

# 1 VPN Troubleshooting



Document-ID: 108417\_en\_00

Document-Description: AH EN MGUARD VPN TROUBLESHOOTING

© PHOENIX CONTACT 2019-03-04



Make sure you always use the latest documentation.

It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

## Contents of this document

This document should help to narrow down problems related to VPN connections. The log examples were taken from mGuard devices running firmware version 7.6.

1.1	Introduction .....	1
1.2	VPN connection not displayed in the IPsec Status .....	4
1.3	ISAKMP SA (Phase I) can not be established .....	5
1.4	IPSec SA (phase II) can not be established .....	18
1.5	Remote network clients can not be reached through established VPN tunnel ....	21
1.6	Other Problems .....	24
1.7	Quick Reference: VPN Log Error Messages .....	25

## 1.1 Introduction

A VPN connection is established in two phases:

1. **Phase I:** In *phase I (ISAKMP SA, SA = Security Association)* the VPN peers authenticate each other and an encryption key to protect *phase II* is securely negotiated. This SA is a connection between the two VPN peers only and is used to exchange new keys and DPD messages (DPD = *Dead Peer Detection*).
2. **Phase II:** VPN peers only proceed with *phase II (IPsec SA)* if *phase I* was established successfully. In *phase II* IPsec connection parameters are negotiated. This SA connects the two networks and is used for the data exchange between the clients of those networks.

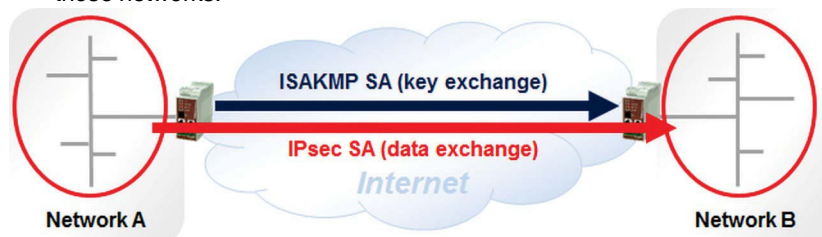



Figure 1-1 Establishment of the two phases of the VPN connection (*ISAKMP SA* and *IPSEC SA*)

Most frequently establishing a VPN connection fails during *phase I (ISAKMP SA)*, caused either by a wrong configuration of the VPN connection or by routers in-between the two VPN peers. If the establishment fails during *phase II (IPsec SA)*, it is caused by a configuration mismatch.


If the establishment of a VPN connection fails, inspect at first the *IPsec Status* (menu **IPsec VPN >> IPsec Status**) to get the information, at which stage the failure happens. In the screenshot below, the VPN connection was established successfully.

IPsec VPN » IPsec Status


IPsec Status

 Waiting

(no entries)

 Pending

(no entries)

 Established

ISAKMP SA	Local	10.1.0.55:500 / C=DE, O=KBS Incorporation, OU=TR, CN=M_1061_261	main-i4 replace in 42m 53s (active)
	Remote	77.245.33.76:500 / C=DE, O=KBS Incorporation, OU=TR, CN=KBS12000DE_M-GW	aes-256;sha1;modp-(1024 1536 2048 3072 4096 6144
IPsec SA		KBS12000DEM1061: 101.27.7.0/24...5.28.0.0/16	quick-i2 replace in 7h 47m 17s (active) aes-256;sha1

Figure 1-2 IPsec status – VPN connection successfully established

### 1.1.1 The following situations may occur

Table 1-1 The following situations may occur

Situation that may occur	Refer to chapter
VPN connection not displayed in the "IPsec Status" at all	Section 1.2, "VPN connection not displayed in the IPsec Status"
ISAKMP SA not established ("ISAKMP State" empty)	Section 1.3, "ISAKMP SA (Phase I) can not be established"
IPsec SA not established ("IPsec State" empty)	Section 1.4, "IPSec SA (phase II) can not be established"
Problem transferring data through an established VPN connection ("ISAKMP SA" and "IPsec SA" established)	Section 1.5, "Remote network clients can not be reached through established VPN tunnel"

In the following chapters **Initiator** stands for the mGuard device which initiates the VPN connection, **Responder** for the mGuard device which waits for the VPN connection.

If the establishment of the *ISAKMP SA* or *IPsec SA* fails (2 and 3), in most cases the VPN logs of both VPN peers need to be inspected for being able to locate the reason for the failure.

Request a support snapshot (menu **Support >> Advanced >> Snapshot**) of **both** VPN peers from the customer.

## 1.2 VPN connection not displayed in the IPsec Status

If the VPN connection does not appear in the *IPsec Status*, it may be caused by the following reasons:

### 1.2.1 VPN connection not enabled

Disabled VPN connections do not appear in the *IPsec Status*.

- Ensure the VPN connection is enabled (menu **IPsec VPN >> Connections**).
- If the VPN connection is triggered by CMD contact, ensure the button or On/Off switch was pressed to activate the VPN connection.
- If the VPN connection is triggered by calling the script *nph-vpn.cgi*, ensure the according command was called to activate the VPN connection.

### 1.2.2 Option "Disable VPN until the user is authenticated via HTTP" is enabled

- Ensure the option *Disable VPN until the user is authenticated via HTTP* is not enabled in the menu **Authentication >> Administrative Users**.

If this option is enabled, the user will be prompted to enter the user's password when trying to access any web side after a reboot of the mGuard device. The configured VPN connection will only be added to the VPN service if the entered password is correct. This option was implemented to protect mGuard devices with a configured VPN connection to the headquarters used by road warriors.

### 1.2.3 Wrong configuration

The problem may also be caused by a wrong configuration.

- Apply a minor change to the VPN configuration, click the icon <Save> and inspect the System Message.
- If the System Message does not report any problem, inspect the VPN logs (menu **Logging >> Browse Local Logs**) for any error messages, as for example:

```
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 General network problems

The problem may also be caused by some general network problems.

- The mGuard device (*Router mode*) is configured to receive its external IP settings from a DHCP server but did not receive them yet.
- A DNS name is specified as "Address of the remote site's VPN gateway" in the VPN connection but the mGuard device could not resolve the DNS name due to problems with the DNS resolution.

### 1.3 ISAKMP SA (Phase I) can not be established

The *ISAKMP SA* is established using the *Main Mode* provided by the *Internet Key Exchange* (IKE) protocol. IKE also provides the *Aggressive Mode* but this mode is less secure and only supported by newer mGuard firmware.

In *Main Mode*, three pairs of messages are exchanged between both VPN peers. Keep the following diagram in mind when narrowing down a problem. It helps a lot understanding what could cause the problem.

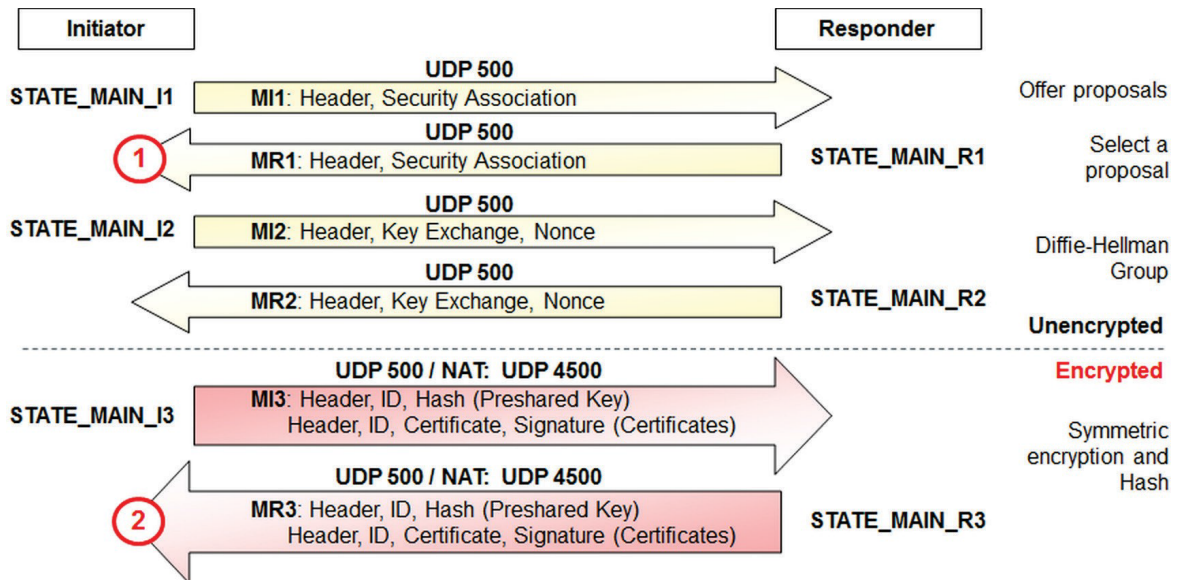


Figure 1-3 ISAKMP SA - Phase I

Every time when the **initiator** has sent out a message, its state changes from STATE\_MAIN\_I1 to STATE\_MAIN\_I2 and STATE\_MAIN\_I3, the **responder's** state from STATE\_MAIN\_R1 to STATE\_MAIN\_R2 and STATE\_MAIN\_R3 respectively. The state changes are reflected in the logs. The VPN connection is established through UDP port 500. If the connection is established across one or more gateways that have NAT activated, starting with the third *Main Mode* message MI3 the exchange happens through UDP port 4500.

Problems usually occur at the above marked points ① and ②:

- ① The **initiator** does not receive a response from the **responder**.
- ② The **initiator** receives an unexpected packet or an error message from the **responder**.

### 1.3.1 Log example of a successfully established ISAKMP SA

Initiator

Responder

## Initiator Log:

08:53:47.90161 "MAI1950251842\_1" #2: initiating Main Mode

STATE\_MAIN\_I1

MI1: Header, Security Association

Offer proposals

## 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**

UDP 500

MR1: Header, Security Association

STATE\_MAIN\_R1

Select a proposal

## 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**

UDP 500

STATE\_MAIN\_I2

MI2: Header, Key Exchange, Nonce

Diffie-Hellman Group

## 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**

UDP 500

MR2: Header, Key Exchange, Nonce

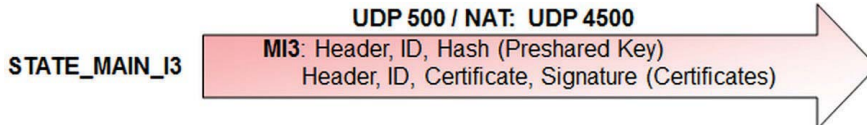
STATE\_MAIN\_R2

## Initiator

## Responder

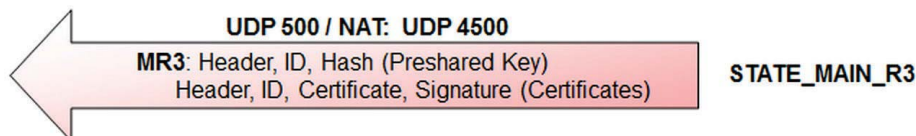
## Initiator Log:

```
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}
```



The log entries **issuer cacert not found** and **X.509 certificate rejected** do not indicate that there is a problem.

the mGuard device tries CA authentication first before identifying the remote side by its certificate stored in the VPN connection. If there is no CA certificate present or if there is no matching CA certificate, the above mentioned log entries appear and the mGuard device continues identifying the remote side by its certificate.

### 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
```

The mGuard device initiates the VPN connection by sending the first *Main Mode* message (MI1) but there is no response from the **responder**. The mGuard device keeps on initiating the VPN connection.

Now it is important to inspect the VPN logs of the **responder** to determine whether this message has reached the **responder** or not.

#### 1.3.2.1 Resp.: No received Packet registered in the VPN Logs of the Responder

#### Responder Log:

No entries for a new VPN connect request appear in the logs. At least **packet from w.x.y.z: received Vendor ID payload** should appear in the logs if the responder has received the first *Main Mode* message. If such a log entry does not appear, the first *Main Mode* message of the initiator did not reach the responder.

#### Possible reasons:

- The specified IP address or DNS name of the **responder** is incorrect (menu **IPsec VPN >> Connections >> (Edit) >> General**, parameter *Address of the remote site's VPN gateway*).
- If the **initiator** is located behind a firewall, this firewall may block outgoing traffic to UDP port 500.
- If the **responder** is located behind a NAT router, either port forwarding for incoming traffic on UDP port 500 to the IP address of the **responder** is not configured on the NAT router or it is not configured properly.
- The **responder** does not listen for incoming VPN connections (e.g. no VPN connections configured or all VPN connections disabled).



Check on the **initiator** with the Tool *IKE Ping* (menu **Support >> Tools >> IKE Ping**) if the IP address or DNS name of the **responder** is reachable.



### 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
```

The **responder** has received the first *Main Mode* message from the **initiator**. The **initiator** informs the **responder**, among other things, about the encryption and hash algorithm (e.g. AES-256/SHA-1) that shall be used for the establishment of the *ISAKMP SA*. The **responder** checks if there is any VPN connection configured which also supports these algorithms. If there is no accordance, the above mentioned message appears in the logs. In this case the **responder** does not send a reply to the **initiator**.

**Reason:**

Mismatch of the specified encryption and/or hash algorithms for the *ISAKMP SA*. Check the specified encryption and hash algorithms for the *ISAKMP SA* on the **initiator** and on the **responder** (menu **IPsec VPN >> Connections >> (Edit) >> IKE Options**, section *ISAKMP SA (Key Exchange)*). Both VPN connections need to support the same encryption and hash algorithm.

### 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

```

The **initiator** has sent his third *Main Mode* message (MI3) and expects now the response from the **responder** (MR3). But he has received MR2 again from the **responder**. Thus he exclaims “*discarding duplicate packet; already STATE\_MAIN\_I3*”.

If the VPN connection is established across one or more gateways that have NAT activated, starting with the third *Main Mode* message (MI3) the exchange happens through UDP port 4500 instead of UDP port 500 due to NAT-Traversal.

The log of the **responder** will tell us more about the reason.

#### 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

```

The **responder** is in STATE\_MAIN\_R2 and is expecting the third *Main Mode* message (MI3) from the **initiator** but did not receive it. Thus the **responder** keeps on retransmitting MR2.

**Reason:**

- Some entity in-between the two VPN peers blocks UDP traffic directed to port 4500.
- If the **initiator** is located behind a firewall, most likely this firewall drops outgoing traffic to UDP port 4500.
- If the **responder** is located behind a NAT router, either port forwarding for UDP 4500 to the IP address of the **responder** is not configured on the NAT router or it is not configure properly.

### 1.3.4 Initiator: “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
```

The **initiator** has sent his third *Main Mode* message (MI3) and expects now the response from the **responder** (*STATE\_MAIN\_I3: sent MI3, expecting MR3*). The **initiator** has sent with the third message its certificate or hash value of the PSK and expects now the according information from the **responder**.

But the **responder** did not send its certificate or hash value of the PSK, it returns an informational payload of the type INVALID\_ID\_INFORMATION.

The log of the **responder** will tell us more about the reason.

### 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_inl1_outR1)
10:00:08.88320 "MAI0874627901_1"[1] 77.245.32.68 #73: enabling Innominate Always Send NAT-OA (main_inl1_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

```

The **responder** has received the third *Main Mode* message (MI3) but there is not VPN connection configured with a certificate matching to the subject of the received certificate.

#### Possible Reasons:

- Certificate or PSK mismatch. If PSK is used for authentication, ensure that the same Pre-Shared Secret Key was entered on both sides (menu **IPsec VPN >> Connections >> (Edit) >> Authentication**, parameter *Pre-Shared Secret Key (PSK)*). If certificates are used for authentication, compare the MD5 or SHA1 fingerprint of the machine certificate of the **initiator** (menu **Authentication >> Certificates >> Machine Certificates**) with the fingerprint of the Remote Certificate in the corresponding VPN connection of the **responder** (menu **IPsec VPN >> Connections >> (Edit) >> Authentication**).
- Mismatch of the specified VPN identifier (VPN connection tab *Authentication*), log entry e.g. “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_inl1_outR1)
10:30:56.12212 "MAI0874627901_1"[1] 77.245.32.68 #94: enabling Innominate Always Send NAT-OA (main_inl1_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
```

#### Reason:

The machine certificate has been replaced by a new one on the **initiator**. The new certificate has the same subject attributes as the previous certificate. On the **responder**, the certificate of the **initiator** specified as remote certificate in the VPN connection (VPN connection tab *Authentication*) is still the previous one.

### 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 *AwEABns8
10:34:01.24566 "MAI1950251842_1" #85: sending encrypted notification INVALID_KEY_INFORMATION to 77.245.33.67:4500

```

#### Reason:

The machine certificate has been replaced by a new one on the **responder**. The new certificate has the same subject attributes as the previous certificate. On the **initiator**, the certificate of the **responder** specified as remote certificate in the VPN connection (VPN connection tab *Authentication*) is still the previous one.

### 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

```

The **initiator** has received the third *Main Mode* response from the **responder** (MR3) with the certificate of the remote side but the certificate's subject does not match to the one specified in the VPN connection as remote certificate (VPN connection tab *Authentication*).



## 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_inl1_outR1)
10:06:14.03120 "MAI0874627901_1"[1] 77.245.32.68 #79: enabling Innominate Always Send NAT-OA (main_inl1_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

```

Due to the certificate failure, the **initiator** responds with INVALID\_ID\_INFORMATION.

The **ISAKMP SA** was established successfully for the **responder**. Thus he is expecting now the first packet for the establishment of the **IPsec SA** but did not receive it.

**Possible reasons:**

- Certificate mismatch. Compare the MD5 or SHA1 fingerprint of the machine certificate of the **responder** (menu **Authentication >> Certificates >> Machine Certificates**) with the fingerprint of the Remote Certificate in the corresponding VPN connection of the **initiator** (menu **IPsec VPN >> Connections >> (Edit) >> Authentication**).
- Mismatch of the specified VPN identifier (VPN connection tab *Authentication*), log entry e.g. "we require peer to have ID 'O=Innominate, OU=Support, CN=mGuard 2', but peer declares '@mGuard 2'".

## 1.4 IPSec SA (phase II) can not be established

The *IPsec SA* is established using the *Quick Mode* provided by the *Internet Key Exchange* (IKE) protocol. Basically three messages are exchanged in this mode.

If the establishment of the *IPsec SA* fails, it is caused by a configuration mismatch. Either the specified VPN networks do not match, or there is a mismatch of the specified encryption and/or hash algorithm for the *IPsec SA* (tab *IKE Options*), or *Perfect Forward Secrecy* is enabled on the **responder** but not on the **initiator**.

### 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
```

#### Reason:

Mismatch of the specified encryption and/or hash algorithms for the *IPsec SA*. Check the specified encryption and hash algorithms for the *IPsec SA* on the **initiator** and on the **responder** (menu **IPsec VPN >> Connections >> (Edit) >> IKE Options**, section *IPsec SA (Data Exchange)*). Both VPN connections need to support the same encryption and hash algorithm.

## 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
```

### Reason:

The specified VPN networks (VPN connection tab *General*) do not match on both sides. The local network specified on one side must be specified as remote network on the other side and vice versa.

### 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
```

#### Reason:

*Perfect Forward Secrecy (PFS)* is enabled on the **responder** but not on the **initiator** (VPN connection tab *IKE Options*, section *IPsec SA (Data Exchange)*).

## 1.5 Remote network clients can not be reached through established VPN tunnel

If the VPN connection was established successfully, problems related to transferring data through the VPN tunnel are usually not caused by the mGuard devices and have external reasons.



If VPN masquerading is configured on one mGuard, connections can only be established from the masqueraded network to the other network, not vice versa.

The following steps help to narrow down the reason for the problem, assuming the VPN firewall does not block ICMP traffic.

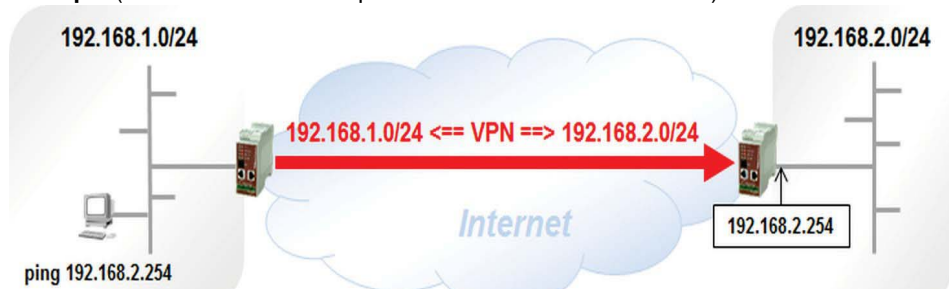
### Step 1: Is the internal IP of the local mGuard reachable from the internal Client?

- The first step is to check if the internal IP of the local mGuard is reachable from the client from which the remote VPN network should be accessed.
- From the client, send a “ping” to the internal IP of the local mGuard.
- If the “ping” is not replied, the reason is located in the internal network. If the “ping” is replied, proceed with the next step.

### Step 2: Internal IP of the Remote mGuard reachable through VPN?

- The next step is to check if a “ping” to the internal IP of the remote mGuard through the VPN connection is replied.

**Example** (no local VPN 1:1 NAT performed on the remote mGuard):



**Example** (Local VPN 1:1 NAT from 172.16.0.0/24 to 192.168.2.0/24 performed on the remote mGuard):



If the “ping” is replied, the reason for the problem why clients of the remote VPN network cannot be accessed is located in the remote network. Maybe the internal IP of the remote mGuard is not specified as default gateway on the remote clients.

If the “ping” is not replied, proceed with the next step.

**Step 3: Do the Packets enter the VPN and are they received on the remote Side?**

The next step is to verify if the sent packets enter the VPN connection and if they are received by the remote side. To check this, enable the VPN firewall logging on both sides.

- Edit the VPN connection (menu **IPsec VPN >> Connections**).
- Switch to the tab *Firewall*.
- Enable the logging.

The screenshot shows the 'IPsec VPN >> Connections' configuration window. The 'Firewall' tab is selected. Under the 'Incoming' section, there is a table with columns: Seq., Protocol, From IP, From port, To IP, To port, Action, Comment, and Log. The first row shows a rule with Seq. 1, Protocol 'All', From IP '0.0.0.0/0', To IP '0.0.0.0/0', Action 'Accept', and Comment 'default rule - please adapt'. The 'Log' checkbox is checked. A similar setup is shown for the 'Outgoing' section. The 'Log' column header in both sections is highlighted with a red box.

- Click the icon <Save>.

The VPN connection will be interrupted due to the configuration change. Wait until the connection is up again (menu **IPsec VPN >> IPsec Status**), send the data and then check the VPN firewall logs. The log entries are displayed in the menu **Logging >> Browse local logs**, option *Network Security*.

**Example, 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
```

**Example, 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
```

**Possible results of this test:**

1. Local mGuard does not display according outgoing (entering the VPN tunnel) log messages (fw-vpn\_...-out-...).
  - The internal IP address of the local mGuard is not specified as default gateway on the client on which the command has been issued.
  - If the client has to use a different default gateway than the local mGuard, no route is defined to direct the packets for the remote VPN network to the local mGuard.

- A firewall between the client and the local mGuard blocks the traffic.
  - Reason located somewhere in the internal network.
2. Remote mGuard does not display according incoming (received through the VPN tunnel) log messages (fw-vpn-...-in-...).
- Some entity (gateway, router) between the two VPN peers blocks the encrypted traffic. The following cases already have been observed:
    - Some provider only allow incoming encrypted packets from the Internet to their network if outgoing encrypted packets have already been seen for this connection. This was observed with a satellite network provider as well as with a telephone network provider. To verify this, try to access the clients of the local network from the remote VPN network.
    - A router has blocked ESP traffic between the mGuard devices. This problem could be solved by forcing UDP encapsulation on the mGuard device. This option can only be activated from the command line  
(*gaiconfig --set VPN\_CONNECTION.x.FORCE\_UDP\_ENCAPS yes, 'x'*  
standing for the number of the configured VPN connection (0, 1, 2, 3, ...)). The router has blocked the ESP traffic but not UDP packets encapsulating the ESP packets.

## 1.6 Other Problems

### 1.6.1 VPN connections fails after 24 hours

This problem usually happens if the **responder** has a dynamic public IP address which changes every 24h, registers the current IP address under a specific name in a DynDNS service, the **initiator** refers to this DNS name as “*Address of the remote VPN gateway*”, but DynDNS monitoring is not enabled on the **initiator**.

- On the **initiator**, switch to the menu **IPsec VPN >> Global >> DynDNS Monitoring**.
- Set *Watch hostnames of remote VPN Gateways* to *Yes*.
- Click the icon <Save>.

### 1.6.2 Problems transferring huge Data

A remote client responds to small packets (e.g. “pings”) without problems but transferring huge data (e.g. Remote Desktop Application) fails. This problem is usually caused by routers in the Internet, which reduce the MTU size but do not support UDP fragmentation. The mGuard device receives fragments of encrypted UDP packets and cannot decode them.

This problem can be solved by reducing the IPsec MTU size on the mGuard device. Thus encrypted packets have a smaller size and will not be fragmented when passing the router which reduces the MTU size.

The IPsec MTU size needs to be reduced on the mGuard device where the huge data enter the VPN connection.

- Switch to the menu **IPsec VPN >> Global >> Options**.
- Reduce the size of the *IPsec MTU* in the section *IP Fragmentation*.
- Click the icon <Save>.

You need to reduce the IPsec MTU size successively until the huge data get through the tunnel.



## 1.7 Quick Reference: VPN Log Error Messages

Table 1-2 Quick Reference: VPN Log Error Messages

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

