Probleemoplossing afgewezen registratie van GETVPN-groepslid voor lange SA-incompatibiliteit

Inhoud

Inleiding

Dit document beschrijft hoe u het probleem van de afwijzing van uw registratie kunt oplossen voor de levensoncompatibiliteit van Long Security Association (SA) tussen Group Encrypted Transport Virtual Private Network (GETVPN) Key Server (KS) en Group Member (GM).

Bijgedragen door Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- GM's die een release uitvoeren eerder dan Internetwork Operating System (IOS) 15.3(2)T die geen lange-termijn optie ondersteunt.
- GM's die een release uitvoeren eerder dan IOS XE 15.3(2)S die geen lange-termijn optie ondersteunen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

De lange SA leven optie is in IOS platforms van release 15.3(2)T en van XE3.9 (15.3(2)S) in IOS XE apparaten opgenomen. Het biedt de mogelijkheid om de levensduur van Traffic Encryption Key (TEK) en Key Encryption Key (KEK) te verlengen van 24 uur tot 30 dagen. Wanneer de Long SA-levensfunctie wordt gebruikt in de Key Server; Dit is het moment waarop de GDOI-groepsconfiguratie is gewijzigd in meer dan één dag, GETVPN KS de softwareversie van alle GM's controleert en de registratie blokkeert voor degenen die deze optie niet ondersteunen.

> **Opmerking:** Het gebruik van Long of SA leven vereist Advanced Encryption Standard-algoritme chaining (AES-CBC) of Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) met een AES-toets van 128 bits of sterker.

De lange SA leven optie is ingesteld in Group Domain of Interpretation (GDOI)-groep van Key Server.

Apparaten kunnen de ISAKMP-tunnel voltooien en met elkaar authentiseren.

```
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
```

Wanneer GM echter encryptiesleutels probeert te krijgen, detecteert KS de IOS-versie in GM niet altijd de lange SA-levensfunctieondersteuning en genereert hij een foutmelding om de verbinding af te breken.

```
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 probeert een nieuwe ISAKMP-tunnel te maken, maar kan niet met registratieproces afsluiten. Op dit punt kun je meerdere gevallen van dezelfde onderhandeling waarnemen.

```
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:
```

Om een verdere beoordeling van functietoepassing te doen, **moet** de opdracht **de crypto-godfunctie lange tijd na leven** in de KS **laten zien**. Deze uitvoer toont een voorbeeld van twee GM's. De eerste voert al een IOS afbeelding uit met ondersteuning voor deze functionaliteit en de tweede is de beïnvloede 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
```

Oplossing

- U kunt het probleem met een upgrade van het GGM naar IOS 15.3(2) of hoger oplossen. Een mapping tussen GDOI-versies en IOS/IOS-XE releases kan worden gevonden in GETVPN-Ontwerphandleiding.
- Een tweede mogelijkheid is om de levensduur van de GDOI-groep te wijzigen in minder dan 86400 seconden. Deze verandering veroorzaakt geen verstoring voor de leden van de werkgroep omdat het geen rekey veroorzaakt.