Fehlerbehebung bei häufigen GETVPN-Problemen

Inhalt

Einführung

In diesem Dokument wird beschrieben, welche Debug-Daten für die meisten häufigen GETVPN-

Probleme (Group Encrypted Transport VPN) gesammelt werden müssen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- GETVPN
- Syslog-Serververwendung

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen - GETVPN-Tools zur Fehlerbehebung

GETVPN bietet eine umfangreiche Auswahl an Tools zur Fehlerbehebung, um die Fehlerbehebung zu vereinfachen. Es ist wichtig zu verstehen, welche dieser Tools verfügbar sind und wann sie für jede Fehlerbehebungsaufgabe geeignet sind. Bei der Fehlerbehebung ist es immer ratsam, mit den geringstmöglichen Eingriffen zu beginnen, damit die Produktionsumgebung nicht negativ beeinflusst wird. Um diesen Prozess zu unterstützen, werden in diesem Abschnitt einige der gebräuchlichsten verfügbaren Tools beschrieben:

Debugtools für die Kontrollebene

Befehle anzeigen

Befehlszeilenbefehle werden häufig verwendet, um Laufzeitoperationen in einer GETVPN-Umgebung anzuzeigen.

Syslogs

GETVPN verfügt über eine erweiterte Reihe von Syslog-Meldungen für wichtige Protokollereignisse und Fehlerzustände. Dies sollte immer der erste Ort sein, der vor dem Ausführen von Debuggen gesucht wird.

Group Domain of Interpretation (GDOI) Event Trace

Diese Funktion wurde in Version 15.1(3)T hinzugefügt. Die Ereignisablaufverfolgung bietet leichte, stets verfügbare Ablaufverfolgung für erhebliche GDOI-Ereignisse und -Fehler. Es gibt auch Exit-Path-Ablaufverfolgung, bei der die Ablaufverfolgung für Ausnahmebedingungen aktiviert ist.

Bedingtes GDOI-Debuggen

Diese Funktion wurde in Version 15.1(3)T hinzugefügt. Es ermöglicht gefilterte Debugging für ein bestimmtes Gerät basierend auf der Peer-Adresse und sollte immer verwendet werden, wenn möglich, insbesondere auf dem Key-Server.

Globale Krypto- und GDOI-Debugger

Dies sind die verschiedenen GETVPM-Debugger. Administratoren müssen beim Debuggen in großen Umgebungen vorsichtig sein. Bei GDOI-Debuggen werden fünf Debug-Ebenen bereitgestellt, um die Detailgenauigkeit des Debuggens zu erhöhen:

```
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
```

Debug-	Ihre Vorteile

Ebene	
Fehler	Fehlerbedingungen
Kurz	Wichtige Mitteilungen an Benutzer- und Protokollprobleme
Veranstaltung	Zustandsübergänge und Ereignisse wie Senden und Empfangen von Neuschlüsseln
Details	Ausführlichste Informationen zu Debugmeldungen
Paket	Beinhaltet Dump von detaillierten Paketinformationen
Alle	Alle oben genannten Optionen

Debugtools für die Datenebene

Hier sind einige Debugtools für die Datenebene:

- Zugriffslisten
- IP Precedence Accounting
- NetFlow
- Schnittstellenzähler
- Krypto-Zähler
- Globale IP Cisco Express Forwarding (CEF)- und Funktionsabbruchzähler
- Embedded Packet Capture (EPC)
- Debugs auf Datenebene (IP-Paket- und CEF-Debugger)

Fehlerbehebung

Vorbereitung der Protokollierungseinrichtung und andere Best Practices

Bevor Sie mit der Fehlerbehebung beginnen, stellen Sie sicher, dass Sie die Protokollierungseinrichtung wie hier beschrieben vorbereitet haben. Einige Best Practices finden Sie auch hier:

- Prüfen Sie die Menge des freien Arbeitsspeichers des Routers, und konfigurieren Sie die **Protokollierung des gepufferten Debuggens** auf einen großen Wert (10 MB oder mehr, wenn möglich).

- Deaktivieren Sie die Protokollierung für die Konsolen-, Monitor- und Syslog-Server.

- Rufen Sie den Inhalt des Protokollierungspuffers mit dem Befehl **show log** in regelmäßigen Abständen alle 20 Minuten bis eine Stunde ab, um Protokollverluste aufgrund der

Wiederverwendung des Puffers zu vermeiden.

- Geben Sie in jedem Fall den Befehl **show tech** von betroffenen Gruppenmitgliedern (GMs) und Schlüsselservern (KSs) ein, und überprüfen Sie die Ausgabe des Befehls **show ip route** in global und jeder beteiligten Virtual Routing and Forwarding (VRF), falls erforderlich.

- Verwenden Sie das Network Time Protocol (NTP), um die Uhr zwischen allen debuggten Geräten zu synchronisieren. Aktivieren von Millisekunde-Zeitstempeln für Debug- und Protokollmeldungen:

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

- Stellen Sie sicher, dass die Ausgaben des Befehls show mit einem Zeitstempel versehen sind.

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

- Wenn Sie Befehlsausgaben für Ereignisse auf der Kontrollebene oder für Datenebenenindikatoren erfassen, sammeln Sie immer mehrere Iterationen derselben Ausgabe.

Fehlerbehebung bei IKE-Einrichtung

Wenn der Registrierungsvorgang zum ersten Mal beginnt, handeln GMs und KSs Internetschlüssel-Exchange-Sitzungen (IKE) aus, um den GDOI-Datenverkehr zu schützen.

- Überprüfen Sie auf der GM, ob IKE erfolgreich eingerichtet wurde:

```
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
```

Hinweis: Der GDOI_IDLE-Status, der die Basis der Registrierung ist, überschreitet schnell und verschwindet, da er nach der Erstregistrierung nicht mehr benötigt wird.

- Im KS-Fenster sollten Sie Folgendes sehen:

```
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
```

Hinweis: Die Tastatursitzung wird nur angezeigt, wenn sie auf dem KS benötigt wird.

Gehen Sie wie folgt vor, wenn Sie diesen Zustand nicht erreichen:

- Informationen zur Fehlerursache finden Sie in der Ausgabe dieses Befehls:
  ```
  router# show crypto isakmp statistics
  ```
- Wenn der vorherige Schritt nicht hilfreich ist, können Sie Einblicke auf Protokollebene erhalten, wenn Sie die üblichen IKE-Debugger aktivieren:
  ```
  router# debug crypto isakmp
  ```
  Hinweise:
  * Obwohl IKE verwendet wird, wird es nicht auf dem üblichen UDP/500-Port, sondern auf UDP/848 verwendet.
  * Wenn auf dieser Ebene ein Problem auftritt, geben Sie die Debug für KS und die betroffene GM an.

- Aufgrund der Abhängigkeit von Rivest-Shamir-Adleman (RSA) Signs für die Gruppenschlüssel **muss** der KS einen RSA-Schlüssel konfiguriert **haben** und den gleichen Namen wie der in der Gruppenkonfiguration angegebene haben.

  Geben Sie den folgenden Befehl ein, um dies zu überprüfen:

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

Fehlerbehebung bei der Erstregistrierung

Auf der GM-Seite überprüfen Sie zur Überprüfung des Registrierungsstatus die Ausgabe dieses Befehls:

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

Wenn die Ausgabe andere als **Registrierte** Elemente anzeigt, geben Sie die folgenden Befehle ein:

Zu den GMs:

- Schließen Sie kryptoaktivierte Schnittstellen.
  Vorsicht: Es wird erwartet, dass die Out-of-Band-Verwaltung aktiviert ist.

- Aktivieren Sie diese Debugger:

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

- Aktivieren Sie Debugging auf KS-Seite (siehe nächster Abschnitt).

- Wenn die KS-Debug fertig sind, deaktivieren Sie kryptoaktivierte Schnittstellen, und warten

Sie auf die Registrierung (um den Prozess zu beschleunigen, geben Sie den Befehl **clear crypto gdoi** auf dem GM).

Für KS:

- Überprüfen Sie, ob der RSA-Schlüssel auf dem KS vorhanden ist:

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

- Aktivieren Sie diese Debugger:

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

Fehlerbehebung bei richtlinienbezogenen Problemen

Richtlinienproblem tritt VOR der Registrierung auf (im Zusammenhang mit Richtlinie zum fehlgeschlagenen Abschluss)

Dieses Problem betrifft nur GMs. Sammeln Sie also diese Ausgabe von der GM:

```
gm1# show crypto ruleset
```

> **Hinweis**: In Cisco IOS-XE? ist diese Ausgabe immer leer, da die Paketklassifizierung in der Software nicht erfolgt.

Die Ausgabe des Befehls **show tech** vom betroffenen Gerät enthält die übrigen erforderlichen Informationen.

Das Richtlinienproblem tritt nach der Registrierung auf und bezieht sich auf die globale Richtlinie, die überlastet wird.

Dieses Problem kann in der Regel auf zwei Arten auftreten:

- Die KS kann die Richtlinien nicht an die GM übertragen.
- Die Politik wird teilweise auf die GM angewandt.

Gehen Sie wie folgt vor, um bei der Fehlerbehebung zu helfen:

1. Erfassen Sie auf dem betroffenen GM diese Ausgabe:

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

2. Aktivieren Sie diese Debugging-Optionen auf GM:

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

3. Auf den KS, bei denen die betroffene GM registriert, wird diese Ausgabe erfasst:

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

   Hinweis: Geben Sie den Befehl **show crypto gdoi group** ein, um zu ermitteln, mit welchem KS die GM verbunden ist.

4. Aktivieren Sie auf demselben KS die folgenden Debugging-Optionen:

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

5. Erzwingen Sie die Registrierung des GM mit diesem Befehl für GM:

```
clear crypto gdoi
```

Das Richtlinienproblem tritt nach der Registrierung auf und bezieht sich auf die Zusammenführung globaler Richtlinien und lokaler Überschreibungen.

Dieses Problem manifestiert sich in der Regel in Form von Nachrichten, die darauf hinweisen, dass ein verschlüsseltes Paket empfangen wurde, für das die lokalen Richtlinien angeben, dass es nicht verschlüsselt werden soll, und umgekehrt. Alle im vorherigen Abschnitt angeforderten Daten sowie die Ausgabe des Befehls **show tech** sind in diesem Fall erforderlich.

Fehlerbehebung bei Neuschlüsselproblemen

Zu den GMs:

- Sammeln Sie diese Debugger:

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

- Geben Sie diesen Befehl ein, um zu überprüfen, ob der GM noch über eine IKE Security Association (SA) vom Typ GDOI_REKEY verfügt:

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

Für KS:

- Sammeln Sie die Ausgabe des Befehls **show crypto key mypubkey rsa** von **EACH** KS. Es wird erwartet, dass die Schlüssel **identisch** sind.

- Geben Sie diese Debugger ein, um anzuzeigen, was auf dem KS geschieht:

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

Fehlerbehebung zeitbasiertes Anti-Replay (TBAR)

Die TBAR-Funktion erfordert eine gruppenübergreifende Zeiterfassung. Daher müssen die GMs Pseudo-Time-Uhren fortlaufend neu synchronisiert werden. Dies wird während des Rekurses oder alle zwei Stunden durchgeführt, je nachdem, was zuerst kommt.

> **Hinweis**: Alle Ausgaben und Debugging müssen gleichzeitig von GM und KS erfasst werden, damit sie entsprechend korreliert werden können.

Um Probleme zu untersuchen, die auf dieser Ebene auftreten, sammeln Sie diese Ausgabe.

- Zu den GMs:

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

- Auf KS:

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

Um die TBAR-Zeiterfassung dynamischer zu untersuchen, aktivieren Sie folgende Debugging-Optionen:

- GM:

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

- Auf KS:

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

Seit Cisco IOS Version 15.2(3)T können nun auch noch TBAR-Fehler aufgezeichnet werden, wodurch sich diese Fehler leichter erkennen lassen. Verwenden Sie für GM diesen Befehl, um zu überprüfen, ob TBAR-Fehler vorliegen:

```
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
```

Weitere Informationen zur Behebung von TBAR-Problemen finden Sie unter Zeitbasierter Anti-Replay-Fehler.

Fehlerbehebung: KS-Redundanz

Cooperative (COOP) richtet eine IKE-Sitzung ein, um die Kommunikation zwischen KSs zu schützen. Die zuvor für IKE-Einrichtung beschriebene Fehlerbehebungstechnik ist daher auch hier anwendbar.

Die COOP-spezifische Fehlerbehebung umfasst die Ausgabekontrollen dieses Befehls für alle beteiligten KSs:

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

> **Hinweis**: Der häufigste Fehler bei der Bereitstellung von COOP KSs ist zu vergessen, den gleichen RSA-Schlüssel (sowohl privat und öffentlich) für die Gruppe auf allen KSs zu importieren. Dies verursacht Probleme bei Neuschlüsseln. Um öffentliche Schlüssel zwischen KSs zu überprüfen und zu vergleichen, vergleichen Sie die Ausgabe des **show crypto key mypubkey rsa** Befehl von jedem KS.

Wenn eine Fehlerbehebung auf Protokollebene erforderlich ist, aktivieren Sie dieses Debugging auf allen beteiligten KS:

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

Häufig gestellte Fragen

Warum sehen Sie die Fehlermeldung "% Setting rekey authentication abgelehnte"?

Sie sehen diese Fehlermeldung, wenn Sie das KS konfigurieren, nachdem diese Zeile hinzugefügt wurde:

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

Der Grund für diese Fehlermeldung ist in der Regel, weil der Schlüssel mit der Bezeichnung GETVPN_KEYS nicht vorhanden ist. Um dies zu beheben, erstellen Sie mit dem folgenden Befehl einen Schlüssel mit der richtigen Bezeichnung:

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

> **Hinweis**: Fügen Sie am Ende das exportfähige Schlüsselwort hinzu, wenn es sich um eine COOP-Bereitstellung handelt, und importieren Sie dann den gleichen Schlüssel in den anderen KS.

Kann ein als KS konfigurierter Router für eine GETVPN-Gruppe auch als GM für dieselbe Gruppe fungieren?

Nein. Für alle GETVPN-Bereitstellungen ist ein dediziertes KS erforderlich, das nicht als GM für dieselben Gruppen teilnehmen kann. Diese Funktion wird nicht unterstützt, da das Hinzufügen von GM-Funktionen zu KS mit allen möglichen Interaktionen wie Verschlüsselung, Routing, QoS usw. für den Zustand dieses wichtigen Netzwerkgeräts nicht optimal ist. Sie muss jederzeit verfügbar sein, damit die gesamte GETVPN-Bereitstellung funktioniert.

Zugehörige Informationen

- Group Encrypted Transport VPN (GET VPN) - Cisco Systems
- Technischer Support und Dokumentation - Cisco Systems