Long SA 비호환성에 대해 GETVPN 그룹 구성원의 거부된 등록 문제 해결

목차

소개

이 문서에서는 그룹 GETVPN(Encrypted Transport Virtual Private Network) KS(Key Server)와 GM(Group Member) 간의 SA(Long Security Association) 수명 비호환성에 대한 등록 거부 문제를 해결하는 방법에 대해 설명합니다.

기고자: Daniel Perez Vertti Vazquez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IOS(Internetwork Operating System) 15.3(2)T 이전 릴리스를 실행하는 GM으로, 긴 수명 기능을 지원하지 않습니다.
- IOS XE 15.3(2)S 이전 릴리스를 실행하는 GM은 긴 수명 기능을 지원하지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

문제

Long SA lifetime 기능은 릴리스 15.3(2)T 및 IOS XE 디바이스의 XE3.9(15.3(2)S)에서 IOS 플랫폼에 포함됩니다.TEK(Traffic Encryption Key) 및 KEK(Key Encryption Key)의 수명을 24시간에서 30일로 연장할 수 있습니다. Long SA lifetime 기능이 키 서버에서 사용되는 경우이는 GDOI 그룹 컨

피그레이션의 수명이 하루 이상으로 변경된 경우입니다. GETVPN KS는 모든 GM의 소프트웨어 버전을 확인하고 해당 기능을 지원하지 않는 GM의 등록을 차단합니다.

> **참고:**Long of SA 수명을 사용하려면 AES-CBC(Advanced Encryption Standard-Cipher Block Chaining) 또는 AES-GCM(Advanced Encryption Standard-Galois/Counter Mode)이 128비트 이상인 것이 필요합니다.

긴 SA 수명 기능은 키 서버의 GDOI(Group Domain of Interpretion) 그룹에 구성됩니다.

디바이스는 ISAKMP 터널을 성공적으로 완료하고 서로 인증할 수 있습니다.

```
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
```

그러나 GM이 암호화 키를 가져오려고 하면 KS는 GM에서 IOS 버전을 감지하여 긴 SA 수명 기능 지원을 포함하지 않으며 연결을 끊어버리는 오류 메시지를 생성합니다.

```
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
```

GM은 새 ISAKMP 터널을 생성하려고 시도하지만 등록 프로세스를 완료할 수 없습니다.이 시점에서 동일한 협상의 여러 인스턴스를 확인할 수 있습니다.

```
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:
```

기능 호환성을 자세히 검토하려면 KS에서 **show crypto gdoi feature long-sa-lifetime 명령**을 실행합니다.이 출력은 두 GM의 예를 보여 줍니다. 첫 번째 GM은 이 기능을 지원하는 IOS 이미지를 이미 실행하고 두 번째 GM은 영향을 받는 GM입니다.

```
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
```

솔루션

- GM을 IOS 15.3(2) 이상으로 업그레이드하면 문제를 해결할 수 있습니다.GDOI 버전과 IOS/IOS-XE 릴리스 간의 매핑은 GETVPN 설계 가이드에서 확인할 수 있습니다.
- 두 번째 해결 방법은 GDOI 그룹의 키 재설정 수명을 86400초 미만으로 변경할 수 있습니다.이 컨피그레이션을 변경해도 키 재설정을 트리거하지 않으므로 작업 그룹 구성원이 중단되지 않습니다.