Risoluzione dei problemi relativi alla registrazione rifiutata di un membro del gruppo GETVPN per incompatibilità SA estesa

Sommario

Introduzione

In questo documento viene descritto come risolvere il problema di rifiuto della registrazione per l'incompatibilità della durata SA (Long Security Association) tra il server chiavi Group Encrypted Transport Virtual Private Network (GETVPN) e il membro del gruppo (GM).

Contributo di Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- GM con release precedenti a Internetwork Operating System (IOS) 15.3(2)T che non supportano la funzione di durata a lungo termine.
- GM con release precedenti a IOS XE 15.3(2)S che non supportano la funzionalità di durata prolungata.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

La funzione Long SA lifetime è inclusa nelle piattaforme IOS dalla versione 15.3(2)T e da XE3.9 (15.3(2)S) nei dispositivi IOS XE. Consente di estendere la durata della chiave di crittografia del traffico (TEK) e della chiave di crittografia della chiave (KEK) da 24 ore a 30 giorni. Quando nel server di chiavi viene utilizzata la funzione Durata SA estesa; In questo caso, la durata della configurazione del gruppo GDOI è stata modificata in più di un giorno. GETVPN KS controlla la versione software di tutti gli GM e blocca la registrazione per quelli che non supportano la funzione.

> **Nota:** L'uso di Lunga durata SA richiede Advanced Encryption Standard-cipher block chaining (AES-CBC) o Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) con una chiave AES di 128 bit o superiore.

La funzionalità di durata SA estesa è configurata nel gruppo Group Domain of Interpretation (GDOI) di Key Server.

I dispositivi possono completare correttamente il tunnel ISAKMP e autenticarsi tra loro.

```
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
```

Tuttavia, quando GM tenta di ottenere le chiavi di crittografia, KS rileva che la versione IOS in GM non include il supporto per la funzionalità di lunga durata SA e genera un messaggio di errore per interrompere la connessione.

```
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 tenta di creare un nuovo tunnel ISAKMP ma non riesce a completare il processo di

registrazione. A questo punto è possibile notare più istanze della stessa negoziazione.

```
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:
```

Per un'ulteriore analisi della compatibilità delle funzionalità, eseguire il comando **show crypto gdoi feature long-sa-lifetime** nel KS. Questo output mostra un esempio di due GM, il primo esegue già un'immagine IOS con supporto per questa funzionalità e il secondo è il GM interessato.

```
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
```

Soluzione

- Il problema può essere risolto con un aggiornamento di GM a IOS 15.3(2) o versioni successive. Una mappatura tra le versioni GDOI e IOS/IOS-XE è disponibile nella guida alla progettazione di GETVPN.
- Una seconda soluzione alternativa può essere rappresentata dalla modifica della durata della chiave nel gruppo GDOI a meno di 86400 secondi. Questa modifica della configurazione non causa alcuna interruzione per i membri del gruppo di lavoro in quanto non attiva alcuna

rigenerazione delle chiavi.