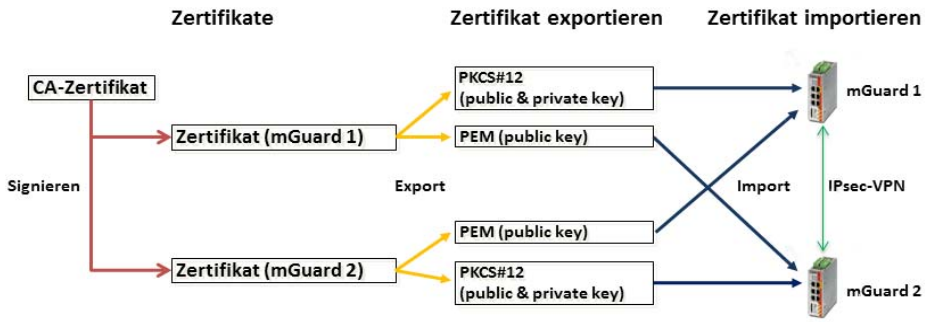
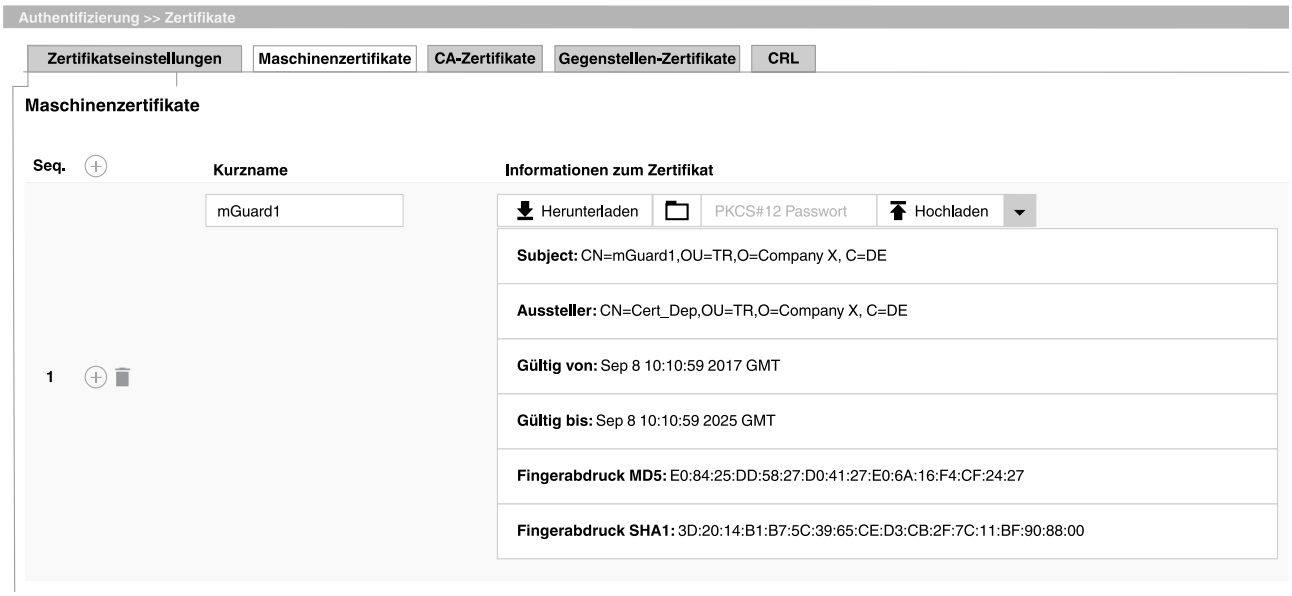


Bild 11-3 Beteiligte Zertifikate in einer IPsec-VPN-Verbindung

Tabelle 11-1 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*

11.3 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.*

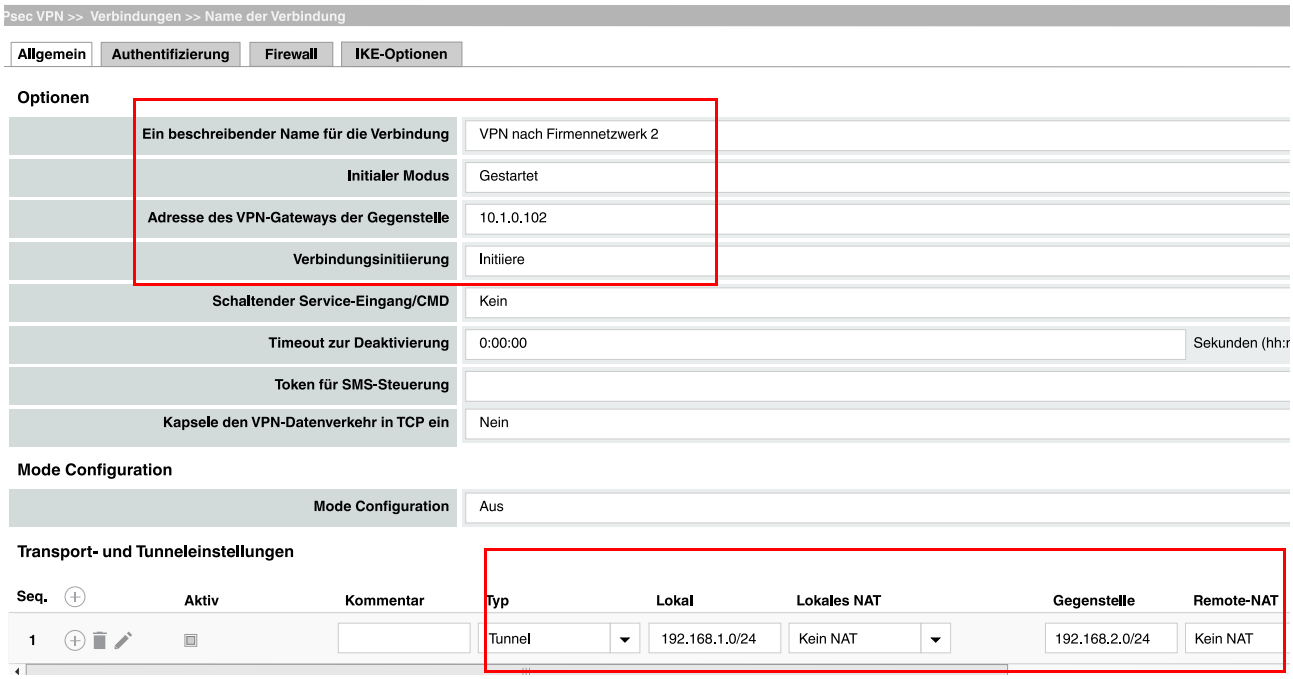
11.4 VPN-Verbindung mGuard1 anlegen

11.4.1 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.

11.4.2 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.

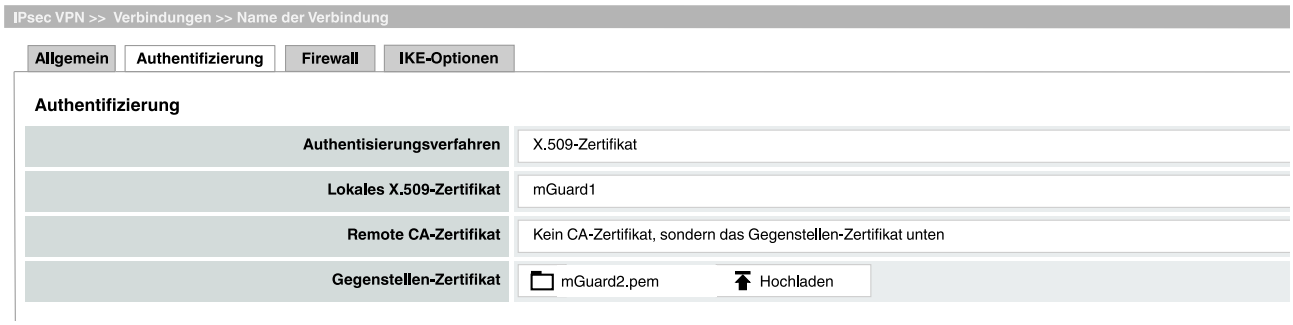
Sektion „Optionen“

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.

11.4.3 Authentifizierung der VPN-Verbindung konfigurieren



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

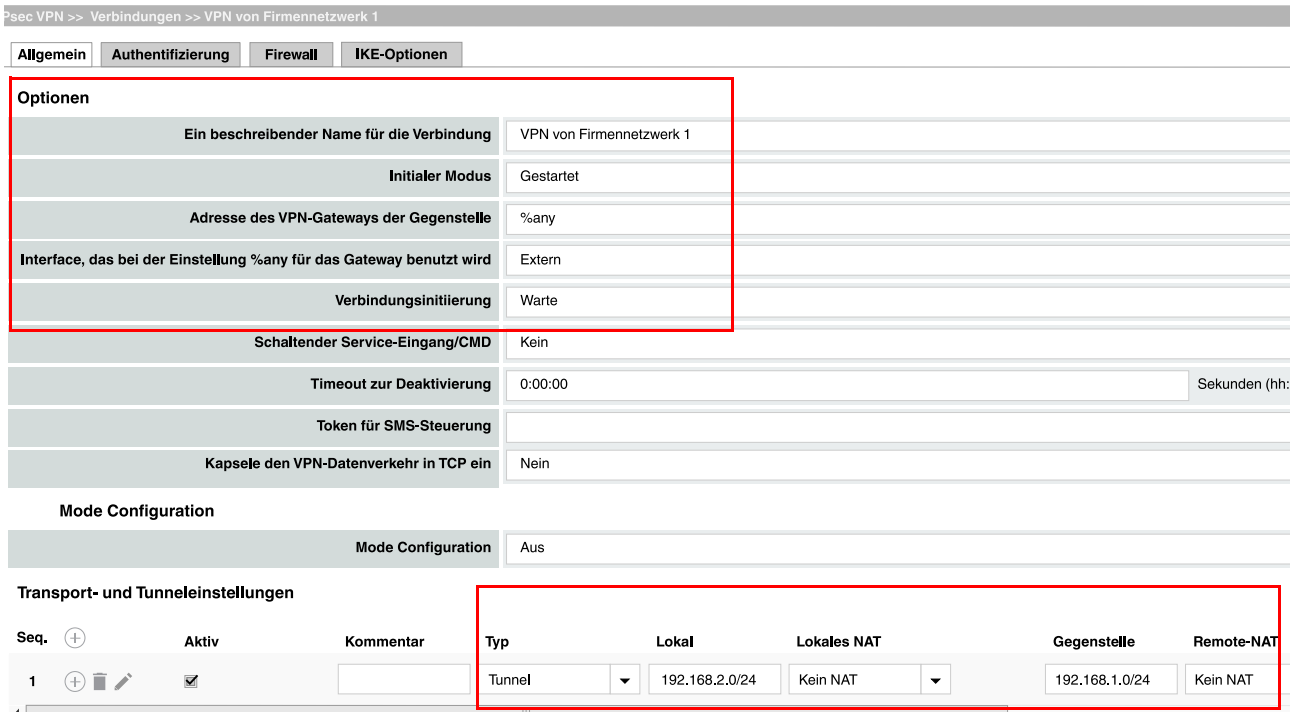
1. Gehen Sie zu **IPsec VPN >> Verbindungen** (Registerkarte *Authentifizierung*)
2. Wählen Sie unter **Lokales X.509-Zertifikat** das Zertifikat aus, das Sie zuvor als Maschinenzertifikat für *mGuard1* in das Gerät importiert haben (*mGuard1*).
3. Wählen Sie unter **Remote CA-Zertifikat** die Option *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.

11.5 VPN-Verbindung mGuard2 anlegen

11.5.1 Voraussetzung

Es gelten die gleichen Voraussetzungen wie bei mGuard1 (siehe „Voraussetzung“ auf Seite 72).

11.5.2 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*)

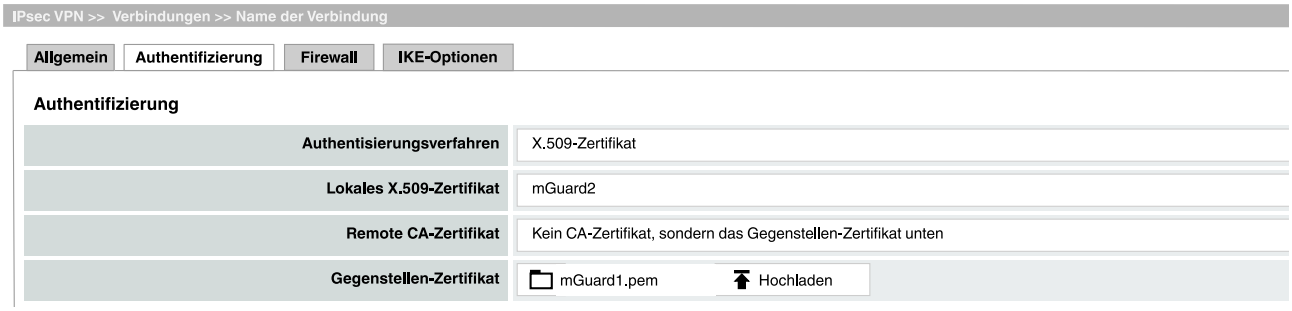
Sektion „Optionen“

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.

11.5.3 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.

11.6 VPN-Verbindung testen

11.6.1 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).

11.6.2 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.

12 VPN-Verbindungen mit variierenden Netzwerkmodi konfigurieren

Dokument-ID: 108410_de_00

Dokument-Bezeichnung: AH DE MGUARD IPSEC VPN NW MODE

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 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**.

12.1 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.

12.2 VPN-Transportverbindung (Stealth <-> Stealth)

12.2.1 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.

12.2.2 Beispiel

Zwei Clients (Hosts) im gleichen Netzwerk sollen über eine IPsec-VPN-Verbindung miteinander verbunden werden, um einen permanenten verschlüsselten Datenaustausch zu gewährleisten. Bild 12-1 zeigt die Netzwerkkonfiguration der beteiligten Clients.

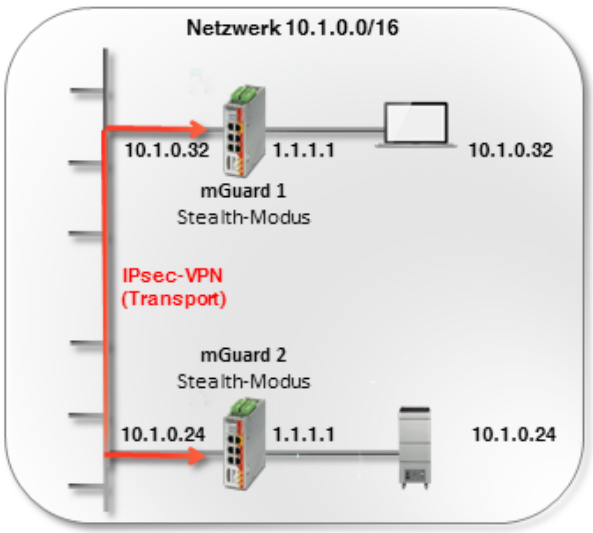


Bild 12-1 VPN-Transportverbindung im Netzwerkmodus *Stealth*

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).

12.2.3 VPN-Verbindung konfigurieren

Bild 12-2 zeigt die Konfiguration der mGuard-Geräte (zur besseren Übersicht in einer Abbildung). Die Transport- und Tunneleinstellungen sind auf beiden Geräten gleich.

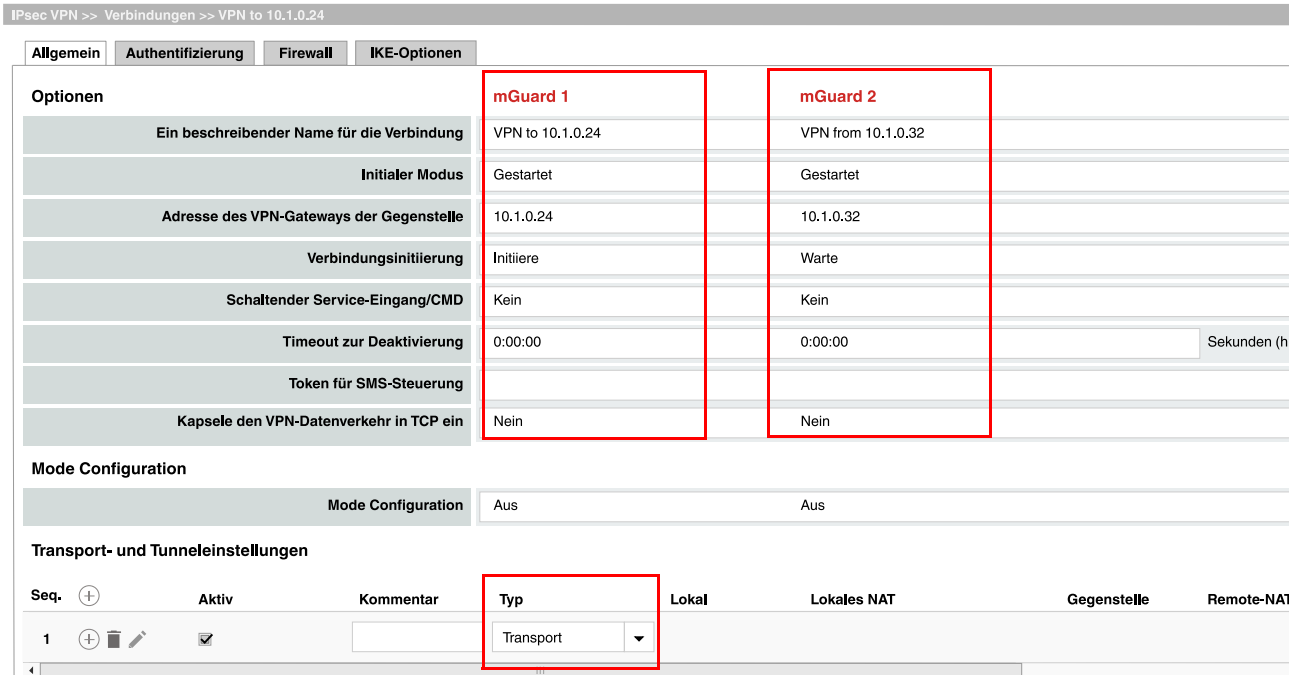


Bild 12-2 VPN-Verbindung (Typ: *Transport)*: Stealth-Modus <-> Stealth-Modus

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 12-2 bzw. Tabelle 12-1.

Tabelle 12-1 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
	Verbindungsinitiierung	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*.

12.3 VPN-Tunnelverbindung (Router <-> Router)

12.3.1 Einleitung

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

12.3.2 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 13, „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.

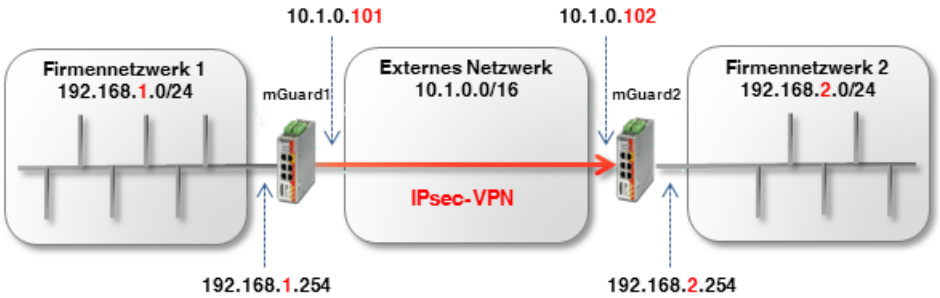


Bild 12-3 Zwei Netzwerke über IPsec-VPN verbinden

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 12-2 Netzwerkkonfiguration der Interfaces

Parameter	mGuard 1	mGuard 2
Externe IP-Adresse	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
Interne IP-Adresse	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 12-4). 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 initiierende 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 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.

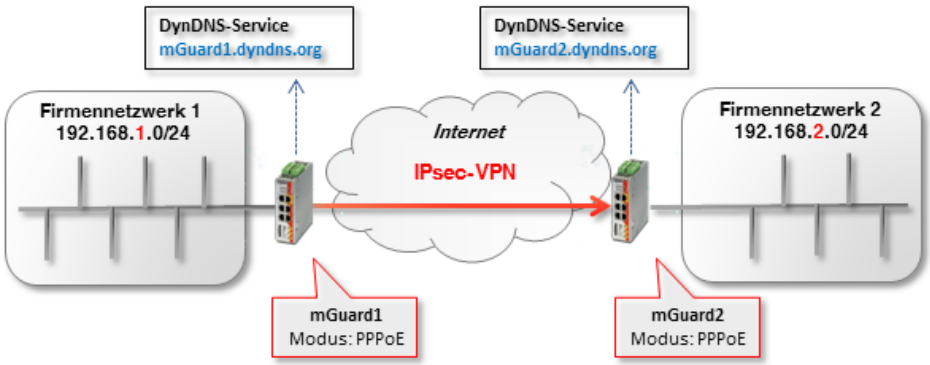


Bild 12-4 Zwei Netzwerke über IPsec-VPN verbinden (*Router/PPPoE* <-> *Router/PPPoE*). Festlegung der Hostnamen für die mGuard-Geräte mittels DynDNS. (Da die Initiierung der VPN-Verbindung durch *mGuard 1* erfolgt, benötigt dieser in diesem Beispiel prinzipiell keine DynDNS-Adresse.)

12.3.3 VPN-Verbindung konfigurieren

Konfigurieren Sie die VPN-Verbindung gemäß Bild 12-5 und 12-6 bzw. Tabelle 12-3.

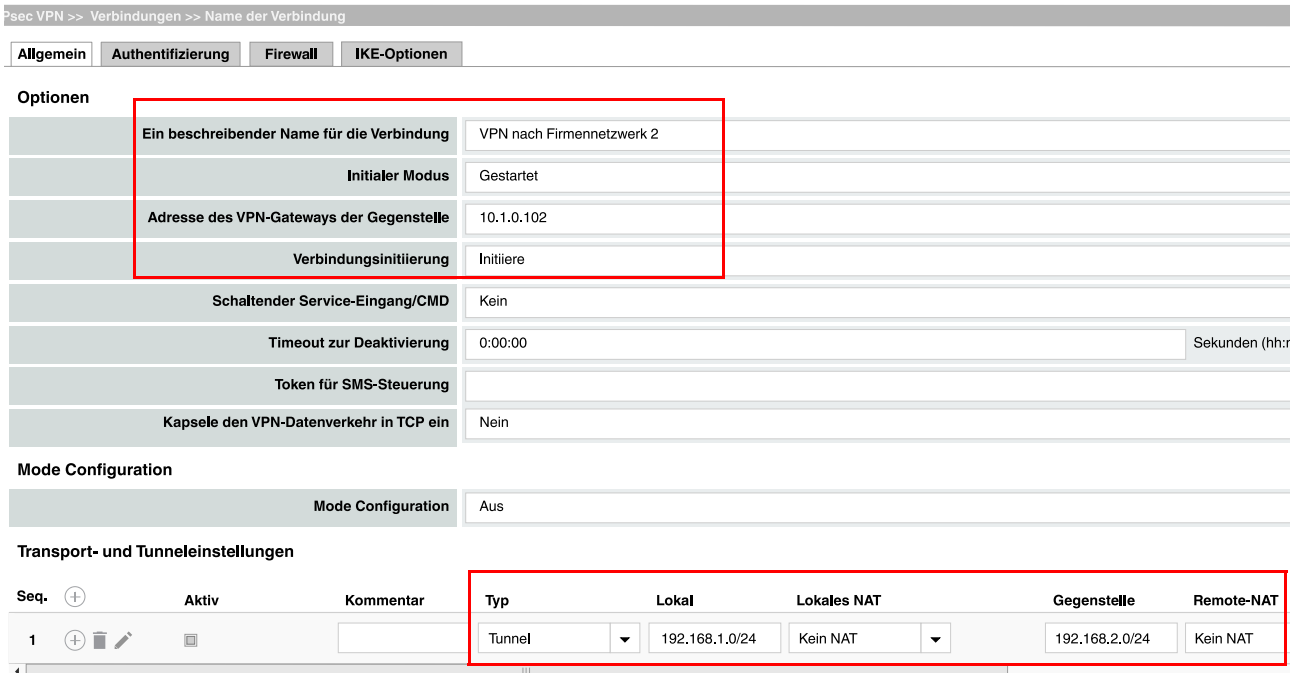


Bild 12-5 *mGuard 1* (*Initiator*): Konfiguration der VPN-Verbindung

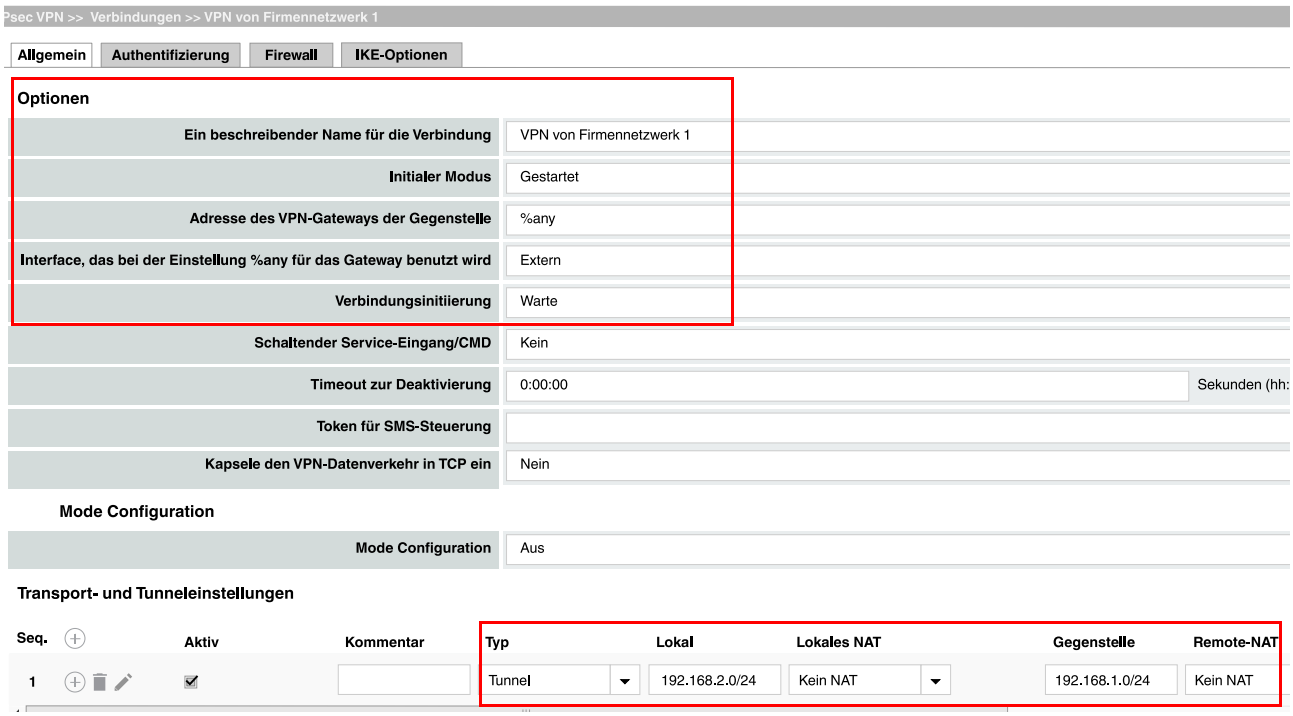


Bild 12-6 *mGuard 2* (*Responder*): Konfiguration der VPN-Verbindung

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 12-5 und 12-6 bzw. Tabelle 12-3.

Tabelle 12-3 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).

12.4 VPN-Tunnelverbindung (Single Stealth <-> Router)

12.4.1 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.

12.4.2 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.

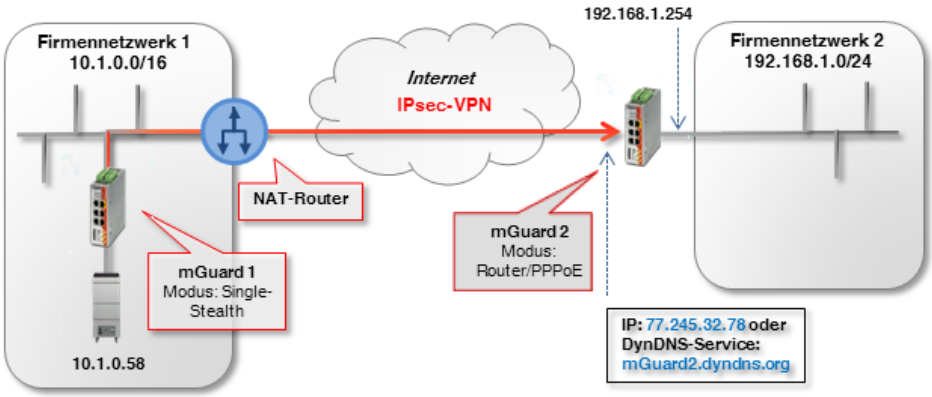


Bild 12-7 Zwei Netzwerke über IPsec-VPN verbinden (*Single-Stealth <-> Router*)

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 initiierende 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.

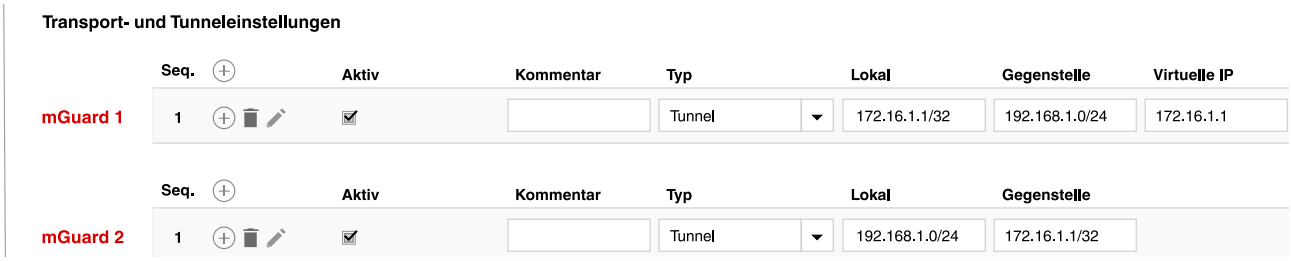
Aktivieren Sie in diesem Fall die **DynDNS-Überwachung** (**IPsec VPN >> Global >> DynDNS-Überwachung**) in der VPN-Verbindung des initiierenden Geräts (*mGuard 1*). Andernfalls weiß das Gerät nicht, wenn sich die IP-Adresse der Gegenstelle geändert hat und der Aufbau der VPN-Verbindung schlägt fehl.

12.4.3 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.



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 12-4.

Tabelle 12-4 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	-----

12.5 VPN-Tunnelverbindung (Multi Stealth <-> Router)

12.5.1 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.

12.5.2 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.

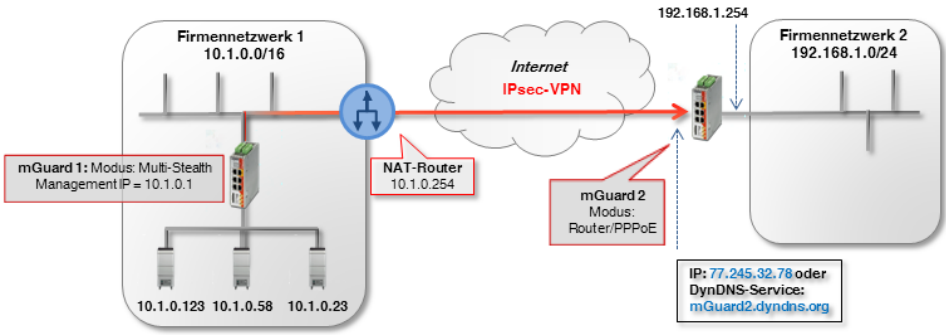


Bild 12-8 Zwei Netzwerke über IPsec-VPN verbinden (Multi-Stealth <-> Router)

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 12.4.1).

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

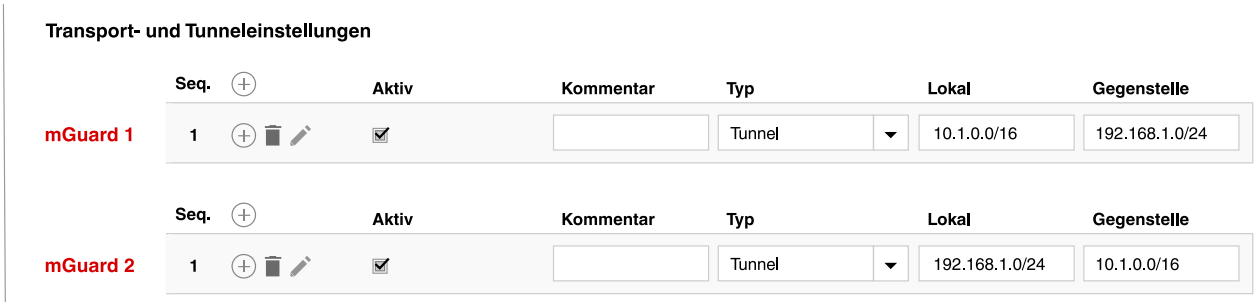
Tabelle 12-5 Netzwerkkonfiguration der Interfaces

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

12.5.3 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.



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 12-6.

Tabelle 12-6 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

13 NAT in VPN-Verbindungen verwenden

Dokument-ID: 108411_de_00
Dokument-Bezeichnung: AH DE MGUARD IPSEC VPN NAT

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 Konfigurationen von IPsec-VPN-Verbindungen unter Verwendung von 1:1-NAT und IP-Maskierung (IP-Masquerading) beschrieben.

13.1 Einleitung

Eine VPN-Verbindung kann in der Regel nur zwischen unterschiedlichen Netzwerken (z. B. Netz A: 192.168.**1**.0/24 <-> Netz B: 192.168.**2**.0/24).

Werden an zwei Standorten die gleichen internen Netze (z. B. 192.168.**1**.0/24) verwendet, können folgende Probleme auftreten:

1. Wenn die Standorte über einen VPN-Tunnel verbunden sind, würde dies zu Routing-Problemen führen. Es wäre nicht klar, für welches Netz Pakete, die an IP-Adressen des auf beiden Seiten gleichen internen Netzwerks gesendet werden, bestimmt sind.

   Das Problem lässt sich durch die Verwendung von **1:1-NAT** umgehen (siehe Kapitel 13.2).
2. Wenn sich mehrere Standorte mit teilweise gleichen internen Netzen über einen VPN-Tunnel mit einem zentralen Standort verbinden, würde dies ebenfalls zu Routing-Problemen führen. Das Problem lässt sich durch die Verwendung von **1:1-NAT** oder zum Teil mittels **IP-Maskierung** umgehen (siehe Kapitel 13.3 und 13.5).

13.1.1 1:1-NAT

1:1-NAT bedeutet, dass der **Netzwerk-Teil** einer IP-Adresse einem anderen Netzwerk zugeordnet wird und der **Host-Teil** unverändert bleibt (z. B. **192.168.1.102**/24 <-> **192.168.2.102**/24). Der Netzwerkteil wird durch die Subnetzmaske definiert.

Dabei wird ein *Reales Netzwerk* (z. B. das interne Netzwerk) einem *Virtuellen Netzwerk* zugeordnet, um vorhandene Netzwerküberschneidung zu umgehen. Der Aufbau von VPN-Tunneln erfolgt dann nicht mehr über die *Realen* sondern über *Virtuelle Netzwerke*.

13.1.2 IP-Maskierung

IP-Maskierung (*IP-Masquerading*) ist eine besondere Form des NAT. Sie muss z. B. auf Gateways aktiviert werden, die private Netzwerke mit dem Internet verbinden, um auf das Internet zugreifen zu können.

Beim Zugriff auf eine Webseite von einem internen Netzwerk ersetzt das Gateway (NAT-Router) die private IP-Adresse des Absenders (z. B. 192.168.1.100) durch seine eigene öffentliche IP-Adresse (z. B. 77.245.32.78). Damit weiß der Ziel-Webserver, an welche öffentliche Adresse er die Antwort zurückschicken muss.

Die Antwort des Webservers an den NAT-Router (77.245.32.78) wird dann von diesem durch die IP-Adresse des ursprünglichen Absenders ersetzt (192.168.1.100) und an den Client im internen Netzwerk weitergeleitet.

IP-Maskierung wird nur in eine Richtung angewendet, z. B. aus dem internen in ein externes Netzwerk bzw. das Internet. Ein Client im internen Netzwerk (z. B. 192.168.1.100) könnte dann auf Ziele im externen Netzwerk bzw. auf Webseiten im Internet zugreifen, aber er wäre nicht über seine private IP-Adresse aus dem externen Netzwerk oder dem Internet erreichbar.

IP-Maskierung in VPN-Verbindungen

IP-Maskierung in VPN-Verbindungen bietet die gleiche Funktionalität, jedoch innerhalb einer VPN-Verbindung.

Wenn Datenpakete durch den VPN-Tunnel an ein Remote-Netzwerk gesendet werden, ersetzt das mGuard-Gerät die IP-Adresse des Absenders durch eine bestimmte, einzelne IP-Adresse und kehrt die Maskierung beim Empfang der Antwort aus dem Remote-Netzwerk um.

Der große Vorteil ist, dass das gesamte reale (lokale) Netzwerk von einer einzigen IP-Adresse *maskiert* wird.

Wenn mehrere VPN-Verbindungen an einem zentralen VPN-Gateway enden, reduziert diese Funktion den benötigten Adressraum für die VPN-Verbindungen und macht die VPN-Konfiguration übersichtlicher.

13.2 Standorte mit gleichen internen Netzen miteinander verbinden (1:1-NAT)

13.2.1 Beispiel

Zwei Standorte mit dem gleichen internen Netzwerk (192.168.1.0/24) sollen über einen VPN-Tunnel miteinander verbunden werden. Dazu muss auf beiden mGuard-Geräten **Lokales NAT für IPsec-Tunnelverbindungen (1:1-NAT)** verwendet werden.

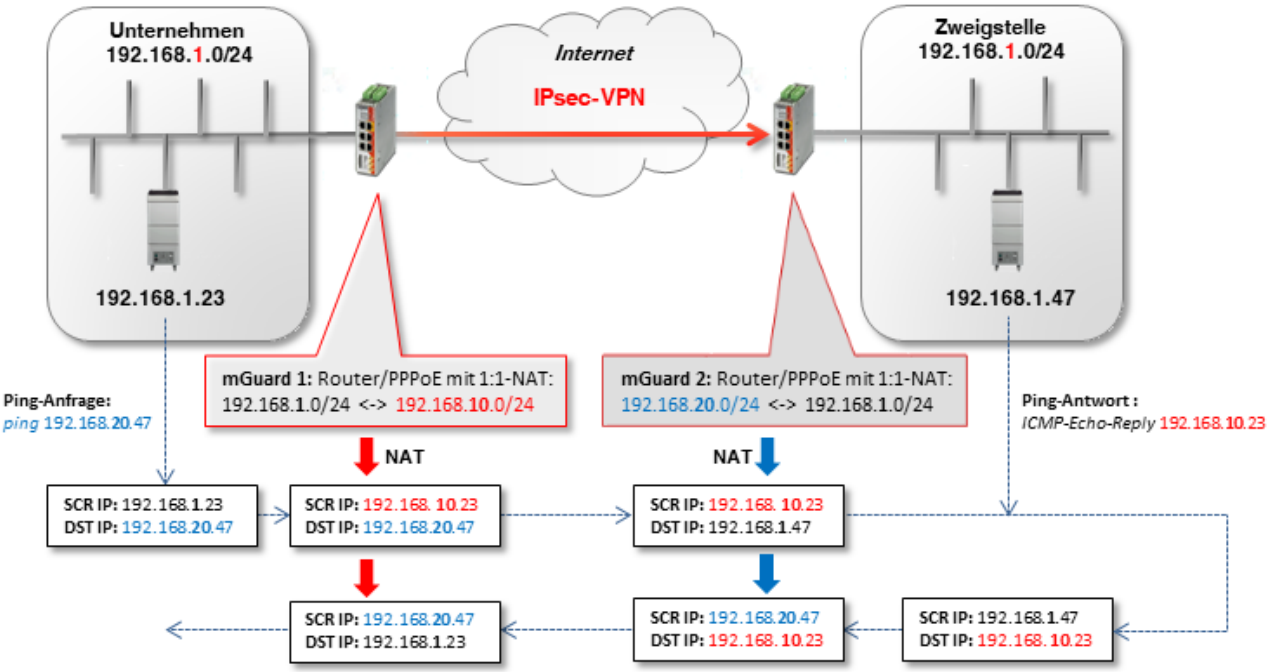


Bild 13-1 Gleiche interne Netze: Ping-Anfrage durch einen VPN-Tunnel unter Verwendung von lokalem 1:1-NAT

- **mGuard 1** macht 1:1-NAT: 192.168.**1**.0/24 <-> 192.168.**10**.0/24.
  Der Netzwerkteil wird umgeschrieben und der Hostteil beibehalten. Damit sind die Clients im Unternehmensnetzwerk durch den VPN-Tunnel im *Virtuellen Netzwerk* 192.168.**10**.0/24 erreichbar.
- **mGuard 2** macht ebenfalls 1:1-NAT: 192.168.**1**.0/24 <-> 192.168.**20**.0/24.
  Die Clients im Zweigstellennetzwerk sind durch den VPN-Tunnel im *Virtuellen Netzwerk* 192.168.**20**.0/24 erreichbar.

13.2.2 VPN-Verbindung konfigurieren

Der VPN-Tunnel muss zwischen *Virtuellen Netzwerken* aufgebaut werden. Dazu wird auf beiden Geräten ein lokales 1:1-NAT durchgeführt.

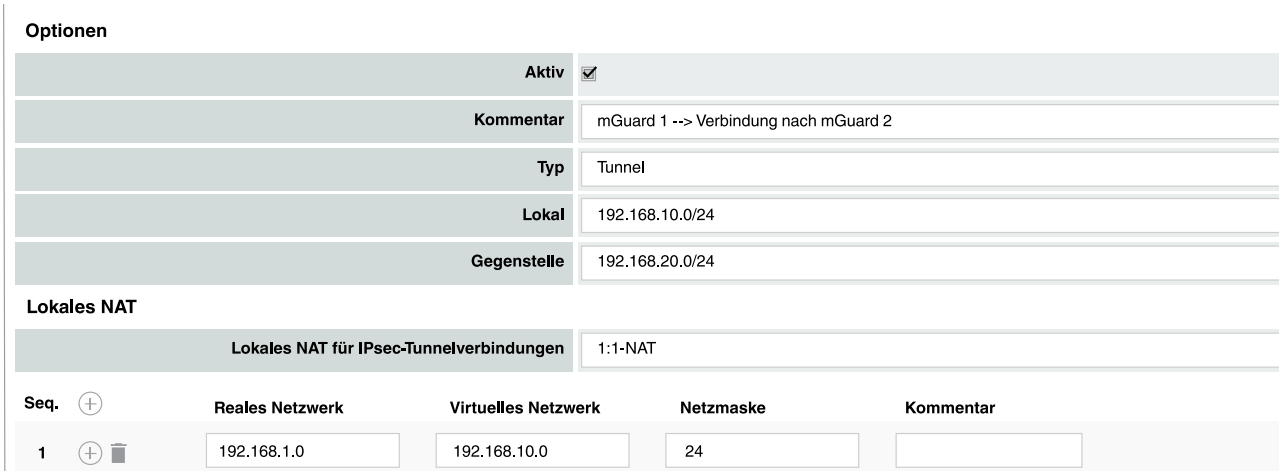


Bild 13-2 **mGuard 1**: IPsec VPN >> Allgemein (Tunneleinstellungen mit 1:1-NAT)

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 ✎.
4. Klicken Sie unter **Transport- und Tunneleinstellungen** auf das Icon ✎.
5. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 13-1 und Bild 13-2.

Tabelle 13-1 VPN-Verbindung konfigurieren

Sektion	Parameter	Unternehmen / mGuard 1	Zweigstelle / mGuard 2
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein			
Optionen	**Ein beschreibender Name für die Verbindung**	VPN nach Zweigstelle	VPN von Unternehmen
	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 >> (Edit) >> Allgemein			
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel
	Lokal	192.168.**10**.0/24	192.168.**20**.0/24
	Gegenstelle	192.168.**20**.0/24	192.168.**10**.0/24
Lokales NAT	**Lokales NAT für IPsec-Tunnelverbindungen**	1:1-NAT	1:1-NAT
	Reales Netzwerk	192.168.**1**.0	192.168.**1**.0
	Virtuelles Netzwerk	192.168.**10**.0	192.168.**20**.0
	Netzmaske	24	24

Ergebnis

– Pakete an das Unternehmensnetzwerk im internen Netz von *mGuard 1* müssen an das *Virtuelle Netzwerk* 192.168.**10**.0/24 gesendet werden.
– Pakete an das Zweigstellennetzwerk im internen Netz von *mGuard 2* müssen an das *Virtuelle Netzwerk* 192.168.**20**.0/24 gesendet werden.

13.3 Standorte mit gleichen internen Netzen mit Zentrale verbinden (1:1-NAT)

13.3.1 Beispiel

Zwei Standorte, die das gleiche interne Netzwerk verwenden (192.168.1.0/24), sollen gleichzeitig über jeweils einen VPN-Tunnel mit der Unternehmens-Zentrale verbunden werden. Dazu muss auf beiden mGuard-Geräten **Lokales NAT für IPsec-Tunnelverbindungen (1:1-NAT)** verwendet werden.

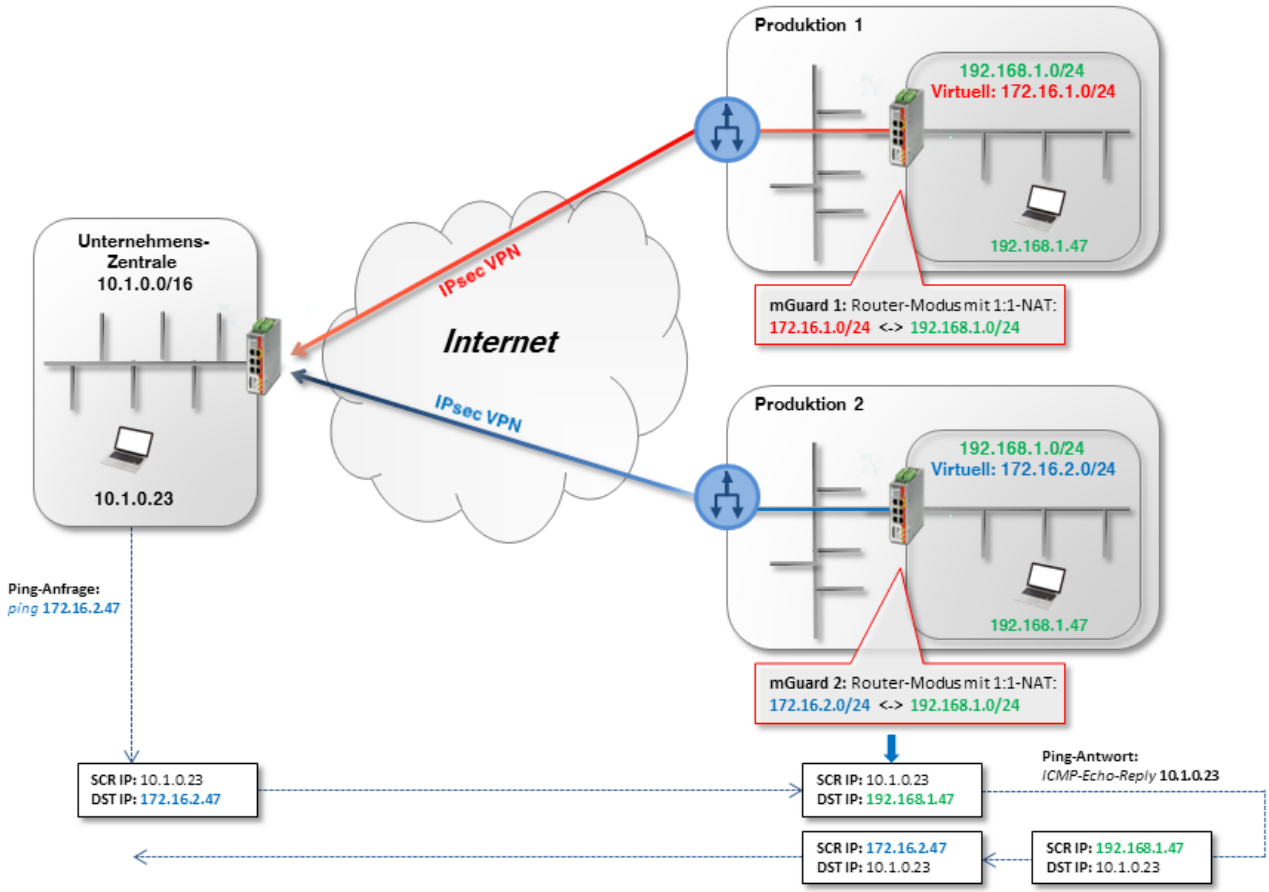


Bild 13-3 (Beispiel *mGuard 2*) Gleiche interne Netze: Ping-Anfrage (nach Produktion 2) aus der Unternehmens-Zentrale durch den VPN-Tunnel unter Verwendung von lokalem 1:1-NAT

- **mGuard 1** macht 1:1-NAT: 192.168.1.0/24 <-> 172.16.**1**.0/24).
  Die Clients in seinem internen Netzwerk (**Produktion 1**) sind durch den VPN-Tunnel im *Virtuellen Netzwerk* 172.16.**1**.0/24 erreichbar.
- **mGuard 2** macht 1:1-NAT (192.168.1.0/24 <-> 172.16.**2**.0/24).
  Die Clients in seinem internen Netzwerk (**Produktion 2**) sind durch den VPN-Tunnel im *Virtuellen Netzwerk* 172.16.**2**.0/24 erreichbar.

VPN-Verbindung konfigurieren

Auf dem mGuard-Gerät der Zentrale müssen zwei VPN-Verbindungen konfiguriert und jeweils ein lokales 1:1-NAT durchgeführt werden. In den Tunneleinstellungen muss dort als Gegenstelle jeweils das *Virtuelle Netzwerk* von mGuard **1** bzw. **2** angegeben werden (172.16.**1**.0/24 bzw. 172.16.**2**.0/24).

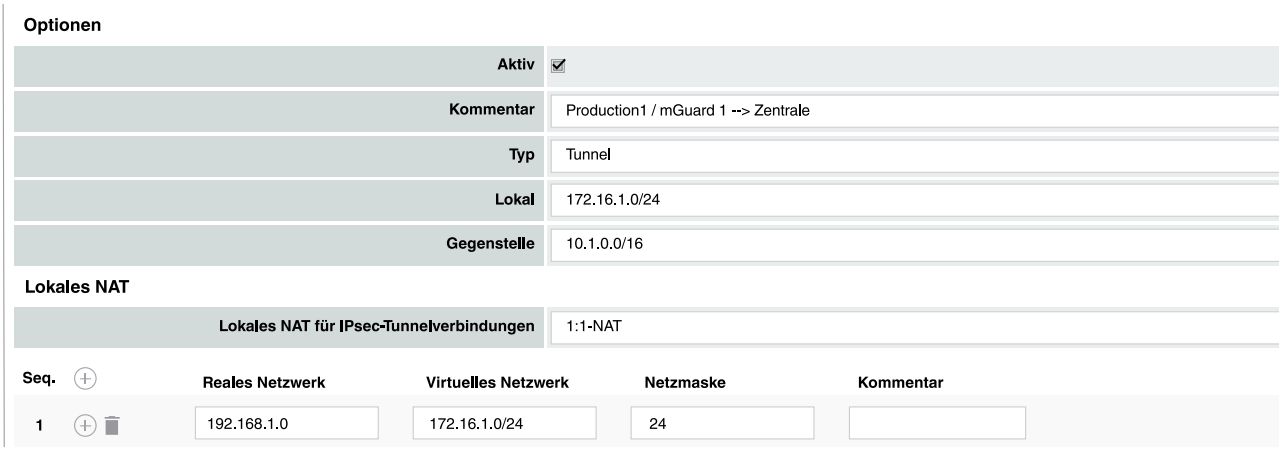


Bild 13-4 **mGuard 1**: IPsec VPN >> Allgemein (Tunneleinstellungen mit 1:1-NAT)

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 ✎.
4. Klicken Sie unter **Transport- und Tunneleinstellungen** auf das Icon ✎.
5. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 13-2 und Bild 13-3.

Tabelle 13-2 VPN-Verbindung konfigurieren

Sektion	Parameter	Produktion mGuard 1	Produktion mGuard 2	Zentrale
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein				
Optionen	**Ein beschreibender Name für die Verbindung**	VPN nach Zentrale	VPN nach Zentrale	Nach Produktion (**1** bzw. **2**)
	Adresse des VPN-Gateways der Gegenstelle	77.245.32.78	77.245.32.78	%any
	Interface, das bei der Einstellung %any für das Gateway benutzt wird	-----	-----	Extern
	Verbindungsinitiierung	Initiiere	Initiiere	Warte
Transport- und Tunneleinstellungen >> (Edit) >> Allgemein				
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel	Tunnel
	Lokal	172.16.**1**.0/24	172.16.**2**.0/24	10.1.0.0/16
	Gegenstelle	10.1.0.0/16	10.1.0.0/16	172.16.**1**.0/24 bzw. 172.16.**2**.0/24
Lokales NAT (Nur mGuard 1 bzw. 2)	**Lokales NAT für IPsec-Tunnelverbindungen**	1:1-NAT	1:1-NAT	
	Reales Netzwerk	192.168.**1**.0	192.168.**1**.0	
	Virtuelles Netzwerk	172.16.**1**.0/24	172.16.**2**.0/24	
	Netzmaske	24	24	

Ergebnis

Pakete an das Netzwerk **Produktion 1** (im internen Netz von *mGuard 1*) bzw. **Produktion 2** (im internen Netz von *mGuard 2*) müssen an das *Virtuelle Netzwerk* 172.10.**1**.0/24 bzw. 172.16.**2**.0/24 gesendet werden.

13.4 Standorte mit gleichen internen Netzen mit Zentrale verbinden (Maskierung)

Die Zentrale soll über ein zentrales VPN-Gateway über VPN-Tunnel mit mehreren externen Standorten (Produktion) verbunden werden. Die externen Standorte verwenden teilweise die gleichen internen Netze oder das gleiche interne Netz wie die Zentrale.

13.4.1 Beispiel 1: Übertragung in eine Richtung (IP-Maskierung)

Wenn die Datenübertragung in nur eine Richtung – von den Maschinensteuerungen zur Zentrale – erfolgen soll, kann IP-Maskierung verwendet werden.

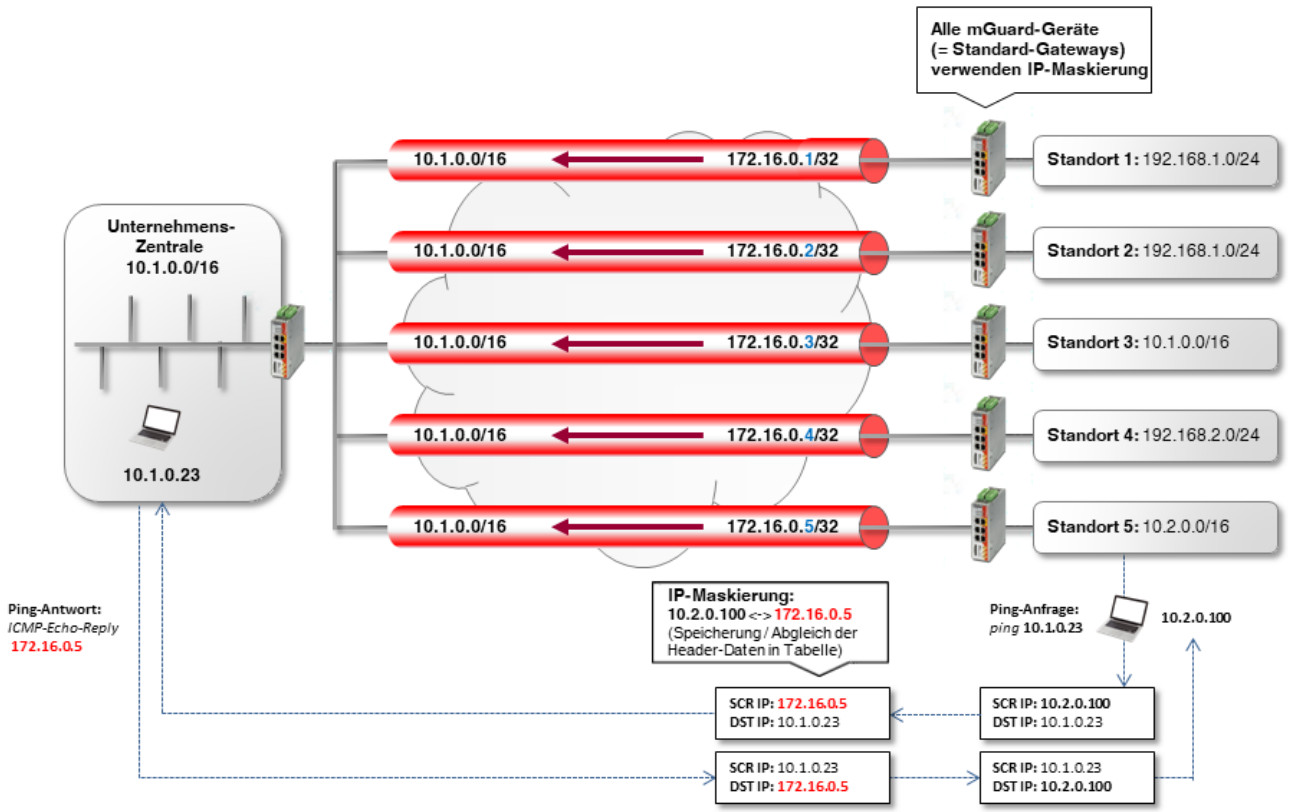


Bild 13-5 **Übertragung in nur eine Richtung (IP-Maskierung)**: Clients (z. B. SPS) in den externen Netzwerken können Daten über VPN an die Zentrale schicken. Die Zentrale kann jedoch **nicht** auf die Clients zugreifen. Das jeweilige mGuard-Gerät ist das Standard-Gateway der internen Clients.

VPN-Verbindung konfigurieren

Um VPN-Verbindungen von allen Standorten zur Zentrale aufzubauen, muss an jedem Standort IP-Maskierung verwendet werden. Dabei kann die für das Maskieren verwendete IP-Adresse einfach bei jedem Standort erhöht werden.

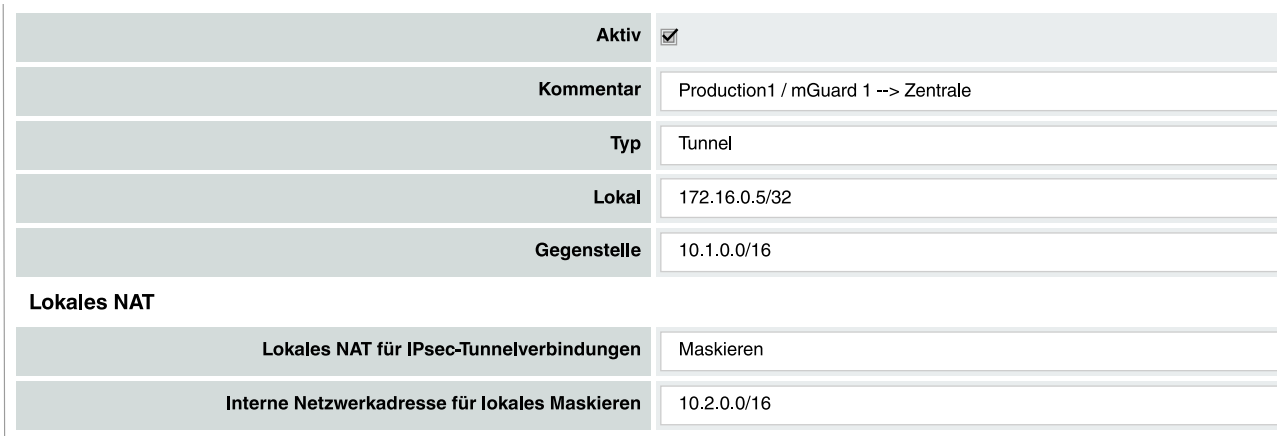


Bild 13-6 Konfigurationsbeispiel *Standort 5* (Tunneleinstellungen mit IP-Maskierung)

Tabelle 13-3 VPN-Verbindung konfigurieren

Sektion	Parameter	Zentrale	Standort 5
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein			
Optionen	**Ein beschreibender Name für die Verbindung**	VPN von Standort 5	VPN nach Zentrale
	Adresse des VPN-Gateways der Gegenstelle	%any	77.245.32.78
	Interface, das bei der Einstellung %any für das Gateway benutzt wird	Extern	-----
	Verbindungsinitiierung	Warte	Initiiere
Transport- und Tunneleinstellungen >> (Edit) >> Allgemein			
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel
	Lokal	10.1.0.0/16	172.16.0.5/32
	Gegenstelle	172.16.0.5/32	10.1.0.0/16
Lokales NAT	**Lokales NAT für IPsec-Tunnelverbindungen**	Kein NAT	Maskieren
	Interne Netzwerkadresse für lokales Maskieren	-----	10.2.0.0/16

Ergebnis

Die Clients im Netzwerk der Zentrale sind unter ihren realen IP-Adressen zu erreichen.

Vorteile

Die VPN-Konfigurationen ist unkompliziert und leicht nachvollziehbar. Der Adressraum für die Gegenstellen ist reduziert.

Nachteile

Die VPN-Verbindungen können nur in eine Richtung genutzt werden. Im obigen Beispiel können nur die Standorte auf die Zentrale zugreifen.

13.4.2 Beispiel 2: Übertragung in beide Richtungen (1:1-NAT)

Wenn die Datenübertragung in beide Richtungen erfolgen soll, muss lokales 1:1-NAT verwendet werden (siehe auch Kapitel 13.3).

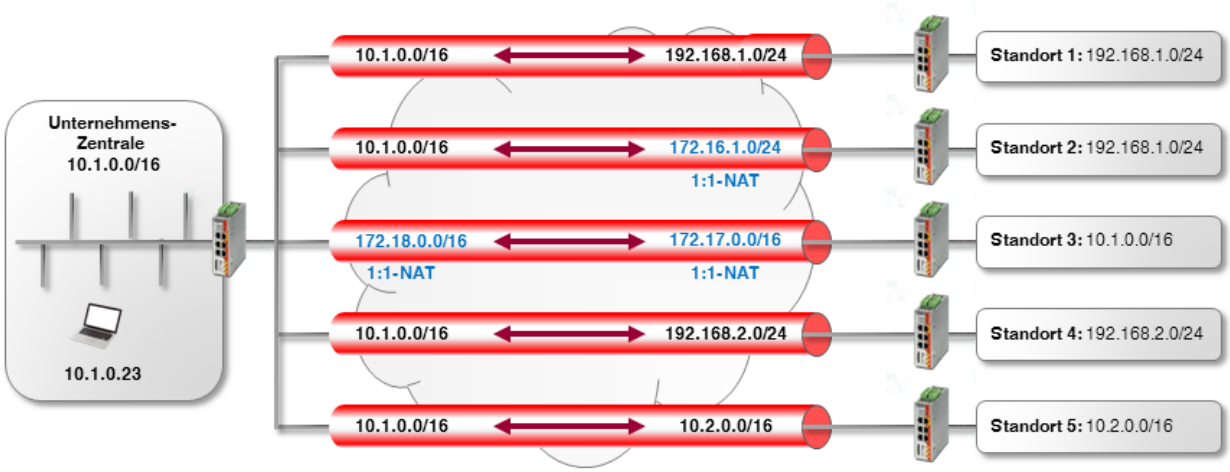


Bild 13-7 **Übertragung in beide Richtungen (Lokales 1:1-NAT)**: Die Clients (z. B. SPS) in den externen Netzwerken können durch den VPN-Tunnel auf das Netzwerk der Zentrale zugreifen und umgekehrt.

1. **Standort 1**: Beide Standorte haben unterschiedliche interne Netzwerke, so dass der VPN-Tunnel zwischen den Netzwerken 10.1.0.0/16 und 192.168.1.0/24 aufgebaut werden kann.
2. **Standort 2**: Das interne Netzwerk von *Standort 2* (192.168.1.0/24) wird bereits für die VPN-Verbindung zu *Standort 1* verwendet.

   Um auf das interne Netzwerk von Standort 2 über VPN zugreifen zu können, muss auf dem dortigen VPN-Gateway 1:1-NAT verwendet werden. Der VPN-Tunnel wird zwischen dem realen Netzwerk 10.1.0.0/16 und dem virtuellen Netzwerk 172.16.1.0/24 aufgebaut (siehe auch Kapitel 13.3).
3. **Standort 3**: Beide Standorte haben das gleiche interne Netzwerk 10.1.0.0/16.

   Um eine VPN-Verbindung zwischen den beiden Netzwerken herzustellen muss auf beiden VPN-Gateways 1:1-NAT verwendet werden. Der VPN-Tunnel wird zwischen den virtuellen Netzwerken 172.18.0.0/16 und 172.17.0.0/16 aufgebaut (siehe auch Kapitel 13.2).
4. **Standort 4 und 5**: Beide Standorte verfügen über interne Netzwerke, die von keiner anderen VPN-Verbindung genutzt werden. Es muss daher weder 1:1-NAT noch IP-Maskierung verwendet werden, um auf das jeweils andere Netzwerk zugreifen zu können.

ACHTUNG: Verwenden Sie keine virtuellen Netzwerke, die bereits für andere VPN-Verbindungen genutzt werden.

VPN-Verbindung konfigurieren

Die Konfiguration der Verbindungen erfolgt analog Kapitel 13.3.

Vorteile

Die VPN-Verbindungen können in beide Richtungen genutzt werden. Die Standorte sind von der Zentrale aus über die VPN-Verbindungen erreichbar und umgekehrt.

Nachteile

Jede VPN-Verbindung muss einzeln konfiguriert werden, abhängig davon, welche interne Netzwerkkonfiguration die beteiligten Gegenstellen verwenden.

Bei einer steigenden Anzahl von Remote-Standorten wird die Konfiguration zunehmend unübersichtlich, was leicht zu Fehlkonfigurationen führen kann.

13.5 1:1-NAT für das Remote-Netzwerk verwenden

Das Unternehmensnetzwerk ist mit einer Zweigstelle über eine VPN-Verbindung verbunden. Die Clients (Zielsysteme) im Zweigstellennetzwerk können über den VPN-Tunnel erreicht werden.

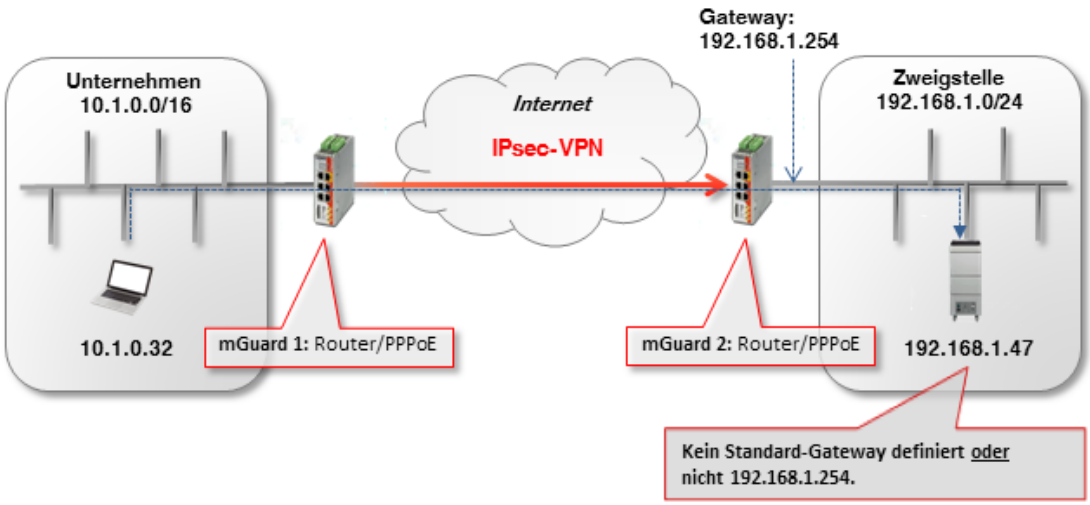
Auf einem Zielsystem (z. B. eine Maschinensteuerung, die in der Regel nur intern erreicht werden muss) ist allerdings kein Standard-Gateway definiert oder das definierte Standard-Gateway ist nicht das mGuard-Gerät, das als VPN-Gateway den VPN-Tunnel zur Verfügung stellt.

Damit kann das Zielsystem nicht auf VPN-Zugriffe aus dem Unternehmensnetzwerk antworten. Wenn sich die IP-Einstellung des Zielsystems nicht ändern lässt, kann die Funktion **Remote-NAT für IPsec-Tunnelverbindungen** genutzt werden, um das Problem zu umgehen.

13.5.1 Beispiel

Das Unternehmensnetz (10.1.0.0/16) ist dem Zielsystem (192.168.1.47/24) nicht bekannt. Wenn das Ziel (z. B. Maschinensteuerung) ein Paket über den VPN-Tunnel aus dem Unternehmensnetz empfängt,

– antwortet es entweder gar nicht (wenn kein Standard-Gateway definiert ist) oder
– es sendet die Antwort an sein Standard-Gateway (und nicht an den VPN-Gateway *mGuard 2*).

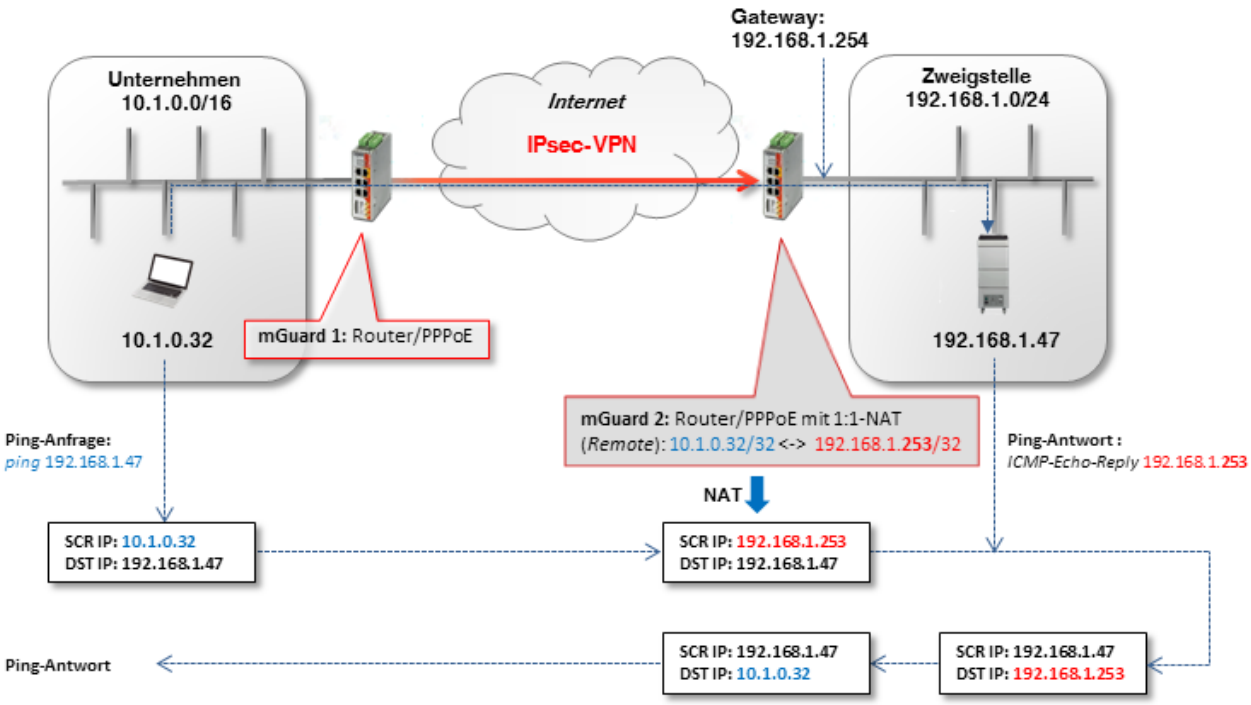


Lösung

In den VPN-Tunneleinstellungen von *mGuard 2* (VPN-Gateway der Zweigstelle) wird die Funktion **Remote-NAT für IPsec-Tunnelverbindungen** (*1:1-NAT*) verwendet.

13.5.2 VPN-Verbindung konfigurieren

Um eine Antwort des Zielsystem (z. B. Maschinensteuerung mit der IP 192.168.1.47) an den „unbekannten“ Absender zu ermöglichen, muss Remote-1:1-NAT verwendet werden.



Optionen

Aktiv	☑
Kommentar	Von Unternehmen nach Zweigstelle
Typ	Tunnel
Lokal	192.168.1.0/24
Gegenstelle	10.1.0.32/32
Lokales NAT	
Lokales NAT für IPsec-Tunnelverbindungen	Kein NAT
Remote-NAT	
Remote-NAT für IPsec-Tunnelverbindungen	1:1-NAT
Netzwerkadresse für 1:1-NAT im Remote-Netz	192.168.1.253

Bild 13-8 **mGuard 2**: IPsec VPN >> Allgemein (Tunneleinstellungen mit 1:1-NAT)

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 ✎.
4. Klicken Sie unter **Transport- und Tunneleinstellungen** auf das Icon ✎.
5. Konfigurieren Sie die VPN-Verbindung gemäß Tabelle 13-4 und Bild 13-8.

Tabelle 13-4 VPN-Verbindung konfigurieren

Sektion	Parameter	Unternehmen / mGuard 1	Zweigstelle / mGuard 2
IPsec VPN >> Verbindungen >> (Edit) >> Allgemein			
Optionen	**Ein beschreibender Name für die Verbindung**	VPN nach Zweigstelle	VPN von Unternehmen
	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 >> (Edit) >> Allgemein			
Transport- und Tunneleinstellungen	**Typ**	Tunnel	Tunnel
	Lokal	**10.1.0.32/32**	192.168.1.0/24
	Gegenstelle	192.168.1.0/24	**10.1.0.32/32**
Remote NAT	**Remote-NAT für IPsec-Tunnelverbindungen**	Kein NAT	1:1-NAT
	Netzwerkadresse für 1:1-NAT im Remote-Netz	-----	192.168.1.**253**

Das Remote-Netzwerk oder die Remote-IP-Adresse wird auf eine **freie (virtuelle) IP-Adresse** im internen Netzwerk der Zweigestelle umgeschrieben (*gemapped*): **10.1.0.32/32 <-> 192.168.1.253**.

Eine Netzmaske muss für das Remote-Netz (192.168.1.253) nicht angegeben werden. Diese wird automatisch vom angegebenen Netz der Gegenstelle übernommen.

Das virtuelle Netzwerk/die virtuelle IP-Adresse darf von keinem Netzwerk-Client im internen Netzwerk der Zweigstelle verwendet werden.

Entsprechend der im Beispiel verwendeten Konfiguration hat nur der Client 10.1.0.32 im Unternehmensnetzwerk Zugriff auf das Ziel in der Zweigstelle.

Seien Sie vorsichtig, wenn Sie die Subnetzmaske für das Remote-Netzwerk auswählen und das Netzwerk angeben, dem das Remote-Netzwerk zugeordnet werden soll (siehe „Problem bei 1:1-NAT für Remote-Netzwerke“).

Der ARP-Proxy von *Guard 2* liefert die ARP-Auflösung für das virtuelle Netzwerk/ IP-Adresse. Das Zielsystem sendet seine Antworten an *mGuard 2*:

– Pakete aus dem Unternehmensnetzwerk (10.1.0.0/16) werden über das VPN-Gateway (*mGuard 1*) an die reale IP-Adresse des Ziel-Clients in der Zweigstelle (**192.168.1.47)** gesendet.
– *mGuard 2* erhält die Anfrage, führt ein 1:1-NAT für das Remote-Netzwerk/IP-Adresse durch (**10.1.0.32/32** <-> **192.168.1.253**) und leitet die Anfrage an den Ziel-Client (**192.168.1.47**) weiter.
– Der Ziel-Client empfängt die Anfrage und sendet seine Antwortpakte an die virtuelle Absender-IP-Adresse (**192.168.1.253**).
– *mGuard 2* erhält die Antwort, macht das 1:1-NAT rückgängig (**192.168.1.253** <-> **10.1.0.32/32**) und leitet die Antwort an *mGuard 1* bzw. den Absender im Unternehmensnetzwerk (**10.1.0.32**) weiter.

Problem bei 1:1-NAT für Remote-Netzwerke

Die Subnetzmaske */24* für das Remote-Netzwerk (z. B. 10.1.0.0/24) und eine Remote-1:1-NAT-Adresse (z. B. 192.168.1.0) würde nicht funktionieren, da in diesem Fall der ARP-Proxy von *mGuard 2* auf alle ARP-Anfragen des internen Netzwerks der Zweigstelle antworten würde (192.168.1.0 – 192.168.1.255).

Eine Erhöhung der Subnetzmaske des Remote-Netzwerks würde auch die Anzahl der Clients im Unternehmensnetzwerk erhöhen, von denen aus auf den Client in der Zweigstelle zugegriffen werden kann. Es würde aber auch die erforderliche Anzahl unbenutzter IP-Adressen in der Zweigstelle für die Zuordnung der Quell-IP-Adresse erhöhen.

Die folgende Tabelle zeigt, den Zusammenhang zwischen

– der Remote-Subnetzmaske,
– den Clients, die auf das Zielsystem zugreifen können,
– der Anzahl der benötigten unbenutzten IP-Adressen im internen Netzwerk.

	Beispiel 1	**Beispiel 2**	**Beispiel 3**	**Beispiel 4**
Angegebenes Remote-Netzwerk	10.1.0.0**/26**	10.1.0.64**/26**	10.1.0.128**/28**	10.1.0.32**/32**
Remote-IP-Adressen, die auf das Zielsystem zugreifen können	10.1.0.0 – 10.1.0.63	10.1.0.64 – 10.1.0.127	10.1.0.128 – 10.1.0.143	10.1.0.32
Internes Netzwerk	192.168.1.0**/24**			
Netzwerkadresse für Remote 1:1-NAT	192.168.1.128**/26**	192.168.1.192**/26**	192.168.1.240**/28**	192.168.1.253**/32**
Hosts, denen der mGuard auf ARP-Anfragen antworten würde **(Dürfen nicht im internen Netzwerk verwendet werden!)**	192.168.1.128 – 192.168.1.191 **64 Hosts**	192.168.1.192 – 192.168.1.255 **64 Hosts**	192.168.1.240 – 192.168.1.255 **16 Hosts**	192.168.1.253 **1 Host**

Zusätzlicher NAT-Router

Wenn von mehreren Clients im Unternehmensnetzwerk auf die Zielsysteme in der Zweigstelle zugegriffen werden soll, kann ein NAT-Router verwendet werden, bevor die Pakete in den VPN-Tunnel übergeben werden.

Damit muss als Remote-Netzwerk die IP-Adresse des NAT-Routers mit der Subnetzmaske */32* angegeben werden. Nur eine unbenutzte IP-Adresse würde benötigt.

IP-Maskierung

Wenn die VPN-Verbindung nur in eine Richtung genutzt werden muss, z. B. vom Unternehmensnetzwerk zur Zweigstelle (Fernwartung), kann statt eines weiteren NAT-Routers auf *mGuard 1* auch IP-Maskierung (*IP-Masquerading*) im VPN-Tunnel verwendet werden (siehe auch Kapitel 13.4).

Auf diese Weise hätten die ankommenden Datenpakete bei *mGuard 2* immer die gleiche Quell-IP-Adresse (/32).

14 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.

14.1 Einleitung

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

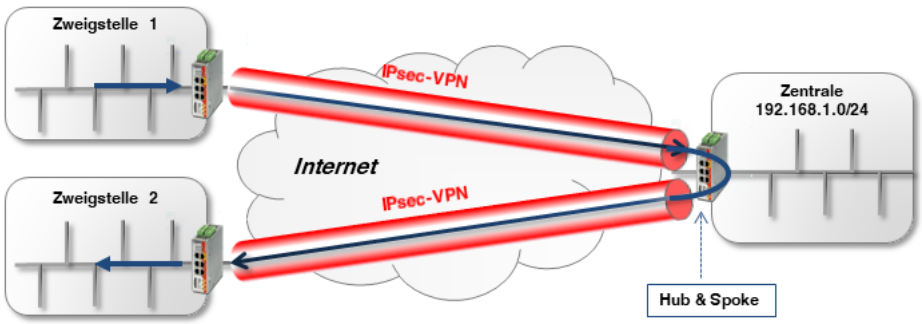


Bild 14-1 *Hub & Spoke* über Firmenzentrale (IPsec VPN)

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.

14.2 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).

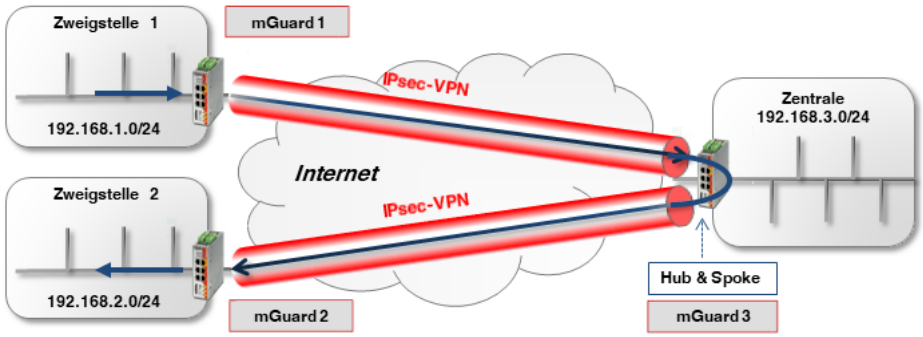


Bild 14-2 *Hub & Spoke* über Firmenzentrale (IPsec VPN)

14.2.1 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 11 und 12 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

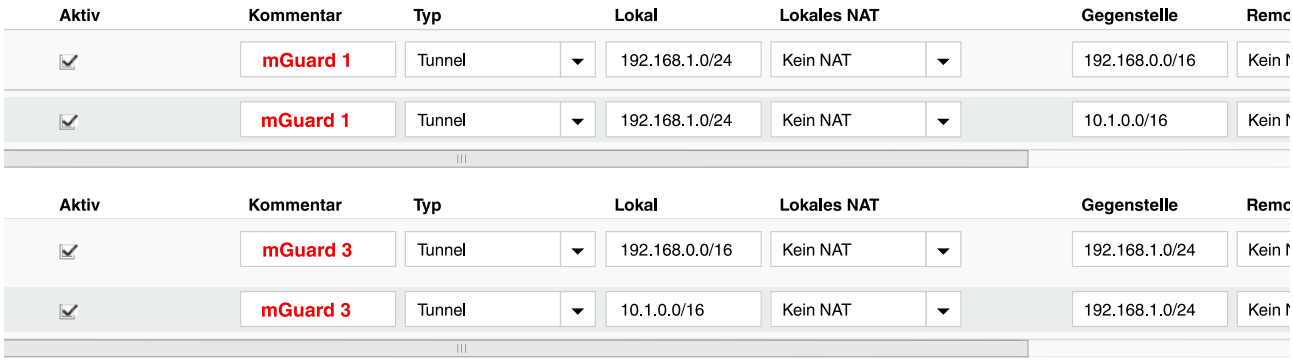


Tabelle 14-1 zeigt für diesen Fall die Transport- und Tunneleinstellungen für alle Geräte (*mGuard 1, 2* und *3*):

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

Tabelle 14-1 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

14.3 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.

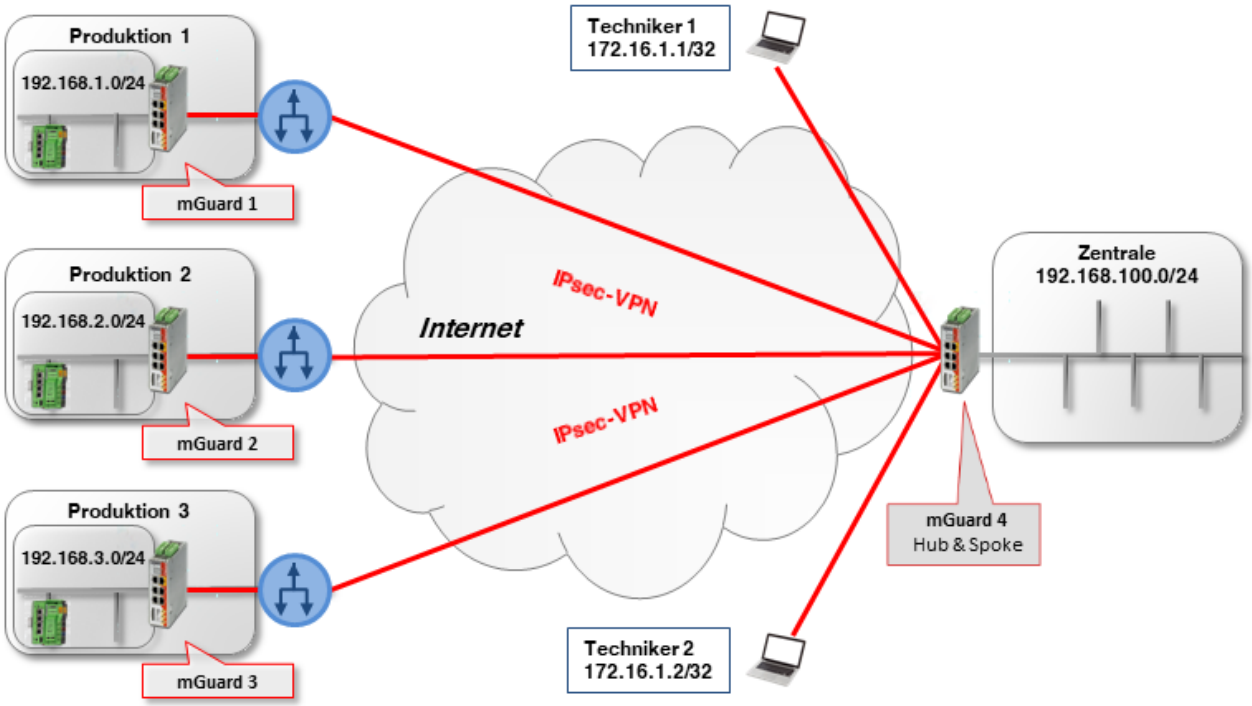


Bild 14-3 Fernwartung via *Hub & Spoke* über die Firmenzentrale (IPsec VPN)

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 14.2.1):

Tabelle 14-2 *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 13.3, „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 14-3 und Bild 14-4).

Tabelle 14-3 *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

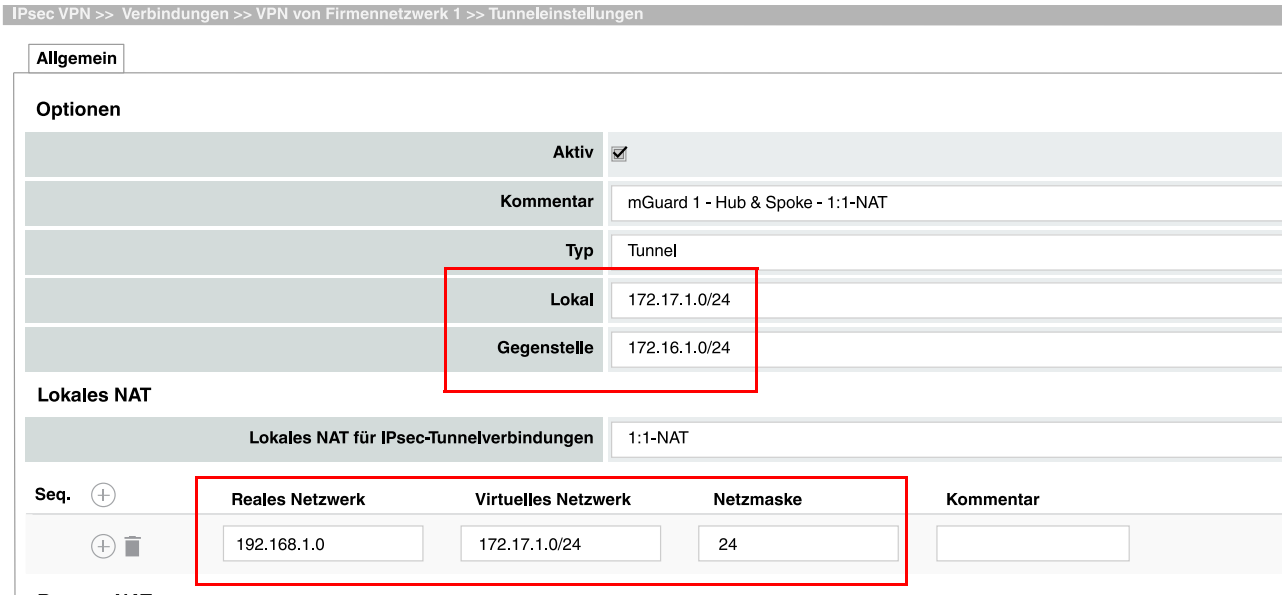


Bild 14-4 *Hub & Spoke*: Beispiel *mGuard 1* – Tunneleinstellungen + lokales 1:1-NAT

15 VPN-Fehlersuche (Troubleshooting)

Document-ID: 108417_de_00
Dokument-Bezeichnung: AH DE MGUARD VPN TROUBLESHOOTING

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

Dieses Dokument soll dabei helfen, Probleme im Zusammenhang mit VPN-Verbindungen zu erkennen und zu bewerten. Die Beispiele von Log-Einträgen wurden von mGuard-Geräten mit Firmware-Version 7.6 übernommen.

15.1 Einleitung

Eine VPN-Verbindung wird in zwei Phasen aufgebaut:

1. **Phase I**: In *Phase I* (**ISAKMP SA**, SA = *Security Association*) authentifizieren sich die VPN-Gegenstellen gegenseitig und handeln einen Schlüssel aus, mit dem anschließend *Phase II* verschlüsselt bzw. abgesichert wird.

   Die SA verbindet nur die beiden VPN-Gegenstellen und wird für den Schlüsselaustausch und den Austausch von DPD-Nachrichten verwendet (DPD = *Dead Peer Detection*).

2. **Phase II**: VPN-Gegenstellen gehen erst dann in *Phase II* (**IPsec SA**) über, wenn *Phase I* erfolgreich gestartet wurde. In *Phase II* werden die Parameter der IPsec-Verbindung ausgehandelt.

   Die SA verbindet die beiden Netzwerke und vermittelt den Datenaustausch zwischen den Netzwerk-Clients beider Netzwerke.

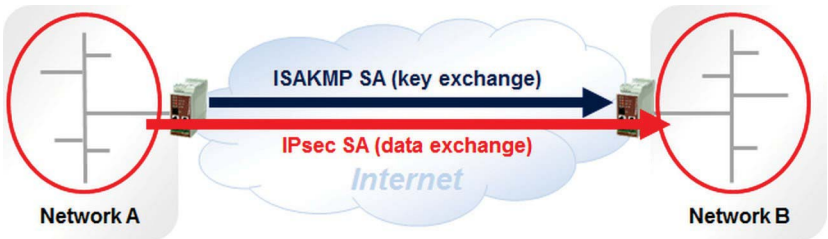


Bild 15-1 Ablauf der beiden Phasen während des Aufbaus einer VPN-Verbindung (*ISAKMP SA* und *IPSEC SA*)

Häufig schlägt der Aufbau einer VPN-Verbindung währen *Phase* I (*ISAKMP SA*) fehl. Mögliche Gründe sind eine falsche Konfiguration der VPN-Verbindung oder falsch konfigurierte Router zwischen den beiden VPN-Gegenstellen.

Wenn der Aufbau währen der *Phase II* (*IPsec SA*) fehlschlägt, liegt eine Fehlkonfiguration einer oder beider VPN-Konfiguration der VPN-Gegenstellen vor.

Wenn ein Fehler vorliegt, sollten Sie als erstes den IPsec Status der VPN-Verbindung prüfen (Menü **IPsec >> IPsec-Status**).Dort können Sie erkennen, an welcher Stelle der Fehler auftritt. Abbildung Bild 15-2 unten zeigt eine erfolgreich aufgebaute VPN-Verbindung.

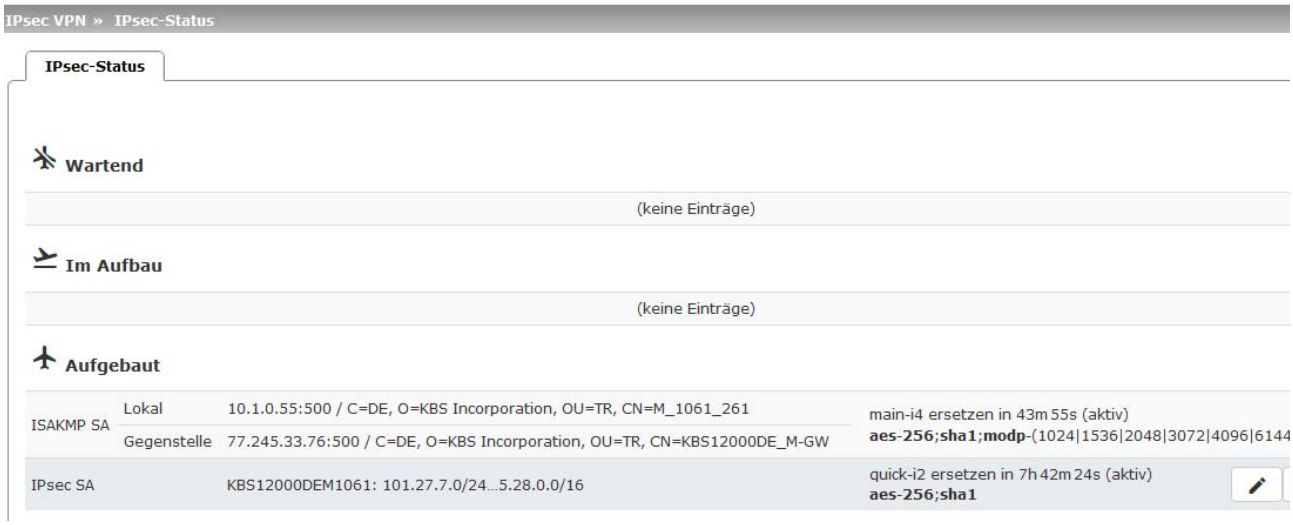


Bild 15-2 IPsec-Status – VPN-Verbindung wurde erfolgreich aufgebaut

15.1.1 Die folgenden Situationen können auftreten

Tabelle 15-1 Die folgenden Situationen könne auftreten.

Situationen, die auftreten könnten	Siehe Kapitel
Die VPN-Verbindung wird nicht auf der IPsec-Status-Seite angezeigt.	Kapitel 15.2, „Die VPN-Verbindung wird nicht auf der IPsec-Status-Seite angezeigt“
ISAKMP SA wurde nicht aufgebaut ("ISAKMP-Status" empty)	Kapitel 15.3, „ISAKMP SA (Phase I) kann nicht aufgebaut werden“
IPsec SA wurde nicht aufgebaut ("IPsec-Status" empty)	Kapitel 15.4, „IPSec SA (Phase II) kann nicht aufgebaut werden“
Daten können nicht oder nicht problemlos durch eine aufgebaute VPN-Verbindung transportiert werden ("ISAKMP SA" und "IPsec SA" wurden erfolgreich aufgebaut).	Kapitel 15.5, „Remote-Clients können nicht über aufgebauten VPN-Tunnel erreicht werden“

In den folgenden Kapiteln, stehe **Initiator** für das mGuard-Gerät, das die VPN-Verbindung initiiert, also startet. **Responder** steht für das mGuard-Gerät, das auf die VPN-Verbindung wartet.

Wenn der Aufbau der ISAKMP SA oder *IPsec SA* fehlschlägt (Situation 1 und 2), müssen in der Regel immer die Log-Dateien beider Geräte der VPN-Gegenstellen untersucht werden, um den Grund für den Fehler zu finden.

Es wird empfohlen in diesem Fall umgehend – und vor einen Neustart der Geräte – einen Support-Snapshot von beiden Geräten zu erstellen (Menü **Support >> Erweitert >> Snapshot**). Eine weitergehende Analyse kann anschließend auf Basis der Daten der Snapshots vorgenommen werden.

15.2 Die VPN-Verbindung wird nicht auf der IPsec-Status-Seite angezeigt

Wenn die VPN-Verbindung nicht auf der IPsec-Status-Seite des Geräts erscheint, könnten folgende Fehler vorliegen.

15.2.1 VPN-Verbindung nicht aktiviert

Deaktivierte VPN-Verbindungen erscheinen nicht auf der IPsec-Status-Seite.

- Stellen Sie sicher, dass die VPN-Verbindung aktiviert wurde. (Menu **IPsec VPN >> Verbindung**).
- Wenn die VPN-Verbindung durch einen CMD-Kontakt gestartet wird, stellen Sie sicher, dass der An-/Aus-Schalter oder der Taster so eingestellt bzw. gedrückt wurde, wurde, dass die VPN-Verbindung damit gestartet wird.
- Wenn die VPN-Verbindung durch ein Skript gestartet wird, z. B. durch das Skript nph-vpn.gci, stellen Sie sicher, dass das entsprechende Kommando so aufgerufen bzw. ausgeführt wurde, dass die richtige VPN-Verbindung gestartet wird.

15.2.2 Option "Deaktiviere das VPN, bis sich der Benutzer über HTTP authentifiziert" is aktiviert

- Stellen Sie sicher, dass die Option „*Deaktiviere das VPN, bis sich der Benutzer über HTTP authentifiziert*“ nicht aktiviert ist (Menü **Authentifizierung >> Administrative Benutzer***)*.

Wenn die Option aktiviert ist, wird der Benutzer bei jedem Aufruf einer beliebigen Web-Seite aufgefordert, sein Benutzer-Passwort einzugeben, nachdem das mGuard-GErät neu gestartet wurde.

Eine konfigurierte VPN-Verbindung wird nur dann als VPN-Service gestartet, wenn das Passwort korrekt eingegeben wurde.

Mit dieser Option kann verhindert werden, dass entwendete mGuard-Geräte nach dem Einschalten ihre konfigurierten VPN-Verbindungen starten und somit eine VPN-Verbindung zu geschützten Bereichen zulassen.

15.2.3 Falsche Konfiguration

Das Problem kann auch durch eine falsche Konfiguration hervorgerufen werden.

- Übernehmen Sie eine kleinere Änderung an der VPN-Verbindung und klicken Sie auf das Icon <*Übernehmen*>. Prüfen Sie anschließend die System-Meldungen.
- Wenn die System-Meldungen keine Fehler melden, prüfen Sie die VPN-Log-Dateien (Menu **Logging >> Logs ansehen***)* auf Fehlermeldungen, wie z. B.:

```
firestarter: vpnd: whack error: "MAI1825301978_1" ikelifetime [3600] must be greater than
                                rekeymargin*(100+rekeyfuzz)/100 [5400*(100+100)/100 = 10800]

firestarter: tunnel ignored: local address '10.1.80.100' within remote network '10.0.0.0/8'
```

15.2.4 Generelle Netzwerkprobleme

Das Problem kann auch durch allgemeine Netzwerkprobleme hervorgerufen werden.

- Das mGuard-Gerät (im Netzwerkmodus *Router*) wurde so konfiguriert, dass es seine externen IP-Einstellungen von einem DHCP-Server erhält. Die Einstellungen kommen aber nicht beim Gerät an.
- In der VPN-Verbindung wurde als **Adresse des VPN-Gateways der Gegenstelle** ein DNS-Name (*Hostname*) angegeben. Das mGuard-Gerät konnten den DNS-Namen allerdings nicht auflösen, da die Adressauflösung nicht korrekt konfiguriert wurde.

15.3 ISAKMP SA (Phase I) kann nicht aufgebaut werden

Die *ISAKMP SA* wird unter verwenden des *Main Modes* aufgebaut, der von dem *Internet Key Exchange* (IKE) Protokoll bereitgestellt wird. IKE kann auch im weniger sicheren *Aggressive Mode* betrieben werden, der allerdings nur von aktuellerer mGuard-Firmware unterstützt wird.

Im *Main Mode* werden drei Meldungspaare zwischen beiden VPN-Gegenstellen ausgetauscht. Das folgende Diagramm verdeutlicht den Austausch der Meldungen. Es sollte im Fehlerfall zur Interpretation des Problems herangezogen werden.

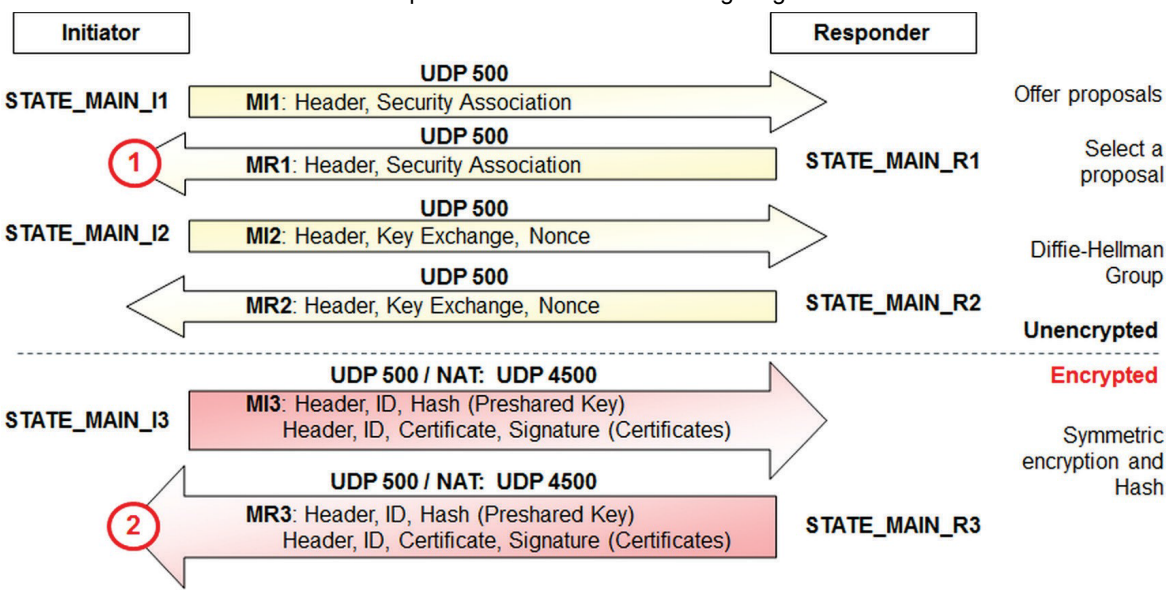


Bild 15-3 *ISAKMP SA* - Phase I

Jedesmal, wenn der **Initiator** eine Meldung gesendet hat, ändert sich sein Status von:
STATE_MAIN_I1 to STATE_MAIN_I2 und STATE_MAIN_I3,

der Satus des **Responders** ändert sich entsprechend von:
STATE_MAIN_R1 to STATE_MAIN_R2 und STATE_MAIN_R3.

Die Statusänderungen werden in den Log-Einträgen protokolliert.

Die VPN-Verbindung wird über den **UDP-Port 500** aufgebaut. Wenn die Verbindung zwischen zwei oder mehr Gateways aufgebaut wird, die NAT verwenden, findet der Austausch im *Main Mode* ab **Meldung MI3** über den **UDP-Port 4500** statt.

Die Probleme tauchen in der Regel an einem der im Schema mit ① und ② markierten Punkte auf:

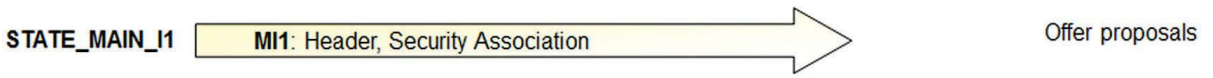
1. Der **Initiator** erhält keine Antwort vom **Responder**.
2. Der **Initiator** erhält ein unerwartetes Paket oder eine Fehlermeldung vom **Responder**.

15.3.1 Log-Eintrag zu einem erfolgreich aufgebauten ISAKMP SA

Initiator | **Responder**

Initiator Log:

```
08:53:47.90161 "MAI1950251842_1" #2: initiating Main Mode
```

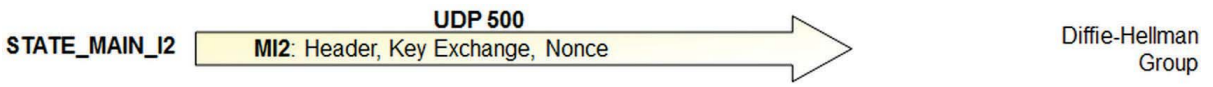


Responder Log:

```
08:53:47.90165 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
08:53:47.90186 packet from 77.245.32.68:500: received Vendor ID payload [Dead Peer Detection]
08:53:47.90194 packet from 77.245.32.68:500: received Vendor ID payload [RFC 3947] method set to=109
08:53:47.90202 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
08:53:47.90210 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
08:53:47.90218 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
08:53:47.90226 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
08:53:47.90279 packet from 77.245.32.68:500: received Vendor ID payload [Innominate IKE Fragmentation]
08:53:47.90297 packet from 77.245.32.68:500: received Vendor ID payload [Innominate always send NAT-OA]
08:53:47.90305 "MAI0874627901_1"[1] 77.245.32.68 #2: responding to Main Mode from unknown peer 77.245.32.68
08:53:47.90333 "MAI0874627901_1"[1] 77.245.32.68 #2: enabling Innominate IKE Fragmentation (main_inI1_outR1)
08:53:47.90344 "MAI0874627901_1"[1] 77.245.32.68 #2: enabling Innominate Always Send NAT-OA (main_inI1_outR1)
08:53:47.90369 "MAI0874627901_1"[1] 77.245.32.68 #2: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
08:53:47.90384 "MAI0874627901_1"[1] 77.245.32.68 #2: STATE_MAIN_R1: sent MR1, expecting MI2
```

Initiator Log:

```
08:53:48.15255 "MAI1950251842_1" #2: received Vendor ID payload [Openswan (this version) 2.6.24 ]
08:53:48.15259 "MAI1950251842_1" #2: received Vendor ID payload [Dead Peer Detection]
08:53:48.15263 "MAI1950251842_1" #2: received Vendor ID payload [RFC 3947] method set to=109
08:53:48.15267 "MAI1950251842_1" #2: received Vendor ID payload [Innominate IKE Fragmentation]
08:53:48.15271 "MAI1950251842_1" #2: received Vendor ID payload [Innominate always send NAT-OA]
08:53:48.15275 "MAI1950251842_1" #2: enabling possible NAT-traversal with method 4
08:53:48.15279 "MAI1950251842_1" #2: enabling Innominate IKE Fragmentation (main_inR1_outI2)
08:53:48.15296 "MAI1950251842_1" #2: enabling Innominate Always Send NAT-OA (main_inR1_outI2)
08:53:48.37178 "MAI1950251842_1" #2: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
08:53:48.37186 "MAI1950251842_1" #2: STATE_MAIN_I2: sent MI2, expecting MR2
```



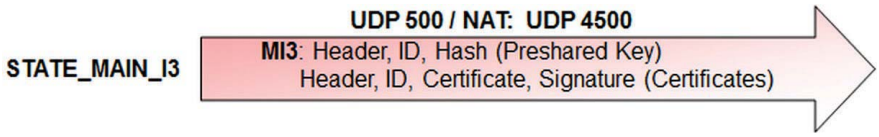
Responder Log:

```
08:53:48.52717 "MAI0874627901_1"[1] 77.245.32.68 #2: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
08:53:50.24004 "MAI0874627901_1"[1] 77.245.32.68 #2: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
08:53:50.24027 "MAI0874627901_1"[1] 77.245.32.68 #2: STATE_MAIN_R2: sent MR2, expecting MI3
```

Initiator **Responder**

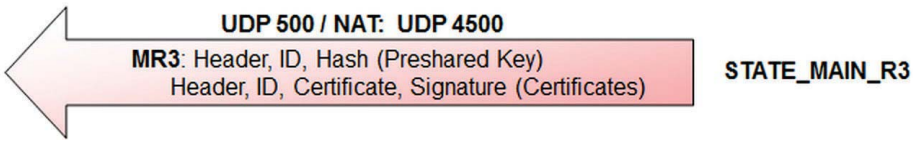
Initiator Log:

```
08:53:50.72881 "MAI1950251842_1" #2: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
08:53:50.72892 "MAI1950251842_1" #2: I am sending my cert
08:53:50.72896 "MAI1950251842_1" #2: I am sending a certificate request
08:53:50.72942 "MAI1950251842_1" #2: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
08:53:50.72961 "MAI1950251842_1" #2: STATE_MAIN_I3: sent MI3, expecting MR3
```



Responder Log:

```
08:53:50.76811 "MAI0874627901_1"[1] 77.245.32.68 #2: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 1'
08:53:50.76831 "MAI0874627901_1"[1] 77.245.32.68 #2: issuer cacert not found
08:53:50.76839 "MAI0874627901_1"[1] 77.245.32.68 #2: X.509 certificate rejected
08:53:50.76846 "MAI0874627901_1"[1] 77.245.32.68 #2: I am sending my cert
08:53:50.76887 "MAI0874627901_1"[1] 77.245.32.68 #2: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
08:53:50.76905 "MAI0874627901_1"[1] 77.245.32.68 #2: new NAT mapping for #2, was 77.245.32.68:500, now 77.245.32.68:4500
08:53:50.76914 "MAI0874627901_1"[1] 77.245.32.68 #2: new NAT mapping for #1, was 77.245.32.68:500, now 77.245.32.68:4500
08:53:50.76922 "MAI0874627901_1"[1] 77.245.32.68 #2: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_RSA_SIG
                                                     cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
08:53:50.76932 "MAI0874627901_1"[1] 77.245.32.68 #2: Dead Peer Detection (RFC 3706): enabled
```



Initiator Log:

```
08:53:50.97225 "MAI1950251842_1" #2: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 2'
08:53:50.97229 "MAI1950251842_1" #2: issuer cacert not found
08:53:50.97233 "MAI1950251842_1" #2: X.509 certificate rejected
08:53:50.97236 "MAI1950251842_1" #2: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
08:53:50.97244 "MAI1950251842_1" #2: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_RSA_SIG cipher=oakley_3des_cbc_192
                                      prf=oakley_md5 group=modp8192}
```

Die Log-Einträge **issuer cacert not found** und **X.509 certificate rejected** bedeuten nicht, dass ein Fehler vorliegt.

Das mGuard-Gerät versucht zunächst Authentifizierung der VPN-Gegenstelle mittels CA-Zertifikat durchzuführen. Wenn kein passendes CA-Zertifikat vorliegt, werden die im Schema angegebenen Log-Einträge generiert.

Erst danach versucht das mGuard-Gerät, die Gegenstelle über ein in der VPN-Verbindung übermittelte Gegenstellen-Zertifikat zu authentifizieren.

15.3.2 Initiator: “pending Quick Mode with w.x.y.z took too long – replacing phase 1”

Initiator Log:

```
08:56:40.12570 "MAI1950251842_1" #6: initiating Main Mode
09:02:50.03792 pending Quick Mode with 77.245.33.66 "MAI1950251842_1" took too long -- replacing phase 1
09:02:50.03804 "MAI1950251842_1" #7: initiating Main Mode to replace #6
09:04:50.04538 pending Quick Mode with 77.245.33.66 "MAI1950251842_1" took too long -- replacing phase 1
09:04:50.04550 "MAI1950251842_1" #8: initiating Main Mode to replace #7
```

Das mGuard-Gerät (**Initiator**) initiiert die VPN-Verbindung mit dem Senden der ersten *Main Mode* Meldung (**MI1**). Es erhält allerdings keine Antwort vom **Responder**. Das Gerät versucht daraufhin weiter, die VPN-Verbindung zu initiieren.

An dieser Stelle müssen nun die VPN-Log-Einträge des **Responders** analysiert werden, um zu klären, ob diese Meldung (**MI1**) den **Responder** erreicht hat.

15.3.2.1 Responder: Im VPN-Log-Einträgen des Reposnders wurde ein Empfang von Paketen nicht registriert

Responder Log:

In den Log-Einträgen erscheinen keine Einträge zu neuen VPN-Verbindungsanfragen. Zumindest **packet from w.x.y.z: received Vendor ID payload** sollte in den Log-Einträgen auftauchen, wenn der **Responder** die erste *Main Mode* Meldung erhalten hat. Wenn ein solcher Log-Eintrag nicht erscheint, ist das ein Hinweis darauf, dass die erste *Main Mode* Meldung des **Initiators** den **Responder** nicht erreicht hat.

Mögliche Gründe:

- Die angegebene IP-Adresse oder der DNS-Name (*hostname*) des **Responders** ist nicht korrekt (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Allgemein**, Parameter: *Adresse des VPN-Gateways der Gegenstelle*).
- Wenn der **Initiator** sich hinter einer Firewall befindet, könnte es sein, dass die Firewall den ausgehenden *Traffic* über den UDP-Port 500 blockiert.
- Wenn der **Responder** sich hinter einem NAT-Router befindet, könnte es sein, dass Port-Weiterleitung für eingehenden *Traffic* auf UDP-Port 500 zur IP-Adresse des **Responders** nicht konfiguriert ist. Oder der NAT-Router ist an anderer Stelle „falsch“ konfiguriert.
- Der **Responder** horcht nicht auf eingehende VPN-Verbindungen (z. B. weil keine VPN-Verbindung konfiguriert ist oder alle VPN-Verbindungen deaktiviert sind.

Prüfen Sie mit dem Tool *IKE Ping* (Menü **Support >> Erweitert >> Werkzeuge**) auf dem **Initiator-Gerät**, ob IP-Adresse oder DNS-Hostname des **Responders** erreichbar ist.

15.3.2.2 Responder.: “initial Main Mode message received on w.x.y.z:500 but no connection has been authorized

Responder Log:

```
09:07:35.94714 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
09:07:35.94748 packet from 77.245.32.68:500: received Vendor ID payload [Dead Peer Detection]
09:07:35.94757 packet from 77.245.32.68:500: received Vendor ID payload [RFC 3947] method set to=109
09:07:35.94764 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
09:07:35.94772 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
09:07:35.94780 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
09:07:35.94789 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
09:07:35.94796 packet from 77.245.32.68:500: received Vendor ID payload [Innominate IKE Fragmentation]
09:07:35.94803 packet from 77.245.32.68:500: received Vendor ID payload [Innominate always send NAT-OA]
09:07:35.94811 packet from 77.245.32.68:500: initial Main Mode message received on 192.168.3.1:500 but no connection has been authorized
                                             with policy=RSASIG
```

Der **Responder** hat eine erste *Main Mode* Meldung vom **Initiator** erhalten. Der **Initiator** informiert den **Responder** unter anderem über die Verschlüsselungs- und Hash-Algorithmen (z. B. AES-256/SHA-256) die für den Aufbau der *ISAKMP SA* verwendet werden sollen.

Der **Responder** prüft, ob es eine konfigurierte VPN-Verbindung gibt, die diese Algorithmen ebenfalls verwendet. Wenn dabei keine Übereinstimmung gefunden wird, erscheint die oben angegebene meldung in den Log-Einträgen des **Responders**. In diesem Fall sendet der **Responder** keine Antwort an den **Initiator**.

Gründe:

Die angegebenen Verschlüsselungs- und oder Hash-Algorithmen stimmen nicht überein. Beide konfigurierten VPN-Verbindungen müssen allerdings die gleichen Verschlüsselungs- und Hash-Algorithmen unterstützen.

Prüfen Sie die angegebenen Verschlüsselungs- und Hash-Algorithmen für die *ISAKMP SA* auf der Seite des Initiators und des Responders (Menü **IPsec VPN >> Verbindungen >> (Edit) >> IKE-Optionen**, Sektion *ISAKMP SA* **/ Schlüsselaustausch**).

15.3.3 Initiator: “Possible authentication failure: no acceptable response to our first encrypted message”

Initiator Log:

```
09:54:06.14104 "MAI1950251842_1" #55: initiating Main Mode
09:54:08.02489 "MAI1950251842_1" #55: received Vendor ID payload [Openswan (this version) 2.6.24 ]
09:54:08.02493 "MAI1950251842_1" #55: received Vendor ID payload [Dead Peer Detection]
09:54:08.02497 "MAI1950251842_1" #55: received Vendor ID payload [RFC 3947] method set to=109
09:54:08.02501 "MAI1950251842_1" #55: received Vendor ID payload [Innominate IKE Fragmentation]
09:54:08.02505 "MAI1950251842_1" #55: received Vendor ID payload [Innominate always send NAT-OA]
09:54:08.02509 "MAI1950251842_1" #55: enabling possible NAT-traversal with method 4
09:54:08.02513 "MAI1950251842_1" #55: enabling Innominate IKE Fragmentation (main_inR1_outI2)
09:54:08.02528 "MAI1950251842_1" #55: enabling Innominate Always Send NAT-OA (main_inR1_outI2)
09:54:08.35894 "MAI1950251842_1" #55: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
09:54:08.35902 "MAI1950251842_1" #55: STATE_MAIN_I2: sent MI2, expecting MR2
09:54:10.71933 "MAI1950251842_1" #55: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
09:54:10.71945 "MAI1950251842_1" #55: I am sending my cert
09:54:10.71948 "MAI1950251842_1" #55: I am sending a certificate request
09:54:10.72057 "MAI1950251842_1" #55: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
09:54:10.72076 "MAI1950251842_1" #55: STATE_MAIN_I3: sent MI3, expecting MR3
09:54:20.23466 "MAI1950251842_1" #55: discarding duplicate packet; already STATE_MAIN_I3
09:54:40.23282 "MAI1950251842_1" #55: discarding duplicate packet; already STATE_MAIN_I3
09:55:21.23123 "MAI1950251842_1" #55: max number of retransmissions (2) reached STATE_MAIN_I3. Possible authentication failure:
                                      no acceptable response to our first encrypted message
```

Der **Initiator** hat seine dritte *Main Mode* Meldung (**MI3**) gesendet und erwartet nun einen Antwort (**MR3**) vom **Responder**. Er erhält aber erneut eine MR2-Meldung vom **Responder**. Der **Responder** erstellt deshalb folgenden Log-Eintrag: “*discarding duplicate packet; already STATE_MAIN_I3*”

Wenn die VPN-Verbindung über einen oder mehrere Gateways mit aktiviertem NAT aufgebaut wird, dann wird ab *Main Mode* Meldung (**MI3**) der Austausch über den UDP-Port 4500 statt über UDP-Port 500 ausgeführt (aufgrund von *NAT-Traversal*).

Die Log-Einträge des Responders teilen uns mehr über die Gründe mit.

Responder Log:

```
09:54:07.89904 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
09:54:07.89913 packet from 77.245.32.68:500: received Vendor ID payload [Dead Peer Detection]
09:54:07.89921 packet from 77.245.32.68:500: received Vendor ID payload [RFC 3947] method set to=109
09:54:07.89928 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
09:54:07.89936 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
09:54:07.89989 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
09:54:07.90049 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
09:54:07.90061 packet from 77.245.32.68:500: received Vendor ID payload [Innominate IKE Fragmentation]
09:54:07.90089 packet from 77.245.32.68:500: received Vendor ID payload [Innominate always send NAT-OA]
09:54:07.90100 "MAI0874627901_1"[1] 77.245.32.68 #67: responding to Main Mode from unknown peer 77.245.32.68
09:54:07.90108 "MAI0874627901_1"[1] 77.245.32.68 #67: enabling Innominate IKE Fragmentation (main_inI1_outR1)
09:54:07.90117 "MAI0874627901_1"[1] 77.245.32.68 #67: enabling Innominate Always Send NAT-OA (main_inI1_outR1)
09:54:07.90142 "MAI0874627901_1"[1] 77.245.32.68 #67: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
09:54:07.90171 "MAI0874627901_1"[1] 77.245.32.68 #67: STATE_MAIN_R1: sent MR1, expecting MI2
09:54:08.55076 "MAI0874627901_1"[1] 77.245.32.68 #67: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
09:54:10.24331 "MAI0874627901_1"[1] 77.245.32.68 #67: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
09:54:10.24355 "MAI0874627901_1"[1] 77.245.32.68 #67: STATE_MAIN_R2: sent MR2, expecting MI3
09:55:18.23344 "MAI0874627901_1"[1] 77.245.32.68 #66: max number of retransmissions (2) reached STATE_MAIN_R2
09:55:20.23351 "MAI0874627901_1"[1] 77.245.32.68 #67: max number of retransmissions (2) reached STATE_MAIN_R2
```

Der **Responder** ist ein STATE_MAIN_R2 und erwartet die dritte *Main Mode* Meldung (**MI3**) vom **Initiator**. Er erhält jedoch keine Meldung. Deshalb er damit fort, **MR2-Meldungen** zu versenden.

Grund:

- UDP-Daten, die an den UDP-Port 4500 gesendet werden, werden von irgendeiner Instanz zwischen den beiden VPN-Gegenstellen geblockt.
- Wenn der **Initiator** sich hinter einer Firewall befindet, könnte es sein, dass die Firewall den ausgehenden *Traffic* über den UDP-Port 500 blockiert.
- Wenn der **Responder** sich hinter einem NAT-Router befindet, könnte es sein, dass Port-Weiterleitung für eingehenden *Traffic* auf UDP-Port 500 zur IP-Adresse des **Responders** nicht konfiguriert ist. Oder der NAT-Router ist an anderer Stelle „falsch“ konfiguriert.

15.3.4 Init.: “ignoring informational payload, type INVALID_ID_INFORMATION”

Initiator Log:

```
10:00:07.10837 "MAI1950251842_1" #61: initiating Main Mode
10:00:09.02070 "MAI1950251842_1" #61: received Vendor ID payload [Openswan (this version) 2.6.24 ]
10:00:09.02074 "MAI1950251842_1" #61: received Vendor ID payload [Dead Peer Detection]
10:00:09.02077 "MAI1950251842_1" #61: received Vendor ID payload [RFC 3947] method set to=109
10:00:09.02081 "MAI1950251842_1" #61: received Vendor ID payload [Innominate IKE Fragmentation]
10:00:09.02085 "MAI1950251842_1" #61: received Vendor ID payload [Innominate always send NAT-OA]
10:00:09.02089 "MAI1950251842_1" #61: enabling possible NAT-traversal with method 4
10:00:09.02093 "MAI1950251842_1" #61: enabling Innominate IKE Fragmentation (main_inR1_outI2)
10:00:09.02108 "MAI1950251842_1" #61: enabling Innominate Always Send NAT-OA (main_inR1_outI2)
10:00:09.34262 "MAI1950251842_1" #61: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
10:00:09.34270 "MAI1950251842_1" #61: STATE_MAIN_I2: sent MI2, expecting MR2
10:00:11.70805 "MAI1950251842_1" #61: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
10:00:11.70817 "MAI1950251842_1" #61: I am sending my cert
10:00:11.70821 "MAI1950251842_1" #61: I am sending a certificate request
10:00:11.70929 "MAI1950251842_1" #61: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
10:00:11.70948 "MAI1950251842_1" #61: STATE_MAIN_I3: sent MI3, expecting MR3
10:00:11.71746 "MAI1950251842_1" #61: ignoring informational payload, type INVALID_ID_INFORMATION msgid=00000000
10:00:11.71750 "MAI1950251842_1" #61: received and ignored informational message
```

Der **Initiator** hat seine dritte Main Mode Meldung (**MI3**) gesendet und erwartet nun die Antwort des **Responders** (*STATE_MAIN_I3: sent MI3, expecting MR3*). Zusammen mit der Meldung (**MI3**) hat der Initiator sein Gegenstellen-Zertifikat oder den Hash-Wert des PSK gesendet und erwartet nun entsprechende Information vom **Responder**.

Der Responder sendet nun aber kein Zertifikat oder keine Hash-Werr des PSK, sondern liefert eine *informational payload* des Typs INVALID_ID_INFORMATION.

Die Log-Einträge des Responders teilen uns mehr über die Gründe mit.

15.3.4.1 Responder: “no suitable connection for peer‘…’”

Responder Log:

```
10:00:08.88221 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
10:00:08.88231 packet from 77.245.32.68:500: received Vendor ID payload [Dead Peer Detection]
10:00:08.88238 packet from 77.245.32.68:500: received Vendor ID payload [RFC 3947] method set to=109
10:00:08.88245 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
10:00:08.88253 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
10:00:08.88261 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
10:00:08.88270 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
10:00:08.88277 packet from 77.245.32.68:500: received Vendor ID payload [Innominate IKE Fragmentation]
10:00:08.88295 packet from 77.245.32.68:500: received Vendor ID payload [Innominate always send NAT-OA]
10:00:08.88304 "MAI0874627901_1"[1] 77.245.32.68 #73: responding to Main Mode from unknown peer 77.245.32.68
10:00:08.88312 "MAI0874627901_1"[1] 77.245.32.68 #73: enabling Innominate IKE Fragmentation (main_inI1_outR1)
10:00:08.88320 "MAI0874627901_1"[1] 77.245.32.68 #73: enabling Innominate Always Send NAT-OA (main_inI1_outR1)
10:00:08.88389 "MAI0874627901_1"[1] 77.245.32.68 #73: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
10:00:08.88433 "MAI0874627901_1"[1] 77.245.32.68 #73: STATE_MAIN_R1: sent MR1, expecting MI2
10:00:09.45098 "MAI0874627901_1"[1] 77.245.32.68 #73: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
10:00:11.23116 "MAI0874627901_1"[1] 77.245.32.68 #73: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
10:00:11.23140 "MAI0874627901_1"[1] 77.245.32.68 #73: STATE_MAIN_R2: sent MR2, expecting MI3
10:00:11.71884 "MAI0874627901_1"[1] 77.245.32.68 #73: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 3'
10:00:11.71893 "MAI0874627901_1"[1] 77.245.32.68 #73: issuer cacert not found
10:00:11.71900 "MAI0874627901_1"[1] 77.245.32.68 #73: X.509 certificate rejected
10:00:11.71908 "MAI0874627901_1"[1] 77.245.32.68 #73: no suitable connection for peer 'O=Innominate, OU=Support, CN=mGuard 3'
10:00:11.71916 "MAI0874627901_1"[1] 77.245.32.68 #73: sending encrypted notification INVALID_ID_INFORMATION to 77.245.32.68:500
```

Der **Responder** hat die dritte *Main Mode* Meldung (MI3) erhalten. Es ist aber keine VPN-Verbindung konfiguriert, die ein Zertifikat entählt, das mit dem *Subject* des übermittelten Zertifikats übereinstimmt.

Möglich Gründe:

– Das Zertifikat oder der *Pre-Shared Key* (PSK) stimmten nicht überein.

  Wenn ein PSK für die Authentifizierung verwendet wird, stellen Sie sicher, dass auch der gleich PSK von beiden Gegenstellen verwendet wird. (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**, Parameter Pre-Shared Secret Key (PSK))

  Wenn Zertifikate für die Authentifizierung verwendet werden, vergleichen Sie die SHA-256-Fingerprints des Maschinenzertifikats (Client-Zertifikat) des **Initiators** (Menu **Authentifizierung >> Zertifikate >> Maschinenzertifikat**) mit dem Fingerprint des Remote-Zertifikats in der entsprechenden VPN-Verbindung des Responders (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**).

– Der angegebene VPN-Identifier (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**) stimmt nicht überein. Log-Eintrag: z. B. "*no suitable connection for peer '@mGuard 1'*"

15.3.4.2 Responder: "Signature check (on …) failed (wrong key?)"

Responder Log:

```
10:30:56.12114 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
10:30:56.12123 packet from 77.245.32.68:500: received Vendor ID payload [Dead Peer Detection]
10:30:56.12130 packet from 77.245.32.68:500: received Vendor ID payload [RFC 3947] method set to=109
10:30:56.12138 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
10:30:56.12146 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
10:30:56.12154 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
10:30:56.12162 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
10:30:56.12169 packet from 77.245.32.68:500: received Vendor ID payload [Innominate IKE Fragmentation]
10:30:56.12187 packet from 77.245.32.68:500: received Vendor ID payload [Innominate always send NAT-OA]
10:30:56.12196 "MAI0874627901_1"[1] 77.245.32.68 #94: responding to Main Mode from unknown peer 77.245.32.68
10:30:56.12204 "MAI0874627901_1"[1] 77.245.32.68 #94: enabling Innominate IKE Fragmentation (main_inI1_outR1)
10:30:56.12212 "MAI0874627901_1"[1] 77.245.32.68 #94: enabling Innominate Always Send NAT-OA (main_inI1_outR1)
10:30:56.12324 "MAI0874627901_1"[1] 77.245.32.68 #94: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
10:30:56.12371 "MAI0874627901_1"[1] 77.245.32.68 #94: STATE_MAIN_R1: sent MR1, expecting MI2
10:30:56.71292 "MAI0874627901_1"[1] 77.245.32.68 #94: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
10:30:58.51165 "MAI0874627901_1"[1] 77.245.32.68 #94: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
10:30:58.51189 "MAI0874627901_1"[1] 77.245.32.68 #94: STATE_MAIN_R2: sent MR2, expecting MI3
10:30:59.00185 "MAI0874627901_1"[1] 77.245.32.68 #94: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 1'
10:30:59.00233 "MAI0874627901_1"[1] 77.245.32.68 #94: issuer cacert not found
10:30:59.00241 "MAI0874627901_1"[1] 77.245.32.68 #94: X.509 certificate rejected
10:30:59.00248 "MAI0874627901_1"[1] 77.245.32.68 #94: Signature check (on O=Innominate, OU=Support, CN=mGuard 1) failed (wrong key?);
                                                      tried *AwEAAcBS4
```

Grund:

Das Maschinenzertifikat des **Initiators** wurde durch ein neues ersetzt. Das neue Zertifikat hat die gleichen *subject*-Attribute wie das ursprüngliche.

Auf der Seite des **Responders** ist das angegebene Gegenstellenzertifikat (Maschinenzertifikat des **Initiators**) immer noch das ursprünglich Maschinenzertifikat des **Initiators** (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**).

15.3.5 Initiator: “Signature Check (on …) failed (wrong key?)”

Initiator Log:

```
10:33:56.63023 "MAI1950251842_1" #85: initiating Main Mode
10:33:58.47973 "MAI1950251842_1" #85: received Vendor ID payload [Openswan (this version) 2.6.24 ]
10:33:58.47977 "MAI1950251842_1" #85: received Vendor ID payload [Dead Peer Detection]
10:33:58.47981 "MAI1950251842_1" #85: received Vendor ID payload [RFC 3947] method set to=109
10:33:58.47985 "MAI1950251842_1" #85: received Vendor ID payload [Innominate IKE Fragmentation]
10:33:58.47989 "MAI1950251842_1" #85: received Vendor ID payload [Innominate always send NAT-OA]
10:33:58.47993 "MAI1950251842_1" #85: enabling possible NAT-traversal with method 4
10:33:58.47997 "MAI1950251842_1" #85: enabling Innominate IKE Fragmentation (main_inR1_outI2)
10:33:58.48012 "MAI1950251842_1" #85: enabling Innominate Always Send NAT-OA (main_inR1_outI2)
10:33:58.81901 "MAI1950251842_1" #85: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
10:33:58.81909 "MAI1950251842_1" #85: STATE_MAIN_I2: sent MI2, expecting MR2
10:34:01.19738 "MAI1950251842_1" #85: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
10:34:01.19750 "MAI1950251842_1" #85: I am sending my cert
10:34:01.19753 "MAI1950251842_1" #85: I am sending a certificate request
10:34:01.19861 "MAI1950251842_1" #85: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
10:34:01.19880 "MAI1950251842_1" #85: STATE_MAIN_I3: sent MI3, expecting MR3
10:34:01.24550 "MAI1950251842_1" #85: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 2'
10:34:01.24554 "MAI1950251842_1" #85: issuer cacert not found
10:34:01.24558 "MAI1950251842_1" #85: X.509 certificate rejected
10:34:01.24561 "MAI1950251842_1" #85: Signature check (on O=Innominate, OU=Support, CN=mGuard 2) failed (wrong key?); tried *AwEAAbns8
10:34:01.24566 "MAI1950251842_1" #85: sending encrypted notification INVALID_KEY_INFORMATION to 77.245.33.67:4500
```

Grund:

Das Maschinenzertifikat des **Responders** wurde durch ein neues ersetzt. Das neue Zertifikat hat die gleichen *subject*-Attribute wie das ursprüngliche.

Auf der Seite des **Initiators** ist das angegebene Gegenstellenzertifikat (Maschinenzertifikat des **Responders**) immer noch das ursprünglich Maschinenzertifikat des **Responders** (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**).

15.3.6 Initiator: “we require peer to have ID ‘…’, but peer declares ‘…’”

Initiator Log:

```
10:06:12.36092 "MAI1950251842_1" #67: initiating Main Mode
10:06:14.17361 "MAI1950251842_1" #67: received Vendor ID payload [Openswan (this version) 2.6.24 ]
10:06:14.17365 "MAI1950251842_1" #67: received Vendor ID payload [Dead Peer Detection]
10:06:14.17369 "MAI1950251842_1" #67: received Vendor ID payload [RFC 3947] method set to=109
10:06:14.17373 "MAI1950251842_1" #67: received Vendor ID payload [Innominate IKE Fragmentation]
10:06:14.17377 "MAI1950251842_1" #67: received Vendor ID payload [Innominate always send NAT-OA]
10:06:14.17381 "MAI1950251842_1" #67: enabling possible NAT-traversal with method 4
10:06:14.17385 "MAI1950251842_1" #67: enabling Innominate IKE Fragmentation (main_inR1_outI2)
10:06:14.17400 "MAI1950251842_1" #67: enabling Innominate Always Send NAT-OA (main_inR1_outI2)
10:06:14.48008 "MAI1950251842_1" #67: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
10:06:14.48016 "MAI1950251842_1" #67: STATE_MAIN_I2: sent MI2, expecting MR2
10:06:16.85786 "MAI1950251842_1" #67: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
10:06:16.85798 "MAI1950251842_1" #67: I am sending my cert
10:06:16.85801 "MAI1950251842_1" #67: I am sending a certificate request
10:06:16.85848 "MAI1950251842_1" #67: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
10:06:16.85867 "MAI1950251842_1" #67: STATE_MAIN_I3: sent MI3, expecting MR3
10:06:16.90526 "MAI1950251842_1" #67: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 3'
10:06:16.90531 "MAI1950251842_1" #67: issuer cacert not found
10:06:16.90534 "MAI1950251842_1" #67: X.509 certificate rejected
10:06:16.90538 "MAI1950251842_1" #67: we require peer to have ID 'O=Innominate, OU=Support, CN=mGuard 2', but peer declares
                                      'O=Innominate, OU=Support, CN=mGuard 3'
10:06:16.90543 "MAI1950251842_1" #67: sending encrypted notification INVALID_ID_INFORMATION to 77.245.33.67:4500
10:06:16.90933 "MAI1950251842_1" #67: received 1 malformed payload notifies
```

Der **Initiator** hat die dritte *Main Mode* Antwort (**MR3**) des **Responders** erhalten. Darin enthalten sind das Gegenstellen-Zertifikat (Maschinenzertifikat des Responders), aber das *subject* des Zertifikats stimmt nicht mit dem *subject* überein, das im Gegenstellen-Zertifikat der VPN-Verbindung angegeben wurde (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**).

Responder Log:

```
10:06:14.03024 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
10:06:14.03033 packet from 77.245.32.68:500: received Vendor ID payload [Dead Peer Detection]
10:06:14.03040 packet from 77.245.32.68:500: received Vendor ID payload [RFC 3947] method set to=109
10:06:14.03047 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
10:06:14.03055 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
10:06:14.03063 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
10:06:14.03071 packet from 77.245.32.68:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
10:06:14.03078 packet from 77.245.32.68:500: received Vendor ID payload [Innominate IKE Fragmentation]
10:06:14.03096 packet from 77.245.32.68:500: received Vendor ID payload [Innominate always send NAT-OA]
10:06:14.03105 "MAI0874627901_1"[1] 77.245.32.68 #79: responding to Main Mode from unknown peer 77.245.32.68
10:06:14.03113 "MAI0874627901_1"[1] 77.245.32.68 #79: enabling Innominate IKE Fragmentation (main_inI1_outR1)
10:06:14.03120 "MAI0874627901_1"[1] 77.245.32.68 #79: enabling Innominate Always Send NAT-OA (main_inI1_outR1)
10:06:14.03188 "MAI0874627901_1"[1] 77.245.32.68 #79: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
10:06:14.03232 "MAI0874627901_1"[1] 77.245.32.68 #79: STATE_MAIN_R1: sent MR1, expecting MI2
10:06:14.65862 "MAI0874627901_1"[1] 77.245.32.68 #79: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): both are NATed
10:06:16.39205 "MAI0874627901_1"[1] 77.245.32.68 #79: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
10:06:16.39228 "MAI0874627901_1"[1] 77.245.32.68 #79: STATE_MAIN_R2: sent MR2, expecting MI3
10:06:16.90888 "MAI0874627901_1"[1] 77.245.32.68 #79: Main mode peer ID is ID_DER_ASN1_DN: 'O=Innominate, OU=Support, CN=mGuard 1'
10:06:16.90896 "MAI0874627901_1"[1] 77.245.32.68 #79: issuer cacert not found
10:06:16.90904 "MAI0874627901_1"[1] 77.245.32.68 #79: X.509 certificate rejected
10:06:16.90911 "MAI0874627901_1"[1] 77.245.32.68 #79: I am sending my cert
10:06:16.91022 "MAI0874627901_1"[1] 77.245.32.68 #79: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
10:06:16.91038 "MAI0874627901_1"[1] 77.245.32.68 #79: new NAT mapping for #79, was 77.245.32.68:500, now 77.245.32.68:4500
10:06:16.91091 "MAI0874627901_1"[1] 77.245.32.68 #79: new NAT mapping for #78, was 77.245.32.68:500, now 77.245.32.68:4500
10:06:16.91111 "MAI0874627901_1"[1] 77.245.32.68 #79: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_RSA_SIG
                                                      cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
10:06:16.91121 "MAI0874627901_1"[1] 77.245.32.68 #79: Dead Peer Detection (RFC 3706): enabled
10:06:16.91576 "MAI0874627901_1"[1] 77.245.32.68 #79: next payload type of ISAKMP Hash Payload has an unknown value: 234
10:06:16.91604 "MAI0874627901_1"[1] 77.245.32.68 #79: next payload type of ISAKMP Hash Payload has an unknown value: 234
```

Aufgrund des Zertifikats-Fehlers, antwortet der **Responder** mit INVALID_ID_INFORMATION.

Die *ISAKMP SA* wurde erfolgreich vom **Responder** aufgebaut. Er erwartet nun die ersten Pakte für den Aufbau einer *IPsec SA*, aber er erhält keine.

Mögliche Gründe:

– Die Zertifikate stimmen nicht überein.

  Vergleichen Sie die SHA-256-Fingerprints des Maschinenzertifikats des **Responders** (Menü **Authentifizierung >> Zertifikate >> Maschinenzertifikat)** mit dem Fingerprint des Gegenstellenzertifikats (Maschinenzertifikat des **Responders**) in der entsprechenden VPN-Verbindung des **Initiators** (Menü **IPsec VPn >> Verbindungen >> (Edit) >> Authentifizierung**).

– Der angegebene VPN-Identifier (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Authentifizierung**) stimmt nicht überein. Log-Eintrag: z. B. “*we require peer to have ID 'O=Innominate, OU=Support, CN=mGuard 2', but peer declares '@mGuard 2*'”.

15.4 IPSec SA (Phase II) kann nicht aufgebaut werden

Die *IPsec SA* wird unter Verwendung des *Quick Mode*, der über das *Internet Key Exchange* (IKE) Protokoll bereitgestellt wird. Grundsätzlich werden in diesem Modus drei Meldungen ausgetauscht.

Wenn der Aufbau einer *IPsec SA* fehlschlägt, liegt der Grund in einer unterschiedlichen Konfiguration.

Entweder passen die konfigurierten VPN-Netzwerke und/oder die Hash-Algorithmen für die *IPsec SA* (Menü **IPsec VPN >> Verbindungen >> (Edit) >> IKE-Optionen**) nicht überein oder die Option *Perfect Forward Secrecy* ist nur beim **Responder** und nicht beim **Initiator** aktiviert.

15.4.1 Initiator: “ignoring informational payload, type NO_PROPOSAL_CHOSEN”

Initiator Log:

```
15:50:00.48413 "MAI1950251842_1" #80: initiating Main Mode
---------- Establishment of the ISAKMP SA ----------
15:50:05.34633 "MAI1950251842_1" #80: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_RSA_SIG cipher=oakley_3des_cbc_192
                                      prf=oakley_md5 group=modp8192}
15:50:05.34638 "MAI1950251842_1" #80: Dead Peer Detection (RFC 3706): enabled

15:50:05.34642 "MAI1950251842_1" #81: initiating Quick Mode RSASIG+ENCRYPT+TUNNEL+PFS+UP {using isakmp#80 msgid:738f09c4
                                      proposal=AES(12)_128-MD5(1)_128 pfsgroup=OAKLEY_GROUP_MODP8192}
15:50:05.64835 "MAI1950251842_1" #80: ignoring informational payload, type NO_PROPOSAL_CHOSEN msgid=00000000
15:50:05.64839 "MAI1950251842_1" #80: received and ignored informational message
```

Responder Log:

```
15:50:00.94309 "MAI0874627901_1"[1] 77.245.32.68 #90: responding to Main Mode from unknown peer 77.245.32.68
---------- Establishment of the ISAKMP SA ----------
15:50:03.83320 "MAI0874627901_1"[1] 77.245.32.68 #90: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_RSA_SIG
                                                      cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
15:50:03.83330 "MAI0874627901_1"[1] 77.245.32.68 #90: Dead Peer Detection (RFC 3706): enabled

15:50:04.32312 "MAI0874627901_1"[1] 77.245.32.68 #90: the peer proposed: 192.168.20.0/24:0/0 -> 192.168.10.0/24:0/0
15:50:04.32337 "MAI0874627901_1"[1] 77.245.32.68 #91: IPsec Transform [ESP_AES (128), AUTH_ALGORITHM_HMAC_MD5] refused due to strict
                                                      flag
15:50:04.32424 "MAI0874627901_1"[1] 77.245.32.68 #91: no acceptable Proposal in IPsec SA
```

Grund:

Die angegebenen Verschlüsselungs- und/oder Hash-Algorithmen für die *IPsec SA* stimmen nicht überein. Beide VPN-Verbindungen müssen die gleichen Verschlüsselungs- und Hashalgorithmen unterstützen.

Prüfen Sie die angegebenen Verschlüsselungs- und Hash-Algorithmen für die *IPsec SA* auf der Seite des Initiators und des Responders (Menü **IPsec VPN >> Verbindungen >> (Edit) >> IKE-Optionen,** Sektion **IPsec SA (Datenaustausch)**).

15.4.2 Initiator: “ignoring informational payload, type INVALID_ID_INFORMATION”

Initiator Log:

```
16:08:21.07207 "MAI1950251842_1" #104: initiating Main Mode
---------- Establishment of the ISAKMP SA ----------
16:08:25.85346 "MAI1950251842_1" #104: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_RSA_SIG
                cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
16:08:25.85351 "MAI1950251842_1" #104: Dead Peer Detection (RFC 3706): enabled
16:08:25.85354 "MAI1950251842_1" #105: initiating Quick Mode RSASIG+ENCRYPT+TUNNEL+PFS+UP {using isakmp#104 msgid:ed708573
                proposal=3DES(3)_192-MD5(1)_128 pfsgroup=OAKLEY_GROUP_MODP8192}
16:08:26.20417 "MAI1950251842_1" #104: ignoring informational payload, type INVALID_ID_INFORMATION msgid=00000000
16:08:26.20422 "MAI1950251842_1" #104: received and ignored informational message
```

Responder Log:

```
16:08:21.51698 "MAI0874627901_1"[1] 77.245.32.68 #126: responding to Main Mode from unknown peer 77.245.32.68
---------- Establishment of the ISAKMP SA ----------
16:08:24.41158 "MAI0874627901_1"[1] 77.245.32.68 #126: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_RSA_SIG
                cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
16:08:24.41169 "MAI0874627901_1"[1] 77.245.32.68 #126: Dead Peer Detection (RFC 3706): enabled
16:08:24.87992 "MAI0874627901_1"[1] 77.245.32.68 #126: the peer proposed: 192.168.20.0/24:0/0 -> 192.168.10.0/24:0/0
16:08:24.88001 "MAI0874627901_1"[1] 77.245.32.68 #126: cannot respond to IPsec SA request because no connection is known for
                192.168.20.0/24===192.168.3.1[O=Innominate, OU=Support, CN=mGuard 2]...77.245.32.68[O=Innominate, OU=Support,
                CN=mGuard 1]===192.168.10.0/24
16:08:24.88012 "MAI0874627901_1"[1] 77.245.32.68 #126: sending encrypted notification INVALID_ID_INFORMATION to 77.245.32.68:4500
```

Grund:

Die angegebenen VPN-Netzwerke stimmen beim Initiator und beim Responder nicht überein (Menü **IPsec VPN >> Verbindungen >> (Edit) >> Allgemein**).

Das Netzwerk, das auf der einen Seite als *Lokales Netzwerk* angegeben wurde, muss auf der anderen Seite als *Remote-Netzwerk* (Netzwerk der Gegenstelle) angegeben werden und umgekehrt.

15.4.3 Initiator: “No acceptable response to our first Quick Mode message: perhaps peer likes no proposal”

Initiator Log:

```
09:20:12.96824 "MAI1950251842_1" #15: initiating Main Mode
---------- Establishment of the ISAKMP SA ----------
09:20:17.64568 "MAI1950251842_1" #15: STATE_MAIN_I4: ISAKMP SA established {auth=OAKLEY_RSA_SIG
                                      cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
09:20:17.64573 "MAI1950251842_1" #15: Dead Peer Detection (RFC 3706): enabled
09:20:17.64577 "MAI1950251842_1" #16: initiating Quick Mode RSASIG+ENCRYPT+TUNNEL+UP {using isakmp#15 msgid:1acc17dd
                                      proposal=3DES(3)_192-MD5(1)_128 pfsgroup=no-pfs}
09:21:27.63790 "MAI1950251842_1" #16: max number of retransmissions (2) reached STATE_QUICK_I1. No acceptable response to our
                                      first Quick Mode message: perhaps peer likes no proposal
```

Responder Log:

```
09:20:14.74888 packet from 77.245.32.68:500: received Vendor ID payload [Openswan (this version) 2.6.24 ]
---------- Establishment of the ISAKMP SA ----------
09:20:17.63925 "MAI0874627901_1"[1] 77.245.32.68 #5: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_RSA_SIG
                                                     cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp8192}
09:20:17.63935 "MAI0874627901_1"[1] 77.245.32.68 #5: Dead Peer Detection (RFC 3706): enabled
09:20:17.65065 "MAI0874627901_1"[1] 77.245.32.68 #5: the peer proposed: 192.168.20.0/24:0/0 -> 192.168.10.0/24:0/0
09:20:17.65090 "MAI0874627901_1"[1] 77.245.32.68 #6: we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION
```

Grund:

Die Option *Perfect Forward Secrecy* (PFS) ist nur beim **Responder** und nicht beim **Initiator** aktiviert (Menü **IPsec VPN >> Verbindungen >> (Edit) >> IKE-Optionen**, Sektion **IPsec SA (Datenaustausch)**).

15.5 Remote-Clients können nicht über aufgebauten VPN-Tunnel erreicht werden

Wenn die VPN-Verbindung erfolgreich aufgebaut wurde, aber keine Daten durch den VPN-Tunnel gesendet werden können, dann liegt das Problem häufig nicht in der Konfiguration der mGuard-Geräte sonder hat externe Gründe.

Wenn VPN-Maskierung (*Masquerading*) von einem mGuard-Gerät verwendet wird, kann die Verbindung nur von dem maskierten Netzwerk aus zum anderen Netzwerk aufgebaut werden. Ein Aufbau in die andere Richtung ist nicht möglich.

Die folgenden Schritte helfen dabei, das Problem einzukreisen und genauer zu analysieren (vorausgesetzt, ICPM-Pakete werden nicht von einer VPN-Firewall geblockt).

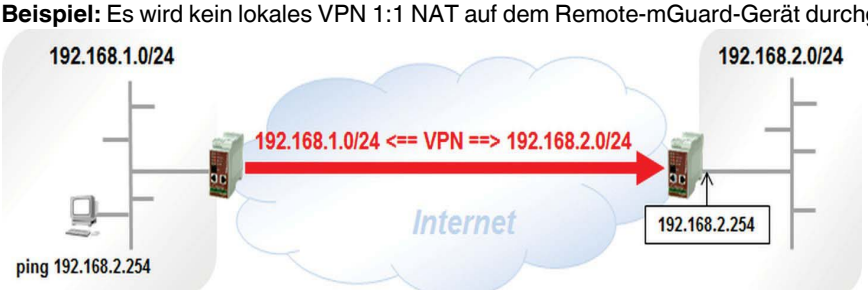
Schritt 1: Kann eine Client im lokalen Netzwerk die interne IP-Adresse des lokalen mGuard-Geräts erreichen?

- Prüfen Sie mit einem Client, der das VPN-Netzwerk der Gegenstelle erreichen soll, ob er auf die interne IP-Adresse des lokalen mGuard-Geräts zugreifen kann.
- Senden Sie eine Ping-Anfrage von dem Client zur internen IP-Adresse des lokalen mGuard-Geräts.
- Wenn die Ping-Anfrage nicht beantwortet wird, liegt das Problem im internen Netzwerk.
- Wenn die Ping-Anfrage beantwortet wird, fahren Sie mit fort mit Schritt 2.

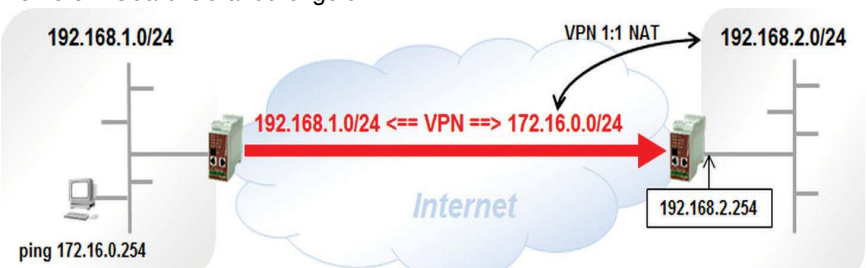
Schritt 2: Ist die interne IP-Adresse des mGuard-Geräts der Gegenstelle durch den VPN-Tunnel erreichbar?

- Prüfen Sie mit einem Client, der das VPN-Netzwerk der Gegenstelle erreichen soll, ob er die interne IP-Adresse des Remote-mGuard-Geräts erreichen kann.
- Senden Sie eine Ping-Anfrage von dem Client zur internen IP-Adresse des Remote-mGuard-Geräts (mGuard-Gerät der Gegenstelle) durch den VPN-Tunnel.
- Prüfen Sie, ob die Ping-Anfrage vom mGuard-Gerät der Gegenstelle durch den VPN-Tunnel beantwortet wird.

Beispiel: Es wird kein lokales VPN 1:1 NAT auf dem Remote-mGuard-Gerät durchgeführt.



Beispiel: Es wird ein lokales VPN 1:1 NAT von 172.16.0.0/24 nach 192.168.2.0/24 auf dem Remote-mGuard-Gerät durchgeführt.



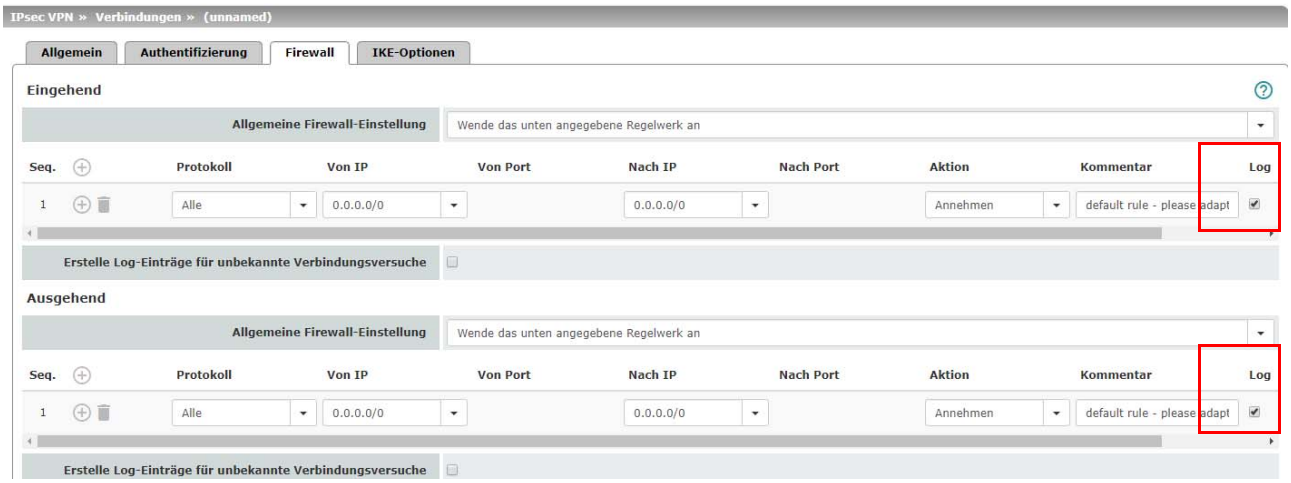
Wenn die Ping-Anfrage beantwortet wird, liegt der Grund dafür, dass Clients im Remote-Netzwerk nicht über VPN erreicht werden können, im Remote-Netzwerk selbst.

Ein möglicher Grund wäre, dass die interne IP-Adresse des Remote-mGuard-Geräts nicht als Standard-Gateway der Remote-Clients angegeben ist.

Wenn die Ping-Anfrage nicht beantwortet wird, fahren Sie fort mit Schritt 3.

Schritt 3: Werden die Pakete durch den VPN-Tunnel gesendet und kommen Sie bei der Gegenseite an?

- Prüfen Sie, ob die gesendeten Pakete durch den VPN-Tunnel gesendet werden und ob sie im Netzwerk der Gegenstelle ankommen.
- Aktivieren Sie das Logging für die VPN-Firewall auf beiden mGuard-Geräten (Lokal und Remote).
- Bearbeiten Sie die entsprechende VPN-Verbindung (Menu **IPsec VPN >> Verbindungen >> (Edit) >> Firewall**).
- Setzen Sie ein Häkchen bei der Checkbox *Log*.



- Klicken Sie auf das Icon <*Übernehmen*>.

Die VPN-Verbindung wird durch die Konfigurationsänderung kurzzeitig unterbrochen. Warten Sie, bis die VPN-Verbindung erneut aufgebaut wurde (Menü **IPsec VPN >> IPsec-Status**). Senden Sie Daten vom lokalen in das Remote-Netzwerk und prüfen Sie anschließend die Log-Einträge für die VPN-Firewall (Menu **Logging >> Logs ansehen**, Option Netzwerksicherheit).

Beispiel Log-Eintrag: ICMP echo requests entering the VPN tunnel (fw-vpn_...-out-...)

14:57:33.68468 kernel: **fw-vpn**_MAI1950251842-**out**-1-123bacb5-b892-103f-88ac-000cbe020f10 act=ACCEPT IN=eth1 OUT=eth0 SRC=192.168.1.100 DST=192.168.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=20250 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=5632
14:57:38.95374 kernel: **fw-vpn**_MAI1950251842-**out**-1-123bacb5-b892-103f-88ac-000cbe020f10 act=ACCEPT IN=eth1 OUT=eth0 SRC=192.168.1.100 DST=192.168.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=20251 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=5888

Beispiel Log-Eintrag: ICMP echo requests received through the VPN tunnel (fw-vpn_...-in-…)

```
14:57:33.68384 kernel: fw-vpn_MAI0874627901-in-1-2a407f3f-1020-1141-a3a4-000cbe020e08 act=ACCEPT IN=eth0 OUT=eth1 SRC=192.168.10.100
DST=192.168.1.1 LEN=60 TOS=0x00 PREC=0x00 TTL=126 ID=20250 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=5632
14:57:38.95130 kernel: fw-vpn_MAI0874627901-in-1-2a407f3f-1020-1141-a3a4-000cbe020e08 act=ACCEPT IN=eth0 OUT=eth1 SRC=192.168.10.100
DST=192.168.1.1 LEN=60 TOS=0x00 PREC=0x00 TTL=126 ID=20251 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=5888
```

Mögliche Ergebnisse dieses Tests:

1. Das lokale mGuard-Gerät zeigt keine entsprechenden Log-Einträge für durch den VPN-Tunnel ausgehende Pakete (*fw-vpn-...-out-...*).

   Mögliche Gründe:
   - Die interne IP-Adresse des lokalen mGuard-Geräts ist nicht als Standard-Gateway auf dem Client angegeben, der die ICMP-Anfrage sendet.
   - Wenn der Client ein anderes Standard-Gateway verwenden muss, also nicht das lokale mGuard-Gerät, dann wurde keine Route definiert, um Pakete zum Remote-VPN-Netzwerk über das lokale mGuard-Gerät zu leiten.
   - Eine Firewall zwischen dem Client und dem lokalen mGuard blockiert den Netzwerkverkehr.
   - Ein unbekanntes Problem liegt im internen Netzwerk vor.
2. Das Remote-mGuard-Gerät zeigt keine entsprechenden Log-Einträge für durch den VPN-Tunnel eingehende Pakete (*fw-vpn-...-in-...*).

   Mögliche Gründe:
   - Irgendein Netzwerkteilnehmen (Gateway, Router) zwischen den zwei VPN-Gegenstellen blockiert den verschlüsselten Netzwerkverkehr. Zwei mögliche Fälle kommen dabei in Frage:
     - Einige Netzwerkprovider erlauben eingehende verschlüsselte Pakete aus dem Internet in ihr Netzwerk nur dann, wenn ausgehende verschlüsselte Pakete für diese Verbindung bereits registriert wurden. Dies wurde sowohl bei einem Satellitennetzbetreiber als auch bei einem Telefonnetzbetreiber beobachtet. Um dies zu überprüfen, versuchen Sie, vom Remote-VPN-Netzwerk auf die Clients des lokalen VPN-Netzwerks zuzugreifen.
     - Ein Router blockiert ESP-Traffic zwischen den beiden VPN-Gegenstellen. Dieses Problem könnte durch die Verwendung von UDP-Kapselung (*UDP Encapsulation*) auf dem mGuard-Gerät gelöst werden. Die Option ist allerdings nur über die Kommandozeile verfügbar:
       gaiconfig --set VPN_CONNECTION.x.FORCE_UDP_ENCAPS yes,
       'x' steht für die Nummer der konfigurierten VPN-Verbindung (0, 1, 2, 3, …).
       Der Router blockiert dann ESP-Traffic, aber nicht UDP-Pakete, die ESP-Pakete einkapseln.

15.6 Andere Probleme

15.6.1 VPN-Verbindung wird nach 24 Stunden abgebrochen

Dieses Problem tritt üblicherweise auf, wenn der **Responder** eine dynamische öffentliche IP-Adresse verwendet, die alle 24 Stunden vom Provider neu vergeben wird. In diesem Fall wird der **Responder** seine aktuelle IP-Adresse unter einem spezifischen Namen bei einem DynDNS-Service registrieren. Der **Initiator** bezieht sich dann bei der *Adresse des VPN-Gateways der Gegenstelle* nicht auf eine IP-Adresse, sondern auf deren DynDNS-Namen.

Ein Problem ergibt sich, wenn D*ynDNS-Überwachung* auf dem **Initiator**-Gerät nicht aktiviert ist (Menü **IPsec VPN >> Global >> DynDNS-Überwachung**).

- Aktivieren Sie auf dem Initiator-Gerät die Option *Hostnamen von VPN-Gegenstellen überwachen.*
- Klicken Sie auf das Icon <*Übernehmen*>.

15.6.2 Probleme bei der Übertragung großer Daten

Ein Remote-Client reagiert problemlos auf kleine Pakete (z. B. Ping-Anfragen), aber die Übertragung großer Datenmengen (z. B. *Remote Desktop Application*) schlägt fehl.

Dieses Problem wird in der Regel durch Router im Internet verursacht, die die MTU-Größe reduzieren, aber keine UDP-Fragmentierung unterstützen. Das mGuard-Gerät empfängt Fragmente von verschlüsselten UDP-Paketen und kann diese nicht dekodieren.

Das Problem kann durch eine Reduzierung der MTU-Größe für IPsec auf dem mGuard-Gerät gelöst werden. Verschlüsselte Pakete haben dann eine geringere Größe und werden beim Passieren des Routers, der die MTU-Grüße reduziert, nicht fragmentiert.

Die IPsec MTU-Größe muss bei dem mGuard-Gerät reduziert werden, bei dem die großen Daten in den VPN-Tunnel gesendet werden (Menü **IPsec VPN >> Global >> Optionen**).

- Sektion *IP-Fragmentierung*: Reduzieren Sie die Größe der *MTU für IPsec*.
- Klicken Sie auf das Icon <Übernehmen>.

Sie müssen die MTU-Größe für IPsec sukzessive reduzieren, bis die großen Daten den Tunnel passieren können.

15.7 Quick Reference: Fehlermeldungen im VPN-Log

Tabelle 15-2 Quick Reference: Fehlermeldungen in VPN-Log-Einträgen

VPN-Log Fehlermeldungen	Gehe zu Kapitel
– ikelifetime […] must be greater than rekeymargin*(100+rekeyfuzz)/100	Kapitel 15.2
– tunnel ignored: local address 'w.x.y.x' within remote network 'a.b.c.d/e'	Kapitel 15.2
Initiator – Fehlermeldungen	
– pending Quick Mode with w.x.y.z took too long – replacing phase 1	Kapitel 15.3.2
– Possible authentication failure: no acceptable response to our first encrypted message	Kapitel 15.3.3
– discarding duplicate packet; already STATE_MAIN_I3	Kapitel 15.3.3
– ignoring informational payload, type INVALID_ID_INFORMATION (during establishment of ISAKMP SA)	Kapitel 15.3.4
– Signature Check (on ...) failed (wrong key?)	Kapitel 15.3.5
– we require peer to have ID '...', but peer declares '...'	Kapitel 15.3.6
– ignoring informational payload, type NO_PROPOSAL_CHOSEN	Kapitel 15.4.1
– ignoring informational payload, type INVALID_ID_INFORMATION (during establishment of IPsec SA)	Kapitel 15.3.4
– No acceptable response to our first Quick Mode message: perhaps peer likes no proposal	Kapitel 15.4.3
Responder – Fehlermeldungen	
– initial Main Mode message received on w.x.y.z:500 but no connection has been authorized	Kapitel 15.3.2.2
– max number of retransmissions (2) reached STATE_MAIN_R2	Kapitel 15.3.3
– no suitable connection for peer '...'	Kapitel 15.3.4.1
– Signature check (on ...) failed (wrong key?)	Kapitel 15.3.4.2
– next payload type of ISAKMP Hash Payload has an unknown value	Kapitel 15.3.6
– IPsec Transform [...] refused due to strict flag	Kapitel 15.4.1
– no acceptable Proposal in IPsec SA	Kapitel 15.4.1
– cannot respond to IPsec SA request because no connection is known for ...	Kapitel 15.3.4
– sending encrypted notification INVALID_ID_INFORMATION to …	Kapitel 15.3.4
– we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION	Kapitel 15.4.3

16 CIFS-Integrity-Monitoring verwenden

Dokument-ID: 108419_de_00
Dokument-Bezeichnung: AH DE MGUARD CIFS

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

Die Verwendung von CIFS-IM ist lizenzabhängig und nicht auf allen Geräten verfügbar.

Inhalt dieses Dokuments

In diesem Dokument wird die Verwendung der mGuard-Funktion *CIFS-Integrity-Monitoring* beschrieben.

16.1 Einleitung

CIFS steht für *Common Internet File System*, besser bekannt als *Windows File Sharing*.

CIFS-Integrity-Monitoring (CIFS-IM) ist ein industrietauglicher Antivirenschutz bzw. Antivirensensor, der ohne das Nachladen von Virussignaturen erkennen kann, ob ein Windows-basiertes System (z. B. Maschinensteuerung, Bedieneinheit, PC) mit einer Schadsoftware infiziert ist.

Bei der CIFS-Integritätsprüfung werden dabei Windows-Netzlaufwerke daraufhin geprüft, ob sich bestimmte Dateien (z. B. *.exe, *.dll) verändert haben. Eine Veränderung dieser Dateien deutet auf einen Virus oder unbefugtes Eingreifen hin.

CIFS-IM kann ebenfalls zur Versionskontrolle bzw. -überwachung verwendet werden.

16.1.1 Einsatzzweck

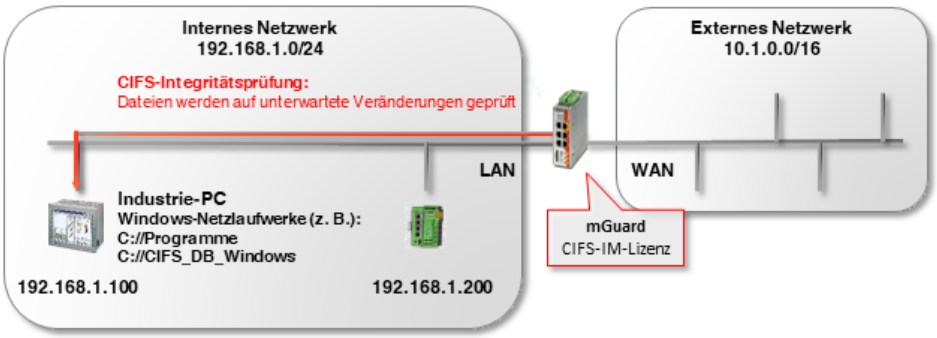


Bild 16-1 CIFS-Integrity-Monitoring – Schema

CIFS-IM wird in der Regel zusammen mit der Firewall-Funktionalität der mGuard-Geräte zur Absicherung sogenannter *Non-patchable systems* eingesetzt.

Non-patchable systems sind überwiegend Windows-basierte Systeme, die entweder

a) **über ein veraltetes Betriebssystem verfügen**, für das keine Security-Updates mehr bereitgestellt werden (z. B. Windows 2000/Windows XP),

b) **nicht verändert werden dürfen**, da der Auslieferungszustand seitens des Herstellers oder einer Behörde zertifiziert wurde, und bei einer Veränderung die Gewährleistung oder die Zulassung verlorengehen würde,

c) **nicht mit einem Virenscanner ausgerüstet werden dürfen**, z. B. aufgrund zeitkritischer industrieller Anwendungen (*Realtime*-Fähigkeit); oder es besteht keine Möglichkeit, ein Virussignatur-Update durchzuführen, da z. B. keine Verbindung ins Internet besteht.

Non-patchable systems finden sich in unterschiedlichen Bereichen der Industrie. Unter anderem in der Medizin (z. B. MRT, CT), Chemie- und Pharmaindustrie (z. B. Analysesysteme), aber auch in der Produktion (z. B. PC-basierte Maschinensteuerungen, BDE).

16.1.2 Funktionsweise

Bei der **CIFS-Integritätsprüfung** werden Windows-Netzlaufwerke darauf geprüft, ob sich bestimmte (ausführbare) Dateien (z. B. *.exe, *.dll) im Vergleich zu einem Referenzstatus in der Integritätsdatenbank unerwartet verändert haben.

Die **Integritätsdatenbank** enthält die Prüfsummen (Hash-Werte) aller geprüfter Dateien. Eine Veränderung der Prüfsumme einer Datei deutet auf eine Veränderung dieser Datei und somit auf einen Virus/Wurm oder unbefugtes Eingreifen hin. Neu hinzugefügte oder gelöschte Dateien werden ebenfalls erkannt.

Die Integritätsdatenbank wird entweder bei der ersten Prüfung eines Laufwerks erstellt oder auf explizite Veranlassung (z. B. nach einer gewollten Änderung einer oder mehrerer Dateien auf dem Netzlaufwerk). Sie ist mit einem Maschinenzertifikat des mGuard-Geräts signiert und somit vor Manipulationen geschützt.

Wird bei der CIFS-Integritätsprüfung eine Abweichung festgestellt, kann eine Alarmierung per E-Mail oder SNMP (SNMP-Trap) ausgelöst werden.

16.1.3 Vorteile gegenüber anderen Antivirus-Systemen

CIFS-Integrity-Monitoring bietet im industriellen Bereich folgende Vorteile:

a) Die Ressourcen des überwachten Systems (CPU Leistung, Netzwerkbelastung) werden nicht bzw. kaum belastet.
b) Eine Verbindung ins Internet oder zu einem Update Server ist nicht erforderlich.
c) Ein Nachladen von Virussignaturen ist nicht erforderlich.
d) Fehlalarme/falsche Treffer (*FalsePositives*) kommen in der Regel nicht vor – und falls doch, haben sie keine Auswirkungen auf das überwachte System, da keine Dateien gelöscht oder in Quarantäne verschoben werden.

16.2 Konfigurationsbeispiel

Auf einem Windows-PC soll das Verzeichnis *C://Programme* überwacht werden. Auf dem überwachten PC ist ein Benutzer mit dem Benutzernamen *CIFS* angelegt, der Lesezugriff auf das Verzeichnis *C://Programme* besitzt.

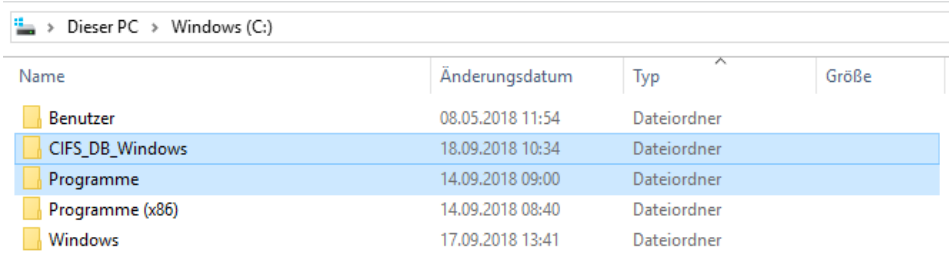


Bild 16-2 Anlage von Verzeichnissen / Integritätsdatenbank

Die Integritätsdatenbank soll auf dem überwachten PC im Verzeichnis *CIFS_DB_Windows* abgelegt werden. Der Benutzer *CIFS* besitzt auf dieses Verzeichnis ebenfalls Lese-/Schreibzugriff.

16.3 Voraussetzung

– Der zu überwachende PC befindet sich im Netzwerk 192.168.1.0/24 und ist unter der IP-Adresse 192.168.1.100 erreichbar.
– Das mGuard-Gerät ist unter der IP Adresse 192.168.1.1 erreichbar.
– Die optional zu erwerbende Lizenz *CIFS-Integrity-Monitoring* ist auf dem Gerät vorhanden.

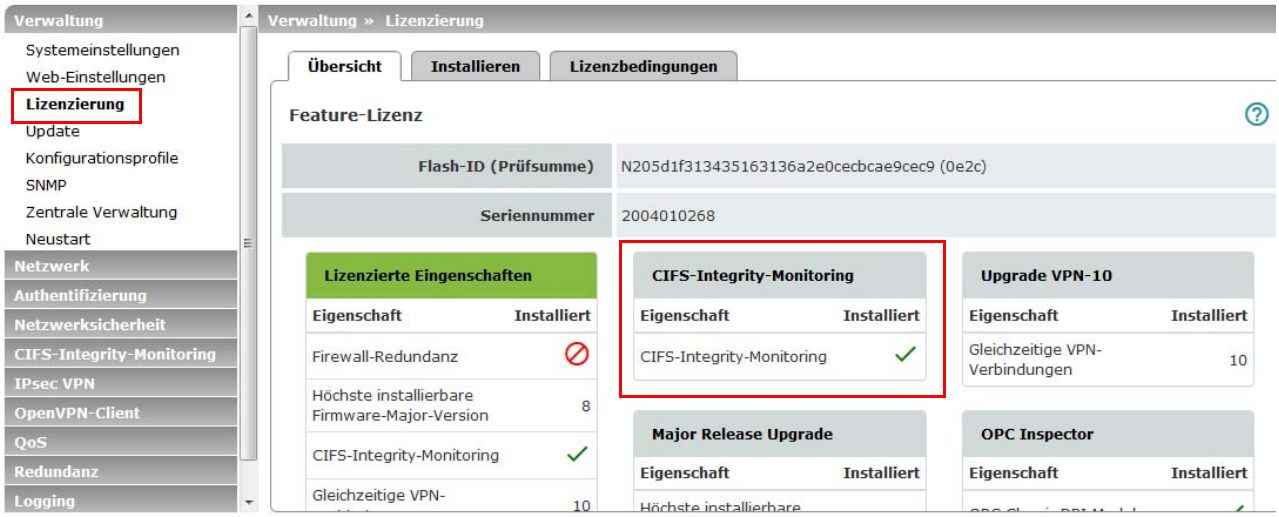


Bild 16-3 CIFS-Integrity-Monitoring-Lizenz auf dem Gerät vorhanden

Die Konfiguration von CIFS-IM wird über das Web-based Management des mGuard-Geräts vorgenommen (hier: Firmwareversion 8.7.0).

16.4 Maschinenzertifikat importieren

Das Maschinenzertifikat, das im CIFS-IM-Menü als *Integritätszertifikat* ausgewählt wird, dient zum Signieren und Prüfen der Integritätsdatenbank, damit diese nicht unbemerkt durch einen Angreifer ausgetauscht oder manipuliert werden kann.

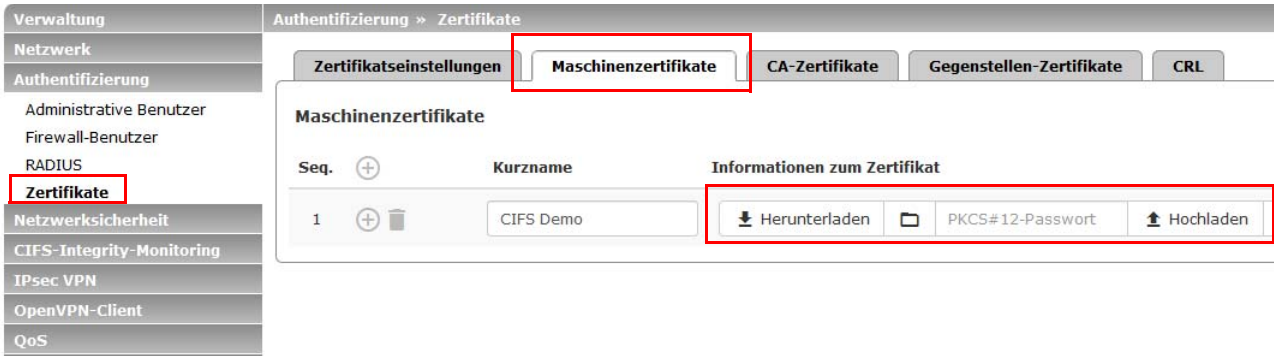


Bild 16-4 Installiertes Maschinenzertifikat zur Verwendung mit CIFS-IM

Um eine Maschinenzertifikat zu importieren, gehen Sie wie folgt vor:

1. Melden Sie sich beim Web-based Management des mGuard-Geräts an.
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 (PKCS#12) auf dem Installationsrechner auszuwählen.
5. Geben Sie das bei der Erzeugung des Zertifikats vergebene PKCS#12-Passwort an.
6. Geben Sie dem Zertifikat einen eindeutigen Kurznamen. Wenn Sie das Feld freilassen, wird automatisch der *CommonName (CN)* des Zertifikats verwendet.
7. Klicken Sie auf die Schaltfläche **Hochladen**, um das Zertifikat in das mGuard-Gerät zu importieren.
8. Klicken Sie auf das Icon 💾 „*Übernehmen*“, um den Import abzuschließen.

16.5 Netzlaufwerke konfigurieren/importieren

Die Windows-Netzlaufwerke, die überwacht werden sollen, werden auf dem mGuard-Gerät konfiguriert bzw. importiert. Der Ort, an dem die Integritätsdatenbank und der Prüfbericht gespeichert werden sollen, wird ebenfalls als Netzlaufwerk konfiguriert/importiert.

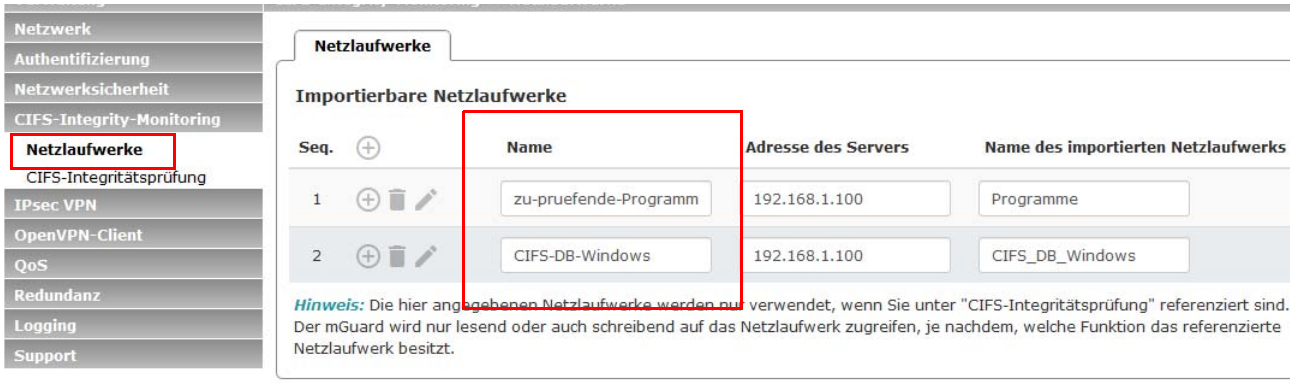


Bild 16-5 Importierte Netzlaufwerke zur Verwendung mit CIFS-IM

Um Netzlaufwerke in das mGuard-Gerät zu importieren, gehen Sie wie folgt vor:

- Gehen Sie zu **CIFS-Integrity-Monitoring >> Netzlaufwerke**.
- Klicken Sie auf das Icon ⊕, um ein neues Netzlaufwerk hinzuzufügen.
- Klicken Sie auf das Icon ✎, um das Netzlaufwerk zu konfigurieren.

Unter **Name** wird die jeweilige Bezeichnung angegeben, mit der das mGuard-Gerät die Netzlaufwerke intern verwaltet. **Name des importierten Netzlaufwerks** bezeichnet das freigegebene Windwos-Verzeichnis und muss exakt übernommen werden:

- Der **Name** *„zu-pruefende-Programme“* ist die mGuard-interne Bezeichnung für den **Namen des importierten Netzlaufwerks** *„C:\Programme“*.
- Der **Name** *„CIFS-DB-Windows“* ist die mGuard-interne Bezeichnung für den **Namen des importierten Netzlaufwerks** *„C:\CIFS_DB_Windows“*.

⇒ Die Netzlaufwerke sind dem mGuard-Gerät nun bekannt und können geprüft werden.

16.6 Parameter für Integritätsprüfung konfigurieren

Das zu verwendende Integritäts-Zertifikat, mit dem die Integritätsdatenbanken signiert werden, wird ausgewählt. Soll über durchgeführte Integritätsprüfungen per E-Mail berichtet werden, müssen die entsprechenden Angaben an dieser Stelle konfiguriert werden.

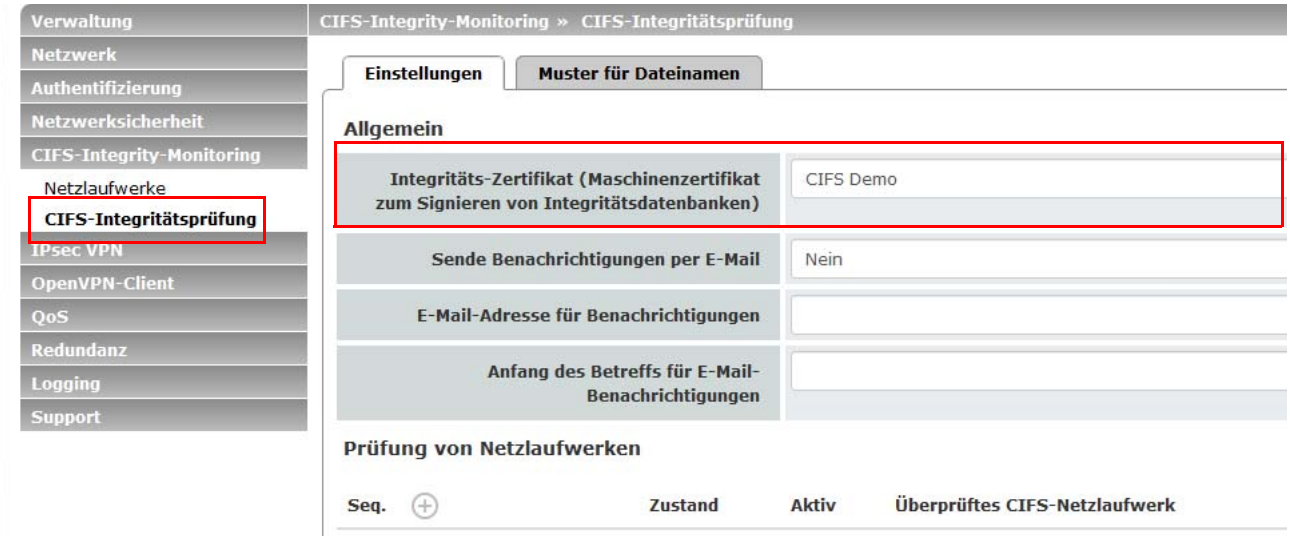


Bild 16-6 Auswahl des Maschinenzertifikats und Konfiguration der E-Mail-Benachrichtigung

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Wählen Sie das Maschinenzertifikat aus, das für CIFS-IM verwendet werden soll.
- **Optional**: Legen Sie fest, ob eine E-Mail-Benachrichtigung (bei jeder Integritätsprüfung oder nur bei gefundenen Fehlern/Abweichungen) versendet werden soll.

  Dafür benötigt das mGuard-Gerät Zugriff auf einem E-Mail-Server. Dieser wird unter **Verwaltung >> Systemeinstellungen** (Registerkarte *E-Mail*) konfiguriert.

16.7 Zu überprüfende Dateien festlegen

Auf der Registerkarte *Muster für die Dateinamen* werden die Dateitypen und/oder Dateiverzeichnisse, die in die Überwachung ein- oder ausgeschlossen werden sollen, festgelegt.

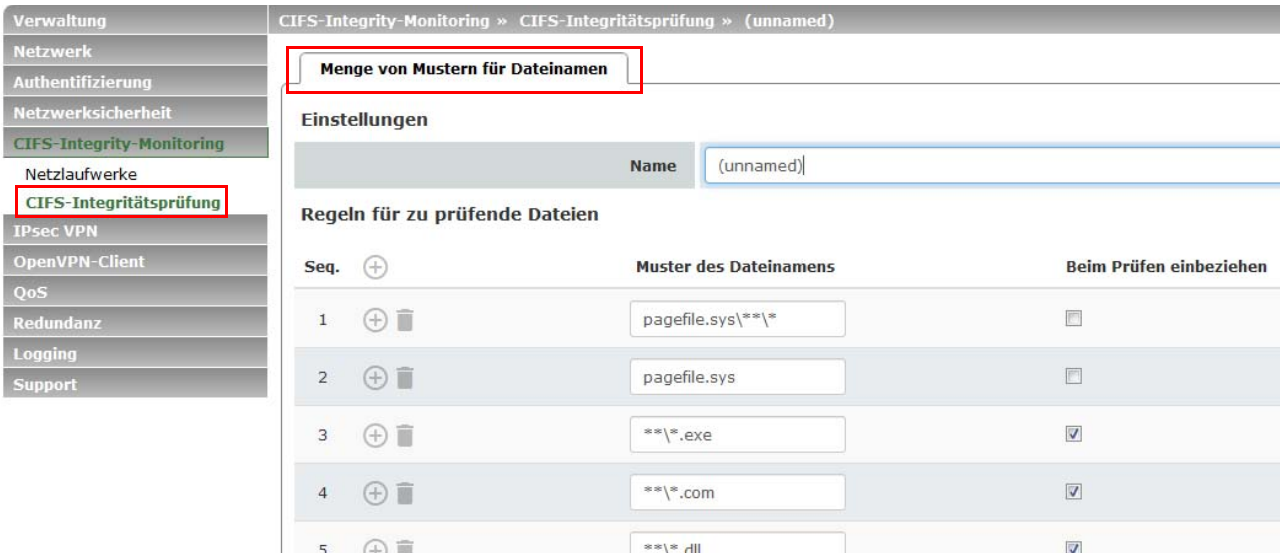


Bild 16-7 Die Dateien, die überprüft werden sollen, werden mittels Mustern festgelegt

Gehen Sie wie folgt vor:

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Muster für Dateinamen*).
- Legen Sie die Dateitypen bzw. Dateimuster fest, die überprüft werden sollen.
  Das mGuard-Gerät bietet bereits einige Datei-Muster an, die entweder übernommen oder angepasst werden können.

Muster für Dateinamen

***.exe bedeutet, dass Dateien einbezogen (oder ausgenommen) werden, die in einem beliebigen Verzeichnis liegen und die Dateiendung **.exe* haben.

** am Anfang bedeutet, dass in einem beliebigen Verzeichnis gesucht wird, auch in der obersten Ebene, wenn diese leer ist. Es kann nicht mit Zeichen kombiniert werden (z. B. *c*** ist nicht erlaubt).

Platzhalter (*) stehen für beliebige Zeichen, z. B. findet *win**.exe* Dateien mit der Endung *.exe*, die in einem Verzeichnis liegen, dass mit *win...* beginnt. Nur ein Platzhalter ist pro Verzeichnis oder Dateiname erlaubt.

Beispiel: *Name***.exe* bezieht alle Dateien mit der Endung *.exe* ein, die in dem Verzeichnis „*Name*“ und beliebigen Unterverzeichnissen liegen.

Beim Prüfen einbeziehen

Funktion **aktivieren** (= einbeziehen): Dateien werden in die Prüfung einbezogen.
Funktion **deaktivieren** (= ausnehmen): Dateien werden aus der Prüfung ausgenommen.

(Jeder Dateiname wird mit den Mustern der Reihe nach verglichen. Der erste Treffer entscheidet, ob die Datei in die Integritätsprüfung einbezogen wird. Ohne einen Treffer wird die Datei nicht einbezogen.)

16.8 Prüf-Sequenzen anlegen

Es können eine oder mehrere Prüf-Sequenzen angelegt werden, die unterschiedliche Netzlaufwerke, Verzeichnisse oder Dateitypen überprüfen.

Für jede Prüf-Sequenz wird eine zeitgesteuerte Prüfung konfiguriert (siehe auch mGuard-Firmwarehandbuch, erhältlich unter phoenixcontact.net/products oder help.mguard.com).

Bild 16-8 Prüf-Sequenz anlegen und Netzlaufwerke auswählen

Um eine Prüf-Sequenz anzulegen und dieses zu konfigurieren, gehen Sie wie folgt vor:

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Sektion **Prüfung von Netzlaufwerken**: Klicken Sie auf das Icon ⊕, um eine neue Prüf-Sequenz anzulegen.
- Wählen Sie das Netzlaufwerk, das überprüft werden soll aus der Drop-Down-Liste.
- Wählen Sie das Netzlaufwerk, das als Prüfsummenspeicher dienen soll, aus der Drop-Down-Liste.
- Klicken Sie auf das Icon ✎, um die Parameter einer Prüf-Sequenz zu konfigurieren.

Auf der Registerkarte *Überprüftes Netzlaufwerk* sind alle Parameter voreingestellt. Bei Bedarf können Sie jedoch an dieser Stelle Änderungen vornehmen.

Bild 16-9 Parameter-Einstellungen zur Überprüfung des Netzlaufwerks

16.9 Integritätsdatenbank initialisieren

Wenn ein zu prüfendes Netzlaufwerk neu konfiguriert wird, muss eine entsprechende Integritätsdatenbank angelegt werden. Diese Integritätsdatenbank dient als Vergleichsgrundlage für die regelmäßige Prüfung des Netzlaufwerks. In ihr sind die Prüfsummen aller zu überwachender Dateien aufgezeichnet. Die Integritätsdatenbank selbst ist mit dem Integritäts-Zertifikat signiert und somit gegen Manipulationen gesichert.

Auf der Registerkarte *Verwaltung* wird die Integritätsdatenbank initialisiert.

Prüfen Sie als erstes, ob das mGuard-Gerät lesenden Zugriff auf alle Dateien und Verzeichnisse im überwachten Netzlaufwerk hat (*Zugriffsüberprüfung starten*).

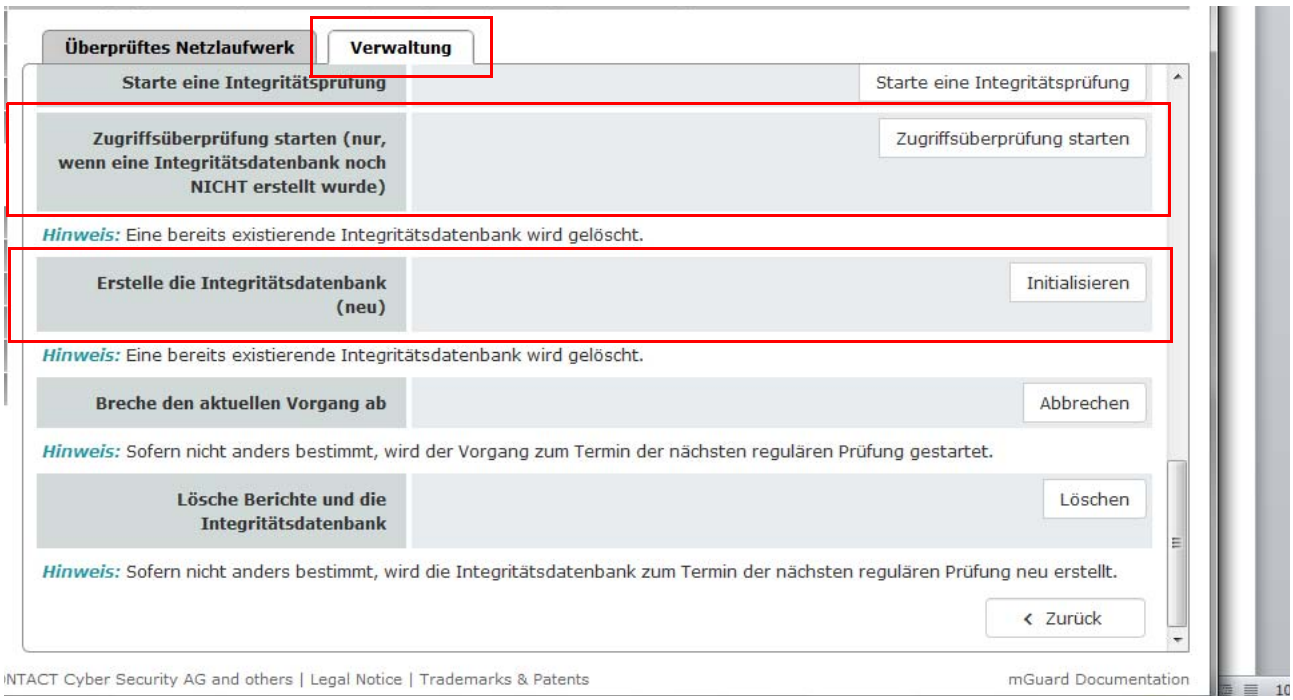


Bild 16-10 Integritätsprüfung vorbereiten und starten

Um die Integritätsdatenbank (neu) zu initialisieren, gehen Sie wie folgt vor:

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Klicken Sie in der Sektion **Prüfung von Netzlaufwerken** auf das Icon , um die Parameter einer Prüf-Sequenz zu konfigurieren.
- Auf der Registerkarte *Überprüftes Netzlaufwerk* sind alle Parameter voreingestellt. Bei Bedarf können an dieser Stelle Änderungen vorgenommen werden.
- Wechseln Sie zur Registerkarte *Verwaltung*.
- Klicken Sie auf die Schaltfläche **Zugriffsüberprüfung** starten (siehe Tabelle 16-1).

⇒ Es wird überprüft, ob die benötigten Zugriffsrechte für die Prüfung bestehen.

- Sind die Zugriffsrechte vorhanden, klicken Sie auf die Schaltfläche **Initialisieren** (siehe Tabelle 16-1).

⇒ Die Integritätsdatenbank wird erstellt und anschließend als Referenz für weitere Prüfungen verwendet.

16.10 Mögliche Aktionen bei der Erstellung einer Integritätsdatenbank

Die Aktionen, die im Rahmen des CIFS-Integrity-Monitorings ausgeführt werden können, sind in Tabelle 16-1 kurz beschrieben.

Für eine genaue Beschreibung siehe auch mGuard-Firmwarehandbuch, erhältlich unter phoenixcontact.net/products oder help.mguard.com.

Tabelle 16-1 Integritätsprüfung vorbereiten und starten – Funktionsbeschreibung

Funktionsname	Beschreibung
Starte eine Integritätsprüfung	Durch einen Klick auf die Schaltfläche *Integritätsprüfung starten*, wird mit der Integritätsprüfung begonnen. Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche *Bericht herunterladen* im Prüfbericht eingesehen werden.
Zugriffsüberprüfung starten **(nur, wenn eine Integritätsdatenbank noch NICHT erstellt wurde)**	**ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!** Durch einen Klick auf die Schaltfläche *Zugriffsüberprüfung starten* wird geprüft, ob auf dem importierten Netzlaufwerk Dateien vorhanden sind, auf die das mGuard-Gerät nicht zugreifen kann. Damit wird im Vorfeld verhindert, dass eine umfangreichere Erstellung der Integritätsdatenbank aufgrund fehlender Berechtigungen abgebrochen wird. Das Ergebnis der Prüfung kann durch einen Klick auf die Schaltfläche *Bericht herunterladen* im Prüfbericht eingesehen werden.
Erstelle die Integritätsdatenbank (neu)	**ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!** Das mGuard-Gerät legt eine Datenbank mit Prüfsummen an, um später feststellen zu können, ob sich Dateien verändert haben. Eine Veränderung von ausführbaren Dateien deutet auf einen Virenbefall hin. Wenn Dateien absichtlich neu erstellt, gelöscht oder verändert wurden, muss durch einen Klick auf die Schaltfläche *Initialisieren* eine neue Datenbank erzeugt werden, um Fehlalarme zu verhindern. Das Erzeugen einer Integritätsdatenbank ist auch sinnvoll, wenn Netzlaufwerke neu eingerichtet worden sind. Ansonsten wird statt der Prüfung beim ersten Prüftermin eine Integritätsdatenbank eingerichtet (wenn zuvor keine Zugriffsüberprüfung durchgeführt wurde).
Breche den aktuelle Vorgang ab	Durch einen Klick auf die Schaltfläche Abbrechen, wird die Integritätsprüfung gestoppt.

Tabelle 16-1 Integritätsprüfung vorbereiten und starten – Funktionsbeschreibung

Funktionsname	Beschreibung
Lösche Berichte und die Integritätsdaten-bank	**ACHTUNG: Eine bestehende Integritätsdatenbank wird gelöscht!** Durch einen Klick auf die Schaltfläche *Löschen* werden die vorhandenen Berichte/Datenbanken gelöscht. Für eine weitere Integritätsprüfung muss eine neue Integritätsdatenbank angelegt/initialisiert werden. Sie können dies über die Schaltfläche *Initialisieren* anstoßen. Ansonsten wird eine neue Integritätsdatenbank zum nächsten Prüftermin automatisch erzeugt (wenn zuvor keine Zugriffsüberprüfung durchgeführt wurde). Dieser Vorgang ist nicht sichtbar.

16.11 Erfolgreich durchgeführte Zugriffsüberprüfung

Wurde die Zugriffsüberprüfung erfolgreich durchgeführt, wird folgende Meldung angezeigt (siehe Bild 16-11).

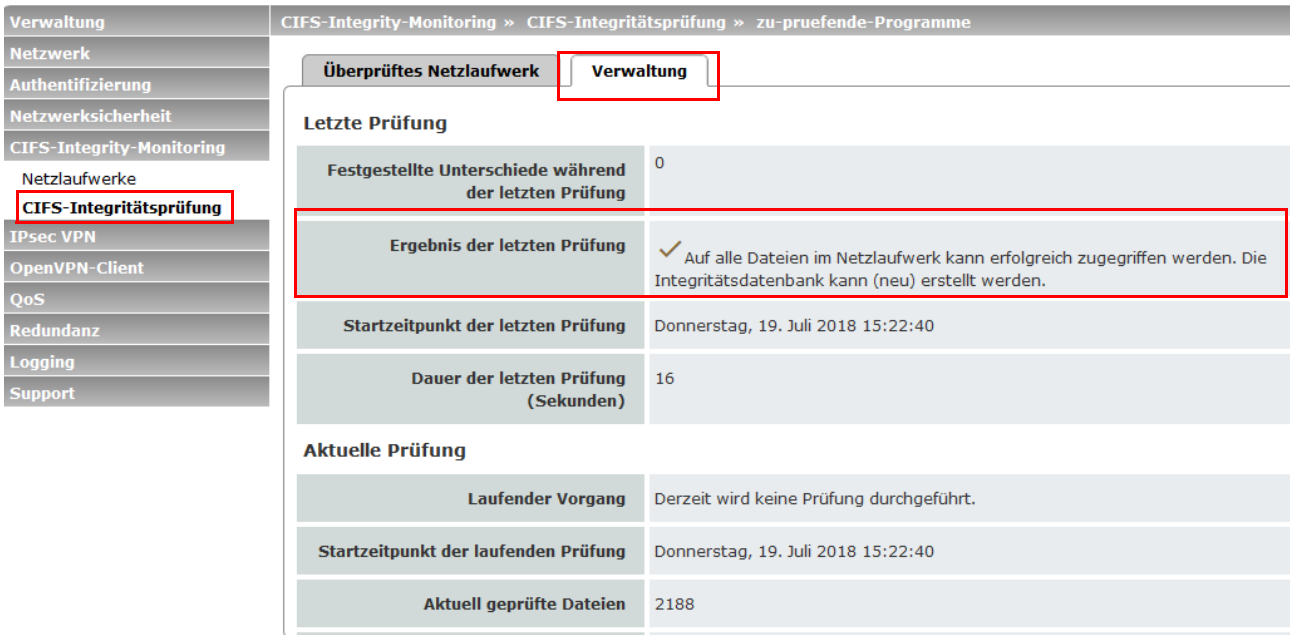


Bild 16-11 Zugriffsüberprüfung erfolgreich

⇒ Ist eine Zugriffsüberprüfung erfolgreich verlaufen, kann die Integritätsdatenbank unter „*Erstelle die Integritätsdatenbank (neu)*“ über den Button „*Initialisieren*“ (neu) generiert werden.

16.12 Erfolgreich erstellte Integritätsdatenbank

Wurde die Integritätsdatenbank erfolgreich erstellt, wird folgendes Bild angezeigt (siehe Bild 16-12).

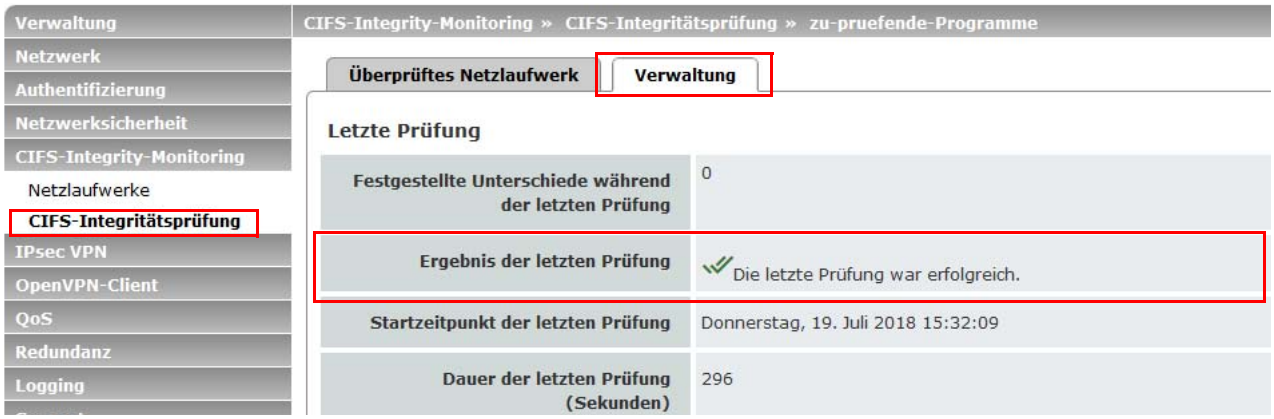


Bild 16-12 Integritätsdatenbank erfolgreich erstellt

⇒ Damit wurde die Integritätsdatenbank erstellt. Die Konsistenzprüfung erfolgt nun manuell oder automatisch, dem konfigurierten Zeitintervall entsprechend.

16.13 Fehlende Zugriffsrechte (Schreib-/Leserechte)

Wurde dem mGuard-Gerät der Zugriff auf einige Dateien/Verzeichnisse verweigert, erscheint folgende Fehlermeldung.

Bild 16-13 Zugriff auf Dateien/Verzeichnisse fehlgeschlagen

Die betroffenen Verzeichnisse oder Dateien werden im Prüfbericht angegeben. Dieser befindet sich auf dem überprüften PC und kann dort oder über das WBM des mGuard-Geräts heruntergeladen werden.

Beispiel:

```
/var/cic/mnt/MAIv042835620-memory/integrity-check-log.txt
START_OF_LOG 2aa83b0b-6484-1787-a2d9-000cbe040098 Thu Jul 19
15:12:53 2018
SUBJECT check-access name=zu-pruefende-Programme
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Permission
denied" path=Gemeinsame Dateien type=d
DIR_TRAVERSAL_ERR errno=13 syscall=readdir error="Permission
denied" path=Windows NT/ZubehÃ¶r type=d
ACCESS_CHECK_FAILED
END_OF_LOG
```

Bild 16-14 Beispiel: Eintrag im Prüfbericht bezüglich fehlender Leserechte

In diesem Fall verhindert Windows den Zugriff auf die folgenden Unterverzeichnisse:

– *Gemeinsame Dateien*
– *Windows NT/Zubehör*

16.14 Dateien und Verzeichnisse von der Überprüfung ausnehmen

Ist der Zugriff auf eine oder mehrere Dateien/Verzeichnisse nicht möglich, können diese von der Überprüfung ausgeschlossen werden.

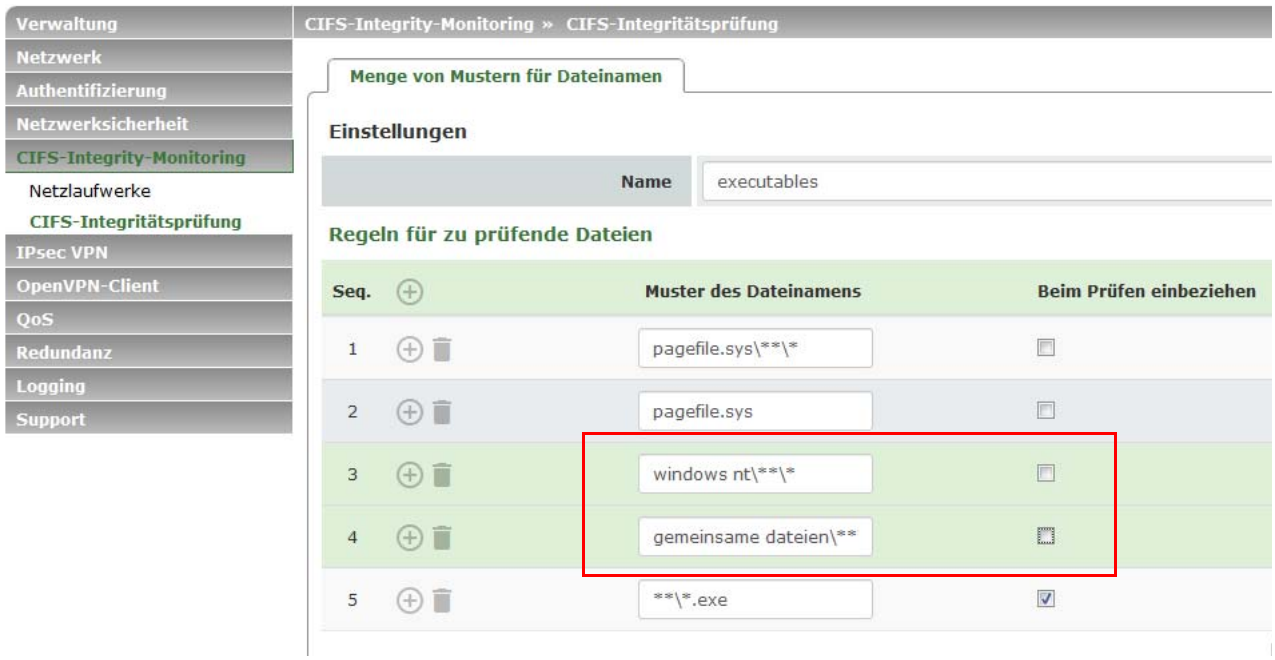


Bild 16-15 Verzeichnisse von der Überprüfung ausnehmen

Siehe auch Kapitel 16.7, „Zu überprüfende Dateien festlegen“

Verzeichnisse, die ausgeschlossen werden sollen, müssen in der Tabelle auf einer Position vor dem ersten *** eingefügt werden.

16.15 CIFS-Integritätsprüfung durchführen

Nachdem die Integritätsdatenbank erfolgreich erstellt wurde, kann eine Integritätsprüfung durchgeführt werden. Dies kann entweder

– manuell über das Web-based Management oder
– zeitgesteuert erfolgen (siehe Kapitel 16.8, „Prüf-Sequenzen anlegen“).

Für die Beschreibung aller Konfigurationsparameter siehe mGuard-Firmwarehandbuch, erhältlich unter phoenixcontact.net/products oder help.mguard.com.

Bild 16-16 Integritätsprüfung durchführen

Vorgehen

- Gehen Sie zu **CIFS-Integrity-Monitoring >> CIFS-Integritätsprüfung** (Registerkarte *Einstellungen*).
- Klicken Sie in der Sektion **Prüfung von Netzlaufwerken** auf das Icon , um die Parameter einer Prüf-Sequenz zu konfigurieren.
- Auf der Registerkarte *Überprüftes Netzlaufwerk* sind alle Parameter voreingestellt. Bei Bedarf können an dieser Stelle Änderungen vorgenommen werden.
- Wechseln Sie zur Registerkarte *Verwaltung*.
- Klicken Sie auf die Schaltfläche **Starte eine Integritätsprüfung** (siehe Tabelle 16-1).

⇒ Das Ergebnis der aktuellen Prüfung wird in der Sektion **Aktuelle Prüfung** angezeigt. Ein Prüfbericht wurde erstellt.

- Klicken Sie auf die Schaltfläche **Bericht validieren**, um die Integrität des Prüfberichts sicherzustellen.
- Klicken Sie auf die Schaltfläche **Prüfbericht herunterladen**, um den Prüfbericht herunterzuladen und zu analysieren.

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

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

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com