GETVPN トラブルシューティング ガイド

内容

概要

このドキュメントの目的は、Group Encrypted Transport VPN（GETVPN）の問題を特定して切り分ける際に役立つ構造化されたトラブルシューティング手法と有効なツールを紹介し、考えられる解決策を提供することです。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 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

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

GETVPN トラブルシューティング手法

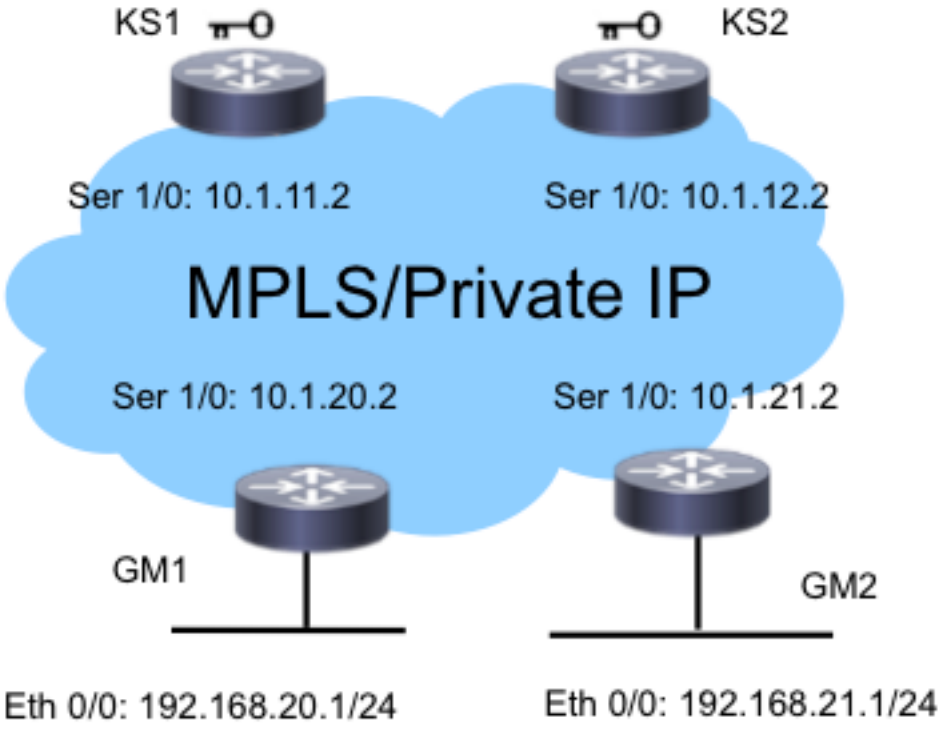
複雑なテクノロジー問題をトラブルシューティングする場合と同様、問題を特定の機能、サブシステム、またはコンポーネントに切り分けることができるかどうかが重要となります。GETVPNソリューションは、以下をはじめ、いくつもの機能コンポーネントで構成されています。

- Internet Key Exchange(IKE)：コントロールプレーンを認証および保護するために、グループメンバー(GM)とキーサーバ(KS)間、およびCooperative Protocol(COOP)KS間で使用されます。
- Group Domain of Interpretation(GDOI)：グループキーを配布し、すべてのGMにキー再生成などのキーサービスを提供するためにKSで使用されるプロトコル。
- COOP:KSが相互に通信し、冗長性を提供するために使用されるプロトコル。
- ヘッダーの保持：エンドツーエンドのトラフィック配信のために元のデータパケットヘッダーを保持する、トンネルモードのIPsec。
- Time Based Anti-Replay(TBAR)：グループキー環境で使用されるリプレイ検出メカニズム。

また、トラブルシューティングプロセスを簡素化するための広範なトラブルシューティングツールも用意されています。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。トラブルシューティングを行う場合は、実稼働環境に悪影響を与えないように、最も干渉の少ない方法から始めることをお勧めします。この構造化されたトラブルシューティングで鍵となるのは、問題をコントロール プレーンの問題またはデータ プレーンの問題に切り分けられるかどうかです。プロトコルまたはデータ フローに従い、このドキュメントで紹介する各種のツールを使用してチェックポイントを確認することで、問題を切り分けることができます。

参照トポロジ

このトラブルシューティング ガイドでは以降、一貫して以下に示す GETVPN トポロジとアドレッシング方式を使用します。



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：簡潔にするために、KS2 設定と GM2 設定は記載しません。

用語

- KS：キー サーバ
- GM：グループ メンバー
- COOP：Cooperative Protocol
- TBAR：Time Based Anti-Replay
- KEK – キー暗号化キー
- 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。**
- 何が起きても、該当するGMおよびKSから**show techコマンドを入力し**て、必要に応じて、グローバルおよび関連する各仮想ルーティングおよび転送(VRF)での**show ip routeコマンドの出力を調べます。**
- 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コマンドの出力にタイムスタンプが付いていることを確認します。

```
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 プレーンはすべてのプロトコル イベントを意味し、これらのイベントによって、データ プレーン トラフィックの暗号化および復号に対応できるよう GM 上でポリシーおよびセキュリティ アソシエーション（SA）が作成されます。以下に、GETVPN コントロール プレーンでの主要なチェックポイントの例を示します。

コントロール プレーンをデバッグする際のベスト プラクティス

このドキュメントで紹介する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。これらのベスト プラクティスは、ほぼすべてのコントロール プレーンのデバッグに適用されます。最も効果的なトラブルシューティングを行うには、次のベストプラクティスに従うことが重要です。

- コンソール ロギングをオフにして、ロギング バッファまたは syslog を使用してデバッグを収集します。
- デバッグされるすべてのデバイスでルータクロックを同期するには、NTPを使用します。
- 以下のコマンドを使用して、デバッグ メッセージとログ メッセージに対してミリ秒（msec）タイムスタンプを有効にします。

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

- デバッグ出力と関連付けられるよう、show コマンド出力にタイムスタンプが付けられることを確認します。

```
terminal exec prompt timestamp
```

- 大規模な環境では、可能な場合は条件付きデバッグを使用します。

GETVPNコントロールプレーンのトラブルシューティングツール

GETVPN show コマンド

一般に、ほぼすべての GETVPN 問題では以下のコマンド出力を収集する必要があります。

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 では、重要なプロトコル イベントやエラー状態に関する包括的な syslog メッセージが提供されます。GETVPN トラブルシューティングを行う際は、常に最初に syslog を調べてください。

共通の KS syslog メッセージ

syslog メッセージ	説明
COOP_CONFIG_MISMATCH	プライマリキーサーバとセカンダリキーサーバの間の設定が一致してい
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 サーバのグループ内でのロールが、セカンダリ サーバから**
COOP_KS_UNAUTH	承認済みリモート サーバが、グループ内のローカル キー サーバに接続し
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。これは、潜在**
KS_GM_REVOKED	キー再生成プロトコルの実行中に、許可されていないメンバーがグループ
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 登録プロトコルの実行中に、許可されていないメンバーがグループ
UNAUTHORIZED_IPADDR	登録要求が、要求を行っているデバイスがグループの参加を許可されなか

共通の 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 メンバー用のクリプト マップが追加されました
GM_CM_DETACH	ローカルグループメンバーの暗号マップがデタッチされました。&
GM_RE_REGISTER	**あるグループのために作成された IPsec SA が期限切れになったか、消 れた可能性があります。キー サーバに登録する必要があります。**
GM_RECV_REKEY	**キー再生成を受信しました。**
GM_REGS_COMPL	**登録が完了しました。**
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環境で最も一般的または重要なメッ

セージです。

グローバル暗号化および GDOI デバッグ

GETVPNデバッグは次のように分割されます。

1. 最初に、トラブルシューティングを行うデバイスを使用します。
```
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. 次に、トラブルシューティングする問題のタイプを示します。
```
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. 3つ目は、有効にする必要があるデバッグのレベルです。バージョン 15.1(3)T 以降ではすべての GDOI 機能のデバッグが標準化されて、以下に示すデバッグ レベルが使用されるようになっています。この標準化は、大規模な GETVPN 環境でも十分なデバッグ精度でトラブルシューティングを行えるよう意図されたものです。GETVPN 問題をデバッグする際は、適切なデバッグ レベルを適用することが重要です。一般に、最小のデバッグ レベル（エラー）で開始して、必要に応じて精度を高くしてください。
```
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 トラブルシューティングに利用できるように、GDOI 条件付きデバッグが追加されています。Internet Security Association and Key Management Protocol（ISAKMP）および GDOI デバッグのすべては、グループまたはピア IP アドレスを基準とした条件フィルタでトリガーできるようになっています。GDOI デバッグでは GDOI に固有の操作しか示されないため、GETVPN 問題については概して、適切な条件フィルタを設定して ISAKMP デバッグと GDOI デバッグの両方を有効にすることを推奨します。ISAKMP および GDOI の条件付きデバッグを使用するには、次の単純な 2 つのステップに従います。

1. 条件フィルタを設定します。
2. 関連する ISAKMP および GDOI を通常通りに有効にします。

以下に、いくつかの例を示します。

```
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 の条件付きデバッグではいずれも、**unmatched フラグを有効にすることで、条件フィルタの情報 (デバッグ パスの IP アドレスなど) が含まれないデバッグ メッセージでも捕捉できるようになります。**ただし、これにより大量のデバッグ情報が生成される可能性があるため、このフラグは慎重に使用してください。

GDOI イベント トレース

GDOI イベント トレースはバージョン 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 イベントとエラーに関する軽量の、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 トレースにより、従来の syslog より多くの GETVPN イベント履歴情報を入手できます。

GDOI イベント トレースはデフォルトで有効にされます。トレース バッファから GDOI イベント トレースを取得するには、**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
```

traceback オプションはデフォルトで有効にされることから、出口パス トレースから出口パス (例外およびエラー条件) に関する詳細な情報を入手し、その情報を基に、トレースバックを使用して、出口パス条件の原因となった正確なコード シーケンスを解読できます。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 個のエントリに対応します。問題が断続的に発生する場合は、このサイズでは十分でない可能性があります。デフォルトのトレース バッファ 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以下のように変更します。

```
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よくある問題

ここでは、GETVPN コントロール プレーンでよく発生する問題について説明します。繰り返しますが、コントロール プレーンは、GM でデータ プレーン暗号化および復号を可能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ます。おおまかに言うと、データ プレーン暗号化および復号を可能にするためには、GM 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、そしてそれに続く KEK/TEK キー再生成が成功する必要があります。

COOP 設定とポリシーの作成

KS がセキュリティ ポリシーおよび関連する KEK/TEK を正常に作成したことを確認するには、以下のコマンドを入力します。

```
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 ポリシー設定でよくある問題の 1 つは、プライマリ KS とセカンダリ KS で設定されているポ

リシーが異なる場合に発生します。この 2 つのポリシーが異なると、KS 動作が予測不可能なものになり、以下のエラーが報告されます。

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

現在、プライマリ KS とセカンダリ KS 間では設定が自動的に同期されないため、手動で設定を同期しなければなりません。

COOPはGETVPNの重要な（ほぼ常に必須）設定であるため、COOPが正しく動作し、COOP KSの役割が正しいことを確認することが重要です。

```
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
```

機能するCOOPセットアップでは、次のプロトコルフローが観察されます。

IKE 交換 > COOP プライオリティ交換による ANN > COOP 選定 > プライマリからセカンダリ KS への ANN（ポリシー、GM データベース、およびキー）

COOP が正常に機能していないか、COOP スプリットが発生した場合（複数の KS がプライマリ KS になるなど）、問題をトラブルシューティングするために以下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 設定

GETVPN で IKE 交換が正常に完了していなければ、以降のポリシーおよび SA のダウンロードで制御チャネルが保護されません。正常なIKE交換の最後に、GDOI_REKEY saが作成されます。

Cisco IOS 15.4(1)Tよりも前のバージョンでは、**show crypto isakmp saコマンド**を使用してGDOI_REKEYを表示できます。

```
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以降では、次のGDOI_REKEY saが**show crypto gdoi rekey saコマンドで表示されます。**

```
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**：初期 IKE 交換が完了した後は、以降のポリシーおよびキーは、GDOI_REKEY SA を使用して KS から GM にプッシュされます。したがって、GDOI_IDLE SAが期限切れになってもキー再生成は行われません。ライフタイムが満了すると同時にキーは消失します。ただし、GM 上には常に、キー再生成パケットを受信するための GDOI_REKEY SA がなければなりません。

GETVPN 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 と変わりません。したがって、トラブルシューティング手法も同じです。IKE の認証問題をトラブルシューティングするには、以下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のインストール

IKE 認証が成功すると、GM は KS に登録されます。登録が正常に行われると、以下の syslog メッセージが表示されるはずです。

```
%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
```

ポリシーとキーは、以下のコマンドで確認できます。

```
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、インバウンドおよびアウトバウンド SA は同じ SPI を使用します。

GETVPN 登録およびポリシー インストールに関する問題をトラブルシューティングに以下のデ

バッグが必要になります。

```
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)
```

注：上記の出力結果に応じて、追加のデバッグが必要になることがあります。

GETVPN 登録は、一般に GM リロードの直後に行われるため、これらのデバッグを収集するには、以下の EEM スクリプトが役立つちます。

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

キー再生成

GM が KS に登録されて GETVPN ネットワークが適切に設定されると、プライマリ KS が登録済み GM のすべてにキー再生成メッセージを送信します。キー再生成メッセージは、GM 上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使用されます。キー再生成メッセージは、ユニキャストまたはマルチキャスト方式で送信できます。

キー再生成メッセージが送信されると、KS 上に以下の syslog メッセージが表示されます。

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

GM 上では、キー再生成メッセージを受信すると以下の syslog が表示されます。

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

KS でのキー再生成に関する 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キーが存在する必要があります。KSは、登録時にこのセキュア・チャネルを通じて、RSAキー・ペアの公開キーをGMに提供します。続いて KS は、GM に送信される GDOI メッセージの GDOI SIG ペイロードに RSA 秘密キーで署名します。GM はこの GDOI メッセージを受信すると、RSA 公開キーを使用してメッセージを検証します。KS と GM の間で送受信されるメッセージは KEK で暗号化されます。この KEK も登録プロセス中に GM に配信されます。登録が完了した後は、以降のキー再生成メッセージは KEK で暗号化され、RSA 秘密鍵で署名されるようになります。

GM 登録プロセス中に RSA キーが KS 上にない場合、以下のメッセージが syslog に示されます。

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

KS 上にキーがない場合、GM は 1 回目は登録しますが、KS からの次のキー再生成は失敗します。最終的に GM 上の既存のキーが期限切れになると、GM はキーを再登録します。

```
%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.
```

RSA キー ペアはキー再生成メッセージへの署名に使用されるため、プライマリ KS とセカンダリ KS との間で RSA キー ペアが**同一でなければなりません。**同一であれば、プライマリ KS で障害が発生している間、セカンダリ KS (新しいプライマリ KS) から送信されたキー再生成メッセージを、GM が正常に検証できます。GM がプライマリ KS 上で RSA キー ペアを生成する際は、**exportable オプションを設定してキー ペアを生成する必要があります。これにより、キー ペアをすべてのセカンダリ KS にエクスポートして、プライマリ KS とセカンダリ KS を同一にするという要件を満たすことができます。**

キー再生成のトラブルシューティング

KEK/TEK キー再生成エラーは、顧客導入環境で最も発生しがちな GETVPN 問題の 1 つとして挙げられます。キー再生成の問題をトラブルシューティングするには、以下に概説するキー再生成手順に従ってください。

1. KS によってキー再生成メッセージが送信されたかどうかを確認します。

   これは、%GDOI-5-KS_SEND_UNICAST_REKEY syslogメッセージを確認するか、より正確に次のコマンドで確認できます。

```
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
```

   キー再生成メッセージが再送信された回数が、kS でキー再生成確認応答パケットを受信していないことがキー再生成問題の原因であるかどうかの判断基準になります。GDOI キー再生成メッセージには信頼性に欠ける UDP がトランスポート メカニズムとして使用されるため、基礎となるネットワークの信頼性によってはキー再生成パケットがドロップされる可能性がありますが、キー再生成送信回数が増加の傾向にある場合は、必ずその原因を調査してください。

   GM ごとの詳細なキー再生成統計情報を取得することもできます。通常はこの統計情報が、潜在的なキー再生成問題を調べる出発点となります。

```
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. 基盤となるインフラストラクチャのネットワークでキー再生成パケットが配信されたかどうかを確認します。

   KS と GM 間の中継ネットワークでキー再生成パケットがドロップされていないことを確認するには、キー再生成メッセージの転送パスに沿って標準 IP をトラブルシューティングします。ここで使用される一般的なトラブルシューティングツールには、入出力アクセスコントロールリスト(ACL)、Netflow、および中継ネットワークでのパケットキャプチャがあります。

3. キー再生成パケットが、キー再生成を処理する GDOI プロセスに到達したかどうかを確認します。

   それには、GM キー再生成統計情報を調べます。

```
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
```

4. キー再生成確認応答パケットが KS に返されたかどうかを確認します。

   GM から KS に返されるキー再生成確認応答パケットをトレースするには、ステップ 1 から 3 に従います。

マルチキャスト キー再生成

マルチキャスト キー再生成パケットは、以下の点でユニキャスト キー再生成パケットと異なります。

- マルチキャストはキー再生成パケットを KS から GM に転送するために使用されるため、KS がキー再生成パケット自体を複製する必要があります。KS はキー再生成パケットのコピーを 1 つだけ送信し、そのコピーがマルチキャスト対応ネットワークで複製されます。
- マルチキャスト キー再生成パケットには確認応答メカニズムがありません。したがって、

GM がキー再生成パケットを受信していなくても、KS はそれを把握しないため、GM データベースから GM を削除することはありません。さらに、確認応答がないことから、KS は常に、キー再生成パケットの再送信設定に基づいて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キー再生成の問題は、キー再生成がGMで受信されない場合です。この問題には、たとえば以下の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内で有効にされていない

マルチキャスト キー再生成パケットの問題をトラブルシューティングするための最初のステップは、マルチキャストからユニキャストに方式を切り替えるとキー再生成パケットが機能するかどうかを調べることです。

問題がマルチキャスト キー再生成パケットにあることがわかったら、KS がキー再生成パケットを指定のマルチキャスト アドレスに送信していることを確認します。

```
%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
```

Internet Control Message Protocol（ICMP）要求をマルチキャスト アドレスに送信して、KS と GM 間のマルチキャスト接続をテストします。マルチキャストグループに属するすべてのGMは、pingに応答する必要があります。このテストでは、KS 暗号化ポリシーから ICMP を除外してください。

```
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、マルチキャストのトラブルシューティングを行う必要があります。その方法については、このドキュメントの範囲外です。

コントロール プレーンのリプレイ チェック

症状

GMを新しいCisco IOSバージョンにアップグレードすると、syslogに次のメッセージが表示され、KEKキー再生成エラーが発生する可能性があります。

```
%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
```

この動作の原因は、コントロール プレーン メッセージに追加されたアンチリプレイ チェックによる運用互換性の問題にあります。具体的には、古いコードを実行している KS が KEK キー再生成シーケンス番号を 1 にリセットし、それによって新しいコードを実行している GM がキー再生成パケットのリプレイが行われたと解釈してキー再生成パケットをドロップするという問題です。詳細については、Cisco Bug ID CSCta05809 (GETVPN:リプレイに敏感な GETVPN コントロール プレーン）および GETVPN 設定に関する制限事項を参照してください。

背景

GETVPN では、コントロール プレーン メッセージに時間に制約のある情報を含めて、Time Based Anti-Replay チェック サービスを実行できます。したがって、時間の精度を確保するために、これらのメッセージ自体にアンチリプレイ保護が必要となります。該当するメッセージは以下のとおりです。

- **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**

このアンチリプレイ保護実装の一環として、再生されたメッセージを保護するためにシーケンス番号チェックが追加され、TBARが有効な場合は疑似時間チェックが追加されました。

解決方法

この問題を解決するには、GM と KS の両方を、コントロール プレーン リプレイ チェック機能が追加された後の 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 にリセットする代わりに、現行のシーケンス番号を引き続き使用します。KS は TEK キー再生成に対してのみ、シーケンス番号をリセットします。

リプレイ チェック機能が備わっている Cisco IOS バージョンは以下のとおりです。

- 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 リプレイ チェック失敗による COOP エラー（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

その他のコントロール プレーン リプレイ失敗については、以下の情報を収集します。その際、KS と GM の時間が同期されていることを確認してください。

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

コントロール プレーンのパケット フラグメンテーションの問題

GETVPN では、コントロール プレーンのパケット フラグメンテーションに問題があることがよくあります。コントロール プレーン パケット サイズが大きく、IP フラグメンテーションが必要になった場合、以下の 2 つのシナリオで、この問題が顕著になります。

- 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

COOPアナウンスパケットはGMデータベース情報を伝送するため、大規模なGETVPN展開では大きく成長する可能性があります。過去の経験から、1500 を超える GM で構成される GETVPN ネットワークでは、生成されるアナウンス パケットのサイズが、Cisco IOS のデフォルト大容量バッファ サイズである 18024 バイトを超えてしまいます。この場合、KS は ANN パケットを送信するのに十分なバッファを割り当てられることができず、以下のエラーが発生します。

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

この状況を修正するには、以下のようにバッファを調整することを推奨します。

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

キー再生成パケット

暗号化ポリシーのサイズが大きいと（たとえば、暗号化 ACL に 8 行を超えるアクセス コントロール エントリ（ACE）が含まれるポリシーなど）、GETVPN キー再生成パケットも通常の 1500 IP 最大伝送ユニット（MTU）サイズを超える可能性があります。

フラグメンテーションの問題と識別

COOPまたはGDOIキー再生成が正常に動作するためには、前述の両方のシナリオで、GETVPNがフラグメント化されたUDPパケットを正しく送受信できる必要があります。一部のネットワーク環境では、IP フラグメンテーションが問題になる可能性があります。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ているネットワークでは、フォワーディング プレーンの一部のデバイスに、フラグメント化された IP パケットの仮想リアセンブル（Virtual Fragmentation Reassembly（VFR）など）が必要になります。

この問題を識別するには、フラグメント化された UDP 848 パケットを適切に受信していないことが疑われるデバイス上でのリアセンブル 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
```

リアセンブルタイムアウトが増加し続ける場合は、**debug ip error**コマンドを使用して、廃棄がキー再生成/COOPパケットフローの一部であるかどうかを確認します。確認したら、パケットをドロップした可能性のあるフォワーディングプレーン内の正確なデバイスを切り分けるために、通常のIPフォワーディングのトラブルシューティングを実行する必要があります。この場合によく使われるツールには、以下があります。

- 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 の統計情報

GDOI 相互運用性の問題

過去数年にわたり、GETVPN ではさまざまな相互運用性の問題が発生しています。したがって、Cisco IOS リリース バージョンで KS と GM の間、または KS 間の相互運用性の問題を確認することが重要です。

GETVPNの相互運用性に関するその他の既知の問題は次のとおりです。

- コントロール プレーンのリプレイ チェック
- GETVPN KEK キー再生成の動作変更
- Cisco Bug ID CSCub42920(GETVPN:KS が前の GM バージョンからのキー再生成でハッシュを検証できない)
- Cisco Bug ID CSCuw48400(GetVPN GM unable to register or rekey fails - sig-hash > default SHA-1)
- Cisco Bug ID CSCvg19281(新しいKSペアへの移行後、複数のGETVPN GMがクラッシュする。GMバージョンが3.16より前のバージョンで、KSが以前のコードから3.16以降にアップグレードされている場合、この問題が発生する可能性があります)

GETVPN の IOS 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、アップグレード作業の後、以下の Cisco IOS アップグレード手順に従ってください。

1. セカンダリ KS を最初にアップグレードし、COOP KS 選定が完了するまで待ちます。
2. すべてのセカンダリ KS について、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

コントロールプレーンの問題と比較すると、GETVPNデータプレーンの問題は、GMがデータプレーンの暗号化と復号化を実行するポリシーとキーを持っているものの、何らかの理由でエンドツーエンドのトラフィックフローが機能しない問題です。GETVPN でのデータ プレーンの問題のほとんどは、汎用 IPSec フォワーディングに関連するもので、GETVPN に固有の問題ではありません。したがって、ここで説明するトラブルシューティング手法の大部分は、汎用 IPSec データ プレーンの問題にも適用されます。

暗号化に問題がある場合（グループベースまたはペアワイズ トンネルの両方）、問題のトラブルシューティングを行って、問題をデータ パスの特定の部分に切り分けることが重要となります。具体的には、ここで説明するトラブルシューティング手法は以下の質問に対する答えを見つけることを目的としています。

- 暗号化ルータまたは復号ルータのどちらのデバイスが問題の原因になっているか。
- 入力または出力のどちらの方向で問題が発生しているか。

GETVPN データ プレーンのトラブルシューティング ツール

IPSec データ プレーンのトラブルシューティングは、コントロール プレーンの場合とは大幅に異なります。データ プレーンの場合、実行できるデバッグがないか、あるとしても実稼働環境では安全に実行できないことが通常です。したがって、トラブルシューティングでは各種のカウンタとトラフィック統計情報を頼りに、パケットをフォワーディング パスに沿ってトレースすることになります。その概念は、パケットがドロップされている箇所を切り分けるための一連のチェックポイントを開発できるようにすることです（以下の図を参照）。

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
- Interface Counters
- 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）

上記の図に示されているデータ パスのチェックポイントを検証するには、以下のツールを使用できます。

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 Precedence 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 Precedence アカウンティング

復号 GM

- 入力 WAN インターフェイス
  入力 ACL
  入力 NetFlow
  Embedded Packet Capture
  入力 Precedence 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 フローに従います。以降のセクションに、これらのデータ プレーン ツールを使用した例を記載します。

暗号化/復号カウンタ

ルータ上の暗号化/復号カウンタは、IPSec フローに基づきます。残念ながら、これらのカウンタはトラブルシューティングにはそれほど有効ではありません。GETVPN では通常、すべてのものを暗号化する「permit ip any any」ポリシーを導入するためです。したがって、フローのすべてではなく、一部のフローで問題が発生する場合、かなりのバックグラウンド トラフィックが機能している中で、暗号化/復号カウンタを使用してパケットが暗号化または復号されているかどうかを正しく評価するのは難しい話です。

```
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 を使用することで、両方の GM で入力トラフィックと出力トラフィックをモニタできます。GETVPN の **permit ip any any ポリシーでは、暗号化されたトラフィックは集約されるため、フローごとの情報は入手できないことに注意してください。**フローごとの情報は、後で説明する DSCP/Precedence のマーキングで収集する必要があります。

この例の場合、GM1 背後のホストから GM2 背後のホストへの 100 回の ping に対応する NetFlow がさまざまなチェックポイントで示されます。

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 の出力：

```
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：上記の出力で、* は出力トラフィックを示します。最初の行には、WAN インターフェイスからの（プロトコル 0x32 = ESP を使用して）暗号化された出力トラフィックが示されています。2 番目の行に示されているのは、LAN インターフェイスに到達した入力 ICMP トラフィックです。

復号 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 の出力：

```
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 Precedence マーキング

暗号化の問題をトラブルシューティングする際の課題は、パケットが暗号化されると、ペイロードの可視性が失われ、暗号化の内容が不明になり、特定のIPフローのパケットをトレースするのが困難になることです。IPSecの問題のトラブルシューティングに関して、この制限に対処する方法は2つあります。

- IPSec トランスフォームとして ESP-NULL を使用します。この場合、IPsec は引き続き ESP カプセル化を行いますが、ペイロードに暗号化は適用されません。したがって、パケット キャプチャでペイロードが可視になります。
- IP フローの L3/L4 特性に基づく一意の Differentiated Services Code Point（DSCP）/Precedence マーキングを使用して IP フローをマークします。

ESP-NULL を使用するには、トンネルのエンド ポイントの両方で変更が必要になるため、顧客のセキュリティ ポリシーにより許可されないことがよくあります。そのため、一般には DSCP/Precedence マーキングを使用することを推奨します。

DSCP/Precedence リファレンス チャート

ToS（16 進数）	ToS（10 進数）	IP Precedence	DSCP	バイナリ
0xE0	224	7 ネットワーク制御	56 CS7	11100000
0xC0	192	6 インターネットワーク制御	48 CS6	11000000

0xB8	184	5 重大	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4 フラッシュ上書き	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	3 フラッシュ	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2 即時	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1 優先度	8 CS1	00100000
0x00	0	0 ルーチン	0 Dflt	00000000

DSCP/Precedence によるパケットのマーキング

特定の DSCP/Precedence マーキングをパケットに適用するには、一般に以下の手法が使用されます。

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：**常に、マークされたトラフィック フローが一意になるよう、通常のトラフィック フローと DSCP/Precedence プロファイルをモニタしてからマーキングを適用することが推奨されます。

マーク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
```

インターフェイス 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特定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際に役立つツールです。EPC は、クリア テキスト トラフィックでは効果的に機能しますが、キャプチャしたパケットが暗号化されている場合、EPC だけで成果を出すのは困難です。したがって、トラブルシューティングをより効果的にするために、EPC と併せて、前述の DSCP/Precedence マーキングやその他の IP 特性（IP パケット長など）を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、CSR1000v、ASR1000、ISR4451-Xなど、Cisco IOS-XEを実行するすべてのプラットフォームで機能の転送パスをトレースするのに便利な機能です。

GETVPN データ プレーンのよくある問題

GETVPNのIPsecデータプレーンのトラブルシューティングは、従来のポイントツーポイントIPsecデータプレーンの問題のトラブルシューティングと大きく異なりませんが、GETVPNの固有のデータプレーンのプロパティによる2つの例外があります。

Time Based Anti-Replay（TBAR）エラー

GETVPN ネットワークにはペアワイズ トンネルがないため、TBAR エラーをトラブルシューティングするのが困難になることがよくあります。GETVPN TBAR エラーをトラブルシューティングするには、以下の手順に従います。

1. TBAR エラーによってドロップされているパケットを識別した後、そのパケットを基に暗号化 GM を識別します。

   15.3(2)T より前のバージョンでは、TBAR エラーの syslog には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のが非常に困難でした。この点については、Version 15.3(2)T バージョン以降で大幅に改善されており、Cisco IOS は以下を出力するようになっています。

```
%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
```

   TBAR履歴は、次のバージョンにも実装されています。

```
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
```

   注：前述の機能拡張は、Cisco Bug ID CSCun49335によりCisco IOS-XEに、Cisco Bug ID CSCub91811によりCisco IOSに実装されました。
   この機能を持たないCisco IOSバージョンの**debug crypto gdoi gm replay detail**も、この情報を提供できます。ただし、このデバッグでは、すべてのトラフィック（TBARの障害により廃棄されたパケットだけでなく）のTBAR情報が出力されるため、実稼働環境では実行できない場合があります。

```
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. パケットの送信元を特定すると、暗号化 GM を見つけることができます。次に、暗号化 GM と復号 GM の両方の疑似タイムスタンプをモニタして、疑似時間に差があるかどうかを調べます。そのための最善の方法は、両方の GM と KS を NTP に同期し、基準システム クロックで定期的に疑似時間情報を収集し、問題の原因が GM 上のクロックの誤差に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

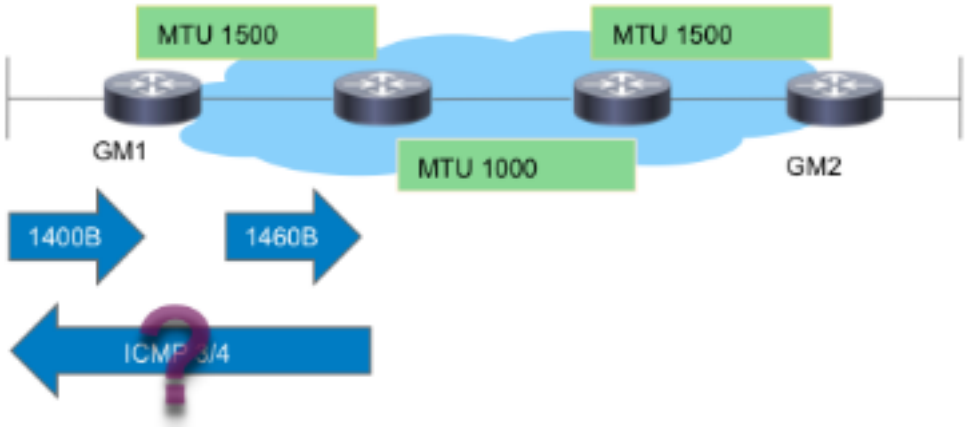
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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、同じ基準時間で出力をキャプチャした際に（「Replay Value」で示されている）疑似時間が、GM の間で大幅に異なっている場合、問題の原因はクロックの誤差にあるはずです。

> **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により、クォンタム フロー プロセッサ（QFP）は実際にウォールクロックを参照して疑似時間をカウントします。これにより、NTPの同期によりウォールクロックの時刻が変更された場合に、TBARに問題が発生します。この問題については、CSCum37911 に文書化されています。

PMTUD と GETVPN ヘッダー保護

GETVPN では、暗号化 GM と復号 GM との間でパス MTU 検出（PMTUD）が機能しないため、Don't Fragment（DF）ビットが設定されたサイズの大きいパケットはブラックホール化される場合があります。PMTUD が機能しない理由は、GETVPN ヘッダー保護により、データの送信元/宛先アドレスが ESP カプセル化ヘッダーで維持されるためです。以下の図に、この仕組みを示します。



上記の図に示されているように、GETVPN では以下のフローで PMTUD が分割されます。

1. サイズの大きいデータ パケットが暗号化 GM1 に到達します。
2. 暗号化された ESP パケットが GM1 から転送され、宛先に向けて配信されます。
3. 中継リンクがある場合、IP MTU が 1400 バイトの ESP パケットはドロップされます。この

場合、ICMP 3/4 パケットが大きすぎるというメッセージがパケット送信先（データ パケットの送信元）に送信されます。
4. GETVPN 暗号化ポリシーから ICMP が除外されていなければ、ICMP3/4 パケットはドロップされます。あるいは、エンド ホストが不明な ESP パケット（未認証ペイロード）としてドロップする場合もあります。

要するに、現在のところ、PMTUD は GETVPN と連動しません。この問題を回避するには、次の手順を推奨します。

1. 暗号化オーバーヘッドと中継ネットワークの最小パスMTUに対応するために、TCPパケットセグメントサイズを減らすために「ip tcp adjust-mss」を実装します。
2. データ パケットが暗号化 GM に到着した時点でパケット内の DF ビットをクリアし、PMTUD を回避します。

汎用 IPSec データ プレーンの問題

IPSec データ プレーンのトラブルシューティングは、従来のポイントツーポイント IPSec トンネルをトラブルシューティングする場合と同様です。一般的な問題の1つが%CRYPTO-4-RECVD_PKT_MAC_ERRです。トラブルシューティングの詳細[については、「Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:」エラーメッセージとIPSecトンネルでのping損失のトラブルシューティング」を参照して](#)ください。

既知の問題

以下のメッセージは、受信した IPSec パケットが SADB に保管されている SPI と一致しない場合に生成されます。GETVPN でフローと一致しないパケットに対して報告される CRYPTO-4-RECVD_PKT_NOT_IPSEC については、Cisco Bug ID CSCtd47420 を参照してください。次に例を表示します。

```
%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
```

このメッセージは%CRYPTO-4-RECVD_PKT_INV_SPIである必要があります。これは、従来のIPsecおよびASRなどの一部のハードウェアプラットフォームで報告されるメッセージです。この表層的な問題は、ESP パケットの CRYPTO-4-RECVD_PKT_NOT_IPSEC を報告する際のエラーに関する Cisco Bug ID CSCup80547で修正されています。

> **注：**上述のメッセージは、TEK キー再生成後に GETVPN GM がトラフィックの復号を停止することに関する別の GETVPN Bug CSCup34371:でも表示される場合があります。

この場合、GMはGETVPNトラフィックを復号化できません。ただし、SADB（キーが再生成されているSA）には有効なIPsec SAがあります。 SA が期限切れになって SADB から削除されると同時に、問題は解消されます。ただし、TEK キー再生成が事前に行われることから、この問題によりかなりの停止時間が発生します。たとえば、TEK のライフタイムが 7200 秒の場合、停止時間は 22 分に及ぶ可能性があります。このバグを発生させる正確な条件については、バグの説明を参照してください。

Cisco IOS-XEが稼働するプラットフォームでのGETVPNのトラブルシューティング

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は、プラットフォーム固有の実装があり、GETVPNの問題に対してプラットフォーム固有のデバッグが必要になることがよくあります。このようなプラットフォームで GETVPN をトラブルシューティングする際に通常使用されるコマンドを以下にリストします。

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の一般的な問題

IPsecポリシーのインストール失敗（継続的な再登録）

暗号化エンジンが受信したIPsecポリシーまたはアルゴリズムをサポートしていない場合、ASR1000 GMはキーサーバへの登録を続行する可能性があります。たとえば、Nitroxベースの ASRプラットフォーム（ASR1002など）では、Suite-BまたはSHA2ポリシーがサポートされていないため、継続的な再登録の症状が発生する可能性があります。

移行/アップグレードに関する一般的な問題

ASR1000 TBARの制限

ASR1000プラットフォームでは、Cisco Bug ID CSCum37911修正により、20秒未満のTBAR時間がサポートされないプラットフォームに制限が導入されました。IOS-XEにおけるGETVPNの制限を参照してください。

この拡張バグは、この制限を解除するために開かれています。Cisco Bug ID CSCuq25476 - ASR1kは20秒未満のGETVPN TBARウィンドウサイズをサポートする必要があります。

更新：この制限は、Cisco Bug ID CSCur57558（登録ユーザ専用）の修正により解除されました。この修正は、XE3.10.5、XE3.13.2以降のコードでの制限ではなくなりました。

また、Cisco IOS XEプラットフォーム（ASR1kまたはISR4k）で稼働するGMの場合、TBARが有効な場合は、この問題の修正を含むバージョンをデバイスで実行することを強く推奨します。Cisco Bug ID CSCut91647 - IOS-XEのGETVPN:TBARの障害により、GMは誤ってパケットをドロップします。

ISR4x00分類の問題

拒否ポリシーが無視されるISR4x00プラットフォームで回帰が見つかりました。詳細については、Cisco Bug ID CSCut14355 - GETVPN - ISR4300 GM ignore deny policyを参照してください。

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