# GETVPN-Ratgeber zur Fehlerbehebung

## Inhalt

# Einführung

In diesem Dokument werden eine strukturierte Fehlerbehebungsmethodik und nützliche Tools vorgestellt, mit denen Sie GETVPN-Probleme (Group Encrypted Transport VPN) identifizieren und isolieren und mögliche Lösungen bereitstellen können.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- GETVPN
  Offizieller GETVPN-Konfigurationsleitfaden
  Offizieller Design- und Implementierungsleitfaden für GETVPN

- Syslog-Serververwendung

## Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# GETVPN-Fehlerbehebungsmethode

Wie bei den meisten Fehlerbehebungen komplexer Technologieprobleme ist es entscheidend, das Problem auf ein bestimmtes Feature, Subsystem oder eine bestimmte Komponente zu isolieren. Die GETVPN-Lösung besteht aus einer Reihe von Funktionskomponenten, insbesondere:

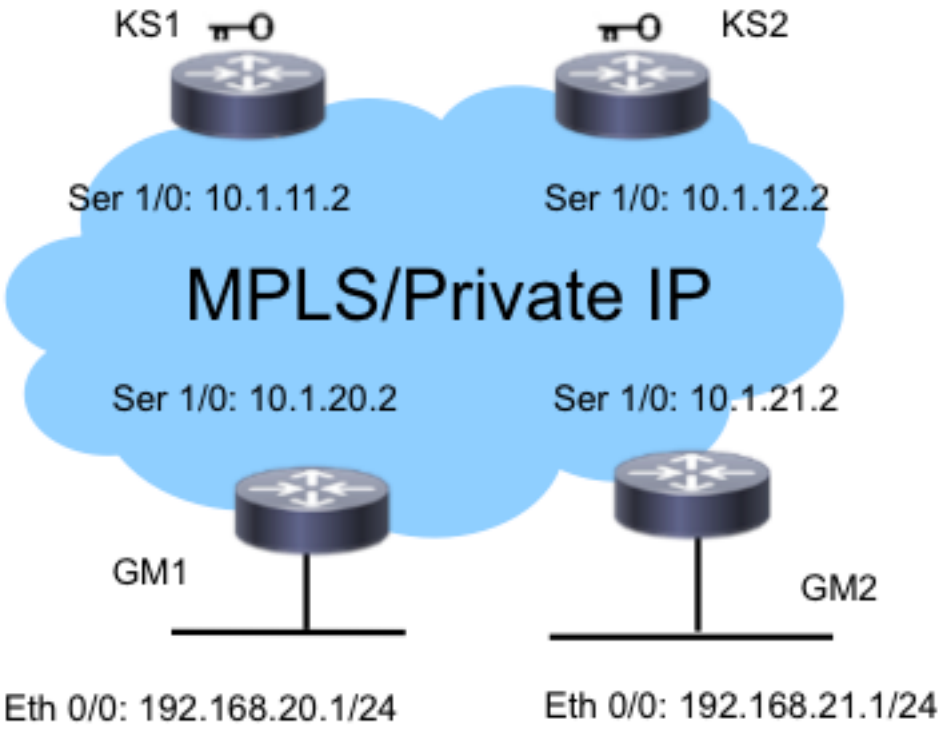
- Internet Key Exchange (IKE) - Wird zwischen Group Member (GM) und Key Server (KS) sowie zwischen Cooperative Protocol (COOP) KS verwendet, um die Kontrollebene zu authentifizieren und zu schützen.
- Group Domain of Interpretation (GDOI) - Das Protokoll, das für die KS verwendet wird, um Gruppenschlüssel zu verteilen und Schlüsseldienste wie rekey für alle GMs bereitzustellen.
- COOP - Protokoll, das für die KS verwendet wird, um miteinander zu kommunizieren und Redundanz zu gewährleisten.
- Header Preservation (Kopfzeilenerhaltung) - IPsec im Tunnelmodus, der den ursprünglichen Datenpaket-Header für die End-to-End-Datenverkehrsübermittlung behält.
- Time Based Anti-Replay (TBAR) - In einer Gruppenschlüsselumgebung verwendeter

Mechanismus zur Replay-Erkennung.

Darüber hinaus bietet es eine umfassende Auswahl an Tools zur Fehlerbehebung, um die Fehlerbehebung zu vereinfachen. Es ist wichtig zu verstehen, welche dieser Tools verfügbar sind und wann sie für jede Fehlerbehebungsaufgabe geeignet sind. Bei der Fehlerbehebung ist es immer ratsam, mit den geringstmöglichen Eingriffen zu beginnen, damit die Produktionsumgebung nicht negativ beeinflusst wird. Der Schlüssel zu dieser strukturierten Fehlerbehebung besteht darin, das Problem entweder auf ein Problem der Kontroll- oder Datenebene zu reduzieren. Sie können dies tun, wenn Sie das Protokoll oder den Datenfluss befolgen und die verschiedenen hier vorgestellten Tools verwenden, um sie zu kontrollieren.

## Referenztopologie

Dieses GETVPN-Topologie- und -Adressierungsschema wird für den Rest dieses Dokuments zur Fehlerbehebung verwendet.




## Referenzkonfigurationen

- KS1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
address ipv4 10.1.11.2
redundancy
local priority 10
peer address ipv4 10.1.12.2
```

- GM1

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

**Hinweis**: Die KS2- und GM2-Konfigurationen sind hier aus Gründen der Kürze nicht enthalten.

## Terminologie

- **KS** - Schlüsselserver
- **GM** - Gruppenmitglied
- **COOP** - Protokoll über Zusammenarbeit
- **TBAR** - Zeitbasierte Anti-Replay-Funktion
- **KEK** - Schlüssel-Verschlüsselungsschlüssel
- **TEK** - Datenverkehrsverschlüsselungsschlüssel

## Vorbereitung der Protokollierungseinrichtung und andere Best Practices

Bevor Sie mit der Fehlerbehebung beginnen, stellen Sie sicher, dass Sie die Protokollierungseinrichtung wie hier beschrieben vorbereitet haben. Einige Best Practices finden Sie auch hier:

- Prüfen Sie die Menge des freien Arbeitsspeichers des Routers, und konfigurieren Sie die **Protokollierung des gepufferten Debuggens** auf einen großen Wert (10 MB oder mehr, wenn möglich).

- Deaktivieren Sie die Protokollierung für die Konsolen-, Monitor- und Syslog-Server.

- Rufen Sie den Inhalt des Protokollierungspuffers mit dem Befehl **show log** in regelmäßigen Abständen alle 20 Minuten bis eine Stunde ab, um Protokollverluste aufgrund der Wiederverwendung des Puffers zu vermeiden.

- Geben Sie in jedem Fall den Befehl **show tech** von betroffenen GMs und KSs ein, und überprüfen Sie die Ausgabe des Befehls **show ip route** in global und alle beteiligten VRFs (Virtual Routing and Forwarding).

- Verwenden Sie das Network Time Protocol (NTP), um die Uhr zwischen allen debuggten Geräten zu synchronisieren. Aktivieren von Millisekunde-Zeitstempeln für Debug- und Protokollmeldungen:

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

- Stellen Sie sicher, dass die Ausgaben des Befehls show mit einem Zeitstempel versehen sind.

```
Router#terminal exec prompt timestamp
```

- Wenn Sie Befehlsausgaben für Ereignisse auf der Kontrollebene oder für Datenebenenindikatoren erfassen, sammeln Sie immer mehrere Iterationen derselben Ausgabe.

# Fehlerbehebung bei Problemen mit der GETVPN-Kontrollebene

Kontrollebene sind alle Protokollereignisse, die zur Erstellung von Richtlinien und Security Association (SA) auf der GM geführt haben, sodass sie zur Verschlüsselung und Entschlüsselung des Datenverkehrs auf der Datenebene bereit sind. Einige der wichtigsten Checkpoints auf der GETVPN-Kontrollebene sind:


## Best Practices für das Debuggen der Kontrollebene

Diese Best Practices zur Fehlerbehebung sind nicht GETVPN-spezifisch. Sie gelten für nahezu jedes Debuggen auf Kontrollebene. Um eine möglichst effektive Fehlerbehebung zu gewährleisten, müssen folgende Best Practices befolgt werden:

- Schalten Sie die Konsolenprotokollierung aus, und verwenden Sie den Protokollierungspuffer oder das Syslog, um die Debug-Dateien zu sammeln.
- Verwenden Sie NTP, um Router-Uhren auf allen Geräten zu synchronisieren, die gedebuggt werden.
- Aktivieren von msec-Timestamping für Debug- und Protokollmeldungen:

```
service timestamp debug datetime msec
service timestamp log datetime msec
```

- Stellen Sie sicher, dass die Ausgaben des Befehls show mit einem Zeitstempel versehen sind, damit sie mit der Debugausgabe korreliert werden können:

```
terminal exec prompt timestamp
```

- Verwenden Sie bedingtes Debuggen in einer Skalierungsumgebung, wenn möglich.

## Tools zur Fehlerbehebung auf GETVPN-Kontrollebene

### GETVPN-Befehle anzeigen

In der Regel sind dies die Befehlsausgaben, die Sie für fast alle GETVPN-Probleme sammeln sollten.

KS

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

### GM

```
show crypto eli
show crypto gdoi rekey sa
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

## GETVPN-Syslog-Meldungen

GETVPN bietet eine umfangreiche Reihe von Syslog-Meldungen für wichtige Protokollereignisse und Fehlerzustände. Das Syslog sollte bei der GETVPN-Fehlerbehebung stets als erste Priorität gelten.

#### Häufige KS-Syslog-Meldungen

| Syslog-Meldungen | Erläuterung |
|---|---|
| *COOP_CONFIG_MISMATCH* | Die Konfiguration zwischen dem primären und dem sekundären Schlüsselserver ist falsch. |
| *COOP_KS_ELECTION* | Der lokale Schlüsselserver hat den Auswahlprozess in einer Gruppe eingegeben. |
| *COOP_KS_REACH* | Die Erreichbarkeit zwischen den konfigurierten Schlüsselservern für die Zusammenarbeit wird wiederhergestellt. |
| *COOP_KS_TRANS_TO_PRI* | Der lokale Schlüsselserver wechselte zu einer primären Rolle, da er kein sekundärer Server in einer Gruppe ist. |
| *COOP_KS_UNAUTH* | Ein autorisierter Remote-Server versuchte, den lokalen Schlüsselserver in Gruppe zu kontaktieren, was als feindseliges Ereignis angesehen werden könnte. |
| *COOP_KS_UNREACH* | Die Erreichbarkeit zwischen den konfigurierten Schlüsselservern für Kooperationen geht verloren, was als feindseliges Ereignis angesehen we kann. |
| *KS_GM_REVOKED* | Während des rekey-Protokolls versuchte ein unbefugtes Mitglied, einer Gr beizutreten, die als feindseliges Ereignis angesehen werden konnte. |
| *KS_SEND_MCAST_REKEY* | Multicast-Schlüssel wird gesendet. |
| *KS_SEND_UNICAST_REKEY* | Senden von Unicast rekey. |
| *KS_UNAUTORISIERT* | Während des GDOI-Registrierungsprotokolls versuchte ein unbefugtes Mit einer Gruppe beizutreten, die als feindseliges Ereignis angesehen werden konnte. |
| *UNAUTHORIZED_IPADDR* | Die Registrierungsanfrage wurde gelöscht, weil das anfordernde Gerät nic Mitgliedschaft in der Gruppe berechtigt war. |

#### Gängige GM-Syslog-Meldungen

| Syslog-Meldungen | Erläuterung |
|---|---|
| *GM_CLEAR_REGISTER* | Der Befehl **clear crypto gdoi** wurde vom lokalen Gruppenmitglied ausge |

| | |
|---|---|
| *GM_CM_ATTACH* | Für das Mitglied der lokalen Gruppe wurde eine Crypto Map angefügt. |
| *GM_CM_DETACH* | Für das lokale Gruppenmitglied wurde eine Crypto Map entfernt.& |
| *GM_RE_REGISTER* | **Die für eine Gruppe erstellte IPsec-SA ist möglicherweise abgelaufen od gelöscht. Anmeldung beim Schlüsselserver erforderlich.** |
| *GM_RECV_REKEY* | **Schlüssel erhalten.** |
| *GM_REGS_COMPL* | **Die Registrierung ist abgeschlossen.** |
| *GM_REKEY_TRANS_2_MULTI* | Gruppenmitglied hat von der Verwendung eines Unicast-erneuten Mechanismus zu einem Multicast-Mechanismus übergewechselt. |
| *GM_REKEY_TRANS_2_UNI* | Gruppenmitglied hat von der Verwendung eines Multicast-erneuten Mechanismus zu einem Unicast-Mechanismus übergewechselt. |
| *PSEUDO_TIME_LARGE* | Ein Gruppenmitglied hat eine Pseudozeit mit einem Wert erhalten, der s weitgehend von seiner eigenen Pseudozeit unterscheidet. |
| *REPLAY_FALLS* | Ein Gruppenmitglied oder Schlüsselserver hat eine Anti-Replay-Prüfung bestanden. |

**Hinweis**: Die rot hervorgehobenen Meldungen sind die häufigsten oder wichtigsten Meldungen, die in einer GETVPN-Umgebung angezeigt werden.

### Globale Krypto- und GDOI-Debugger

GETVPN-Debugging wird unterteilt:

1. Zuerst durch das Gerät, auf dem Sie die Fehlerbehebung durchführen.
```
F340.06.15-2900-18#debug cry gdoi ?
 all-features  All features in GDOI
 condition     GDOI Conditional Debugging
 gm            Group Member
 ks            Key Server
```
2. Zweitens, nach der Art des Problems, das Sie beheben.
```
GM1#debug cry gdoi gm ?
 all-features    All Group Member features
 infrastructure  GM Infrastructure
 registration    GM messages related to registration
 rekey           GM messagese related to Re-Key
 replay          Anti Replay
```
3. Drittens durch die Ebene des Debuggens, die aktiviert werden muss. In Version 15.1(3)T und höher wurden alle GDOI-Feature-Debug-Debug standardisiert, um diese Debug-Level zu haben. Diese wurde entwickelt, um bei der Fehlerbehebung in umfangreichen GETVPN-Umgebungen mit ausreichender Debugging-Präzision zu helfen. Beim Debuggen von GETVPN-Problemen ist es wichtig, die entsprechende Debugebene zu verwenden. In der Regel beginnt der Debugging mit der niedrigsten Debugebene, d. h. der Fehlerebene, und erhöht bei Bedarf die Debugging-Granularität.
```
GM1#debug cry gdoi gm all-features ?
 all-levels  All levels
 detail      Detail level
 error       Error level
 event       Event level
 packet      Packet level
 terse       Terse level
```

### Bedingtes Debuggen von GDOI

In Cisco IOS® Version 15.1(3)T und höher wurde GDOI-konditionelles Debugging hinzugefügt, um

die Fehlerbehebung von GETVPN in einer umfangreichen Umgebung zu unterstützen. So können jetzt alle Debugging-Vorgänge für Internet Security Association und Key Management Protocol (ISAKMP) und GDOI mit einem bedingten Filter ausgelöst werden, der auf der Gruppe oder Peer-IP-Adresse basiert. Für die meisten GETVPN-Probleme ist es gut, sowohl ISAKMP- als auch GDOI-Debugger mit dem entsprechenden bedingten Filter zu aktivieren, da GDOI-Debugger nur GDOI-spezifische Operationen anzeigen. Führen Sie die folgenden zwei einfachen Schritte aus, um das bedingte Debuggen von ISAKMP und GDOI zu verwenden:

1. Stellen Sie den bedingten Filter ein.
2. Aktivieren Sie wie gewohnt den relevanten ISAKMP und GDOI.

Beispiel:

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.

KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

> **Hinweis**: Bei bedingten ISAKMP- und GDOI-Debugging-Meldungen, die möglicherweise nicht über die bedingten Filterinformationen verfügen, z. B. die IP-Adresse im Debugpfad, kann das **nicht übereinstimmende** Flag aktiviert werden. Dies muss jedoch mit Vorsicht verwendet werden, da es eine große Menge an Debuginformationen erzeugen kann.

## GDOI-Ereignisspuren

Dies wurde in Version 15.1(3)T hinzugefügt. Die Ereignisablaufverfolgung ermöglicht eine leichte, stets verfügbare Ablaufverfolgung für erhebliche GDOI-Ereignisse und -Fehler. Es gibt auch Exit-Path-Ablaufverfolgung, bei der die Ablaufverfolgung für Ausnahmebedingungen aktiviert ist. Ereignisverfolgungen können mehr Informationen zum GETVPN-Ereignisverlauf bereitstellen als herkömmliche Syslogs.

GDOI-Ereignisverfolgungen sind standardmäßig aktiviert und können mit dem Befehl **show monitor even-trace** aus dem Ablaufverfolgungspuffer abgerufen werden.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
```

```
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

Die Ablaufverfolgung für den Ablaufpfad liefert ausführliche Informationen über den Ausgangspfad, d. h. Ausnahmen- und Fehlerbedingungen, wobei die Option traceback standardmäßig aktiviert ist. Anschließend können die tracebacks verwendet werden, um die genaue Codesequenz zu decodieren, die zum Exit Path-Zustand geführt hat. Verwenden Sie die **detail**-Option, um die Ablaufverfolgungsstapel aus dem Ablaufverfolgungspuffer abzurufen:

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

Die Standardgröße des Ablaufverfolgungspuffers beträgt 512 Einträge, und dies ist möglicherweise nicht ausreichend, wenn das Problem nur gelegentlich auftritt. Um diese Standardgröße für den Ablaufverfolgungseintrag zu erhöhen, können die Konfigurationsparameter für die Ereignisablaufverfolgung wie folgt geändert werden:

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

## GETVPN-Kontrollebenen-Checkpoints und häufige Probleme

Im Folgenden sind einige der häufigsten Probleme auf der Kontrollebene für GETVPN aufgeführt. Zur erneuten Iteration ist die Kontrollebene als alle GETVPN-Funktionskomponenten definiert, die für die Verschlüsselung und Entschlüsselung der Datenspur auf den GMs erforderlich sind. Dies erfordert eine erfolgreiche GM-Registrierung, Sicherheitsrichtlinien und SA Download/Installation sowie anschließendes KEK/TEK-rekey.

### COOP-Einrichtung und Richtlinienerstellung

Um zu überprüfen und zu überprüfen, ob das KS erfolgreich die Sicherheitsrichtlinie und den zugehörigen KEK/TEK erstellt hat, geben Sie Folgendes ein:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
```

```
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Ein häufiges Problem bei der KS-Richtlinieneinrichtung besteht darin, dass zwischen den primären und sekundären KS-Systemen unterschiedliche Richtlinien konfiguriert werden. Dies kann zu unvorhersehbarem KS-Verhalten führen, und dieser Fehler wird gemeldet:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNNING: replay method configuration between
Primary KS and Secondary KS are mismatched
```

Derzeit gibt es keine automatische Konfigurationssynchronisierung zwischen primären und sekundären KSs, daher müssen diese manuell korrigiert werden.

Da COOP eine kritische (und fast immer obligatorische) Konfiguration für GETVPN ist, ist es wichtig, sicherzustellen, dass COOP korrekt funktioniert und die COOP KS-Rollen korrekt sind:

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
Session 1:
Server handle: 2147483651
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
```

```
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

In einer funktionalen COOP-Konfiguration sollte dieser Protokollfluss beachtet werden:

### IKE Exchange > ANN mit ausgetauschten COOP-Prioritäten > COOP-Auswahl > ANN von primärem zu sekundärem KS (Richtlinien, GM-Datenbank und Schlüssel)

Wenn COOP nicht richtig funktioniert oder wenn ein COOP-Split vorhanden ist, z. B. mehrere KSs zum primären KS werden, müssen diese Debugger zur Fehlerbehebung gesammelt werden:

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
show crypto gdoi ks coop
```

## IKE-Einrichtung

Für GETVPN ist ein erfolgreicher IKE-Austausch erforderlich, um den Kontrollkanal für die nachfolgenden Richtlinien und den SA-Download zu sichern. Am Ende des erfolgreichen IKE-Austauschs wird eine GDOI_REKEY sa erstellt.

In Versionen vor Cisco IOS 15.4(1)T kann GDOI_REKEY mit dem Befehl **show crypto isakmp sa** angezeigt werden:

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

In Cisco IOS 15.4(1)T und höher wird diese GDOI_REKEY wie mit dem Befehl **show crypto gdoi rekey sa** angezeigt:

```
GM1#show crypto gdoi rekey sa
GETVPN REKEY SA
dst             src             conn-id         status
10.1.13.2       10.1.11.2       1114            ACTIVE
```

> **Hinweis**: Sobald der erste IKE-Austausch abgeschlossen ist, werden nachfolgende Richtlinien und Schlüssel mithilfe der GDOI_REKEY SA von den KS an die GM **übertragen**. Es gibt also keinen neuen Schlüssel für die GDOI_IDLE SA, wenn diese ablaufen. sie verschwinden, wenn ihre Lebensdauer abläuft. Es sollte jedoch immer GDOI_REKEY SA auf dem GM vorhanden sein, damit es neue Schlüssel empfangen kann.

Der IKE-Austausch für GETVPN unterscheidet sich nicht von dem IKE, das in herkömmlichen Point-to-Point-IPsec-Tunneln verwendet wird, sodass die Fehlerbehebungsmethode unverändert bleibt. Diese Debugger müssen gesammelt werden, um Probleme mit der IKE-Authentifizierung zu beheben:

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)
```

## Registrierung, Richtliniendownload und SA-Installation

Sobald die IKE-Authentifizierung erfolgreich ist, registriert GM die KS. Es wird erwartet, dass diese Syslog-Meldungen angezeigt werden, wenn dies korrekt auftritt:

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2
```

Die Richtlinien und Schlüssel können mit dem folgenden Befehl überprüft werden:

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
```

```
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval


GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
```

```
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
GM1#
```

**Hinweis**: Mit GETVPN verwenden eingehende und ausgehende SAs denselben SPI.

Bei der GETVPN-Registrierung und der Installation von Richtlinien sind diese Fehlerbehebungen erforderlich, um folgende Probleme zu beheben:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

**Hinweis**: Je nach Ergebnis dieser Ausgaben sind möglicherweise weitere Debugging-Vorgänge erforderlich.

Da die GETVPN-Registrierung in der Regel unmittelbar nach dem erneuten Laden von GM erfolgt, kann dieses EEM-Skript hilfreich sein, um diese Debuggen zu sammeln:

```
event manager applet debug
event syslog pattern "RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "debug crypto gdoi all all"
```

## Umschalten

Sobald die GMs beim KS registriert und das GETVPN-Netzwerk ordnungsgemäß eingerichtet ist, ist der primäre KS für das Senden von erneuten Nachrichten an alle registrierten GMs verantwortlich. Die rekey-Meldungen werden zur Synchronisierung aller Richtlinien, Schlüssel und Pseudozeiten auf den GMs verwendet. Die rekey-Meldungen können über eine Unicast- oder eine Multicast-Methode gesendet werden.

Diese Syslog-Meldung wird auf dem KS angezeigt, wenn die erneute Nachricht gesendet wird:

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```

Bei den GMs ist dies das Syslog, das beim Empfang des neuen Schlüssels angezeigt wird:

```
%GDOI-5-GM_RECV_REKEY: Received Rekey for group G1 from 10.1.11.2 to 10.1.20.2
with seq # 11
```

#### RSA-Schlüsselpaar-Anforderung für Schlüssel für KS-Schlüssel

Für die Neuschlüsselfunktionalität ist das Vorhandensein von RSA-Schlüsseln auf dem KS erforderlich. Der KS stellt dem GM den öffentlichen Schlüssel des RSA-Schlüsselpaars während der Registrierung über diesen sicheren Kanal zur Verfügung. Der KS signiert dann die an den GM gesendeten GDOI-Nachrichten mit dem privaten RSA-Schlüssel in der GDOI SIG-Nutzlast. Der GM empfängt die GDOI-Meldungen und verwendet den öffentlichen RSA-Schlüssel, um die Nachricht zu überprüfen. Die Nachrichten zwischen dem KS und dem GM werden mit dem KEK verschlüsselt, der auch während der Registrierung an den GM verteilt wird. Nach Abschluss der Registrierung werden die nachfolgenden erneuten Schlüssel mit dem KEK verschlüsselt und mit dem privaten RSA-Schlüssel signiert.

Wenn der RSA-Schlüssel während der GM-Registrierung auf dem KS nicht vorhanden ist, wird diese Meldung im Syslog angezeigt:

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```

Wenn die Schlüssel nicht auf dem KS vorhanden sind, registriert die GM zum ersten Mal, aber der nächste rekey fehlschlägt aus der KS. Letztlich laufen die vorhandenen Schlüssel auf dem GM ab und es wird erneut registriert.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may have expired/been
cleared, or didn't go through. Re-register to KS.
```

Da das RSA-Schlüsselpaar zum Signieren der rekey-Meldungen verwendet wird, **MÜSSEN** sie zwischen dem primären und allen sekundären KS identisch sein. Dadurch wird sichergestellt, dass bei einem primären KS-Ausfall die von einem sekundären KS (dem neuen primären KS) gesendeten Tasten von den GMs weiterhin korrekt validiert werden können. Wenn das RSA-Schlüsselpaar auf dem primären KS generiert wird, muss das Schlüsselpaar mit der **exportierbaren** Option erstellt werden, damit sie in alle sekundären KS exportiert werden können, um diese Anforderung zu erfüllen.

#### Neuschlüsselfehlerbehebung

KEK/TEK-rekey-Fehler ist eines der häufigsten GETVPN-Probleme, die in Kundenbereitstellungen auftreten. Bei der Fehlerbehebung sollten die hier beschriebenen Schritte befolgt werden:

1. Wurden die Tastenneuheiten von KS gesendet?

   Dies kann durch eine Beobachtung der Syslog-Meldung %GDOI-5-KS_SEND_UNICAST_REKEY oder genauer mit dem folgenden Befehl überprüft werden:

   ```
   KS1#show crypto gdoi ks rekey
   ```

```
Group G1 (Unicast)
Number of Rekeys sent               : 341
Number of Rekeys retransmitted      : 0
KEK rekey lifetime (sec) : 1200
Remaining lifetime (sec) : 894
Retransmit period : 10
Number of retransmissions : 5
IPSec SA 1 lifetime (sec) : 900
Remaining lifetime (sec) : 405
```

Die Anzahl der erneut übertragenen Schlüssel ist ein Hinweis auf rekey Bestätigungspakete, die nicht vom KS empfangen wurden, und somit auf mögliche rekey-Probleme. Bedenken Sie, dass der GDOI-Schlüssel UDP als unzuverlässigen Transportmechanismus verwendet, sodass je nach der Zuverlässigkeit des zugrunde liegenden Transportnetzwerks einige weitere Einbrüche zu erwarten sind, aber es sollte immer ein Trend zu zunehmenden erneuten Übertragungen untersucht werden.

Detailliertere Statistiken nach GM-Schlüssel sind ebenfalls erhältlich. Dies ist in der Regel der erste Ort, um nach potenziellen Problemen zu suchen.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. Wurden die rekey-Pakete im zugrunde liegenden Infrastrukturnetzwerk bereitgestellt?

   Die standardmäßige IP-Fehlerbehebung entlang des rekey Forwarding-Pfads sollte befolgt werden, um sicherzustellen, dass die rekey-Pakete nicht im Transit-Netzwerk zwischen KS und GM verworfen werden. Einige gängige Tools zur Fehlerbehebung sind ACLs (Input/Output Access Control Lists), NetFlow und die Paketerfassung im Transit-Netzwerk.

3. Haben die rekey-Pakete den GDOI-Prozess zur erneuten Verarbeitung erreicht?

   Statistiken zu GM rekey:

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

4. Wurde das rekey-Bestätigungspaket wieder in das KS aufgenommen?

   Folgen Sie den Schritten 1 bis 3, um das rekey-Bestätigungspaket vom GM zurück zum KS zu verfolgen.

#### Multicast-Neuschlüssel

Multicast-Schlüssel unterscheidet sich in folgenden Punkten von Unicast-rekey:

- Da Multicast verwendet wird, um diese rekey-Pakete vom KS zu den GMs zu transportieren, muss der KS die rekey-Pakete nicht selbst replizieren. KS sendet nur eine Kopie des rekey-Pakets und repliziert diese im Multicast-fähigen Netzwerk.
- Es gibt keinen Bestätigungsmechanismus für Multicast-rekey. Wenn also ein GM das rekey-Paket nicht empfangen würde, hätte der KS keine Kenntnis davon und würde daher niemals eine GM aus seiner GM-Datenbank entfernen. Und da es keine Bestätigung gibt, wird der KS die rekey-Pakete immer basierend auf seiner Konfiguration für die erneute Übertragung neu übertragen.

Das am häufigsten festgestellte Multicast-rekey-Problem besteht darin, dass der rekey auf dem GM nicht empfangen wird. Dies kann verschiedene Ursachen haben, z. B.:

- Problem bei der Paketübermittlung in der Multicast-Routing-Infrastruktur
- End-to-End-Multicast-Routing ist im Netzwerk nicht aktiviert.

Der erste Schritt zur Fehlerbehebung bei einem Multicast-erneuten Schlüssel besteht darin, festzustellen, ob rekey beim Wechsel von der Multicast- zur Unicast-Methode funktioniert.

Wenn Sie festgestellt haben, dass das Problem spezifisch für Multicast-Schlüssel ist, stellen Sie sicher, dass KS den Schlüssel an die angegebene Multicast-Adresse sendet.

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group G1 from address
10.1.11.2 to 226.1.1.1 with seq # 6
```

Testen Sie die Multicast-Verbindung zwischen dem KS und GM mithilfe einer ICMP-Anfrage (Internet Control Message Protocol) an die Multicast-Adresse. Alle GMs, die Teil der Multicast-Gruppe sind, sollten auf den Ping antworten. Stellen Sie sicher, dass ICMP für diesen Test von der KS-Verschlüsselungsrichtlinie ausgeschlossen ist.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:
```

```
Reply to request 0 from 10.1.21.2, 44 ms
```

Wenn der Multicast-Ping-Test fehlschlägt, muss eine Fehlerbehebung für Multicast durchgeführt werden, die nicht in den Anwendungsbereich dieses Dokuments fällt.

## Relay-Check der Kontrollebene

### Symptom

Wenn Kunden ihr GM auf eine neue Cisco IOS-Version aktualisieren, tritt möglicherweise wieder KEK-Fehler auf, wenn diese Meldung im Syslog angezeigt wird:

```
%GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 1 in seq payload for
group G1, last seq # 11
%GDOI-3-GDOI_REKEY_FAILURE: Processing of REKEY payloads failed on GM 10.1.13.2 in the group G1,
with peer at 10.1.11.2
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of GDOI mode failed with peer at 10.1.11.2
```

Dieses Verhalten wird durch ein Interoperabilitätsproblem verursacht, das mit der Anti-Replay-Prüfung eingeführt wurde, die für Nachrichten auf Kontrollebene hinzugefügt wird. Insbesondere ein KS, das den älteren Code ausführt, setzt die KEK-rekey-Sequenznummer auf 1 zurück. Dies wird von dem GM verworfen, der den neuen Code ausführt, wenn er dies als wiedergegebenes rekey-Paket interpretiert. Weitere Informationen finden Sie unter Cisco Bug ID CSCta05809 (GETVPN: GETVPN-Kontrollebene (sinnvolle Wiederholung) und GETVPN-Konfigurationseinschränkungen.

### Hintergrund

Mit GETVPN können die Kontrollebenenmeldungen zeitkritische Informationen enthalten, um einen zeitbasierten Anti-Replay-Überprüfungsservice bereitzustellen. Aus diesem Grund müssen diese Nachrichten selbst gegen Wiederholung geschützt werden, um eine zeitgenaue Absicherung zu gewährleisten. Diese Meldungen sind:

- **Nachrichten** von KS zu GM **erneut** markieren
- **COOP-Ansagen** zwischen KSs

Im Rahmen dieser Anti-Replay-Implementierung wurden Sequenzzahlprüfungen hinzugefügt, um wiedergegebene Nachrichten zu schützen, sowie eine Pseudozeitüberprüfung, wenn TBAR aktiviert ist.

## Lösung

Um dieses Problem zu beheben, müssen GM und KS nach der Kontrollebenenprüffunktion auf Cisco IOS-Versionen aktualisiert werden. Mit dem neuen Cisco IOS-Code setzt KS die Sequenznummer für einen KEK-Schlüssel nicht auf 1 zurück, sondern verwendet stattdessen die aktuelle Sequenznummer und setzt nur die Sequenznummer für TEK-Rekeys zurück.

Diese Cisco IOS-Versionen verfügen über die folgenden Funktionen:

- 12,4(15)T10
- 12,4(22)T3
- 12,4(24)T2
- 15.0(1)M und spätere Version

#### Weitere Probleme im Zusammenhang mit Wiederholungen

- COOP-Fehler aufgrund einer fehlgeschlagenen Wiederholungsprüfung für ANN-Nachrichten (Cisco Bug ID CSCtc52655)

#### Fehler beim erneuten Abspielen der Kontrollebene

Bei anderen Fehlern bei Replay auf der Kontrollebene sammeln Sie diese Informationen, und stellen Sie sicher, dass die Zeiten zwischen KS und GM synchronisiert sind.

- Syslog von GM und KS
- ISAKMP-Debugging
- GDOI-Debug (rekey und replay) von KS und GM

### Probleme mit der Fragmentierung von Steuerelementpaketen

Bei GETVPN ist die Fragmentierung von Kontrollebenenpaketen ein häufiges Problem. Sie kann sich in einem der beiden Szenarien manifestieren, wenn die Pakete der Kontrollebene groß genug sind, dass sie eine IP-Fragmentierung erfordern:

- GETVPN COOP Ankündigungspakete
- GETVPN-rekey-Pakete

### COOP Ankündigungspakete

Die COOP-Ankündigungspakete enthalten die GM-Datenbankinformationen und können daher in einer großen GETVPN-Bereitstellung groß werden. Ein GETVPN-Netzwerk, das aus mehr als 1.500 GMs besteht, erzeugt Ankündigungspakete mit mehr als 18.024 Byte. Dies ist die Cisco IOS-Standardgröße für eine große Puffergröße. In diesem Fall vergibt der KS keinen Puffer, der groß genug ist, um die ANN-Pakete mit diesem Fehler zu übertragen:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 18872 -Process= "Crypto IKMP", ipl= 0, pid= 183
```

Um diese Bedingung zu korrigieren, wird folgende Einstellung empfohlen:

```
buffers huge permanent 10
buffers huge size 65535
```

#### Pakete neu schlüsseln

GETVPN-rekey-Pakete können auch die typische Größe der 1500 IP Maximum Transition Unit (MTU) überschreiten, wenn die Verschlüsselungsrichtlinie groß ist, z. B. eine Richtlinie, die aus 8+ Zeilen Access Control Entries (ACEs) in der Verschlüsselungs-ACL besteht.

#### Fragmentierungsproblem und Identifizierung

In beiden vorherigen Szenarien muss GETVPN in der Lage sein, die fragmentierten UDP-Pakete ordnungsgemäß zu übertragen und zu empfangen, damit COOP oder GDOI rekey ordnungsgemäß funktionieren. Die IP-Fragmentierung kann in einigen Netzwerkumgebungen ein Problem darstellen. Beispielsweise erfordert ein Netzwerk, das aus der ECMP-Weiterleitungsebene (Equal Cost Multi Path) besteht, und einige Geräte auf der

Weiterleitungsebene eine virtuelle Reassemblierung der fragmentierten IP-Pakete, z. B. Virtual Fragmentation Reassembly (VFR).

Um das Problem zu identifizieren, überprüfen Sie die Zusammenstellungsfehler auf dem Gerät, bei dem der Verdacht besteht, dass die fragmentierten UDP 848-Pakete nicht ordnungsgemäß empfangen wurden:

```
KS1#show ip traffic | section Frags
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

Wenn die Reassemblierungs-Timeouts weiter inkrementiert werden, können Sie mit dem Befehl **debug ip error** überprüfen, ob der Drop Teil des rekey/COOP-Paketflusses ist. Nach der Bestätigung sollte eine normale Fehlerbehebung bei der IP-Weiterleitung durchgeführt werden, um das genaue Gerät auf der Weiterleitungsebene zu isolieren, das möglicherweise die Pakete verworfen hat. Einige häufig verwendete Tools sind:

- Paketerfassung
- Statistiken zur Weiterleitung von Datenverkehr
- Statistiken zu Sicherheitsfunktionen (Firewall, IPS)
- VFR-Statistiken

### Probleme mit der GDOI-Interoperabilität

Im Laufe der Jahre wurden bei GETVPN verschiedene Interoperabilitätsprobleme entdeckt, und es ist wichtig, bei Interoperabilitätsproblemen die Cisco IOS-Versionen zwischen KS und GM sowie unter den KS zu beachten.

Weitere bekannte GETVPN-Interoperabilitätsprobleme sind:

- Relay-Check der Kontrollebene
- Änderung des Verhaltens des GETVPN KEK-Neuschlüssels
- Cisco Bug-ID CSCub42920 (GETVPN: KS überprüft Hash in rekey ACK aus früheren GM-Versionen nicht.)
- Cisco Bug-ID CSCuw48400 (GetVPN GM kann sich nicht registrieren, oder rekey schlägt fehl - sig-hash > default SHA-1)
- Cisco Bug-ID CSCvg19281 ( Mehrere GETVPN GM-Abstürze nach der Migration zum neuen KS-Paar ; Wenn eine GM-Version älter als 3.16 ist und KS von einem früheren Code auf 3.16 oder höher aktualisiert wird, kann dieses Problem auftreten)

#### Upgrade-Verfahren für GETVPN IOS

Dieses Cisco IOS-Upgrade-Verfahren sollte befolgt werden, wenn ein Cisco IOS-Code-Upgrade in einer GETVPN-Umgebung durchgeführt werden muss:

1. Aktualisieren Sie zuerst ein sekundäres KS und warten Sie, bis die COOP KS-Wahl abgeschlossen ist.
2. Wiederholen Sie Schritt 1 für alle sekundären KSs.
3. Aktualisieren Sie das primäre KS.
4. GMs aktualisieren

# Fehlerbehebung bei Problemen mit der GETVPN-Datenebene

Im Vergleich zu Problemen auf Kontrollebene sind GETVPN-Probleme auf Datenebene Probleme, bei denen GM über die Richtlinien und Schlüssel verfügt, um Datenblattverschlüsselung und -entschlüsselung durchzuführen, aber aus irgendeinem Grund funktioniert der End-to-End-Datenverkehrsfluss nicht. Die meisten Probleme im Zusammenhang mit GETVPN-Datenplänen betreffen die generische IPsec-Weiterleitung und sind nicht GETVPN-spezifisch. Die meisten der hier beschriebenen Fehlerbehebungsmethoden gelten auch für generische IPsec-Datenaplan-Probleme.

Bei Verschlüsselungsproblemen (sowohl in Gruppen- als auch in Zweiertunneln) ist es wichtig, das Problem zu beheben und das Problem auf einen bestimmten Teil des Datenpfads zu isolieren. Der hier beschriebene Ansatz zur Fehlerbehebung soll Ihnen dabei helfen, die folgenden Fragen zu beantworten:

- Welches Gerät ist der Schuldige - Router verschlüsseln oder Router entschlüsseln?
- In welche Richtung geschieht das Problem - ein- oder ausgehend?

## Tools zur Fehlerbehebung für GETVPN-Datenebene

Die Fehlerbehebung für IPsec-Datenpfade unterscheidet sich stark von der für die Kontrollebene. Beim Datenblatt gibt es normalerweise keine Debuggen, die Sie ausführen können, oder zumindest sicher in einer Produktionsumgebung. Die Fehlerbehebung basiert daher in hohem Maße auf unterschiedlichen Zählern und Datenverkehrsstatistiken, die die Nachverfolgung des Pakets über einen Weiterleitungspfad unterstützen. Die Idee besteht darin, eine Reihe von Prüfpunkten zu entwickeln, um zu helfen, zu isolieren, wo Pakete verworfen werden könnten, wie hier gezeigt:


Hier sind einige Debugtools für die Datenebene:

- Zugriffslisten
- IP Precedence Accounting
- NetFlow
- Schnittstellenzähler
- Krypto-Zähler
- Globale IP Cisco Express Forwarding (CEF)- und Funktionsabbruchzähler
- Embedded Packet Capture (EPC)
- Debugs auf Datenebene (IP-Paket- und CEF-Debugger)

Die Prüfpunkte im Datenpfad im vorherigen Bild können mithilfe der folgenden Tools validiert werden:

### Verschlüsselung von GM

- Eingangs-LAN-Schnittstelle
  - ACL eingeben
  - Eingangs-NetFlow
  - Integrierte Paketerfassung
  - Abrechnung mit Eingabeprioritäten

- Krypto-Engine
  - **show crypto ipsec sa**
  - **show crypto ipsec sa detail**
  - **Anzeigen von Krypto-Engine-Beschleunigungsstatistiken**

- Ausgangs-WAN-Schnittstelle
  - Ausgangs-NetFlow
  - Integrierte Paketerfassung
  - Abrechnung der Ausgabepriorität

**Entschlüsselung GM**

- WAN-Eingangsschnittstelle
  - ACL eingeben
  - Eingangs-NetFlow
  - Integrierte Paketerfassung
  - Abrechnung mit Eingabeprioritäten

- Verschlüsselungsmodul
  - **show crypto ipsec sa**
  - **show crypto ipsec sa detail**
  - **Anzeigen von Krypto-Engine-Beschleunigungsstatistiken**

- Ausgangs-LAN-Schnittstelle
  - Ausgangs-NetFlow
  - Integrierte Paketerfassung

Der Rückgabepfad folgt demselben Datenverkehrsfluss. In den folgenden Abschnitten werden einige Beispiele dieser verwendeten DataSpane-Tools aufgeführt.

### Verschlüsselungs-/Entschlüsselungszähler

Die Verschlüsselungs-/Entschlüsselungszähler eines Routers basieren auf einem IPsec-Fluss. Leider funktioniert dies mit GETVPN nicht gut, da GETVPN in der Regel eine Verschlüsselungsrichtlinie "permit ip any any" bereitstellt, die alles verschlüsselt. Wenn das Problem also nur bei einigen und nicht bei allen Datenflüssen auftritt, können diese Zähler etwas schwierig zu verwenden sein, um korrekt zu beurteilen, ob die Pakete verschlüsselt oder entschlüsselt werden, wenn genügend Hintergrunddatenverkehr vorhanden ist.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

### NetFlow

NetFlow kann zur Überwachung des ein- und ausgehenden Datenverkehrs auf beiden GMs verwendet werden. Beachten Sie, dass bei GETVPN **permit ip any** policy der verschlüsselte Datenverkehr aggregiert wird und nicht die Informationen für jeden Datenfluss enthält. Pro-Datenfluss-Informationen müssen dann mit der später beschriebenen DSCP/Precedence-Markierung erfasst werden.

In diesem Beispiel wird der NetFlow für einen Ping mit einer 100-Anzahl von einem Host hinter GM1 zu einem Host hinter GM2 an den verschiedenen Kontrollpunkten angezeigt.

### Verschlüsselung von GM

NetFlow-Konfiguration:

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

NetFlow-Ausgabe:

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

> **Hinweis**: In der vorherigen Ausgabe gibt * den ausgehenden Datenverkehr an. Die erste Zeile zeigt verschlüsselten ausgehenden Datenverkehr (mit Protokoll 0x32 = ESP) von der WAN-Schnittstelle und ICMP-Datenverkehr von der zweiten Zeile über die LAN-Schnittstelle.

### Entschlüsselung GM

Konfiguration:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

NetFlow-Ausgabe:

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

## DSCP/IP Precedence-Markierung

Die Herausforderung bei der Fehlerbehebung bei einem Verschlüsselungsproblem besteht darin, dass Sie nach der Verschlüsselung die Payload nicht mehr sehen können. Dies ist die Funktion der Verschlüsselung. Dadurch wird es schwierig, das Paket für einen bestimmten IP-Fluss nachzuverfolgen. Es gibt zwei Möglichkeiten, diese Einschränkung zu beheben, wenn es um die Behebung eines IPsec-Problems geht:

- Verwenden Sie ESP-NULL als IPsec-Umwandlung. IPsec führt weiterhin ESP-Kapselung durch, aber auf die Nutzlast wird keine Verschlüsselung angewendet, sodass sie in einer Paketerfassung sichtbar sind.
- Markieren Sie einen IP-Datenfluss mit einer eindeutigen DSCP-/Prioritätsmarkierung (Differentiated Services Code Point), die auf den L3-/L4-Eigenschaften basiert.

ESP-NULL erfordert Änderungen an beiden Tunnelendpunkten und ist oft aufgrund der Sicherheitsrichtlinie des Kunden nicht zulässig. Daher empfiehlt Cisco in der Regel stattdessen die Verwendung einer DSCP-/Prioritätsmarkierung.

#### Referenzdiagramm zu DSCP/Precedence

| ToS (Hex) | ToS (Dezimal) | IP-Rangfolge | DSCP | Binär |
|---|---|---|---|---|
| 0 x E0 | 224 | 7 Netzwerksteuerung | 56 CS7 | 11.0000 |
| 0 x C0 | 192 | 6 Internetwork Control | 48 CS6 | 110.0000 |
| 0 x B8 | 184 | 5 Kritisch | 46 EF | 101 11000 |
| 0 x A0 | 160 | | 40 CS5 | 101.0000 |
| 0 x 88 | 136 | 4 Flash-Außerkraftsetzung | 34 AF41 | 10001000 |
| 0 x 80 | 128 | | 32 CS4 | 1000000 |
| 0 x 68 | 104 | 3 Flash | 26 AF31 | 011 01000 |
| 0 x 60 | 96 | | 24 CS3 | 0110000 |
| 0 x 48 | 72 | 2 Sofort | 18 AF21 | 01001000 |
| 0 x 40 | 64 | | 16 CS2 | 0100000 |
| 0 x 20 | 32 | 1 Priorität | 8 CS1 | 0010000 |
| 0 x 00 | 0 | 0 Routine | 0 Pixel | 0000000 |

#### Pakete mit DSCP/Precedence markieren

Diese Methoden werden in der Regel verwendet, um Pakete mit den spezifischen DSCP-/Precedence-Markierungen zu kennzeichnen.

## PBR

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
```

```
match ip address 150
set ip precedence flash-override
```

### MQC

```
class-map match-all my_flow
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

### Router-Ping

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

> **Hinweis**: Es empfiehlt sich, den normalen Datenverkehrsfluss und das DSCP/Precedence-Profil vor der Anwendung von Markierungen zu überwachen, um einen eindeutigen Datenverkehrsfluss zu gewährleisten.

#### Überwachen markierter Pakete

### IP Precedence Accounting

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
```

```
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

### Schnittstelle ACL

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
```

```
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

## Integrierte Paketerfassung

Embedded Packet Capture (EPC) ist ein nützliches Tool zum Erfassen von Paketen auf Schnittstellenebene, um festzustellen, ob ein Paket ein bestimmtes Gerät erreicht hat. Denken Sie daran, dass EPC für den Klartext-Datenverkehr gut funktioniert, aber es kann eine Herausforderung sein, wenn die erfassten Pakete verschlüsselt werden. Daher müssen Techniken wie die zuvor erwähnte DSCP-/Prioritätsmarkierung oder andere IP-Zeichen wie die Länge des IP-Pakets zusammen mit EPC verwendet werden, um die Fehlerbehebung effektiver zu gestalten.

## Cisco IOS-XE Packet Trace

Dies ist eine nützliche Funktion, um den Pfad für die Funktionsweiterleitung auf allen Plattformen nachzuverfolgen, auf denen Cisco IOS-XE ausgeführt wird, z. B. CSR1000v, ASR1000 und ISR4451-X.

## GETVPN-Datenebene Häufige Probleme

Die Fehlerbehebung für das IPsec-Datenaplane für GETVPN unterscheidet sich größtenteils nicht von der Fehlerbehebung für herkömmliche Point-to-Point-Probleme mit dem IPsec-Datenaplan, mit zwei Ausnahmen aufgrund dieser einzigartigen Eigenschaften von GETVPN auf der Datenebene.

### Zeitbasierte Anti-Replay-Fehlermeldung

In einem GETVPN-Netzwerk kann die Fehlerbehebung bei TBAR-Ausfällen häufig schwierig sein, da es keine paarweisen Tunnel mehr gibt. Gehen Sie wie folgt vor, um Fehler bei GETVPN TBAR zu beheben:

1. Identifizieren Sie, welches Paket aufgrund eines TBAR-Fehlers verworfen wird, und identifizieren Sie anschließend die verschlüsselnde GM.

   Vor der Version 15.3(2)T druckte das TBAR-Fehler-Syslog die Quelladresse des fehlerhaften Pakets nicht aus. Dies erschwert die Identifizierung des ausgefallenen Pakets. Dies wurde in Version 15.3(2)T und höher, in der Cisco IOS Folgendes druckt, erheblich verbessert:

   ```
   %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
   connection id=13, sequence number=1

   %GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in group G1:
   my_pseudotime = 620051.84 secs, peer_pseudotime = 619767.09 secs, replay_window =
   4 (sec), src_ip = 192.168.13.2, dst_ip = 192.168.14.2
   ```

   In dieser Version wurde auch ein TBAR-Verlauf implementiert:

   ```
   GM2#show crypto gdoi gm replay
   Anti-replay Information For Group G1:
   Timebased Replay:
   ```

```
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs


TBAR Error History (sampled at 10pak/min):
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

**Hinweis**: Die zuvor erwähnten Erweiterungen wurden seitdem in Cisco IOS-XE durch die Cisco Bug ID CSCun49335 und in Cisco IOS durch den Cisco Bug ID CSCub91811 implementiert.
Bei Cisco IOS-Versionen, die diese Funktion nicht enthielten, können die **Details** zur **Fehlerbehebung für gdoi gm-Wiedergabe** auch diese Informationen bereitstellen, obwohl bei diesem Debuggen die TBAR-Informationen für den gesamten Datenverkehr ausgegeben werden (nicht nur Pakete, die aufgrund eines TBAR-Ausfalls verworfen wurden), sodass es möglicherweise nicht möglich ist, in einer Produktionsumgebung auszuführen.

```
GDOI:GM REPLAY:DET:(0):my_pseudotime is 621602.30 (secs), peer_pseudotime is 621561.14
(secs), replay_window is 4 (secs), src_addr = 192.168.14.2, dest_addr = 192.168.13.2
```

2. Sobald die Quelle des Pakets identifiziert wurde, sollten Sie in der Lage sein, die verschlüsselnde GM zu finden. Anschließend sollte der Pseudozeitstempel sowohl bei der Verschlüsselung als auch bei der Entschlüsselung von GMs auf mögliche Abweichungen bei der Pseudozeit überwacht werden. Die beste Methode hierfür wäre, sowohl die GMs als auch die KS mit NTP zu synchronisieren und die Pseudotime-Informationen periodisch mit einer Referenz-Systemuhr auf allen zu sammeln, um festzustellen, ob das Problem durch einen Uhrenverzerrung auf den GMs verursacht wird.

### GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value             : 625866.26 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

### GM2

```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value             : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

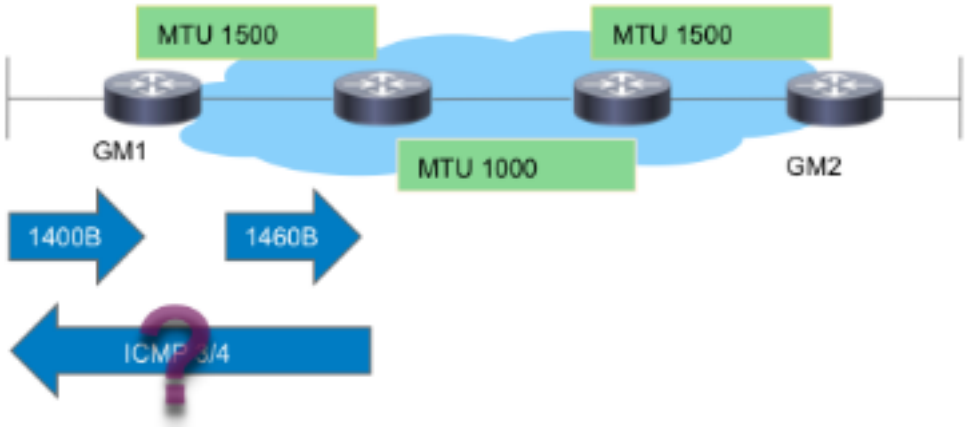
Wenn sich im vorherigen Beispiel die Pseudozeit (wie durch Replay Value angegeben) zwischen

den GMs signifikant unterscheidet, wenn die Ausgaben mit derselben Referenzzeit erfasst werden, kann das Problem auf Uhrschiew zurückgeführt werden.

> **Hinweis**: Auf der Plattform der Cisco Aggregated Services Router der Serie 1000 bezieht sich der Datenpfad auf dem Quantum Flow Processor (QFP) aufgrund der Plattformarchitektur eigentlich auf die Wanduhr zum Zählen von Pseudotime-Ticks. Dies hat zu Problemen mit der TBAR geführt, wenn sich die Uhrzeit der Wanduhr aufgrund der NTP-Synchronisierung ändert. Dieses Problem ist mit der Cisco Bug-ID CSCum37911 dokumentiert.

#### PMTUD und GETVPN-Header-Beibehaltung

Mit GETVPN funktioniert die Path MTU Discovery (PMTUD) zwischen den verschlüsselnden und entschlüsselnden GMs nicht, und große Pakete mit dem Don't Fragment (DF)-Bitsatz können blockiert werden. Der Grund dafür, dass dies nicht funktioniert, liegt in der GETVPN-Header-Reservierung, bei der die Quell-/Zieladressen im ESP-Kapselungsheader erhalten bleiben. Dies wird in diesem Bild dargestellt:




Wie das Bild zeigt, wird die PMTUD mit GETVPN in diesem Fluss unterbrochen:

1. Große Datenpakete kommen auf dem verschlüsselnden GM1 an.
2. Das nachverschlüsselte ESP-Paket wird aus GM1 weitergeleitet und an das Ziel geliefert.
3. Wenn eine Transit-Verbindung mit einer IP-MTU von 1.400 Byte besteht, wird das ESP-Paket verworfen, und ein ICMP-3/4-Paket wird an die Paketquelle gesendet, die die Quelle des Datenpakets ist.
4. Das ICMP3/4-Paket wird entweder aufgrund von ICMP verworfen, der nicht von der GETVPN-Verschlüsselungsrichtlinie ausgeschlossen ist, oder vom Endhost verworfen, da er nichts über das ESP-Paket weiß (nicht authentifizierte Payload).

Zusammenfassend lässt sich sagen, dass die PMTUD derzeit nicht mit GETVPN kompatibel ist. Um dieses Problem zu umgehen, empfiehlt Cisco folgende Schritte:

1. Implementieren Sie "ip tcp adjust-mss", um die Größe des TCP-Pakets zu reduzieren, um Verschlüsselungsaufwand und MTU des Mindestpfads im Transit-Netzwerk zu berücksichtigen.
2. Löschen Sie das DF-Bit im Datenpaket, wenn diese auf dem verschlüsselnden GM eintreffen, um die PMTUD zu vermeiden.

### Generische Probleme mit IPsec-Datenspuren

Der Großteil der Fehlerbehebung für IPsec-Datenpfade ähnelt der Fehlerbehebung bei herkömmlichen Point-to-Point-IPsec-Tunneln. Eines der häufigsten Probleme ist %CRYPTO-4-RECVD_PKT_MAC_ERR. Weitere Informationen zur Fehlerbehebung finden Sie unter Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" Fehlermeldung mit Ping Loss Over IPsec Tunnel Troubleshooting (Fehlerbehebung bei Ping Loss Over IPsec Tunnel).

### Bekannte Probleme

Diese Meldung kann generiert werden, wenn ein IPsec-Paket empfangen wird, das nicht mit einem SPI in der SADB übereinstimmt. Siehe Cisco Bug ID CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC für pkt not matching flow. Ein Beispiel:

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
vrf/dest_addr= /192.168.14.2, src_addr= 192.168.13.2, prot= 50
```

Diese Meldung sollte %CRYPTO-4-RECVD_PKT_INV_SPI lauten. Dies wird sowohl für herkömmliche IPsec als auch für einige Hardwareplattformen wie ASR gemeldet. Dieses kosmetische Problem wurde durch die Cisco Bug ID CSCup80547 behoben: Fehler bei der Meldung CRYPTO-4-RECVD_PKT_NOT_IPSEC für ESP-Paket.

> **Hinweis**: Diese Meldungen können manchmal aufgrund eines anderen GETVPN-Fehlers CSCup34371 angezeigt werden: GETVPN GM stoppt die Entschlüsselung des Datenverkehrs nach TEK-rekey.

In diesem Fall kann der GM den GETVPN-Datenverkehr nicht entschlüsseln, obwohl er in der SADB über eine gültige IPsec-SA verfügt (die SA wird neu verschlüsselt). Das Problem verschwindet, sobald die SA abläuft, und wird aus der SADB entfernt. Dieses Problem verursacht einen erheblichen Ausfall, da TEK-Schlüssel im Voraus durchgeführt wird. Bei einer TEK-Lebensdauer von 7200 Sekunden kann der Ausfall beispielsweise 22 Minuten betragen. In der Fehlerbeschreibung finden Sie die genaue Bedingung, die erfüllt werden muss, um auf diesen Fehler zu stoßen.

# Fehlerbehebung bei GETVPN auf Plattformen, auf denen Cisco IOS-XE ausgeführt wird

## Befehle zur Fehlerbehebung

Plattformen, auf denen Cisco IOS-XE ausgeführt wird, verfügen über plattformspezifische Implementierungen und erfordern häufig plattformspezifisches Debugging für GETVPN-Probleme. Im Folgenden finden Sie eine Liste von Befehlen, die in der Regel zur Fehlerbehebung bei GETVPN auf diesen Plattformen verwendet werden:

### show crypto eli all

### Anzeige von IPSec-Richtlinien für Plattformsoftware

### show plattform software ipsec fp aktives inventar

**show platform hardware qfp active feature ipsec spall**

**show platform hardware qfp active statistics drop clear**

**show platform hardware qfp active feature ipsec data drop clear**

**show crypto ipsec sa**

**Krypto-Gdoi anzeigen**

**show crypto ipsec internal**

**debuggen crypto ipsec**

**debuggen crypto ipsec error**

**debuggen crypto ipsec status**

**debuggen crypto ipsec-Nachricht**

**debuggen crypto ipsec hw-req**

**debuggen crypto gdoi gm infra detail**

**debuggen crypto gdoi gm rekey Detail**

### Häufige ASR1000-Probleme

#### Fehler bei der Installation der IPsec-Richtlinie (kontinuierliche erneute Registrierung)

Wenn die Verschlüsselungs-Engine die empfangene IPsec-Richtlinie oder den empfangenen Algorithmus nicht unterstützt, kann sich ein ASR1000 GM weiterhin beim Schlüsselserver registrieren. So werden beispielsweise auf Nitrox-basierten ASR-Plattformen (wie ASR1002) Suite-B- oder SHA2-Richtlinien nicht unterstützt, was zu fortgesetzten Wiederregistrierungssymptomen führen kann.

## Häufige Migrations-/Upgrade-Probleme

### ASR1000 TBAR-Einschränkung

Auf der ASR1000-Plattform führte der Cisco Bug ID CSCum37911 Fix eine Beschränkung auf diese Plattform ein, wenn eine TBAR-Zeit von weniger als 20 Sekunden nicht unterstützt wird. Siehe Einschränkungen für GETVPN auf IOS-XE.

Dieser Verbesserungsfehler wurde geöffnet, um diese Einschränkung aufzuheben. Die Cisco Bug ID CSCuq25476 - ASR1k muss eine GETVPN TBAR-Fenstergröße von weniger als 20 Sekunden unterstützen.

**Aktualisieren:** Diese Einschränkung wurde seitdem mit der Behebung für die Cisco Bug-ID CSCur57558 aufgehoben, und sie ist keine Einschränkung in XE3.10.5, XE3.13.2 und neueren Codes mehr.

Beachten Sie außerdem, dass für eine GM, die auf Cisco IOS-XE-Plattformen (ASR1k oder ISR4k) ausgeführt wird, dringend empfohlen wird, dass das Gerät eine Version mit dem Fix für dieses Problem ausführt, wenn TBAR aktiviert ist. Cisco Bug-ID CSCut91647 - GETVPN auf IOS-XE: GM verwirft Pakete aufgrund von TBAR-Fehlern falsch.

### ISR4x00-Klassifizierungsproblem

Auf der ISR4x00-Plattform wurde eine Regression gefunden, bei der die Richtlinien zur Ablehnung ignoriert werden. Einzelheiten finden Sie unter Cisco Bug ID CSCut14355 - GETVPN - ISR4300 GM ignoriert Richtlinien zur Ablehnung.

## Zugehörige Informationen

- Group Encrypted Transport VPN (GET VPN) - Cisco Systems
- Technischer Support und Dokumentation - Cisco Systems