GETVPNグループメンバーの長いSA非互換性に対する登録が拒否された場合のトラブルシューティング

内容

概要

このドキュメントでは、Group Encrypted Transport Virtual Private Network(GETVPN)キーサーバ(KS)とグループメンバー(GM)の間のLong Security Association(SA)ライフタイム非互換性に関する登録拒否問題をトラブルシューティングする方法について説明します。

著者：Cisco TACエンジニア、Daniel Perez Vertti Vazquez

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
- Internet Security Association and Key Management Protocol（ISAKMP）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Internetwork Operating System(IOS) 15.3(2)Tより前のリリースを実行しているGMでは、ロングサライフタイム機能はサポートされません。
- IOS XE 15.3(2)Sよりも前のリリースを実行しているGMでは、長saライフタイム機能はサポートされません。

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

Long SAライフタイム機能は、リリース15.3(2)TのIOSプラットフォームと、IOS XEデバイスのXE3.9(15.3(2)S)に含まれています。Traffic Encryption Key(TEK)とKey Encryption Key(KEK)の有効期間を24時間から30日に延長できます。キーサーバでLong SAライフタイム機能を使用すると、これは、GDOIグループ設定のライフタイムが1日以上変更された場合、GETVPN KSはすべてのGMのソフトウェアバージョンをチェックし、この機能をサポートしていないGMの登録をブロックします。

> **注：**Long of SA lifetimeを使用するには、Advanced Encryption Standard-cipher block chaining(AES-CBC)またはAdvanced Encryption Standard-Galois/Counter Mode(AES-GCM)と128ビット以上のAESキーが必要です。

長いSAライフタイム機能は、キーサーバーのグループドメイン(GDOI)グループで構成されています。

デバイスは正常にISAKMPトンネルを完了し、相互に認証できます。

```
208752: Jun 10 22:19:14.380: ISAKMP-PAK: (82124):sending packet to 10.40.10.10 my_port 848
peer_port 848 (R) MM_KEY_EXCH
208753: Jun 10 22:19:14.380: ISAKMP: (82124):Sending an IKE IPv4 Packet.
208754: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
208755: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

208756: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
208757: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

ただし、GMが暗号キーを取得しようとすると、KSはGMのIOSバージョンに長いSAライフタイム機能のサポートが含まれていないことを検出し、接続を切断するエラーメッセージを生成します。

```
208758: Jun 10 22:19:14.433: ISAKMP-PAK: (82124):received packet from 10.40.10.10 dport 848
sport 848 Global (R) GDOI_IDLE
208759: Jun 10 22:19:14.433: ISAKMP: (82124):set new node 1548686329 to GDOI_IDLE
208760: Jun 10 22:19:14.433: ISAKMP: (82124):processing HASH payload. message ID = 1548686329
208761: Jun 10 22:19:14.433: ISAKMP: (82124):processing NONCE payload. message ID = 1548686329
208762: Jun 10 22:19:14.433: ISAKMP: (82124):GDOI Container Payloads:
208763: Jun 10 22:19:14.433:    ID
208764: Jun 10 22:19:14.433: ISAKMP: (82124):Node 1548686329, Input = IKE_MESG_FROM_PEER,
IKE_GDOI_EXCH
208765: Jun 10 22:19:14.434: ISAKMP: (82124):Old State = IKE_KS_LISTEN  New State =
IKE_KS_GET_SA_POLICY_AWAIT
208766: Jun 10 22:19:14.434: ISAKMP: (82124):GDOI Container Payloads:
208767: Jun 10 22:19:14.434:    SA
208768: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):GDOI processing Failed: Deleting node
208769: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):deleting node 1548686329 error TRUE reason
"GDOI QM rejected - failed to process QM"
208770: Jun 10 22:19:21.280: %GDOI-4-REJECT_GM_VERSION_REGISTER: Reject registration of GM
10.40.10.10(ver 0x1000001) in group MYGETVPN as it cannot support these GETVPN features enabled:
Long-SA
```

GMは新しいISAKMPトンネルの作成を試行しますが、登録プロセスを終了できません。この時点で、同じネゴシエーションの複数のインスタンスに気付くことができます。

```
Router# sh crypto isakmp sa | i 10.80.127.20
10.80.127.20    10.40.10.10     MM_NO_STATE       2104 ACTIVE (deleted)
```

```
Router#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPN
    Group Identity           : 1
    Rekeys received          : 0
    IPSec SA Direction       : Inbound Only

     Group Server list       : 10.80.127.20

    Group member             : 10.40.10.10      vrf: None
       Registration status   : Registering
       Registering to        : 10.80.127.20
       Re-registers in       : 44 sec
       Succeeded registration: 0
       Attempted registration: 3
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 0
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Received        : never

 ACL Downloaded From KS UNKNOWN:
```

機能の互換性をさらに確認するには、KSで**show crypto gdoi feature long-sa-lifetimeコマンドを実行**します。次の出力は、2つのGMの例を示しています。最初のGMは、この機能をサポートするIOSイメージをすでに実行しており、2番目のGMは該当するGMです。

```
Router# sh cry gdoi feature long-sa-lifetime
Group Name: GETVPN_GROUP
    Key Server ID       Version   Feature Supported
        10.80.127.20      1.0.18         Yes

Group Member ID Version Feature Supported 10.40.10.9 1.0.17 Yes         10.40.10.10       1.0.4
No
```

解決方法

- この問題は、GMをIOS 15.3(2)以降にアップグレードすることで解決できます。GDOIバージョンとIOS/IOS-XEリリース間のマッピングについては、GETVPN設計ガイドを参照してください。
- 2番目の回避策は、GDOIグループのキー再生成のライフタイムを86400秒未満に変更することです。この設定変更は、キー再生成をトリガーしないため、稼働中のグループメンバーの中断を引き起こしません。