GETVPN トラブルシューティング ガイド

目次

はじめに
前提条件
要件
使用するコンポーネント
GETVPN のトラブルシューティング手順
参照トポロジ
リファレンス構成
用語
ロギング機能の準備および他のベスト プラクティス
GETVPN コントロール プレーンの問題のトラブルシューティング
コントロール プレーン デバッグのベスト プラクティス
GETVPN コントロール プレーン トラブルシューティング ツール
GETVPN show コマンド
GETVPN Syslog メッセージ
グローバル暗号化および GDOI デバッグ
GDOI 条件付きデバッグ
GDOI イベント トレース
GETVPN コントロール プレーンのチェックポイントと一般的な問題
COOP の設定およびポリシーの作成
IKE の設定
登録、ポリシー ダウンロードおよび SA インストール
キー再生成
コントロール プレーン リレー チェック
コントロール プレーン パケット フラグメンテーションの問題
GDOI 相互運用性の問題
GETVPN データ プレーンの問題のトラブルシューティング
GETVPN データ プレーン トラブルシューティング ツール
Encryption/Decryption カウンタ
NetFlow
DSCP/IP 優先順位マーキング
Embedded Packet Capture
Cisco IOS XE パケットトレース
GETVPN データ プレーンの一般的な問題
IPsec 一般的 な Dataplane 問題
既知の問題
Cisco IOS XE を実行するプラットフォームの GETVPN を解決して下さい
トラブルシューティングのためのコマンド
ASR1000 よくある 問題
IPsec ポリシー インストール失敗（連続的な再登録）
よくある移行/アップグレードの問題

[ASR1000 TBAR 制限](#)
[ISR4x00 分類問題](#)
[関連情報](#)

概要

このドキュメントは、Group Encrypted Transport VPN（GETVPN）の問題を特定して切り離し、可能な解決策を示す体系的なトラブルシューティング方法と有用なヒントを説明することを目的としています。

前提条件

要件

次の項目に関する知識が推奨されます。

- GETVPN
  公式 GETVPN コンフィギュレーション ガイド
  公式 GETVPN 設計 および 実装 ガイド

- Syslog サーバの使用

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

GETVPN のトラブルシューティング手順

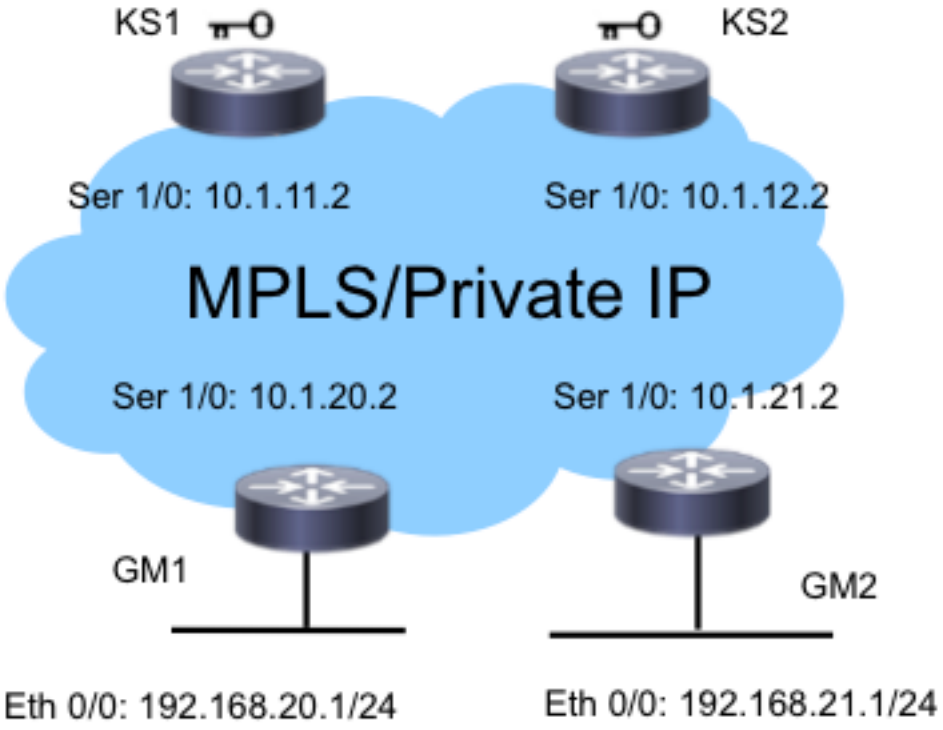
複雑な技術上の問題に関する多くのトラブルシューティングと同様に、問題を特定の機能、サブシステム、またはコンポーネントに切り分けることができることが重要です。 GETVPN ソリューションは、次に示す機能をはじめとする多数の機能コンポーネントで構成されています。

- インターネット キー エクスチェンジ（IKE）-コントロール プレーンを認証し、保護するために KSs グループ メンバー（GM）とキー サーバ（KS）の間で、および協力的なプロトコル（おり）の中で使用される。
- グループ ドメイン オブ インタープリテーション（GDOI）-グループ キーを配り、キーサービスをのような提供するために KS に使用するプロトコルはすべての GMs に鍵変更します。
- COOP： 互いに通信し、冗長性を提供するために KSs に使用するプロトコル。
- ヘッダ保持-エンド ツー エンド トラフィック配信のためにオリジナルデータパケット ヘッダを維持するトンネルモードの IPsec。
- 時間は再生防止を基づかせていました（TBAR） - Group 鍵環境で使用される再生検知機構。

それはまたトラブルシューティング プロセスを楽にするために広範な一組のトラブルシューティング ツールを提供します。 それぞれのトラブルシューティング タスクでどんなツールが使用可能か、またどんな場合にそのツールが適しているかを理解することが重要です。 解決するとき、実稼働環境が悪影響を及ぼされないように最少嵌入的な方式から開始することが常に得策です。 この体系的なトラブルシューティングにおける重要な点は、問題がコントロール プレーンまたはデータ プレーンいずれの問題であるかを特定できることです。 このためには、プロトコルまたはデータ フローを追跡し、ここで説明するさまざまなツールを使用してこれらにチェックポイントを設定します。

参照トポロジ

この GETVPN トポロジおよびアドレス指定方式は、このトラブルシューティング ドキュメントの以降の項で使用されます。



リファレンス構成

- 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
```

注: KS2 と GM2 の設定は簡略化のために省略されています。

用語

- **KS**：キー サーバ
- **GM**：グループ メンバー
- **COOP**：Cooperative Protocol
- **TBAR**：時間ベースのアンチ リプレイ
- **KEK**： キー暗号キー（Key Encryption Key）
- **TEK**： トラフィック暗号キー

ロギング機能の準備および他のベスト プラクティス

トラブルシューティングを開始する前に、次の説明に従ってロギング機能を必ず準備してください。 また、いくつかのベスト プラクティスも示します。

- ルータの空きメモリ量を確認し、[logging buffered debugging] を大きな値（可能であれば 10 MB 以上）に設定します。
- コンソール、モニタ、syslog サーバへのロギングを無効にします。
- バッファ再使用が原因でログが失われるのを防ぐために、**show log コマンド**を使ってロギング バッファの内容を一定間隔（20 分 ~ 1 時間）ごとに取得します。
- 必要となる場合、起こるものは何でも、**show tech コマンドを**影響を受けた GMs および KSs から入力し、グローバルの **show ip route コマンド**の出力を検査すれば各バーチャルルーティングおよび転送（VRF）は含みました。
- デバッグされるすべてのデバイス間でクロックを同期するために、ネットワーク タイム プロトコル（NTP）を使用します。 デバッグ メッセージとログ メッセージに関してミリ秒（msec）タイムスタンプを次のように有効にします。

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- showコマンド出力がタイムスタンプ付きであることを確かめて下さい。

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

- コントロール プレーン イベントまたはデータ プレーン カウンタに関する表示コマンド出力

を収集するときには、必ず同じ出力を何度か反復して収集します。

GETVPN コントロール プレーンの問題のトラブルシューティング

コントロール プレーンは、GM でのポリシーおよびセキュリティ アソシエーション（SA）の作成につながるすべてのプロトコル イベントを意味します。これにより、データ プレーン トラフィックを暗号化および復号化できる状態になります。 GETVPN コントロール プレーンにおける主要チェックポイントには次のものがあります。

コントロール プレーン デバッグのベスト プラクティス

次に示すトラブルシューティングのベスト プラクティスは、GETVPN に固有のものではありません。 ほぼすべてのコントロール プレーン デバッグに適用されます。 ほとんどの効率的な トラブルシューティングを確認するためにこれらの最良の方法に続くことは重要です:

- コンソール ロギングをオフにし、ロギング バッファまたは syslog を使用してデバッグを収集する。
- デバッグされるすべてのデバイスのルータクロックを同期するために NTP を使用して下さい。
- デバッグ メッセージとログ メッセージに対し msec タイムスタンプを有効にする。

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

- show コマンドの出力にタイムスタンプが付けられるようにし、これらの出力をデバッグ出力と相関付けることができるようにする。

```
terminal exec prompt timestamp
```

- 可能であれば、ある程度の規模の環境で条件付きデバッグを使用する。

GETVPN コントロール プレーン トラブルシューティング ツール

GETVPN show コマンド

原則的にほぼすべての GETVPN の問題について収集すべきコマンド出力を次に示します。

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 メッセージ

GETVPN は、重要なプロトコル イベントとエラー状態に関する多数の syslog メッセージの拡張セットを提供します。 GETVPN のトラブルシューティングを行う際には、常に syslog を最初に調べます。

一般的な KS syslog メッセージ

syslog メッセージ	説明
COOP_CONFIG_MISMATCH	主キー サーバとセカンダリ キー サーバ間の設定は組合わせを誤まられま
COOP_KS_ELECTION	ローカル キー サーバによってグループ内の選択プロセスが開始されまし
COOP_KS_REACH	設定済み連携キー サーバ間の到達可能性は回復しています。
COOP_KS_TRANS_TO_PRI	**ローカル キー サーバが、グループ内のセカンダリ サーバからプライマリ**
COOP_KS_UNAUTH	認証されたリモート サーバによって、グループ内のローカル キー サーバ ます。
COOP_KS_UNREACH	**設定済み連携キー サーバ間の到達可能性が失われています。敵対的なイベ**
KS_GM_REVOKED	キー再生成プロトコル中に、認証されていないメンバーによるグループへ
KS_SEND_MCAST_REKEY	**マルチキャスト キー再生成を送信中です。**
KS_SEND_UNICAST_REKEY	**ユニキャスト キー再生成を送信中です。**
KS_UNAUTHORIZED	GDOI 登録プロトコル中に、認証されていないメンバーによるグループへ
UNAUTHORIZED_IPADDR	登録要求が、要求を行っているデバイスがグループへの参加を許可されな

一般的な GM syslog メッセージ

syslog メッセージ	説明
GM_CLEAR_REGISTER	ローカル グループ メンバーによって clear crypto gdoi コマンドが実行 ました。
GM_CM_ATTACH	このローカル グループ メンバー用の暗号マップが追加されました。
GM_CM_DETACH	クリプト マップはローカル グループ member.& のために取り外されま
GM_RE_REGISTER	**1 つグループのために作成される IPsec SA 切れるか、またはクリアさ かもしれません。 キー サーバに対する再登録が必要です。**
GM_RECV_REKEY	**キー再生成を受信しました。**
GM_REGS_COMPL	**登録は完了しています。**
GM_REKEY_TRANS_2_MULTI	グループ メンバーが、ユニキャスト キー再生成メカニズムの使用から ルチキャスト メカニズムの使用へと移行しました。
GM_REKEY_TRANS_2_UNI	グループ メンバーが、マルチキャスト キー再生成メカニズムの使用か ユニキャスト メカニズムの使用へと移行しました。
PSEUDO_TIME_LARGE	グループ メンバーによって、そのグループ メンバーの疑似時間とは大 異なる値を持つ疑似時間が受信されました。
REPLAY_FAILED	グループ メンバーまたはキー サーバによるアンチ リプレイ チェックが しました。

注: 赤で強調表示されているメッセージは GETVPN 環境で見られるもっとも一般的なまたは重要なメッセージです。

グローバル暗号化および GDOI デバッグ

GETVPN デバッグは分けられます:

1. 最初に解決しているデバイスによって。
```
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. 解決している問題の種類による秒。
```
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. 有効になる必要があるデバッグのレベルによる三番目。 バージョン 15.1(3)T 以降では、すべての GDOI 機能デバッグが標準化され、次に示すデバッグ レベルが設定されました。 これは、十分な精度のデバッグにより大規模な GETVPN 環境のトラブルシューティングを支援することを目的としています。 GETVPN の問題をデバッグするときには、適切なデバッグ レベルを使用することが重要です。 原則として、最も低いデバッグレベル（エラー レベル）から開始し、必要に応じてデバッグ精度を上げていきます。
```
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
```

GDOI 条件付きデバッグ

Cisco IOS® バージョン 15.1(3)T 以降では、大規模な環境での GETVPN のトラブルシューティングを支援するために、GDOI 条件付きデバッグが追加されました。 このため、Internet Security Association and Key Management Protocol（ISAKMP）および GDOI デバッグはすべて、グループまたはピア IP アドレスに基づく条件フィルタによって開始できるようになりました。 ほとんどの GETVPN 問題では、適切な条件フィルタを使用して ISAKMP および GDOI デバッグの両方を有効にすることが推奨されます。これは、GDOI デバッグで示されるのは GDOI 固有の操作だけであるためです。 ISAKMP および GDOI の条件付きデバッグを使用するには、次の 2 つの簡単な手順を実行します。

1. 条件フィルタを設定します。
2. 該当する ISAKMP および GDOI を通常の方法で有効にします。

次に、例を示します。

```
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)
```

> **注:** ISAKMP および GDOI 両方の条件付きデバッグでは、条件フィルタ情報 (デバッグ パスの IP アドレスなど) が含まれていない可能性があるデバッグ メッセージをキャッチするために **unmatched** フラグを有効にできます。 ただし、大量のデバッグ情報が生成される場合があるため、十分に注意して使用する必要があります。

GDOI イベント トレース

これはバージョン 15.1(3)T で追加されました。 イベント トレースは、重要な GDOI イベントとエラーを対象とした軽量の常時オンになっているトレースです。 例外状態のトレースバックが有効になっている出口パス トレースもあります。 イベント トレースは、従来の syslog よりも多くの GETVPN イベント履歴情報を提供できます。

GDOI イベント トレースはデフォルトで有効になっています。このトレースをトレース バッファから取得するには **show monitor even-trace** コマンドを使用します。

```
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
```

出口パス トレースは、デフォルトでトレースバック オプションが有効な状態で、例外およびエラー状態である出口パスに関する詳細情報を提供します。 その後、トレースバックを使用して、出口パス状態が発生する原因となったコード シーケンスをデコードすることができます。 トレースバッファからトレースバックを取得するには、**detail** オプションを使用します。

```
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
```

デフォルトのトレース バッファ サイズは 512 エントリですが、問題が断続的に発生する場合はこのサイズでは十分ではないことがあります。 このデフォルトのトレース エントリ サイズを増やすには、イベント トレース設定パラメータを次のように変更できます。

```
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 コントロール プレーンのチェックポイントと一般的な問題

GETVPN の一般的なコントロール プレーンの問題の一部を次に示します。 もう一度説明しますが、コントロール プレーンは、GM でデータプレーンの暗号化と復号化を有効にするために必要なすべての GETVPN 機能コンポーネントとして定義されています。 全体的には、GM の登録、セキュリティ ポリシーと SA のダウンロード/インストール、後続の KEK/TEK キー再生成が正常に完了している必要があります。

COOP の設定およびポリシーの作成

セキュリティ ポリシーと関連する KEK/TEK が正常に KS により作成されたことを確認するには、次のように入力します。

```
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
```

KS ポリシーの設定での一般的な問題の 1 つに、プライマリ KS とセカンダリ KS で設定されるポリシーが異なることがあります。 これが原因で、予測不能な KS の動作が発生することがあります。このエラーは次のように報告されます。

```
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
```

現在プライマリ KS とセカンダリ KS の間では自動設定同期が行われないため、これらは手動で調整する必要があります。

おりは GETVPN のための重要な、（ほとんど常に必須）設定であるので、おりが作業正しくおよびおり KS ロール正しいことを確かめるためにキーです:

```
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
```

機能おり設定では、このプロトコル フローは観察する必要があります:

IKE 交換 > COOP 優先順位が交換された ANN > COOP 選択 > プライマリ KS からセカンダリ KS への ANN (ポリシー、GM データベース、キー)

COOP が正しく機能しない場合、または COOP が分割される場合 (複数の KS がプライマリ KS になる場合など) は、トラブルシューティングのために次のデバッグを収集する必要があります。

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

IKE の設定

後続のポリシーおよび SA のダウンロードのために制御チャネルを保護するため、GETVPN では正常な IKE 交換が必要です。 正常な IKE 交換の終わりに、GDOI_REKEY sa 作成されます。

先のバージョン Cisco IOS 15.4(1)T よりでは、GDOI_REKEY は **show crypto isakmp sa コマンド**で示すことができます:

```
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#
```

Cisco IOS 15.4(1)T およびそれ以降では、この GDOI_REKEY sa **暗号 gdoi が sa** コマンドを**鍵変更する提示**と示されています:

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

> **注:** 最初の IKE 交換が完了すると、GDO_REKEY SA を使用して後続のポリシーとキーが KS から GM に**プッシュ**されます。 それらが切れるときそう GDOI_IDLE SA のために鍵変更しますありません; 有効期間の期限を経過すると、それらは消滅します。 ただし、GM がキー再生成を受信するためには、GM には常に GDOI_REKEY SA が必要です。

GETVPN のための IKE 交換は従来のポイントツーポイント IPSecトンネルで使用される IKE と異なっていません従ってトラブルシューティングの方法は変わりません。 IKE 認証の問題をトラブルシューティングするには、次のデバッグを収集する必要があります。

```
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)
```

登録、ポリシー ダウンロードおよび SA インストール

IKE 認証が成功すると、GM が KS に登録されます。 次の syslog のメッセージは、この動作が正しく行われると表示されるものです。

```
%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
```

ポリシーとキーを検証するには、次のコマンドを使用します。

```
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#
```

注: GETVPN では、インバウンド SA およびアウトバウンド SA が同じ SPI を使用します。

GETVPN の登録とポリシー インストールの問題の場合、トラブルシューティングのために次のデバッグが必要です。

```
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)
```

注: これらの出力の結果に応じて、追加のデバッグが必要となることがあります。

一般に GETVPN 登録は GM リロード直後に行われるため、これらのデバッグを収集するときに次の EEM スクリプトが役立つことがあります。

```
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)
```

キー再生成

GM が KS に登録され、GETVPN ネットワークが正しく設定されると、プライマリ KS は、プライマリ KS に登録されているすべての GM にキー再生成メッセージを送信します。 GM のすべてのポリシー、キー、および疑似時間を同期するためにキー再生成メッセージが使用されます。 キー再生成メッセージは、ユニキャスト方式またはマルチキャスト方式で送信できます。

次の syslog メッセージは、キー再生成メッセージの送信時に KS に表示されます。

```
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)
```

GM では、これはキー再生成を受信するときに表示される syslog です。

```
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)
```

KS でのキー再生成用の RSA キー ペアの要件

キー再生成機能を使用するには、KS に RSA キーが存在している必要があります。 KS は登録時に、このセキュア チャネルを介して GM に RSA キー ペアの公開キーを提供します。 次に KS は、GM に送信された GDOI メッセージに、GDOI SIG ペイロードの秘密 RSA キーで署名します。 GM は GDOI のメッセージを受信し、公開 RSA キーを使用してこのメッセージを検証します。 KS と GM 間で送信されるメッセージは KEK により暗号化されます。KEK は登録時に GM にも配布されます。 登録が完了すると、後続のキー再生成は KEK により暗号化され、秘密 RSA キーで署名されます。

GM 登録時に RSA キーが KS に存在していない場合は、syslog に次のメッセージが表示されます。

```
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)
```

キーが KS に存在しない場合、GM は初回は登録しますが、次回の KS からのキー再生成は失敗します。 GM 上の既存のキーの有効期限が経過すると、GM は再度登録します。

```
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)
```

キー再生成メッセージの署名に RSA キー ペアが使用されるため、これらの RSA キー ペアはプライマリ KS とすべてのセカンダリ KS で**同一である必要があります**。 これにより、プライマリ KS で障害が発生した場合、セカンダリ KS (新しいプライマリ KS) により送信されるキー再生成が、GM により引き続き適切に検証できます。 プライマリ KS で RSA キー ペアが生成される場合、このキー ペアは exportable オプションを使用して作成される必要があります。これにより、この要件に対応するためにすべてのセカンダリ KS へこのキー ペアをエクスポートできます。

キー再生成のトラブルシューティング

KEK/TEK キー再生成の失敗は、顧客の導入環境で発生する最も一般的な GETVPN の問題の 1 つです。 キー再生成の問題をトラブルシューティングするには、次に示すキー再生成手順に従ってください。

1. キー再生成が KS から送信されましたか?

   これを調べるには、%GDOI-5-KS_SEND_UNICAST_REKEY syslog メッセージを確認します。また、より正確に確認するには次のコマンドを使用します。

```
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
```

再送信されるキー再生成の数は、KS が受信していないキー再生成確認応答パケットの数、つまり発生している可能性のあるキー再生成の問題を示します。 GDOI キー再生成では UDP は信頼できないトランスポート メカニズムとして使用されるため、基盤となるトランスポート ネットワークの信頼性によってはキー再生成が廃棄されることがありますが、キー再生成の再送信数が増加傾向にあるかどうかは常に調査する必要がある点に注意してください。

GM 別のキー再生成に関する詳細な統計情報を取得することもできます。 通常、発生している可能性があるキー再生成の問題について、この統計情報で最初に調べます。

```
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. キー再生成パケットが、基盤となるインフラストラクチャ ネットワークで配信されましたか?

キー再生成パケットが KS と GM の間の中継ネットワークで廃棄されていないことを確認するために、キー再生成の転送パスに沿って標準 IP のトラブルシューティングを行う必要があります。 ここでは使用されるいくつかのよくあるトラブルシューティング ツールはトランジットネットワークの入出力アクセス コントロール リスト（ACL）、Netflow およびパケットキャプチャです。

3. キー再生成パケットが、GDOI キー再生成処理プロセスに到達しましたか?

   GM のキー再生成統計情報を調べてください。

```
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. キー再生成確認応答パケットが KS に戻りましたか?

   ステップ 1 から 3 に従って、キー再生成確認応答パケットを GM から KS の方向でトレースします。

マルチキャスト キー再生成

マルチキャスト キー再生成がユニキャスト キー再生成と異なる点は次のとおりです。

- マルチキャストを使用して KS から GM にキー再生成パケットが転送されるため、KS がキー再生成パケット自体を複製する必要はありません。 KS は、キー再生成パケットのコピーを 1 つだけ送信します。キー再生成パケットの複製はマルチキャスト対応ネットワークで行われます。
- マルチキャスト キー再生成には確認応答メカニズムがないため、GM がキー再生成パケットを受信しない場合、KS はそのことを認識せず、その GM データベースから GM を削除することはありません。 確認応答がないことから、KS はキー再生成の再送信設定に基づいて常にキー再生成パケットを再送信します。

最もよく見られるマルチキャストは鍵変更が GM で受け取られないとき問題をあります鍵変更します。 次のようなさまざまな原因が考えられます。

- マルチキャスト ルーティング インフラストラクチャ内でのパケット配信の問題
- エンドツーエンドのマルチキャスト ルーティングがネットワークで有効ではない

マルチキャスト キー再生成の問題のトラブルシューティングでは最初に、マルチキャスト方式からユニキャスト方式に切り替えた場合にキー再生成が機能するかどうかを確認します。

マルチキャスト キー再生成に固有の問題であることを特定した場合は、指定されているマルチキャスト アドレスに KS がキー再生成を送信することを確認します。

```
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
```

このマルチキャスト アドレスへのインターネット制御メッセージ プロトコル (ICMP) 要求を使用して、KS と GM の間のマルチキャスト接続をテストします。 すべての GMs は ping にマルチキャスト グループの一部である答える必要があります。 このテストのために、ICMP が KS 暗号化ポリシーから除外されていることを確認します。

```
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
```

マルチキャスト ping テストが失敗した場合はマルチキャスト トラブルシューティングを行う必要がありますが、このトラブルシューティングについてはこのドキュメントでは説明しません。

コントロール プレーン リレー チェック

症状

顧客が新しい Cisco IOS バージョンに GM をアップグレードするとき、鍵変更します syslog で監視されるこのメッセージを持つ失敗を KEK を経験するかもしれません:

```
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
```

この動作は、コントロール プレーン メッセージのために追加されたアンチ リプレイ チェックに伴う相互運用性の問題が原因で発生します。 具体的には、古いコードを実行する KS が KEK キー再生成シーケンス番号を 1 にリセットし、新しいコードを実行する GM がこれをリプレイ済みキー再生成パケットとして解釈すると、GM によってこれがドロップされます。 詳細については、Cisco Bug ID CSCta05809（GETVPN： リプレイの影響を受ける GETVPN コントロールプレーン）および「GETVPN 設定の制約事項」を参照してください。

背景説明

GETVPN では、時間ベースのアンチ リプレイ チェック サービスを提供するために、コントロール プレーンのメッセージに時間に依存する情報を含めることができます。 したがって、時間の正確さを保証するためこれらのメッセージにはアンチ リプレイ保護が必要です。 これらのメッセージは次のとおりです。

- KS から GM への**キー再生成メッセージ**
- KS 間の **COOP アナウンス メッセージ**

この再生防止保護 実装の一部として再生されたメッセージ、また TBAR がイネーブルになっているとき pseudotime チェックを保護するために、シーケンス番号チェックは追加されました。

解決策

この問題を解決するには、コントロール プレーンのリプレイ チェック機能の後で GM と KS の両方で Cisco IOS バージョンにアップグレードする必要があります。 新しい Cisco IOS コードでは、KS は KEK キー再生成のシーケンス番号を 1 にリセットせず、引き続き現行のシーケンス番号を使用し、TEK キー再生成の場合にのみシーケンス番号をリセットします。

リプレイ チェック機能が搭載されている Cisco IOS バージョンを次に示します。

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2

- 15.0(1)M 以降

その他のリプレイ関連の問題

- ANN メッセージでのリプレイ チェックの失敗による COOP の失敗（Cisco Bug ID CSCtc52655 ）

デバッグ コントロール プレーン リプレイの失敗

他のコントロール プレーン リプレイの失敗の場合は、次の情報を収集し、KS と GM の間で時刻が同期されていることを確認します。

- GM と KS の両方の syslog
- ISAKMP のデバッグ
- GM と KS の両方の GDOI のデバッグ（キー再生成およびリプレイ）

コントロール プレーン パケット フラグメンテーションの問題

GETVPN では、コントロール プレーン パケットのフラグメンテーションはよく発生する問題です。この問題は、コントロール プレーン パケットが大きいために IP フラグメンテーションが必要となる場合に、次の 2 つのシナリオのいずれかで発生します。

- GETVPN COOP アナウンス パケット
- GETVPN キー再生成パケット

COOP アナウンス パケット

おり Announcement パケットは GM データベース情報を伝え、こうして大きい GETVPN 配備で大きくなることができます。 これまでの経験では、1500 以上の GM で構成される GETVPN ネットワークでは、Cisco IOS のデフォルトの Huge バッファ サイズである 18024 バイトを超えるサイズのアナウンス パケットが生成されます。 この場合、KS は ANN パケットを送信できる十分な大きさのバッファを割り当てることができず、次のエラーが発生します。

```
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
```

この状況を解決するため、バッファを調整することを推奨します。

```
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
```

キー再生成パケット

暗号化ポリシーが大規模な場合（暗号化 ACL のアクセス コントロール エントリ（ACE）の行数が 8 以上であるポリシーなど）、GETVPN キー再生成パケットは標準の 1500 IP 最大伝送単位

（MTU）サイズを超えることもあります。

フラグメンテーションの問題と識別

上記のシナリオの両方では、GETVPN はきちんと送信できる必要があり、フラグメント化された UDP パケットをきちんとはたらくためにおりか GDOI のために受信するために鍵変更して下さい。 IP フラグメンテーションは、一部のネットワーク環境で問題となることがあります。 たとえば、等コスト マルチ パス（ECMP）フォワーディング プレーンで構成されるネットワーク、およびフォワーディング プレーン内の一部のデバイスは、Virtual Fragmentation Reassembly（VFR）などのフラグメント化 IP パケットの仮想再構成を必要とします。

この問題を特定するには、フラグメント化 UDP 848 パケットを適切に受信していない可能性があるデバイスで再構成エラーを調べます。

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

再組立てタイムアウトが増分し続ける場合ドロップするが rekey/COOP パケットフローの一部であるかどうか確認するために **debug ip エラー** コマンドを使用して下さい。 確認されてパケットを廃棄するかもしれない転送プレーンの正確なデバイスを隔離するために、正常な IP転送トラブルシューティングは実行された必要があります。 よく利用されるツールには次のものがあります。

- パケット キャプチャ
- トラフィック転送の統計情報
- セキュリティ機能の統計情報（ファイアウォール、IPS）
- VFR 統計情報

GDOI 相互運用性の問題

GETVPN では長年にわたってさまざまな相互運用性の問題が検出されました。相互運用性の問題を確認するため、KS と GM の間、および複数の KS 間で Cisco IOS リリースのバージョンを確認することが重要です。

他のよく知られた GETVPN 相互運用性の問題は次のとおりです:

- コントロール プレーン リレー チェック
- GETVPN KEK のキー再生成動作の変更
- Cisco バグ ID CSCub42920（GETVPN: KS はハッシュを検証しません鍵変更します前の GM バージョンからの ACK を）
- Cisco バグ ID CSCuw48400（登録するか、または鍵変更することが不可能な GetVPN GM は- SIG ハッシュ > デフォルト SHA-1 を失敗します）
- Cisco バグ ID CSCvg19281（多重 GETVPN GM は新しい KS ペアに移行の後でクラッシュします; GM バージョンが 3.16 より早く、KS が以前のコードから 3.16 またはそれ以降へアップグレードされれば場合、この問題は起こる場合があります）

GETVPN IOS のアップグレード手順

GETVPN 環境で Cisco IOS コードをアップグレードする必要がある場合は、この Cisco IOS アッ

プグレード手順に従う必要があります。

1. セカンダリ KS を最初にアップグレードし、COOP KS の選択が完了するまで待ちます。
2. すべてのセカンダリ KS でステップ 1 を繰り返します。
3. プライマリ KS をアップグレードします。
4. GM をアップグレードします。

GETVPN データ プレーンの問題のトラブルシューティング

問題をコントロール プレーンと比較されて、GETVPN データ平面問題は GM にポリシーおよびキーが dataplane 暗号化および復号化を行うあるが、どういうわけかエンド ツー エンド トラフィック トラフィック フローがはたらかない問題です。 GETVPN のための dataplane 問題のほとんどは IPsec 一般的 な転送に関連し、GETVPN 仕様ではないです。 従ってここに記述されている一般的 な IPsec dataplane 問題にトラブルシューティング アプローチのほとんどは同様に適用します。

暗号化の問題（グループベース トンネルおよびペアワイズ トンネルの両方）の場合は、問題のトラブルシューティングを行い、データパスの特定部分に問題を絞り込むことが重要です。 特にここで説明するトラブルシューティング方法は、次の事項を確認できるようにすることを目的としています。

- 原因となるデバイスは、暗号化ルータと復号化ルータのどちらですか？
- 問題は入力と出力のどちらの方向で発生しますか?

GETVPN データ プレーン トラブルシューティング ツール

IPsec dataplane トラブルシューティングはコントロール プレーンのためにそれと非常に異なっています。 データプレーンでは通常、実行できるデバッグ、少なくとも実稼働環境で安全に実行できるデバッグがありません。 そのためトラブルシューティングは、フォワーディング パス上のパケットのトレースに役立つさまざまなカウンタやトラフィック統計情報に大きく依存します。 これは、次に示すように、パケットが廃棄される可能性がある位置を絞り込む上で役立つ一連のチェックポイントを開発できるようにするためです。

いくつかのデータ プレーン デバッグ ツールを次に示します。

- アクセス リスト
- IP Precedence アカウンティング
- NetFlow
- インターフェイス カウンタ
- 暗号化カウンタ
- IP Cisco Express Forwarding（CEF）グローバルおよび機能ごとのドロップ カウンタ
- 組み込みパケット キャプチャ（EPC）

- データ プレーン デバッグ（IP パケットおよび CEF のデバッグ）

上記の図のデータパス上のチェックポイントは、次のツールを使用して検証できます。

暗号化 GM

- 入力 LAN インターフェイス
  - 入力 ACL
  - 入力 NetFlow
  - Embedded Packet Capture
  - 入力優先順位アカウンティング
- 暗号化エンジン
  - **show crypto ipsec sa**
  - ***show crypto ipsec sa detail***
  - **show crypto engine accelerator statistics**
- 出力 WAN インターフェイス
  - 出力 NetFlow
  - Embedded Packet Capture
  - 出力プレシデンス アカウンティング

復号化 GM

- 入力 WAN インターフェイス
  - 入力 ACL
  - 入力 NetFlow
  - Embedded Packet Capture
  - 入力優先順位アカウンティング
- 暗号化エンジン
  - **show crypto ipsec sa**
  - **show crypto ipsec sa detail**
  - **show crypto engine accelerator statistics**
- 出力 LAN インターフェイス
  - 出力 NetFlow
  - Embedded Packet Capture

リターン パスは同じトラフィック フローをたどります。 以降の項では、使用されるこれらのデータプレーン ツールのいくつかの例を示します。

Encryption/Decryption カウンタ

ルータの暗号化 復号化カウンターは IPsec フローに基づいています。 ただし GETVPN は通常、すべてを暗号化する「permit ip any any」暗号化ポリシーを採用しているため、GETVPN ではこれは適切に機能しません。 したがって、この問題がフローの一部でのみ発生し、全体では発生しない場合は、機能するバックグラウンド トラフィックが十分にある場合にパケットが暗号化または復号化されたかどうかを正しく評価する目的で、これらのカウンタを使用することは多少困難なことがあります。

```
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 は、両方の GM で入力トラフィックと出力トラフィックの両方を監視するために使用できます。 GETVPN の **permit ip any any** ポリシーでは、暗号化トラフィックは集約され、フロー単位の情報を提供しないことに注意してください。 DSCP/優先順位マーキングを使用してフロー単位の情報を収集する必要があります。これについては後述します。

この例では、GM1 の背後にあるホストから GM2 の背後にあるホストへの 100 カウントの ping のネットフローがさまざまなチェックポイントで確認されます。

暗号化 GM

NetFlow の設定

```
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 出力：

```
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#
```

> **注:** 上記の出力の * は、出力トラフィックを示します。 最初の行は、WAN インターフェイスからの出力暗号化トラフィック (プロトコル 0x32 = ESP) を示し、2 番目の行は LAN インターフェイスにヒットする入力 ICMP トラフィックを示します。

復号化 GM

設定：

```
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 出力：

```
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 優先順位マーキング

暗号化問題の解決を用いるチャレンジは暗号化がはずである、それは特定の IP フローのためのパケットをトレースすること困難にしますもののするペイロードにパケットが暗号化されればこと失う表示をであり。 IPsec 問題の解決に関してはこの制限をアドレス指定する 2 つの方法があります:

- IPsec トランスフォームとして ESP-NULL を使用して下さい。 IPsec はまだ ESP カプセル化を行いますが、no encryption はペイロードに適用されます、従ってそれらはパケットキャプチャで目に見えます。
- L3/L4 特性に基づいて、一意の Differentiated Services Code Point（DSCP）/優先順位マーキングで IP フローをマーキングします。

ESP-NULL は、両方のトンネル エンド ポイントでの変更を必要とし、顧客のセキュリティ ポリシーに基づき、通常は許可されません。 したがって、その代わりに DSCP/優先順位マーキングを使用することが一般に推奨されます。

DSCP/優先順位チャート

ToS（16 進数）	ToS（10 進数）	IP precedence	DSCP	Binary
0xE0	224	7 Network Control	56 CS7	11100000
0xC0	192	6 Internetwork Control	48 CS6	11000000
0xB8	184	5 Critical	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4 Flash Override	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	3 Flash	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2 Immediate	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1 Priority	8 CS1	00100000
0x00	0	0 Routine	0 Dflt	00000000

DSCP/優先順位によるパケットのマーキング

これらの方式は通常、特定の DSCP/優先順位マーキングを使用してパケットをマーキングするために使用されます。

PBR[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
```

ルータ 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>
```

> **注:** マーキングを適用してマーキングされたトラフィック フローが一意であるようにする前に、通常のトラフィック フローと DSCP/優先順位プロファイルを監視することをお勧めします。

マーキングされたパケットのモニタ

IP Precedence アカウンティング

```
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
```

Interface 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
```

Embedded Packet Capture

Embedded Packet Capture（EPC）は、パケットが特定のデバイスに到達したかどうかを確認するためにインターフェイス レベルでパケットをキャプチャする便利なツールです。 EPC はクリア テキスト トラフィックでは適切に動作しますが、キャプチャしたパケットが暗号化されている場合は困難になる可能性があることに注意してください。 したがって、より効果的なトラブルシューティングを行うためには、前述の DSCP/優先順位マーキングなどのテクニックやその他の IP 特性（IP パケットの長さ）を、EPC と組み合わせて使用する必要があります。

Cisco IOS XE パケットトレース

これは Cisco IOS XE を、CSR1000v のような、ASR1000 実行する、および ISR4451-X ですべてのプラットフォームの機能フォワーディングパスを追跡する有用な機能。

GETVPN データ プレーンの一般的な問題

GETVPN のための IPsec dataplane を解決することは GETVPN のこれらのユニークな dataplane プロパティによる 2 つの例外を除いて従来のポイントツーポイント IPsec dataplane 問題を、解決することと大抵異なっていません。

時間ベースのアンチ リプレイの失敗

GETVPN ネットワークでは、長いペアワイズ トンネルが存在しないために TBAR の失敗のトラブルシューティングが難しいことがあります。 GETVPN TBAR の失敗のトラブルシューティングを行うには、次の手順を実行します。

1. TBAR の失敗が原因で廃棄されたパケットを特定し、次に暗号化 GM を特定します。

   15.3(2)T より前のバージョンでは、TBAR の失敗では syslog に失敗したパケットの送信元アドレスが出力されなかったため、失敗したパケットを特定することが非常に困難でした。バージョン 15.3(2)T 以降ではこれは大幅に改善され、Cisco IOS は次の内容を出力します。

```
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
```

   TBAR 履歴はまたこのバージョンで設定されました:

```
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
```

注: 以前に述べられる機能拡張は Cisco バグ ID CSCub91811 によって Cisco IOS XE と Cisco IOS で Cisco バグ ID CSCun49335 によってその後実装されていました。
この機能がなかった Cisco IOSバージョンの場合このデバッグがすべてのトラフィック (だけでなく、TBAR 失敗がパケットによって廃棄される原因で) のための TBAR 情報を印刷する、従ってそれは実稼働環境で動作することは実行可能ではないかもしれませんが、**debug crypto gdoi GM 再生詳細は**またこの情報を提供できます。

```
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
```

2. パケットの送信元が判明したら、暗号化 GM を検出できます。 次に、暗号化 GM と復号化 GM の両方で pseudotimestamp を監視し、疑似時間ドリフトが発生しているかどうかを確認する必要があります。 このための最適な方法は、両方の GM と KS を NTP と同期し、これらすべてのリファレンス システム クロックを使用して疑似時間情報を定期的に収集し、問題が GM の時間のずれが原因で発生したものであるかどうかを判別することです。

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
```

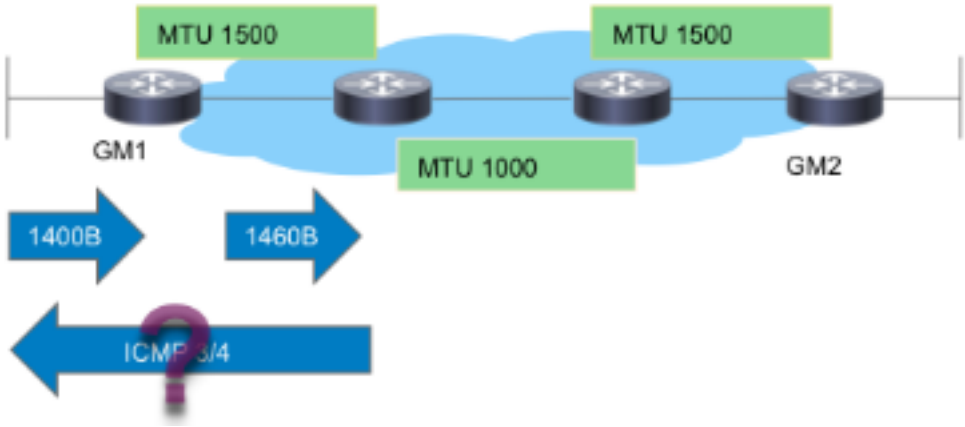
```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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
```

上記の例では、同一基準時刻で出力をキャプチャしたときの（Replay Value により示される）疑似時間が GM によって大きく異なる場合は、問題が時間のずれに起因している可能性があります。

> **注:** Cisco Aggregated Services Router 1000 シリーズ プラットフォームでは、プラットフォームのアーキテクチャが原因で、Quantum Flow Processor（QFS）のデータパスが実際には疑似時間のカウントにウォール クロックを参照しています。 これは TBAR で NTP によるウォール時刻変更が同期するとき問題を引き起こしました。 この問題については、Cisco Bug ID CSCum37911 に文書化されています。

PMTUD および GETVPN ヘッダーの維持

GETVPN では、暗号化 GM と復号化 GM の間で Path MTU Discovery（PMTUD）が機能せず、Don't Fragment（DF）ビットが設定された大きなパケットがブラックホール化されることがあります。 これが機能しない原因は GETVPN ヘッダーの維持（データの送信元アドレスと宛先アドレスが ESP カプセル化ヘッダーで維持される）にあります。 次の図にこれを示します。



この図に示すように、このフローでは PMTUD は GETVPN で失敗します。

1. 大きなデータ パケットが暗号化 GM1 に到達します。
2. 暗号化後の ESP パケットが GM1 から宛先に向けて転送されます。
3. 1400 バイトの IP MTU のトランジット リンクがある場合、ESP パケットがドロップされ、ICMP 3/4 パケットが大きすぎることを示すメッセージがパケットの送信元（データ パケットの送信元）に向けて送信されます。
4. ICMP3/4 パケットは、ICMP が GETVPN 暗号化ポリシーから除外されていないことが原因で廃棄されるか、またはエンド ホストが ESP パケット（未認証ペイロード）を認識しないためにエンド ホストにより廃棄されます。

つまり、現時点では PMTUD は GETVPN で機能しません。 この問題を回避するために、Cisco はこれらのステップを推奨します:

1. 実装する「IP TCP adjust-mss」は TCPパケット セグメント サイズ錫順序 o を減らすために暗号化オーバーヘッドおよびトランジットネットワークのパスMTU 最小の取り扱います。
2. PMTUD を回避するために、データ パケットが暗号化 GM に到着したら、データ パケットの DF ビットをクリアします。

IPsec 一般的 な Dataplane 問題

IPsec dataplane トラブルシューティングのほとんどは従来のポイントツーポイント IPSecトンネルの解決のようです。 よくある 問題の 1 つは %CRYPTO-4-RECVD_PKT_MAC_ERR です。 より多くの詳細のについては解決する IPSecトンネル上の Ping 損失の Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" エラーメッセージをトラブルシューティング参照して下さい。

既知の問題

このメッセージは SADB の SPI を一致する IPsecパケットが受信されるとき生成することができます。 Cisco Bug ID CSCtd47420（GETVPN - パケット不一致フローで報告される CRYPTO-4-RECVD_PKT_NOT_IPSEC）を参照してください。 次に例を表示します。

```
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
```

このメッセージは報告されるものが従来の IPsec のために、また ASR のようないくつかのハードウェアプラットフォームでである %CRYPTO-4-RECVD_PKT_INV_SPI であるはずです。 この表面的な問題は、Cisco Bug ID CSCup80547（ESP pak の CRYPTO-4-RECVD_PKT_NOT_IPSEC の報告でのエラー）で修正されました。

> **注:** これらのメッセージは、別の GETVPN Bug CSCup34371 が原因で出力されることがあります。 GETVPN GM は、TEK キー再生成後にトラフィックの復号化を停止します。

この場合、GM は SADB（鍵変更される SA）で有効な IPsec SA あるが GETVPN トラフィックを復号化できません。 この問題は、SA の有効期限が経過し、SADB から SA が削除されるとすぐに解消します。 TEK キー再生成が事前に実行されるため、この問題が原因で重大な停止が発生します。 たとえば、TEK の有効期間が 7200 秒の場合、停止は 22 分に及ぶことがあります。 このバグが発生するための具体的な条件については、このバグの説明を参照してください。

Cisco IOS XE を実行するプラットフォームの GETVPN を解決して下さい

トラブルシューティングのためのコマンド

Cisco IOS XE を実行するプラットフォームにプラットフォーム別の実装がたいていの場合あり、

GETVPN 問題のためにプラットフォーム別のデバッグを必要とします。 これらのプラットフォームでの GETVPN のトラブルシューティングに通常使用されるコマンドを次に示します。

show crypto eli all

show platform software ipsec policy statistics

show platform software ipsec fp active inventory

show platform hardware qfp active feature ipsec spd all

show platform hardware qfp active statistics drop clear

show platform hardware qfp active feature ipsec data drop clear

show crypto ipsec sa

show crypto gdoi

show crypto ipsec internal

debug crypto ipsec

debug crypto ipsec error

debug crypto ipsec states

debug crypto ipsec message

debug crypto ipsec hw-req

debug crypto gdoi gm infra detail

debug crypto gdoi gm rekey detail

ASR1000 よくある 問題

IPsec ポリシー インストール失敗（連続的な再登録）

ASR1000 GM は暗号化エンジンが受け取った IPsec ポリシーかアルゴリズムをサポートしない場合キー サーバに登録し続けるかもしれません。 たとえば、Nitrox で ASR プラットフォームを（ASR1002 のような）、スイートB 基づかせていましたまたは SHA2 ポリシーはサポートされないし、これにより連続的な再登録現象を引き起こす場合があります。

よくある移行/アップグレードの問題

ASR1000 TBAR 制限

ASR1000 プラットフォームで、Cisco バグ ID CSCum37911 修正は 20 秒以下の TBAR 時間がサポートされないこのプラットフォームの制限をもたらしました。 IOS XE の GETVPN については制限を参照して下さい。

この機能拡張バグはこの制限を解除するために Cisco バグ ID CSCuq25476 - ASR1k 20 秒以下の GETVPN TBAR ウィンドウ サイズをサポートする必要があります開きました。

更新： この制限は Cisco バグ ID CSCur57558 のための修正でその後解除され、それはもはや XE3.10.5 の制限、XE3.13.2 およびそれ以降のコードではないです。

また TBAR がイネーブルになっている場合デバイスがこの問題のための修正でバージョンを実行すること IOS XE プラットフォームを on Cisco 実行する GM のために、（ASR1k か ISR4k）、それに強く推奨されています注意して下さい; Cisco バグ ID CSCut91647 - IOS XE の GETVPN: GM は不正確に TBAR 失敗によるパケットを廃棄します。

ISR4x00 分類問題

回帰は拒否ポリシーが無視される ISR4x00 プラットフォームで見つけられました。 詳細については、参照して下さい Cisco バグ ID CSCut14355 を- GETVPN - ISR4300 GM 無視はポリシーを否定します。

関連情報

- Group Encrypted Transport VPN (GET VPN) - Cisco Systems
- テクニカル サポートとドキュメント – Cisco Systems