1 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.

1.1 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.

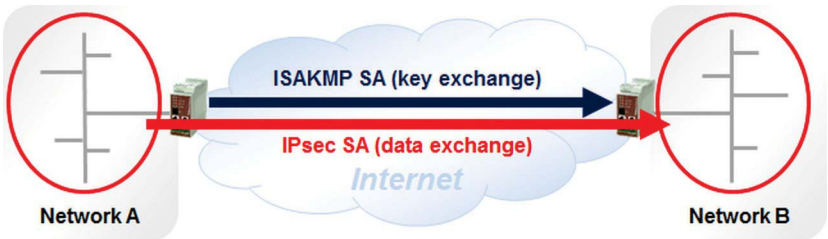


Bild 1-1 Ablauf der beiden Phasen während des Aufbaus einer VPN-Verbindung (*ISAKMP SA* und *IPSEC SA*)

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 1-2 unten zeigt eine erfolgreich aufgebaute VPN-Verbindung.

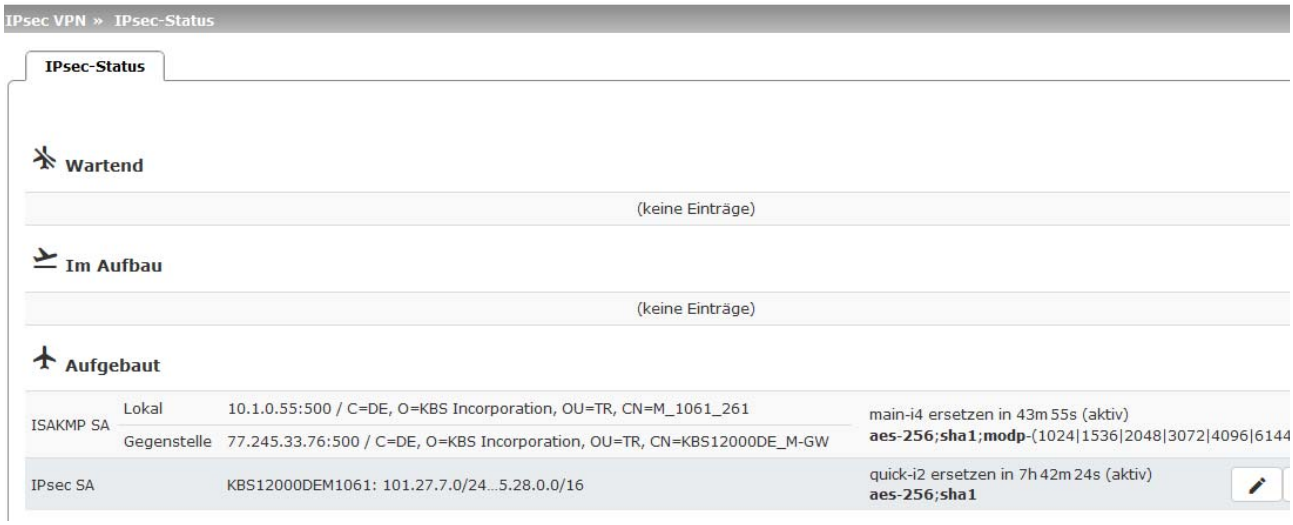


Bild 1-2 IPsec-Status – VPN-Verbindung wurde erfolgreich aufgebaut

1.1.1 Die folgenden Situationen können auftreten

Tabelle 1-1 Die folgenden Situationen könne auftreten.

Situationen, die auftreten könnten	Siehe Kapitel
Die VPN-Verbindung wird nicht auf der IPsec-Status-Seite angezeigt.	Kapitel 1.2, „Die VPN-Verbindung wird nicht auf der IPsec-Status-Seite angezeigt“
ISAKMP SA wurde nicht aufgebaut ("ISAKMP-Status" empty)	Kapitel 1.3, „ISAKMP SA (Phase I) kann nicht aufgebaut werden“
IPsec SA wurde nicht aufgebaut ("IPsec-Status" empty)	Kapitel 1.4, „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 1.5, „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.

1.2 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.

1.2.1 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.

1.2.2 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.

1.2.3 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'
```

1.2.4 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.

1.3 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.

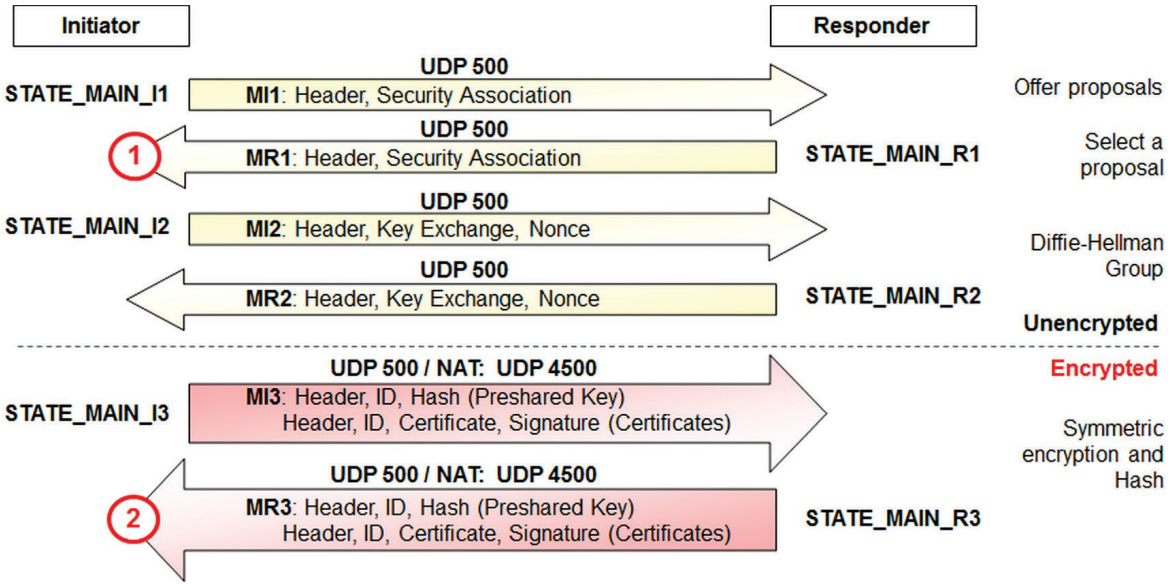


Bild 1-3 *ISAKMP SA* - Phase I

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:

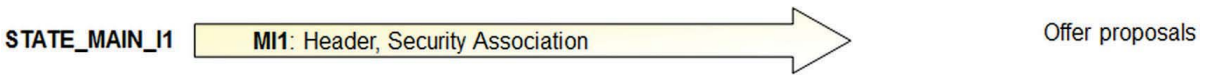
1. Der **Initiator** erhält keine Antwort vom **Responder**.
2. Der **Initiator** erhält ein unerwartetes Paket oder eine Fehlermeldung vom **Responder**.

1.3.1 Log-Eintrag zu einem erfolgreich aufgebauten ISAKMP SA

Initiator **Responder**

Initiator Log:

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

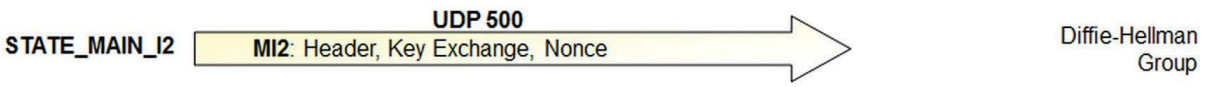


Responder Log:

```
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
```



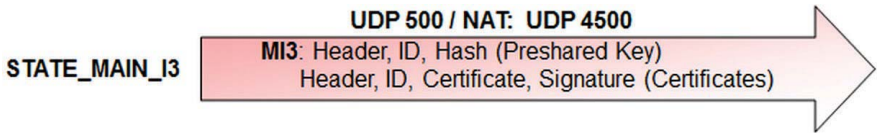
Responder Log:

```
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**

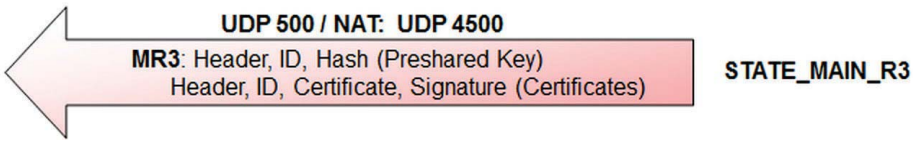
Initiator Log:

```
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.

1.3.2 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.

1.3.2.1 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.

1.3.2.2 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**).

1.3.3 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.

1.3.4 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.

1.3.4.1 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'*"

1.3.4.2 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**).

1.3.5 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**).

1.3.6 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*'”.

1.4 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.

1.4.1 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)**).

1.4.2 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.

1.4.3 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)**).

1.5 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).

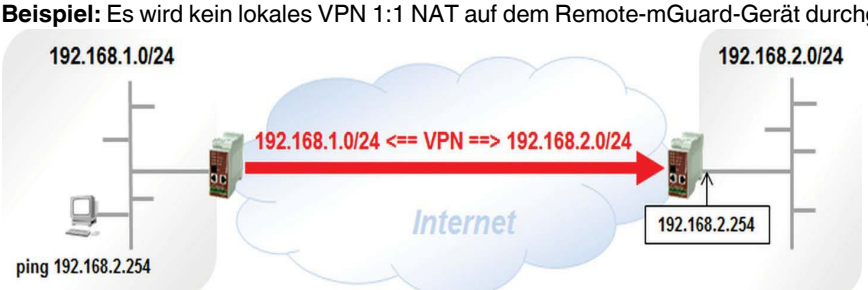
Schritt 1: Kann eine Client im lokalen Netzwerk die interne IP-Adresse des lokalen mGuard-Geräts erreichen?

- 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.

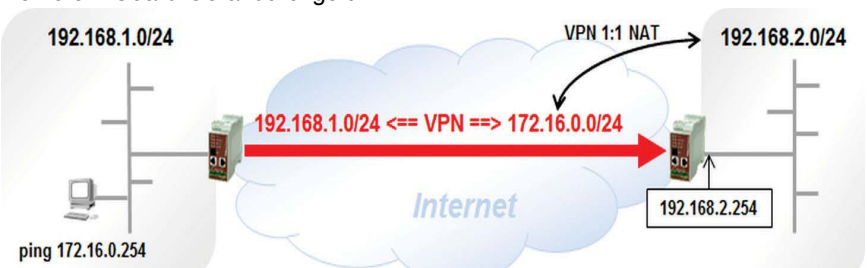
Schritt 2: Ist die interne IP-Adresse des mGuard-Geräts der Gegenstelle durch den VPN-Tunnel erreichbar?

- 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.



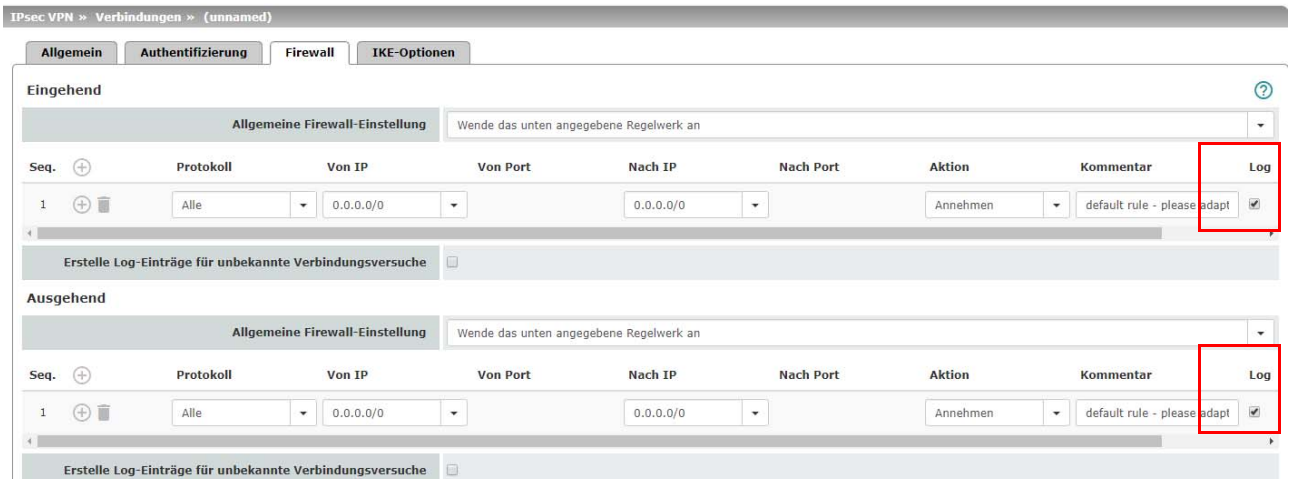
Wenn die Ping-Anfrage beantwortet wird, liegt der Grund dafür, dass Clients im Remote-Netzwerk nicht über VPN erreicht werden können, im Remote-Netzwerk selbst.

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.

1.6 Andere Probleme

1.6.1 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*>.

1.6.2 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.

1.7 Quick Reference: Fehlermeldungen im VPN-Log

Tabelle 1-2 Quick Reference: Fehlermeldungen in VPN-Log-Einträgen

VPN-Log Fehlermeldungen	Gehe zu Kapitel
– ikelifetime […] must be greater than rekeymargin*(100+rekeyfuzz)/100	Kapitel 1.2
– tunnel ignored: local address 'w.x.y.x' within remote network 'a.b.c.d/e'	Kapitel 1.2
Initiator – Fehlermeldungen	
– pending Quick Mode with w.x.y.z took too long – replacing phase 1	Kapitel 1.3.2
– Possible authentication failure: no acceptable response to our first encrypted message	Kapitel 1.3.3
– discarding duplicate packet; already STATE_MAIN_I3	Kapitel 1.3.3
– ignoring informational payload, type INVALID_ID_INFORMATION (during establishment of ISAKMP SA)	Kapitel 1.3.4
– Signature Check (on ...) failed (wrong key?)	Kapitel 1.3.5
– we require peer to have ID '...', but peer declares '...'	Kapitel 1.3.6
– ignoring informational payload, type NO_PROPOSAL_CHOSEN	Kapitel 1.4.1
– ignoring informational payload, type INVALID_ID_INFORMATION (during establishment of IPsec SA)	Kapitel 1.3.4
– No acceptable response to our first Quick Mode message: perhaps peer likes no proposal	Kapitel 1.4.3
Responder – Fehlermeldungen	
– initial Main Mode message received on w.x.y.z:500 but no connection has been authorized	Kapitel 1.3.2.2
– max number of retransmissions (2) reached STATE_MAIN_R2	Kapitel 1.3.3
– no suitable connection for peer '...'	Kapitel 1.3.4.1
– Signature check (on ...) failed (wrong key?)	Kapitel 1.3.4.2
– next payload type of ISAKMP Hash Payload has an unknown value	Kapitel 1.3.6
– IPsec Transform [...] refused due to strict flag	Kapitel 1.4.1
– no acceptable Proposal in IPsec SA	Kapitel 1.4.1
– cannot respond to IPsec SA request because no connection is known for ...	Kapitel 1.3.4
– sending encrypted notification INVALID_ID_INFORMATION to …	Kapitel 1.3.4
– we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION	Kapitel 1.4.3