Dépannez les questions communes GETVPN

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
L'information générale - Outils de dépannage GETVPN
Contrôlez les outils de débogage plats
Commandes show
Syslog
Domaine de groupe de suivi d'événement de la traduction (GDOI)
Debugs conditionnels GDOI
Debugs globaux cryptos et GDOI
Outils de débogage de plan de données
Dépannez
Se connecter la préparation d'installation et d'autres pratiques recommandées
Dépannez l'établissement d'IKE
Dépannez l'enregistrement initial
Dépannez les questions liées à la stratégie
L'enjeu politique se produit avant l'enregistrement (la stratégie rapportée d'Échec-fin)
L'enjeu politique se produit enregistrement de POST, et concerne la stratégie globale qui est poussée
L'enjeu politique se produit enregistrement de POST, et concerne la fusion de la stratégie globale et les gens du pays ignorent
Dépannez les questions de rekey
Dépannez l'anti-relecture basée sur temps (TBAR)
Dépannez la Redondance KS
FORUM AUX QUESTIONS
Peut un routeur configuré comme KS pour un groupe GETVPN également pour fonctionner comme GM pour la même chose groupe ?
Informations connexes

Introduction

Ce document décrit ce qui met au point pour collecter pour la plupart des questions communes du Group Encrypted Transport VPN (GETVPN).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- GETVPN
- Utilisation de serveur de Syslog

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

L'information générale - Outils de dépannage GETVPN

GETVPN fournit un ensemble étendu de dépannage usine afin de soulager le processus de dépannage. Il est important de comprendre lesquels de ces outils sont disponibles, et quand elles sont appropriées pour chaque tâche de dépannage. Pour le dépannage, c'est toujours une bonne idée de commencer par les moins méthodes intrusives, de sorte que l'environnement de production ne soit pas négativement affecté. Afin d'aider ce processus, cette section décrit certains des outils utilisés généralement disponibles :

Contrôlez les outils de débogage plats

Commandes show

Les commandes show sont utilisées généralement afin d'afficher des exécutions d'exécution dans un environnement GETVPN.

Syslog

GETVPN a un ensemble amélioré de messages de Syslog pour des événements et des conditions d'erreurs significatifs de protocole. Ceci devrait toujours être le premier endroit à regarder avant que vous en exécutiez mette au point.

Domaine de groupe de suivi d'événement de la traduction (GDOI)

Cette caractéristique a été ajoutée dans la version 15.1(3)T. Le suivi d'événement offre le poids léger, le suivi illimité pour des événements significatifs GDOI et les erreurs. Il y a également suivi de sortie-chemin avec le retour arrière activé pour des conditions d'exception.

Debugs conditionnels GDOI

Cette caractéristique a été ajoutée dans la version 15.1(3)T. Il laisse filtré met au point pour un périphérique basé donné sur l'adresse de pair, et devrait toujours être utilisé si possible, particulièrement sur le serveur principal.

Debugs globaux cryptos et GDOI

Ce sont les tous les divers GETVPM met au point. Les admins doivent précaution d'usage en mettant au point dans les environnements de grande puissance. Avec GDOI met au point, cinq mettent au point des niveaux sont donnés pour une finesse plus additionnelle d'élimination des imperfections :

```
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 debug	Ce que vous obtiendrez
Erreur	Conditions d'erreurs
Laconique	Importants messages à l'utilisateur et aux

	questions de protocole
Événement	Les transitions et les événements d'état comme envoient et reçoivent des rekeys
Détail	La plupart des informations de message de débogage détaillées
Paquet	Inclut le vidage mémoire des informations de paquet détaillées
Tous	Tout les en haut

Outils de débogage de plan de données

Voici quelques outils de débogage de plan de données :

- Listes d'accès
- Comptabilité de Priorité IP
- NetFlow
- Compteurs d'interface
- Cryptos compteurs
- Technologie Cisco Express Forwarding (CEF) IP global et compteurs de baisse de Par-caractéristique
- Capture incluse de paquet (CPE)
- Debugs de plan de données (le paquet IP et le CEF met au point)

Dépannez

Se connecter la préparation d'installation et d'autres pratiques recommandées

Avant que vous commenciez à dépanner, assurez-vous que vous avez préparé l'installation se connectante comme décrit ici. Quelques pratiques recommandées sont également répertoriées ici :

- Vérifiez la quantité de routeur de mémoire disponible, et configurez le **logging buffered debugging à une** grande valeur (10 Mo ou plus si possible).
- Désactivez se connecter à la console, au moniteur, et aux serveurs de Syslog.
- Récupérez le contenu de tampon de journalisation avec le **show log command** à intervalles réguliers, toutes les 20 minutes à une heure, afin d'empêcher la perte de log devant mettre en mémoire tampon la réutilisation.

- Celui qui se produise, sélectionnez la commande de **tech d'exposition des** membres du groupe affectés (GMs) et des serveurs principaux (KSs), et examinez la sortie de la commande de **show ip route** dans global et chaque Virtual Routing and Forwarding (VRF) a impliqué, si en sont exigés.

- Utilisez le sync de Protocole NTP (Network Time Protocol) l'horloge entre tous les périphériques qui sont mis au point. Activez les horodateurs de la milliseconde (milliseconde) pour chacun des deux mettent au point et des messages de log :
```
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
```

- Assurez-vous que les sorties de commande show sont horodatées.
```
Router#terminal exec prompt timestamp
```

- Quand vous collectez les sorties de commande show pour le contrôle surfacent des événements ou les compteurs de plan de données, collectent toujours de plusieurs itérations de la même sortie.

Dépannez l'établissement d'IKE

Quand la procédure d'enregistrement commence d'abord, GMs et KSs négocient des sessions d'Échange de clés Internet (IKE) afin de protéger le trafic GDOI.

- Sur le GM, contrôle que l'IKE est avec succès 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
```
  Remarque: L'état GDOI_IDLE, qui est la base de l'enregistrement, chronomètre rapidement et disparaît, parce qu'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
```
  Remarque: La session de rekey apparaît seulement une fois nécessaire sur le KS.

Terminez-vous ces étapes si vous n'atteignez pas cet état :

- Pour la vue au sujet de la cause de la panne, vérifiez la sortie de cette commande : `router# show crypto isakmp statistics`
- Si l'étape précédente n'est pas utile, vous pouvez obtenir des vues niveau de la Protocol si vous activez l'IKE habituel met au point : `router# debug crypto isakmp`Remarques :

* Quoique l'IKE soit utilisé, il n'est pas utilisé sur le port UDP/500 habituel, mais plutôt sur UDP/848.
* Si vous rencontrez une question à ce niveau, fournissez met au point pour KS et le GM affecté.

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

  Afin de vérifier ceci, sélectionnez cette commande :

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

Dépannez l'enregistrement initial

Sur le GM, afin de vérifier l'état d'enregistrement, examinez la sortie de cette commande :

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

Si la sortie indique n'importe quoi autre qu'**enregistré**, sélectionnez ces commandes :

Sur le GMs :

- Shut down crypto-a activé des interfaces.
  Attention : On s'attend à ce que la gestion hors bande soit activée.

- Activez ces derniers met au point :
  ```
  gm1# debug crypto gdoi infra packet
  gm1# debug crypto gdoi gm packet
  ```

- L'enable met au point du côté KS (voyez la section suivante).

- Quand le KS met au point soyez prêt, l'unshut crypto-activé relie, et attente l'enregistrement (afin d'accélérer le processus, émettez la commande de **clear crypto gdoi** sur le GM).

Sur le KSs :

- Vérifiez la présence de la clé RSA sur le KS :
  ```
  ks1# show crypto key mypubkey rsa
  ```

- Activez ces derniers met au point :
  ```
  ks1# debug crypto gdoi infra packet
  ks1# debug crypto gdoi ks packet
  ```

Dépannez les questions liées à la stratégie

L'enjeu politique se produit avant l'enregistrement (la stratégie rapportée d'Échec-fin)

Cette question affecte seulement GMs, ainsi collectez cette sortie du GM :

```
gm1# show crypto ruleset
```

> Remarque: Dans le Cisco IOS XE[?] , cette sortie est toujours vide depuis la classification de paquet dans non fait en logiciel.

La sortie de commande de **tech d'exposition du** périphérique affecté fournit le reste de l'information requise.

L'enjeu politique se produit enregistrement de POST, et concerne la stratégie globale qui est poussée

Il y a habituellement deux manières que ce problème manifeste :

- Le KS ne peut pas pousser les stratégies au GM.
- Il y a une application partielle de la stratégie parmi le GMs.

Afin d'aider à dépanner l'un ou l'autre de question, terminez-vous ces étapes :

1. Sur le GM affecté, collectez cette sortie :
   ```
   gm1# show crypto gdoi acl
   gm1# show crypto ruleset
   ```

2. Activez ces derniers met au point sur le GM :
   ```
   gm1# debug crypto gdoi infra packet
   gm1# debug crypto gdoi gm acls packet
   ```

3. Sur le KS auquel les registres affectés GM, collectent cette sortie :
   ```
   ks1# show crypto gdoi ks members
   ks1# show crypto gdoi ks policy
   ```

   > Remarque: Afin d'identifier au lequel KS le GM se connecte, sélectionnez la commande de **groupe de show crypto gdoi**.

4. Sur le même KS, activez ces derniers met au point :
   ```
   ks1# debug crypto gdoi infra packet
   ks1# debug crypto gdoi ks acls packet
   ```

5. Forcez le GM pour s'inscrire à cette commande sur le GM :
   ```
   clear crypto gdoi
   ```

L'enjeu politique se produit enregistrement de POST, et concerne la fusion de la stratégie globale et les gens du pays ignorent

Cette question se manifeste habituellement sous forme de messages qui indiquent qu'un paquet chiffré a été reçu pour lequel les stratégies locales indiquent qu'on ne le cense pas être chiffré et vice versa. On a besoinavoir besoin dans ce cas de tout les demandé dans la section précédente et la sortie de commande de **tech d'exposition**.

Dépannez les questions de rekey

Sur le GMs :

- Collectez ces derniers met au point :
```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- Sélectionnez cette commande afin de vérifier que le GM a toujours une association de sécurité d'IKE (SA) du type GDOI_REKEY :
```
gm1# show crypto isakmp sa
```

Sur le KSs :

- Collectez la sortie de commande de **show crypto key mypubkey rsa de CHAQUE** KS. On s'attend à ce que les clés soient **identiques**.

- Entrez dans ces derniers met au point afin de visualiser ce qui se produit sur le KS :
```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

Dépannez l'anti-relecture basée sur temps (TBAR)

La caractéristique TBAR exige la temps-conservation à travers des groupes, et exige donc des horodateurs de GMs de resynced constamment. Ceci est exécuté pendant le rekey ou toutes les deux heures, celui qui est livré d'abord.

> Remarque: Toute la sortie et met au point doit être collectée en même temps de GMs et de KS de sorte qu'ils puissent être corrélés convenablement.

Afin d'étudier les questions qui se produisent à ce niveau, collectez cette sortie.

- Sur le GMs :
```
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 TBAR temps-gardant de plus de façon dynamique, activez ces derniers met au point :

- Sur le GM :
  ```
  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)
  ```

En date de la version IOS 15.2(3)T de Cisoc, la capacité d'enregistrer des erreurs TBAR a été ajoutée, qui le facilite pour repérer ces erreurs. Sur le GM, employez 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 dépanner des questions TBAR, référez-vous au temps basé panne d'anti-relecture.

Dépannez la Redondance KS

La coopérative (CAGE) établit une session d'IKE afin de protéger la transmission d'interKSs, ainsi la technique de dépannage précédemment décrite pour l'établissement d'IKE s'applique ici aussi bien.

le dépannage de Cage-particularité comporte des contrôles de sortie de cette commande sur tout le KSs a impliqué :

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

> Remarque: L'erreur la plus commune faite avec le déploiement de la CAGE KSs est d'oublier d'importer la même clé RSA (privé et public) pour le groupe sur tout le KSs. Ceci pose des problèmes pendant les rekeys. Afin de vérifier et comparer des clés publiques parmi KSs, comparez la sortie de la commande de **show crypto key mypubkey rsa de** chaque KS.

Si le dépannage niveau de la Protocol est exigé, activez ceci mettent au point sur tout le KSs a impliqué :

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

FORUM AUX QUESTIONS

Pourquoi voyez-vous ce % de rekey authentication de configuration de message d'erreur « rejeté » ?

Vous voyez ce message d'erreur quand vous configurez le KS après que cette ligne soit ajoutée :

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

La raison pour ce message d'erreur est habituellement parce que la clé étiquetée GETVPN_KEYS n'existe pas. Afin de réparer ceci, créez une clé avec l'étiquette correcte utilisant la commande :

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

> Remarque: Ajoutez le mot clé exportable à l'extrémité si c'est un déploiement de CAGE et puis importez la même clé dans l'autre KS

Peut un routeur configuré comme KS pour un groupe GETVPN également pour fonctionner comme GM pour la même chose groupe ?

Non. Tous les déploiements GETVPN exigent un KS dédié qui ne peut pas participer comme GM pour les mêmes groupes. Cette caractéristique n'est pas prise en charge, parce qu'ajoutant la fonctionnalité GM à KS avec toutes les interactions possibles comme le cryptage, le routage, le QoS, etc., n'est pas optimale pour les santés de ce périphérique crucial de réseau. Il doit être disponible à tout moment pour que le déploiement entier GETVPN fonctionne.

Informations connexes

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