Fehlerbehebung: Abgelehnte Registrierung von GETVPN-Gruppenmitgliedern wegen langer SA-Inkompatibilität

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie das Problem der Ablehnung der Registrierung bei GETVPN Key Server (KS) (Group Encrypted Transport Virtual Private Network) und Group Member (GM) wegen Unvereinbarkeit der Long Security Association (SA) Lebensdauer beheben können.

Mitarbeiter: Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- GMs, die eine Version vor Internetwork Operating System (IOS) 15.3(2)T ausführen, die keine Lebenszeitfunktion mit langer Lebensdauer unterstützt.
- GMs, die eine Version vor IOS XE 15.3(2)S ausführen, die keine Lebenszeitfunktion mit langer Lebensdauer unterstützt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Die Long SA Lifetime-Funktion ist in IOS-Plattformen ab Version 15.3(2)T und von XE3.9 (15.3(2)S) in IOS XE-Geräten enthalten. Sie ermöglicht die Verlängerung der Lebensdauer von 24 Stunden auf 30 Tage für den TEK- (Traffic Encryption Key) und KEK-Schlüssel (Key Encryption Key). Wenn die Long SA Lifetime-Funktion im Schlüsselserver verwendet wird; In diesem Fall wurde die Lebensdauer in der GDOI-Gruppenkonfiguration auf mehr als einen Tag geändert. GETVPN KS überprüft die Softwareversion aller GMs und blockiert die Registrierung für diejenigen, die die Funktion nicht unterstützen.

> **Hinweis:** Für die Verwendung von Long of SA Lifetime ist Advanced Encryption Standard-Verschlüsselung (AES-CBC) oder Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) mit einem AES-Schlüssel von 128 Bit oder höher erforderlich.

Die Long SA Lifetime-Funktion wird in der Group Domain of Interpretation (GDOI)-Gruppe von Key Server konfiguriert.

Geräte können den ISAKMP-Tunnel erfolgreich abschließen und sich gegenseitig authentifizieren.

```
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
```

Wenn GM jedoch versucht, Verschlüsselungsschlüssel abzurufen, stellt KS fest, dass die IOS-Version in GM keine Unterstützung für lange SA-Lebenszeitfunktionen beinhaltet und eine Fehlermeldung generiert, um die Verbindung zu trennen.

```
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 versucht, einen neuen ISAKMP-Tunnel zu erstellen, kann aber den Registrierungsprozess

nicht abschließen. An diesem Punkt können Sie mehrere Instanzen derselben Aushandlung feststellen.

```
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:
```

Um eine weitere Überprüfung der Funktionskompatibilität durchzuführen, führen Sie den Befehl **show crypto gdoi feature long-sa-life** in the KS aus. Diese Ausgabe zeigt ein Beispiel für zwei GMs, wobei das erste bereits ein IOS-Image mit Unterstützung dieser Funktion ausführt, das zweite ist das betroffene 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
```

Lösung

- Das Problem kann durch ein Upgrade von GM auf IOS 15.3(2) oder höher behoben werden. Eine Zuordnung zwischen GDOI-Versionen und IOS/IOS-XE-Versionen finden Sie im GETVPN-Designleitfaden.
- Eine zweite Problemumgehung kann die rekey-Lebensdauer in der GDOI-Gruppe auf weniger

als 86.400 Sekunden ändern. Diese Konfigurationsänderung führt nicht zu Unterbrechungen für Mitglieder der Arbeitsgruppe, da sie keinen rekey auslöst.