Probleemoplossing voor gemeenschappelijke problemen met VPN

Inhoud

Inleiding

Dit document beschrijft welke gegevens u moet verzamelen voor de meeste gebruikelijke Group Encrypted Transport VPN (GETVPN)-problemen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- GETVPN
- SLB: servergebruik

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Background-informatie - GETVPN-tools voor probleemoplossing

GETVPN biedt een uitgebreide reeks gereedschappen voor het oplossen van problemen om het proces van probleemoplossing te vergemakkelijken. Het is belangrijk om te begrijpen welke van deze gereedschappen beschikbaar zijn en wanneer ze geschikt zijn voor elke taak om een oplossing te vinden. Wanneer u problemen oplost, is het altijd een goed idee om met de minste opdringerige methoden te beginnen, zodat de productieomgeving niet negatief wordt beïnvloed. Om dit proces te ondersteunen, wordt in dit gedeelte een aantal van de meest gebruikte gereedschappen beschreven:

Debugging-tools van het besturingsplane

Opdrachten weergeven

Opdrachten tonen wordt vaak gebruikt om uitvoering in een GETVPN-omgeving weer te geven.

Syslogs

GETVPN heeft een uitgebreide reeks syslig-berichten voor belangrijke protocolgebeurtenissen en foutvoorwaarden. Dit moet altijd de eerste plaats zijn om te kijken voor je een debugs runt.

Group Domain of Interpretation (GDOI)-Event Trace

Deze optie is toegevoegd in versie 15.1(3)T. Event Tracering biedt lichtgewicht, altijd-on tracering voor belangrijke GDOI-gebeurtenissen en fouten. Er is ook exit-path-tracering die is ingeschakeld voor uitzonderingen.

GDOI-voorwaardelijke uitwerpselen

Deze optie is toegevoegd in versie 15.1(3)T. Hiermee kunnen gefilterde debugs voor een bepaald apparaat worden gegenereerd op basis van het peer-adres. Deze debugs moeten altijd indien mogelijk worden gebruikt, met name op Key Server.

Wereldwijde encryptie en GDOI-uitvindingen

Dit zijn de verschillende GETVPM-debugs. Admins moeten voorzichtigheid gebruiken wanneer het fouilleren in grootschalige omgevingen. Met GDOI debugs worden er vijf debug-niveaus geboden voor verdere debugger granularity:

```
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 Level	Wat u krijgt
Fout	Foutvoorwaarden
Terse	Belangrijke berichten voor de gebruikers- en

	protocolproblemen
gebeurtenis	Overgang van de staat en gebeurtenissen zoals verzenden en ontvangen
Detail	Populairste gedetailleerde informatie over bestanden
Packet	Omvat het dumpen van gedetailleerde pakketinformatie
Alle	Alle bovenstaande punten

Configuratietools van datacenters

Hier zijn een paar gereedschappen voor het fouilleren van datacenters:

- Toegangslijsten
- IP-prioriteitsaccounting
- NetFlow
- Interfacetellers
- Crypto-tellers
- IP Cisco Express Forwarding (CEF) wereldwijde en Drop Per-optie tellers
- Ingesloten pakketvastlegging (EPC)
- Debugs van datacenters (IP-pakketten en CEF-debugs)

Problemen oplossen

Voorbereiding van de opslagfaciliteit en andere beste praktijken

Voordat u begint met het oplossen van problemen, zorg er dan voor dat u de loginstallatie hebt voorbereid zoals hier beschreven. Hieronder worden ook een aantal optimale werkwijzen genoemd:

- Controleer de routerhoeveelheid vrij geheugen en stel de **houtkap** op **gebufferd** voor **het foutoptreden** tot een grote waarde (10 MB of meer indien mogelijk).
- Uitschakelen van loggen op de console-, monitor- en syslogservers.
- Retourneert de houtbufferinhoud met de opdracht log **tonen**, met regelmatige tussenpozen, elke 20 minuten tot een uur, om logverlies door hergebruik van de buffer te voorkomen.
- Wat er ook gebeurt, voer het **show tech** commando van de getroffen groepsleden (GM's) en Key Server (KSs) in en onderzoek de output van de **show ip route** opdracht in mondiaal en

elke Virtual Routing and Forwarding (VRF) indien nodig.

- Gebruik Network Time Protocol (NTP) om de kloktijd te synchroniseren tussen alle apparaten die worden gezuiverd. Tijd van milliseconde (msec) toe te passen voor zowel debug- als logberichten:

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

- Zorg ervoor dat de opdrachtoutput voorzien is van een tijdstempel.

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

- Wanneer u showcommando outputs verzamelt voor besturingsplangebeurtenissen of tellers van het gegevensvliegtuig, verzamelt u altijd meerdere iteraties van dezelfde output.

IKE-instelling voor probleemoplossing

Wanneer het registratieproces voor het eerst begint, onderhandelen GM's en KS's over IKE-sessies (Internet Key Exchange) om het GDOI-verkeer te beschermen.

- Controleer bij de GM of IKE met succes is opgericht:

```
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
```

  Opmerking: De GDOI_IDLE staat, die de basis van de registratie is, verliest snel en verdwijnt, omdat hij niet meer nodig is na de eerste registratie.

- Op de KS moet je zien:

```
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
```

  Opmerking: De rekey sessie verschijnt alleen wanneer het nodig is op de KS.

Voltooi deze stappen als u deze status niet heeft bereikt:

- Voor inzicht in de oorzaak van de mislukking, controleer de uitvoer van deze opdracht:
  `router# show crypto isakmp statistics`
- Als de vorige stap niet behulpzaam is, kunt u protocolniveau inzichten krijgen als u de gebruikelijke IKE-signalen activeert:

```
router# debug crypto isakmp
```

Opmerkingen:
* Hoewel IKE wordt gebruikt, wordt hij niet gebruikt op de normale UDP/500-poort, maar eerder op UDP/848.
* Als u op dit niveau een probleem ondervindt, geef dan de uitwerpselen voor zowel KS als het getroffen GM.

- Vanwege de afhankelijkheid van Rivest-Shamir-Adleman (RSA)-signalen voor de groepsschermen **moeten** de KS een RSA-toets **hebben** geconfigureerd en moet zij dezelfde naam hebben als die in de groepsconfiguratie is gespecificeerd.

  Typ deze opdracht om dit te controleren:

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

Probleemoplossing voor eerste registratie

Kijk in het GM-menu om de registratiestatus te controleren op de uitvoer van deze opdracht:

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

Als de uitvoer iets anders dan **geregistreerd** aangeeft, voert u deze opdrachten in:

Over de genetisch gemodificeerde organismen:

- Sluit crypto-enabled interfaces af.
  Voorzichtig: Verwacht wordt dat out-of-band beheer is ingeschakeld.

- Schakel deze apparaten in:

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

- Schakel debugs aan de kant KS in (zie het volgende gedeelte).

- Wanneer de KS-debugs klaar zijn, crypto-enabled interfaces niet sluiten en op registratie wachten (om het proces te versnellen, geeft u de **duidelijke** opdracht van de **crypto** gdoi op het GM uit).

Aan de KS:

- Controleer de aanwezigheid van de RSA-toets op de KS:

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

- Schakel deze apparaten in:

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

Problemen oplossen

Beleidskwesties doen zich voor vóór de registratie (gerelateerd aan beleid dat failliet gaat)

Dit probleem heeft alleen gevolgen voor GG's. U verzamelt deze producten van het GGM:

```
gm1# show crypto ruleset
```

> Opmerking: In Cisco IOS-XE? is deze uitvoer altijd leeg sinds de pakketclassificatie niet in de software uitgevoerd.

De uitvoer van de technische opdracht van het getroffen apparaat levert de rest van de vereiste informatie op.

Beleidsvraagstuk treedt op na de registratie en houdt verband met het beleid dat wordt doorgevoerd

Er zijn meestal twee manieren waarop dit probleem zich manifesteert:

- De KS kan het beleid niet tot de GM doordrukken.
- Het beleid wordt gedeeltelijk toegepast bij de GV's.

Voltooi de volgende stappen om een probleem op te lossen:

1. Verzamel deze uitvoer voor de beïnvloede GM:

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

2. Schakel deze uitwerpselen op GM in:

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

3. Verzamel op de KS waarop de getroffen GM zich registreert deze productie:

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

Opmerking: Om te identificeren op welke KS de GM is aangesloten, dient u de opdracht van de **showcrypto godgroep** in.

4. Zet deze debugs in op dezelfde KS:

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

5. Dwing de GM om zich met deze opdracht te registreren op de GM:

```
clear crypto gdoi
```

Beleidsvraagstuk treedt op na de registratie en houdt verband met de samenvoeging van mondiaal beleid en lokale overzichten

Deze kwestie manifesteert zich meestal in de vorm van berichten die erop wijzen dat een gecodeerd pakket werd ontvangen waarvoor het lokale beleid aangeeft dat het niet versleuteld zou moeten worden en omgekeerd. Alle in de vorige sectie gevraagde gegevens en de uitvoer van de **show tech-**opdracht zijn in dit geval vereist.

Probleemoplossing problemen oplossen

Over de genetisch gemodificeerde organismen:

- Verzamel deze uitwerpselen:

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

- Voer deze opdracht in om te controleren of het GM nog steeds een IKE Security Association (SA) van het type GDOI_REKEY heeft:

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

Aan de KS:

- Verzamel de **show crypto key mypubkey rsa** opdracht output van **ELKE** KS. Men verwacht dat

de toetsen **identiek** zullen zijn.

- Voer deze debugs in om te bekijken wat er op de KS voorkomt:

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

Probleemoplossing op basis van antireplay (TBAR)

De TBAR-functie vereist dat de tijd tussen de groepen wordt gehouden en dat de pseudo-tijdklokken van de GGM's constant worden gesynchroniseerd. Dit wordt uitgevoerd tijdens rekey of elke twee uur, indien dit eerder is.

> Opmerking: Alle productie- en debugs moeten tegelijkertijd van zowel GG's als KS worden verzameld, zodat ze op een passende wijze kunnen worden gecorreleerd.

Om kwesties te onderzoeken die op dit niveau voorkomen, verzamelt u deze output.

- Over de genetisch gemodificeerde organismen:

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

- Op de KS:

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

Om de tijdsduur van TBAR op een dynamischer manier te onderzoeken, moeten deze uitwerpselen mogelijk worden:

- Op het GGM:

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

- Op de KS:

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

Vanaf Cisco IOS versie 15.2(3)T is de mogelijkheid om TBAR-fouten op te nemen toegevoegd, wat het makkelijker maakt om deze fouten te herkennen. Gebruik deze opdracht op de GM om te controleren of er TBAR-fouten zijn:

```
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
```

Raadpleeg voor meer informatie over problemen met TBAR-problemen bij probleemoplossing de op Time-Based Anti-Replay mislukking.

Redundantie van Troubleshooter KS

Coöperatie (COOP) voert een IKE-sessie in om communicatie tussen de KS te beschermen, zodat de probleemoplossingstechniek die eerder beschreven werd voor IKE-inrichting ook hier van toepassing is.

COOP-specifieke probleemoplossing omvat uitvoercontroles van deze opdracht op alle betrokken KS:

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

> Opmerking: De meest voorkomende fout die met de inzet van COOP KSs is gemaakt, is te vergeten dezelfde RSA-toets (zowel privé als openbaar) voor de groep op alle KSs in te voeren. Dit veroorzaakt problemen tijdens rekeys. Om openbare sleutels onder KS's te controleren en te vergelijken, vergelijk de uitvoer van de **show crypto-toets rsa** opdracht van elke KS.

Als een oplossing op protocolniveau vereist is, schakelt u dit debug in op alle betrokken KS:

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

FAQ

Waarom ziet u deze foutmelding "% instelling van rekelijke authenticatie verworpen"?

U ziet deze foutmelding wanneer u de KS configureren nadat deze regel is toegevoegd:

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

De reden voor deze foutmelding is meestal omdat de genummerde toets GETVPN_KEYS niet

bestaat. Om dit te repareren, maakt u een toets met het juiste label aan de hand van de opdracht:

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

> Opmerking: Voeg het uitvoerbare sleutelwoord aan het eind toe als dit een COOP-toepassing is en voer dan dezelfde sleutel in de andere KS in

Kan een router die als KS voor één GETVPN-groep is geconfigureerd ook als GM voor dezelfde groep werken?

Neen. Alle GETVPN-implementaties vereisen een toegewijd KS die niet als GM voor dezelfde groepen kan deelnemen. Deze optie wordt niet ondersteund, omdat het toevoegen van GM-functionaliteit aan KS met alle mogelijke interacties zoals encryptie, routing, QoS, etc. niet optimaal is voor de gezondheid van dit cruciale netwerkapparaat. Het moet te allen tijde beschikbaar zijn voor de volledige inzet van GETVPN om te kunnen werken.

Gerelateerde informatie

- Group Encrypted Transport VPN (Get VPN) - Cisco Systems
- Technische ondersteuning en documentatie – Cisco Systems