Troubleshoot Rejected Registration of GETVPN Group Member for Long SA Incompatibility

Contents

Introduction

This document describes how to troubleshoot the registration rejection issue for Long Security Association (SA) lifetime incompatibility between Group Encrypted Transport Virtual Private Network (GETVPN) Key Server (KS) and Group Member (GM).

Contributed by Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- GETVPN
- Internet Security Association and Key Management Protocol (ISAKMP)

Components Used

The information in this document is based on these software and hardware versions:

- GMs running a release earlier than Internetwork Operating System (IOS) 15.3(2)T which don't support long-sa lifetime feature.
- GMs running a release earlier than IOS XE 15.3(2)S which don't support long-sa lifetime feature.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

The Long SA lifetime feature is included in IOS platforms from release 15.3(2)T and from XE3.9 (15.3(2)S) in IOS XE devices. It allows to extended lifetime for Traffic Encryption Key (TEK) and Key Encryption Key (KEK) from 24 hours to 30 days. When the Long SA lifetime feature is used in the Key Server; this is when lifetime in GDOI group configuration has been changed to more than one day, GETVPN KS checks the software version of all GMs and blocks registration for those which don´t support the feature.

> **Note**: The use of Long of SA lifetime requires Advanced Encryption Standard-cipher block chaining (AES-CBC) or Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) with an AES key of 128 bits or stronger.

Long SA lifetime feature is configured in Group Domain of Interpretation (GDOI) group of Key Server.

Devices can successfully complete ISAKMP tunnel and authenticate with each other.

```
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
```

However, when GM tries to get encryption keys, KS detects the IOS version in GM doesn´t include long SA lifetime feature support and generates an error message to tear down the connection.

```
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 tries to create a new ISAKMP tunnel but is not able to finish with registration process. At this point you can notice multiple instances of the same negotiation.

```
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:
```

To do a further review of feature compatibility, run the command **show crypto gdoi feature long-sa-lifetime** in the KS. This output shows an example of two GMs, the first one already runs an IOS image with support for this functionality and the second one is the affected GM.

```
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
```

Solution

- The problem can be fixed with an upgrade of the GM to IOS 15.3(2) or later. A mapping between GDOI versions and IOS/IOS-XE releases can be found in GETVPN Design guide.
- A second workaround can be change the rekey lifetime in GDOI group to less than 86400 seconds. This configuration change doesn´t cause any disruption for working Group Members as it doesn´t trigger any rekey.