Risoluzione dei problemi comuni di GETVPN

Sommario

Introduzione

Questo documento descrive i debug da raccogliere per la maggior parte dei problemi comuni relativi alla VPN con crittografia di gruppo (GETVPN).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GETVPN
- Utilizzo server Syslog

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Informazioni generali - Strumenti di risoluzione dei problemi GETVPN

GETVPN fornisce un'ampia gamma di strumenti di risoluzione dei problemi per semplificare il processo di risoluzione. È importante capire quale di questi strumenti è disponibile e quando sono appropriati per ogni attività di risoluzione dei problemi. Quando si esegue la risoluzione dei problemi, è sempre consigliabile iniziare con i metodi meno intrusivi, in modo che l'ambiente di produzione non subisca un impatto negativo. Per agevolare questo processo, questa sezione descrive alcuni degli strumenti più comunemente utilizzati disponibili:

Strumenti di debug Control Plane

Comandi show

I comandi show vengono in genere utilizzati per visualizzare le operazioni di runtime in un ambiente GETVPN.

Syslog

GETVPN dispone di un set avanzato di messaggi syslog per eventi di protocollo e condizioni di errore significativi. Questa deve essere sempre la prima posizione in cui controllare prima di eseguire i debug.

Traccia eventi GDOI (Group Domain of Interpretation)

Questa funzione è stata aggiunta nella versione 15.1(3)T. La funzione Event Tracing offre una funzione di trace leggero e sempre attiva per eventi ed errori GDOI significativi. È inoltre disponibile la traccia del percorso di uscita con il traceback abilitato per le condizioni di eccezione.

Debug condizionali GDOI

Questa funzione è stata aggiunta nella versione 15.1(3)T. Consente i debug filtrati per un determinato dispositivo in base all'indirizzo peer e deve essere sempre utilizzato quando possibile, soprattutto sul server principale.

Debug globali di GDOI e crittografia

Questi sono tutti i vari debug GETVPM. Gli amministratori devono prestare attenzione quando eseguono il debug in ambienti su larga scala. Con i debug GDOI, vengono forniti cinque livelli di debug per un'ulteriore granularità del debug:

```
GM1#debug crypto gdoi gm rekey ?
all-levels All levels
detail Detail level
error Error level
event Event level
packet Packet level
terse Terse level
```

Livello di debug	Informazioni
Errore	Condizioni di errore
Termine	Messaggi importanti per l'utente e problemi di

	protocollo
Evento	Transizioni di stato ed eventi quali l'invio e la ricezione di chiavi di nuovo
Dettaglio	Informazioni più dettagliate sui messaggi di debug
Pacchetto	Include il dump delle informazioni dettagliate sul pacchetto
Tutto	Tutte le opzioni precedenti

Strumenti di debug di Data Plane

Di seguito sono riportati alcuni strumenti di debug del piano dati:

- Elenchi di accesso
- Accounting IP Precedence
- NetFlow
- Contatori interfaccia
- Contatori crittografia
- Contatori globali e per singola funzione di eliminazione IP Cisco Express Forwarding (CEF)
- EPC (Embedded Packet Capture)
- Debug del piano dati (debug di pacchetti IP e CEF)

Risoluzione dei problemi

Preparazione della funzione di registrazione e altre best practice

Prima di iniziare la risoluzione dei problemi, assicurarsi di aver preparato la funzione di registrazione come descritto di seguito. Di seguito sono elencate alcune procedure ottimali:

- Controllare la quantità di memoria disponibile sul router e configurare il **debug con buffer di registrazione** su un valore elevato (10 MB o più, se possibile).
- Disabilita la registrazione nei server console, monitor e syslog.
- Recuperare il contenuto del buffer di registrazione con il comando **show log** a intervalli regolari, da 20 minuti a un'ora, per evitare la perdita del log dovuta al riutilizzo del buffer.
- In ogni caso, immettere il comando **show tech** dai membri del gruppo (GM) e dai server chiave (KS) interessati, quindi esaminare l'output del comando **show ip route** in modalità globale e in ogni VRF (Virtual Routing and Forwarding) interessato, se necessario.

- Utilizzare il protocollo NTP (Network Time Protocol) per sincronizzare l'orologio tra tutti i dispositivi sottoposti a debug. Abilita timestamp in millisecondi (msec) per messaggi di debug e di registro:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- Accertarsi che gli output del comando show abbiano un timestamp.

```
Router#terminal exec prompt timestamp
```

- Quando si raccolgono gli output del comando show per gli eventi del piano di controllo o i contatori del piano dati, si raccolgono sempre più iterazioni dello stesso output.

Risoluzione dei problemi relativi a Definizione IKE

Quando il processo di registrazione inizia per la prima volta, gli GM e i KS negoziano le sessioni IKE (Internet Key Exchange) per proteggere il traffico GDOI.

- Sul GM, verificare che IKE sia stato stabilito correttamente:

```
gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.9 172.16.1.1 GDOI_REKEY 1068 ACTIVE
172.16.1.1 172.16.1.9 GDOI_IDLE 1067 ACTIVE
```

Nota: Lo stato GDOI_IDLE, che è la base della registrazione, scade rapidamente e scompare, perché non è più necessario dopo la registrazione iniziale.

- Sul KS, dovrebbe vedere:

```
ks1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.1 172.16.1.9 GDOI_IDLE 1001 ACTIVE
```

Nota: La sessione di reimpostazione delle chiavi viene visualizzata solo quando necessario sul KS.

Se non si raggiunge tale stato, completare i seguenti passaggi:

- Per informazioni dettagliate sulla causa dell'errore, controllare l'output di questo comando:
  `router# show crypto isakmp statistics`
- Se il passaggio precedente non è utile, è possibile ottenere informazioni dettagliate a livello di protocollo se si abilitano i consueti debug IKE:
  `router# debug crypto isakmp`

Note:
* Anche se viene utilizzato IKE, non viene utilizzato sulla porta UDP/500 standard, bensì su UDP/848.
* Se si verifica un problema a questo livello, fornire i debug sia per KS che per GM interessato.

- A causa della dipendenza dalle firme RSA (Rivest-Shamir-Adleman) per le chiavi di gruppo, l'KS **deve avere** una chiave RSA configurata e deve avere lo stesso nome di quello specificato nella configurazione del gruppo.

  Per verificare questa condizione, immettere questo comando:

```
ks1# show crypto key mypubkey rsa
```

Risoluzione dei problemi relativi alla registrazione iniziale

Per verificare lo stato della registrazione, esaminare l'output di questo comando sull'unità di gestione GM:

```
gm1# show crypto gdoi | i Registration status
Registration status  : Registered
gm1#
```

Se l'output indica un valore diverso da **Registered**, immettere i seguenti comandi:

Per quanto riguarda gli OGM:

- Arrestare le interfacce abilitate per la crittografia.
  Attenzione: È previsto che la gestione fuori banda sia abilitata.

- Abilita questi debug:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
```

- Abilitare i debug sul lato KS (vedere la sezione successiva).

- Quando i debug KS sono pronti, sbloccare le interfacce abilitate per la crittografia e attendere la registrazione (per accelerare il processo, usare il comando **clear crypto gdoi** sul GM).

Sui KS:

- Verificare la presenza della chiave RSA sul servizio KS:

```
ks1# show crypto key mypubkey rsa
```

- Abilita questi debug:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
```

Risoluzione dei problemi correlati ai criteri

Problema di criteri prima della registrazione (correlato al criterio di chiusura errori)

Questo problema riguarda solo gli OGM, quindi raccogliete questo output dall'GM:

```
gm1# show crypto ruleset
```

> **Nota:** In Cisco IOS-XE?, questo output è sempre vuoto perché la classificazione dei pacchetti non viene effettuata nel software.

L'output del comando **show tech** restituito dal dispositivo interessato restituisce le altre informazioni richieste.

Il problema relativo al criterio si verifica dopo la registrazione e riguarda il criterio globale sottoposto a push

Il problema si manifesta in genere in due modi:

- Il KS non può spingere le politiche verso il GM.
- Tale politica è applicata parzialmente tra gli OGM.

Per risolvere uno dei problemi, attenersi alla seguente procedura:

1. Sull'GM interessato, raccogliere questo output:

```
gm1# show crypto gdoi acl
gm1# show crypto ruleset
```

2. Abilita questi debug su GM:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm acls packet
```

3. Nel KS in cui il GM interessato si registra, raccogliere questo output:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks policy
```

Nota: Per identificare a quale KS si connette il GM, immettere il comando **show crypto gdoi group**.

4. Sullo stesso KS, abilitare i seguenti debug:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks acls packet
```

5. Obbligare l'oggetto GM a eseguire la registrazione con questo comando sull'oggetto GM:

```
clear crypto gdoi
```

Il problema relativo ai criteri si verifica dopo la registrazione e riguarda l'unione dei criteri globali e delle sostituzioni locali

Questo problema si presenta in genere sotto forma di messaggi che indicano che è stato ricevuto un pacchetto crittografato per il quale i criteri locali indicano che non deve essere crittografato e viceversa. In questo caso, è necessario usare tutti i dati richiesti nella sezione precedente e l'output del comando **show tech**.

Risoluzione dei problemi di reimpostazione chiavi

Per quanto riguarda gli OGM:

- Raccogli i seguenti debug:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- Immettere questo comando per verificare che il GM disponga ancora di un'associazione di sicurezza IKE (SA) di tipo GDOI_REKEY:

```
gm1# show crypto isakmp sa
```

Sui KS:

- Raccogliere l'output del comando **show crypto key mypubkey rsa** da **EACH** KS. Le chiavi dovrebbero essere **identiche**.

- Immettere questi debug per visualizzare ciò che accade sul KS:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

Risoluzione dei problemi di anti-replay con limiti di tempo (TBAR)

La funzione TBAR richiede la conservazione del tempo tra i gruppi, e quindi richiede la costante risincronizzazione degli orologi pseudo-temporali di GM. Questa operazione viene eseguita durante la reimpostazione delle chiavi o ogni due ore, a seconda della condizione che si verifica per prima.

> **Nota:** Tutti gli output e i debug devono essere raccolti contemporaneamente da GM e KS in modo da poter essere correlati in modo appropriato.

Per analizzare i problemi che si verificano a questo livello, raccogliere questo output.

- Per quanto riguarda gli OGM:

```
gm1# show crypto gdoi
gm1# show crypto gdoi replay
```

- Nel KS:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks replay
```

Per analizzare in modo più dinamico il mantenimento del tempo di TBAR, abilitare i seguenti debug:

- Per quanto riguarda l'GM:

```
gm1# debug crypto gdoi gm rekey packet
gm1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

- Nel KS:

```
ks1# debug crypto gdoi ks rekey packet
ks1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

A partire dalla versione 15.2(3)T di Cisco IOS, è stata aggiunta la possibilità di registrare gli errori TBAR, che rende più facile individuare questi errori. Sull'utilità GM, utilizzare questo comando per verificare se sono presenti errori TBAR:

```
R103-GM#show crypto gdoi gm replay
Anti-replay Information For Group GETVPN:
```

```
 Timebased Replay:
   Replay Value             : 512.11 secs
   Input Packets            : 0        Output Packets           : 0
   Input Error Packets    : 0        Output Error Packets   : 0
   Time Sync Error         : 0        Max time delta            : 0.00secs

TBAR Error History (sampled at 10pak/min):
   No TBAR errors detected
```

Per ulteriori informazioni su come risolvere i problemi relativi alla barra degli strumenti, consultare il documento sull'errore dell'anti-replay basato sul tempo.

Risoluzione dei problemi di ridondanza KS

La cooperativa (COOP) stabilisce una sessione IKE per proteggere la comunicazione tra KS, quindi la tecnica di risoluzione dei problemi descritta in precedenza per la creazione di IKE è applicabile anche in questo caso.

La risoluzione dei problemi specifica della COOP comprende controlli dell'output di questo comando su tutti i KS coinvolti:

```
ks# show crypto gdoi ks coop
```

> **Nota:** L'errore più comune fatto con l'installazione di COOP KS è quello di dimenticare di importare la stessa chiave RSA (sia privata che pubblica) per il gruppo su tutti i KS. Ciò causa problemi durante la reimpostazione delle chiavi. Per controllare e confrontare le chiavi pubbliche tra i KS, confrontare l'output del comando **show crypto key mypubkey rsa** restituito da ciascun KS.

Se è richiesta la risoluzione dei problemi a livello di protocollo, abilitare il debug su tutti i KS coinvolti:

```
ks# debug crypto gdoi ks coop packet
```

Domande frequenti

Perché viene visualizzato il messaggio di errore "% Setting rekey authentication jected" (Impostazione dell'autenticazione della chiave rifiutata)?

Questo messaggio di errore viene visualizzato quando si configura il KS dopo l'aggiunta della riga:

```
KS(gdoi-local-server)#rekey authentication mypubkey rsa GETVPN_KEYS
% Setting rekey authentication rejected.
```

Questo messaggio di errore viene in genere visualizzato perché la chiave con etichetta GETVPN_KEYS non esiste. Per risolvere questo problema, creare una chiave con l'etichetta corretta utilizzando il comando:

```
crypto key generate rsa mod <modulus> label <label_name>
```

> **Nota:** Aggiungere la parola chiave exportable alla fine se si tratta di una distribuzione COOP, quindi importare la stessa chiave nell'altro KS

Un router configurato come KS per un gruppo GETVPN può funzionare anche come GM per lo stesso gruppo?

No. Tutte le distribuzioni GETVPN richiedono un KS dedicato che non può partecipare come GM per gli stessi gruppi. Questa funzione non è supportata, perché l'aggiunta di funzionalità GM a KS con tutte le possibili interazioni come crittografia, routing, QoS, ecc., non è ottimale per lo stato di questo dispositivo di rete cruciale. Deve essere sempre disponibile affinché l'intera distribuzione GETVPN funzioni.

Informazioni correlate

- Group Encrypted Transport VPN (GET VPN) - Cisco Systems
- Documentazione e supporto tecnico – Cisco Systems