Dépannage des problèmes courants de GETVPN

Contenu

Introduction

Ce document décrit les débogages à collecter pour la plupart des problèmes courants de réseau privé virtuel de transport crypté de groupe (GETVPN).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- GETVPN
- Utilisation du serveur Syslog

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales - Outils de dépannage GETVPN

GETVPN fournit un ensemble complet d'outils de dépannage afin de faciliter le processus de dépannage. Il est important de comprendre quels outils sont disponibles et quand ils sont appropriés pour chaque tâche de dépannage. Lors du dépannage, il est toujours judicieux de commencer par les méthodes les moins intrusives, afin que l'environnement de production ne soit pas affecté négativement. Pour faciliter ce processus, cette section décrit certains des outils couramment utilisés disponibles :

Outils de débogage du plan de contrôle

Commandes show

Les commandes show sont couramment utilisées afin d'afficher les opérations d'exécution dans un environnement GETVPN.

SYSLOG

GETVPN dispose d'un ensemble amélioré de messages syslog pour les événements de protocole significatifs et les conditions d'erreur. Ce devrait toujours être le premier endroit à regarder avant d'exécuter n'importe quel débogage.

Suivi des événements GDOI (Group Domain of Interpretation)

Cette fonctionnalité a été ajoutée dans la version 15.1(3)T. Le suivi des événements offre un suivi léger et permanent pour les événements et les erreurs GDOI significatifs. Il existe également un traçage de sortie-path avec la commande traceback activée pour les conditions d'exception.

Débogues conditionnels GDOI

Cette fonctionnalité a été ajoutée dans la version 15.1(3)T. Il autorise les débogages filtrés pour un périphérique donné en fonction de l'adresse de l'homologue, et doit toujours être utilisé lorsque cela est possible, en particulier sur le serveur de clés.

Débogues globaux Crypto et GDOI

Voici tous les différents débogages GETVPM. Les administrateurs doivent être prudents lors du débogage dans des environnements à grande échelle. Avec les débogages GDOI, cinq niveaux de débogage sont fournis pour une granularité de débogage supplémentaire :

```
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
```

Niveau de débogage	Ce que vous obtiendrez
Erreur	Conditions d'erreur
Terme	Messages importants destinés à l'utilisateur et

	problèmes de protocole
Événement	Transitions d'état et événements tels que l'envoi et la réception de clés réutilisables
Détail	Informations détaillées sur le message de débogage
Paquet	Inclut le vidage d'informations détaillées sur les paquets
all	Toutes les réponses ci-dessus

Outils de débogage du plan de données

Voici quelques outils de débogage du plan de données :

- Listes d'accès
- Comptabilité de priorité IP
- Netflow
- Compteurs d’interface
- Compteurs de chiffrement
- Compteurs de transfert global et par fonctionnalité de Cisco Express Forwarding (CEF) IP
- Capture de paquets intégrée (EPC)
- Débogues du plan de données (débogages de paquets IP et CEF)

Dépannage

Préparation des installations de journalisation et autres meilleures pratiques

Avant de commencer le dépannage, assurez-vous d'avoir préparé l'installation de journalisation comme décrit ici. Quelques bonnes pratiques sont également répertoriées ici :

- Vérifiez la quantité de mémoire libre du routeur et configurez le **débogage mis en mémoire tampon de journalisation** à une grande valeur (10 Mo ou plus si possible).
- Désactivez la journalisation sur les serveurs de console, de surveillance et syslog.
- Récupérez le contenu de la mémoire tampon de journalisation à l'aide de la commande **show log** à intervalles réguliers, toutes les 20 minutes à une heure, afin d'empêcher la perte de journal due à la réutilisation de la mémoire tampon.
- Quoi qu'il arrive, entrez la commande **show tech** des membres de groupe affectés (GM) et des serveurs de clés (KS), et examinez le résultat de la commande **show ip route** dans global

et chaque VRF impliqué, le cas échéant.

- Utilisez le protocole NTP (Network Time Protocol) afin de synchroniser l'horloge entre tous les périphériques débogués. Activer les horodatages millisecondes (ms) pour les messages de débogage et de journal :

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

- Assurez-vous que les sorties de la commande show sont horodatées.

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

- Lorsque vous collectez des sorties de commande show pour des événements de plan de contrôle ou des compteurs de plan de données, collectez toujours plusieurs itérations de la même sortie.

Dépannage de l'établissement IKE

Lorsque le processus d'enregistrement commence, les GM et les KS négocient des sessions IKE (Internet Key Exchange) afin de protéger le trafic GDOI.

- Sur le module GM, vérifiez que le protocole IKE est correctement établi :

```
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
```

Note: L'état GDOI_IDLE, qui est la base de l'enregistrement, expire rapidement et disparaît, car il n'est plus nécessaire après l'enregistrement initial.

- Sur le KS, vous devriez voir :

```
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
```

Note: La session rekey n'apparaît que lorsque cela est nécessaire sur le KS.

Complétez ces étapes si vous n'atteignez pas cet état :

- Pour en savoir plus sur la cause de l'échec, consultez le résultat de cette commande : `router# show crypto isakmp statistics`
- Si l'étape précédente n'est pas utile, vous pouvez obtenir des informations au niveau du

protocole si vous activez les débogages IKE habituels :

```
router# debug crypto isakmp
```

Remarques :

* Même si IKE est utilisé, il n'est pas utilisé sur le port UDP/500 habituel, mais plutôt sur UDP/848.

* Si vous rencontrez un problème à ce niveau, fournissez les débogages à la fois pour KS et le GM affecté.

- En raison de la dépendance sur les sigs Rivest-Shamir-Adleman (RSA) pour les rekeys de groupe, le KS **doit avoir** une clé RSA configurée et doit avoir le même nom que celui spécifié dans la configuration de groupe.

  Afin de vérifier ceci, entrez cette commande :

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

Dépannage de l'enregistrement initial

Sur le module GM, afin de vérifier l'état de l'enregistrement, examinez le résultat de cette commande :

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

Si le résultat indique autre chose que **Registered**, entrez ces commandes :

Sur les OGM :

- Arrêtez les interfaces compatibles avec la cryptographie.
  Attention : La gestion hors bande devrait être activée.

- Activez ces débogages :

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

- Activez les débogages côté KS (voir la section suivante).

- Lorsque les débogages KS sont prêts, annulez les interfaces crypto-activées et attendez l'enregistrement (afin d'accélérer le processus, émettez la commande **clear crypto gdoi** sur le GM).

Sur les KS :

- Vérifiez la présence de la clé RSA sur le KS :

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

- Activez ces débogages :

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

Dépannage des problèmes liés aux stratégies

Problème de stratégie survenu avant l'inscription (lié à la stratégie de fermeture échouée)

Cette question n'affecte que les OGM, donc collectez ce résultat du Mécanisme :

```
gm1# show crypto ruleset
```

> **Note**: Dans Cisco IOS-XE?, cette sortie est toujours vide car la classification des paquets n'est pas effectuée dans le logiciel.

La sortie de la commande **show tech** du périphérique affecté fournit le reste des informations requises.

Le problème de stratégie se produit lors de l'enregistrement POST et se rapporte à la stratégie globale qui est poussée

Ce problème se manifeste généralement de deux façons :

- Le KS ne peut pas pousser les politiques au GM.
- Il y a une application partielle de la politique parmi les OGM.

Afin d'aider à résoudre l'un ou l'autre problème, procédez comme suit :

1. Sur le Mécanisme mondial concerné, recueillir ce résultat :

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

2. Activez ces débogages sur GM :

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

3. Sur le KS auquel le Mécanisme mondial concerné s'inscrit, recueillir ce résultat :

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

Note: Afin d'identifier le KS auquel le GM se connecte, entrez la commande **show crypto gdoi group**.

4. Sur le même KS, activez ces débogages :

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

5. Forcer le Mécanisme mondial à s'enregistrer avec cette commande sur le Mécanisme mondial :

```
clear crypto gdoi
```

Un problème de stratégie se produit lors de l'enregistrement POST et se rapporte à la fusion de la politique globale et des remplacements locaux

Ce problème se manifeste généralement sous la forme de messages qui indiquent qu'un paquet chiffré a été reçu pour lequel les politiques locales indiquent qu'il n'est pas censé être chiffré et vice versa. Toutes les données demandées dans la section précédente et la sortie de commande **show tech** sont requises dans ce cas.

Dépannage des problèmes de clé

Sur les OGM :

- Collecter ces débogages :

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

- Entrez cette commande afin de vérifier que l'GM a toujours une association de sécurité IKE de type GDOI_REKEY :

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

Sur les KS :

- Collectez la sortie de commande **show crypto key mypubkey rsa** à partir de **CHAQUE** KS. Les clés devraient être **identiques**.

- Entrez ces débogages afin d'afficher ce qui se passe sur le KS :

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

Dépannage de l'anti-réexécution basée sur le temps (TBAR)

La fonction TBAR nécessite une gestion de l'heure entre les groupes et nécessite donc une resynchronisation constante des horloges pseudo-temporelles des GM. Cette opération est effectuée pendant la retouche ou toutes les deux heures, selon la première de ces deux heures.

> **Note**: Toutes les sorties et tous les débogages doivent être collectés en même temps à la fois à partir de GM et de KS afin qu'ils puissent être corrélés de manière appropriée.

Afin d'étudier les problèmes qui se produisent à ce niveau, collectez ce résultat.

- Sur les OGM :

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

- Sur le KS :

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

Afin d'étudier l'horodatage TBAR de manière plus dynamique, activez ces débogages :

- Sur le Mécanisme mondial :

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

- Sur le KS :

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

Depuis la version 15.2(3)T de Cisco IOS, la possibilité d'enregistrer les erreurs TBAR a été ajoutée, ce qui facilite la détection de ces erreurs. Sur GM, utilisez cette commande afin de vérifier s'il y a des erreurs 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
```

Pour plus d'informations sur la façon de dépanner les problèmes de TBAR, référez-vous à Échec anti-répétition basé sur le temps.

Dépannage de la redondance KS

Cooperative (COOP) établit une session IKE afin de protéger les communications interKS. La technique de dépannage décrite précédemment pour l'établissement d'IKE est donc également applicable ici.

Le dépannage spécifique à COOP comprend des vérifications de sortie de cette commande sur tous les KS concernés :

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

> **Note**: L'erreur la plus courante faite avec le déploiement des KS COOP est d'oublier d'importer la même clé RSA (privée et publique) pour le groupe sur tous les KS. Cela entraîne des problèmes lors des retouches. Afin de vérifier et de comparer les clés publiques entre les KS, comparez la sortie de la commande **show crypto key mypubkey rsa** de chaque KS.

Si le dépannage au niveau du protocole est requis, activez ce débogage sur tous les KS impliqués :

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

Forum aux questions

Pourquoi voyez-vous ce message d'erreur "% Setting rekey authentication rejeté » ?

Ce message d'erreur apparaît lorsque vous configurez le KS après l'ajout de cette ligne :

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

La raison de ce message d'erreur est généralement que la clé étiquetée GETVPN_KEYS n'existe pas. Pour résoudre ce problème, créez une clé avec l'étiquette correcte à l'aide de la commande :

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

> **Note**: Ajoutez le mot clé exportable à la fin s'il s'agit d'un déploiement COOP, puis importez la même clé dans l'autre KS

Un routeur configuré comme KS pour un groupe GETVPN peut-il également fonctionner comme GM pour le même groupe ?

Non. Tous les déploiements GETVPN nécessitent un KS dédié qui ne peut pas participer en tant que GM pour les mêmes groupes. Cette fonctionnalité n'est pas prise en charge, car l'ajout de la fonctionnalité GM à KS avec toutes les interactions possibles telles que le chiffrement, le routage, la qualité de service, etc., n'est pas optimal pour l'état de santé de ce périphérique réseau essentiel. Il doit être disponible à tout moment pour que l'ensemble du déploiement GETVPN fonctionne.

Informations connexes

- VPN GET (Group Encrypted Transport VPN) - Cisco Systems
- Support et documentation techniques - Cisco Systems