Guide de dépannage GETVPN

Contenu

Introduction

Ce document est destiné à présenter une méthodologie de dépannage structurée et des outils utiles pour aider à identifier et à isoler les problèmes de réseau privé virtuel de transport crypté de groupe (GETVPN) et pour fournir des solutions possibles.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- GETVPN
  Guide officiel de configuration GETVPN
  Guide officiel de conception et de mise en oeuvre du 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.

Méthodologie de dépannage GETVPN

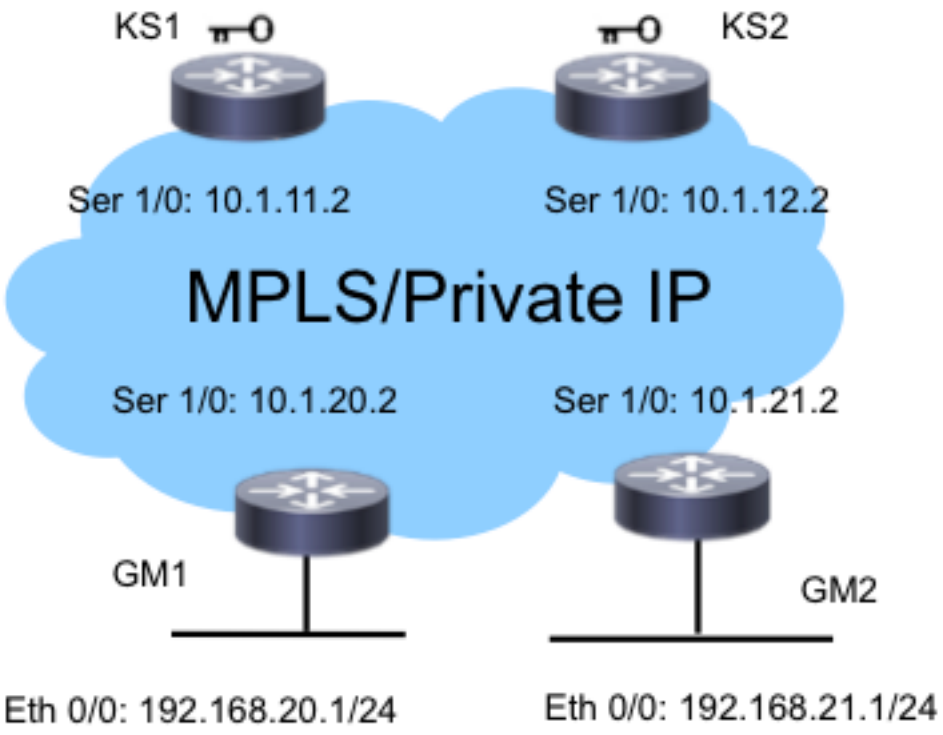
Comme pour la plupart des dépannages de problèmes technologiques complexes, la clé est de pouvoir isoler le problème à une fonction, un sous-système ou un composant spécifique. La solution GETVPN comprend plusieurs composants, notamment :

- IKE (Internet Key Exchange) : utilisé entre les serveurs de clés (KS) et les membres du groupe (GM) et COOP (Cooperative Protocol) afin d'authentifier et de protéger le plan de contrôle.
- Domaine d'interprétation de groupe (GDOI) - Protocole utilisé pour le KS afin de distribuer les clés de groupe et fournir un service clé tel que la recette à tous les GM.
- COOP - Protocole utilisé pour les KS afin de communiquer entre eux et de fournir une redondance.
- Conservation des en-têtes - IPsec en mode tunnel qui préserve l'en-tête de paquet de données d'origine pour la livraison du trafic de bout en bout.
- TBAR (Time Based Anti-Replay) : mécanisme de détection de relecture utilisé dans un environnement de clé de groupe.

Il fournit également 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. La clé de ce dépannage structuré est de pouvoir réduire le problème à un problème de contrôle ou de plan de données. Vous pouvez le faire si vous suivez le protocole ou le flux de données et utilisez les différents outils présentés ici afin de les contrôler.

Topologie de référence

Cette topologie et ce schéma d'adressage GETVPN sont utilisés dans le reste de ce document de dépannage.



Configurations de référence

- KS1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
address ipv4 10.1.11.2
redundancy
local priority 10
peer address ipv4 10.1.12.2
```

- GM1

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

Note: Les configurations KS2 et GM2 ne sont pas incluses ici pour la concision.

Terminologie

- **KS** - Serveur de clés
- **GM** - Membre du groupe
- **COOP** - Protocole de coopération
- **TBAR** - Antirediffusion basée sur le temps
- **KEK** - Clé de chiffrement de clé
- **TEK** - Clé de chiffrement du trafic

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 GM et des KS concernés, et examinez le résultat de la commande **show ip route** dans global et chaque VRF (Virtual Routing and Forwarding) 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 des problèmes du plan de contrôle GETVPN

Plan de contrôle, tous les événements de protocole qui ont conduit à la création de la stratégie et de l'association de sécurité (SA) sur le GM afin qu'ils soient prêts à chiffrer et à décrypter le trafic du plan de données. Voici quelques points de contrôle clés du plan de contrôle GETVPN :

Meilleures pratiques de débogage du plan de contrôle

Ces meilleures pratiques de dépannage ne sont pas spécifiques à GETVPN ; elles s'appliquent à presque tous les débogages de plan de contrôle. Il est essentiel de suivre ces meilleures pratiques afin de garantir un dépannage le plus efficace possible :

- Désactivez la journalisation de console et utilisez la mémoire tampon de journalisation ou syslog afin de collecter les débogages.
- Utilisez NTP afin de synchroniser les horloges du routeur sur tous les périphériques qui sont débogués.
- Activer l'horodatage msec pour les messages de débogage et de journal :

```
service timestamp debug datetime msec
service timestamp log datetime msec
```

- Assurez-vous que les sorties de la commande show sont horodatées afin qu'elles puissent être corrélées avec la sortie de débogage :

```
terminal exec prompt timestamp
```

- Utilisez le débogage conditionnel dans un environnement d'échelle si possible.

Outils de dépannage du plan de contrôle GETVPN

Commandes show GETVPN

En règle générale, il s'agit des sorties de commande que vous devez collecter pour presque tous les problèmes GETVPN.

KS

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

GM

```
show crypto eli
show crypto gdoi rekey sa
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

Messages Syslog GETVPN

GETVPN fournit un ensemble complet de messages syslog pour les événements de protocole significatifs et les conditions d'erreur. Le syslog doit toujours être le premier emplacement à rechercher lors du dépannage de GETVPN.

Messages Syslog KS courants

périodiques	Explication
COOP_CONFIG_MISMATCH	La configuration entre le serveur de clé primaire et le serveur de clé secon ne correspond pas.
COOP_KS_ELECTION	Le serveur de clés local a entré le processus de sélection dans un groupe.
COOP_KS_REACH	L'accessibilité entre les serveurs de clés de coopération configurés est restaurée.
COOP_KS_TRANS_TO_PRI	Le serveur de clés locales est passé d'un serveur secondaire dans un grou un rôle principal.
COOP_KS_UNAUTH	Un serveur distant autorisé a tenté de contacter le serveur de clés local da groupe, ce qui pourrait être considéré comme un événement hostile.
COOP_KS_UNREACH	L'accessibilité entre les serveurs de clés de coopération configurés est per ce qui peut être considéré comme un événement hostile.
KS_GM_REVOKED	Pendant le protocole de retouche, un membre non autorisé a tenté de rejo un groupe, qui pourrait être considéré comme un événement hostile.
KS_SEND_MCAST_REKEY	Envoi de la clé de multidiffusion.
KS_SEND_UNICAST_REKEY	Envoi de la nouvelle clé de monodiffusion.
KS_NON AUTORISÉ	Au cours du protocole d'enregistrement GDOI, un membre non autorisé a de rejoindre un groupe, ce qui pourrait être considéré comme un événeme hostile.
NON AUTORISÉ_IPADDR.	La demande d'enregistrement a été abandonnée car le périphérique demandeur n'était pas autorisé à rejoindre le groupe.

Messages Syslog GM courants

périodiques	Explication
GM_CLEAR_REGISTER	La commande **clear crypto gdoi** a été exécutée par le membre du group local.
GM_CM_ATTACH	Une carte de chiffrement a été jointe pour le membre du groupe local.
GM_CM_DETACH	Une carte de chiffrement a été détachée pour le membre du groupe loca
GM_RE_REGISTER	L'association de sécurité IPsec créée pour un groupe a peut-être expiré été supprimée. Vous devez vous réenregistrer sur le serveur de clés.
GM_RECV_REKEY	Rekey reçu.
GM_REGS_COMPL	Inscription terminée.
GM_REKEY_TRANS_2_MULTI	Le membre du groupe est passé d'un mécanisme de retouche de monodiffusion à un mécanisme de multidiffusion.
GM_REKEY_TRANS_2_UNI	Le membre du groupe est passé de l'utilisation d'un mécanisme de clé d multidiffusion à l'utilisation d'un mécanisme de monodiffusion.

PSEUDO_TIME_LARGE	Un membre du groupe a reçu un pseudo-temps avec une valeur qui est largement différente de son pseudo-temps.
ÉCHEC DE LA RELECTURE	Un membre de groupe ou un serveur de clés a échoué à une vérification relecture.

Note: Les messages mis en surbrillance en rouge sont les messages les plus courants ou les plus significatifs vus dans un environnement GETVPN.

Débogues globaux Crypto et GDOI

Les débogages GETVPN sont divisés :

1. D'abord par le périphérique sur lequel vous effectuez le dépannage.
```
F340.06.15-2900-18#debug cry gdoi ?
 all-features  All features in GDOI
 condition     GDOI Conditional Debugging
 gm            Group Member
 ks            Key Server
```
2. Ensuite, par le type de problème que vous dépannez.
```
GM1#debug cry gdoi gm ?
 all-features    All Group Member features
 infrastructure  GM Infrastructure
 registration    GM messages related to registration
 rekey           GM messagese related to Re-Key
 replay          Anti Replay
```
3. Troisièmement, par le niveau de débogage qui doit être activé. Dans la version 15.1(3)T et les versions ultérieures, tous les débogages de fonctionnalités GDOI ont été standardisés pour avoir ces niveaux de débogage. Ceci a été conçu pour aider à dépanner les environnements GETVPN à grande échelle avec une granularité de débogage suffisante. Lorsque vous déboguez des problèmes GETVPN, il est important d'utiliser le niveau de débogage approprié. En règle générale, commencez par le niveau de débogage le plus bas, c'est-à-dire le niveau d'erreur, et augmentez la granularité de débogage si nécessaire.
```
GM1#debug cry gdoi gm all-features ?
 all-levels  All levels
 detail      Detail level
 error       Error level
 event       Event level
 packet      Packet level
 terse       Terse level
```

Débogage conditionnel GDOI

Dans Cisco IOS® Version 15.1(3)T et ultérieures, le débogage conditionnel GDOI a été ajouté afin d'aider à dépanner GETVPN dans un environnement à grande échelle. Ainsi, tous les débogages ISAKMP (Internet Security Association and Key Management Protocol) et GDOI peuvent maintenant être déclenchés avec un filtre conditionnel basé sur l'adresse IP du groupe ou de l'homologue. Pour la plupart des problèmes GETVPN, il est bon d'activer les débogages ISAKMP et GDOI avec le filtre conditionnel approprié, puisque les débogages GDOI montrent uniquement les opérations spécifiques à GDOI. Afin d'utiliser les débogages conditionnels ISAKMP et GDOI, complétez ces deux étapes simples :

1. Définissez le filtre conditionnel.
2. Activez les ISAKMP et GDOI appropriés comme d'habitude.

Exemple :

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.

KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

> **Note**: Avec les débogages conditionnels ISAKMP et GDOI, afin d'attraper les messages de débogage qui pourraient ne pas avoir les informations de filtre conditionnel, par exemple l'adresse IP dans le chemin de débogage, l'indicateur **sans correspondance** peut être activé. Cependant, ceci doit être utilisé avec prudence car il peut produire une grande quantité d'informations de débogage.

Traces des événements GDOI

Ceci a été ajouté dans la version 15.1(3)T. Le suivi des événements offre un suivi léger et permanent pour les événements et erreurs GDOI significatifs. Il existe également un traçage de sortie-path avec la commande traceback activée pour les conditions d'exception. Les traces d'événements peuvent fournir plus d'informations d'historique d'événements GETVPN que les Syslogs traditionnels.

Les traces d'événements GDOI sont activées par défaut et peuvent être récupérées à partir du tampon de suivi à l'aide de la commande **show monitor even-trace**.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

La trace du chemin de sortie fournit des informations détaillées sur le chemin de sortie, c'est-à-dire les conditions d'exception et d'erreur, avec l'option de redémarrage activée par défaut. Les tracebacks peuvent ensuite être utilisés afin de décoder la séquence de code exacte qui a conduit

à la condition de chemin de sortie. Utilisez l'option **detail** afin de récupérer les tracebacks de la mémoire tampon de trace :

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

La taille du tampon de suivi par défaut est de 512 entrées, ce qui peut ne pas être suffisant si le problème est intermittent. Afin d'augmenter cette taille d'entrée de trace par défaut, les paramètres de configuration de trace d'événement peuvent être modifiés comme indiqué ici :

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

Points de contrôle du plan de contrôle GETVPN et problèmes courants

Voici quelques-uns des problèmes de plan de contrôle courants pour GETVPN. Pour recommencer, le plan de contrôle est défini comme étant tous les composants de la fonction GETVPN requis afin d'activer le chiffrement et le déchiffrement du plan de données sur les GM. À un niveau élevé, cela nécessite l'enregistrement GM réussi, la stratégie de sécurité et le téléchargement/installation de SA, ainsi que la retouche KEK/TEK subséquente.

Configuration et création de politiques COOP

Afin de vérifier et de vérifier que le KS a correctement créé la stratégie de sécurité et le KEK/TEK associé, saisissez :

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1
```

```
TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Un problème courant avec la configuration de la stratégie KS est lorsqu'il y a différentes stratégies configurées entre les KS principal et secondaire. Cela peut entraîner un comportement KS imprévisible et cette erreur sera signalée :

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNNING: replay method configuration between
Primary KS and Secondary KS are mismatched
```

Actuellement, il n'existe pas de synchronisation automatique de configuration entre les KS principaux et secondaires. Ces derniers doivent donc être corrigés manuellement.

Étant donné que COOP est une configuration critique (et presque toujours obligatoire) pour GETVPN, il est essentiel de s'assurer que COOP fonctionne correctement et que les rôles COOP KS sont corrects :

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
Session 1:
Server handle: 2147483651
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

Dans une configuration COOP fonctionnelle, ce flux de protocole doit être observé :

IKE Exchange > ANN avec priorités COOP échangées > Choix COOP > ANN de KS principal à secondaire (stratégie, base de données GM et clés)

Lorsque COOP ne fonctionne pas correctement, ou s'il y a une séparation COOP, comme plusieurs KS deviennent le KS principal, ces débogages doivent être collectés pour le dépannage :

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
show crypto gdoi ks coop
```

Configuration IKE

Un échange IKE réussi est nécessaire pour GETVPN afin de sécuriser le canal de contrôle pour la stratégie et le téléchargement de SA ultérieurs. À la fin de l'échange IKE réussi, un GDOI_REKEY sa est créé.

Dans les versions antérieures à Cisco IOS 15.4(1)T, le GDOI_REKEY peut être affiché avec la commande **show crypto isakmp sa** :

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

Dans Cisco IOS 15.4(1)T et versions ultérieures, cette GDOI_REKEY s'affiche avec la commande **show crypto gdoi rekey sa** :

```
GM1#show crypto gdoi rekey sa
GETVPN REKEY SA
dst             src             conn-id         status
10.1.13.2       10.1.11.2       1114            ACTIVE
```

> **Note**: Une fois l'échange IKE initial terminé, les stratégies et clés suivantes seront **poussées** du KS vers le GM avec l'utilisation de GDOI_REKEY SA. Il n'y a donc pas de retouche pour l'association de sécurité GDOI_IDLE lorsqu'elles expirent ; ils disparaissent à l'expiration de leur vie. Cependant, il devrait toujours y avoir GDOI_REKEY SA sur le GM pour qu'il reçoive des rekeys.

L'échange IKE pour GETVPN n'est pas différent de l'IKE utilisé dans les tunnels IPsec point à point traditionnels. La méthode de dépannage reste donc la même. Ces débogages doivent être collectés afin de dépanner les problèmes d'authentification IKE :

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)
```

Enregistrement, téléchargement de stratégie et installation de SA

Une fois l'authentification IKE réussie, GM s'enregistre auprès du KS. Ces messages syslog doivent être affichés lorsque cela se produit correctement :

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2
```

La stratégie et les clés peuvent être vérifiées à l'aide de cette commande :

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
```

```
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval


GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
```

```
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
GM1#
```

Note: Avec GETVPN, les SA entrantes et sortantes utilisent le même SPI.

Avec l'enregistrement GETVPN et le type d'installation de la stratégie, ces débogages sont nécessaires pour résoudre les problèmes suivants :

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Note: Des débogages supplémentaires peuvent être nécessaires en fonction du résultat de ces sorties.

Puisque l'enregistrement GETVPN se produit généralement immédiatement après le rechargement de GM, ce script EEM peut être utile afin de collecter ces débogages :

```
event manager applet debug
event syslog pattern "RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "debug crypto gdoi all all"
```

Retouche

Une fois que les GM sont enregistrés auprès du KS et que le réseau GETVPN est correctement configuré, le KS principal est responsable de l'envoi de messages de rectification à tous les GM qui lui sont enregistrés. Les messages rekey sont utilisés afin de synchroniser toutes les stratégies, clés et pseudo-heures sur les GM. Les messages de nouvelle clé peuvent être envoyés via une méthode de monodiffusion ou de multidiffusion.

Ce message syslog est affiché sur le KS lors de l'envoi du message de nouvelle clé :

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```

Sur les GM, il s'agit du syslog qui apparaît lorsqu'il reçoit la nouvelle clé :

```
%GDOI-5-GM_RECV_REKEY: Received Rekey for group G1 from 10.1.11.2 to 10.1.20.2
with seq # 11
```

Configuration requise pour la paire de clés RSA pour Rekey sur KS

La fonctionnalité Rekey nécessite la présence de clés RSA sur le KS. Le KS fournit la clé publique

de la paire de clés RSA au GM via ce canal sécurisé lors de l'enregistrement. Le KS signe ensuite les messages GDOI envoyés au GM avec la clé RSA privée dans la charge utile GDOI SIG. Le Mécanisme mondial reçoit les messages GDOI et utilise la clé RSA publique afin de vérifier le message. Les messages entre le KS et le GM sont chiffrés avec la KEK, qui est également distribuée au GM lors de l'enregistrement. Une fois l'enregistrement terminé, les clés suivantes sont cryptées avec la clé et signées avec la clé RSA privée.

Si la clé RSA n'est pas présente sur le KS lors de l'enregistrement GM, ce message apparaît sur le syslog :

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```

Lorsque les clés ne sont pas présentes sur le KS, le GM s'enregistre pour la première fois, mais la prochaine rekey échoue à partir du KS. Finalement, les clés existantes sur le Mécanisme mondial expirent, et il se réenregistre à nouveau.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may have expired/been
cleared, or didn't go through. Re-register to KS.
```

Étant donné que la paire de clés RSA est utilisée pour signer les messages de clé, ils **DOIVENT** être identiques entre le KS principal et tous les KS secondaires. Cela garantit que lors d'une défaillance de KS primaire, les rekeys envoyés par un KS secondaire (le nouveau KS primaire) peuvent toujours être validés correctement par les GM. Lorsqu'il génère la paire de clés RSA sur le KS principal, la paire de clés doit être créée avec l'option **exportable** afin qu'elles puissent être exportées vers tous les KS secondaires afin de répondre à cette exigence.

Dépannage Rekey

La défaillance de clé KEK/TEK est l'un des problèmes GETVPN les plus courants rencontrés dans les déploiements de clients. Le dépannage des problèmes de clé doit suivre les étapes de clé de clé telles que décrites ici :

1. Les rekeys ont-ils été envoyés par le KS ?

   Cette vérification peut être effectuée par une observation du message syslog %GDOI-5-KS_SEND_UNICAST_REKEY ou plus précisément à l'aide de cette commande :

```
KS1#show crypto gdoi ks rekey
Group G1 (Unicast)
Number of Rekeys sent               : 341
Number of Rekeys retransmitted      : 0
KEK rekey lifetime (sec) : 1200
Remaining lifetime (sec) : 894
Retransmit period : 10
Number of retransmissions : 5
IPSec SA 1 lifetime (sec) : 900
Remaining lifetime (sec) : 405
```

   Le nombre de retouches retransmises indique que les paquets d'accusé de réception de la nouvelle clé ne sont pas reçus par le KS et, par conséquent, que des problèmes de retouches sont possibles. Gardez à l'esprit que la nouvelle clé GDOI utilise le protocole UDP comme mécanisme de transport non fiable, de sorte que certaines chutes de clé pourraient

être attendues en fonction de la fiabilité du réseau de transport sous-jacent, mais une tendance à l'augmentation des retransmissions de clé devrait toujours être étudiée.

On peut également obtenir des statistiques plus détaillées par clé de clé GM. Il s'agit généralement du premier endroit à rechercher des problèmes potentiels de retouches.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. Les paquets de nouvelle clé ont-ils été livrés dans le réseau d'infrastructure sous-jacent ?

   Le dépannage IP standard le long du chemin de transfert de clé doit être suivi afin de s'assurer que les paquets de clé de clé ne sont pas abandonnés dans le réseau de transit entre KS et GM. Les listes de contrôle d'accès (ACL) d'entrée/sortie, Netflow et la capture de paquets dans le réseau de transit sont quelques-uns des outils de dépannage courants utilisés ici.

3. Les paquets de nouvelle clé ont-ils atteint le processus GDOI pour le traitement de la nouvelle clé ?

   Vérifiez les statistiques de la clé GM :

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

4. Le paquet d'accusé de réception de la nouvelle clé a-t-il été renvoyé au KS ?

Suivez les étapes 1 à 3 afin de retracer le paquet d'accusé de réception de la clé de nouvelle clé depuis le GM jusqu'au KS.

Retouche de diffusion simultanée

La clé de multidiffusion diffère de la clé de monodiffusion dans ces aspects :

- Puisque la multidiffusion est utilisée pour transporter ces paquets de reclé du KS vers les GM, le KS n'a pas besoin de répliquer les paquets de reclé lui-même. Le KS n'envoie qu'une copie du paquet rekey, et ils sont répliqués dans le réseau compatible multidiffusion.
- Il n'y a pas de mécanisme d'accusé de réception pour la clé de multidiffusion, donc si un GM ne devait pas recevoir le paquet de nouvelle clé, le KS n'en aurait aucune connaissance et ne supprimera donc jamais un GM de sa base de données GM. Et comme il n'y a pas d'accusé de réception, le KS retransmettra toujours les paquets de reclé en fonction de sa configuration de retransmission de clé.

Le problème de clé de multidiffusion le plus souvent observé est lorsque la clé de rediffusion n'est pas reçue sur le GM. Il pourrait y avoir un certain nombre de causes possibles à cela, telles que :

- Problème de livraison de paquets dans l'infrastructure de routage de multidiffusion
- Le routage de multidiffusion de bout en bout n'est pas activé sur le réseau

La première étape du dépannage d'un problème avec multicast rekey consiste à voir si rekey fonctionne lorsqu'il est commuté de multicast à la méthode unicast.

Une fois que vous avez identifié que le problème est spécifique à la reclé de multidiffusion, vérifiez que KS envoie la reclé à l'adresse de multidiffusion spécifiée.

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group G1 from address
10.1.11.2 to 226.1.1.1 with seq # 6
```

Testez la connectivité de multidiffusion entre le KS et GM avec une requête ICMP (Internet Control Message Protocol) à l'adresse de multidiffusion. Tous les GM qui font partie du groupe de multidiffusion doivent répondre à la requête ping. Assurez-vous que le protocole ICMP est exclu de la stratégie de chiffrement KS pour ce test.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Si le test ping multicast échoue, le dépannage multicast doit être effectué, ce qui n'est pas dans le cadre de ce document.

Contrôle du relais du plan de contrôle

Symptôme

Lorsque les clients mettent à niveau leur GM vers une nouvelle version de Cisco IOS, ils peuvent rencontrer des échecs de clé KEK avec ce message observé dans le syslog :

```
%GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 1 in seq payload for
group G1, last seq # 11
%GDOI-3-GDOI_REKEY_FAILURE: Processing of REKEY payloads failed on GM 10.1.13.2 in the group G1,
with peer at 10.1.11.2
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of GDOI mode failed with peer at 10.1.11.2
```

Ce comportement est provoqué par un problème d'interopérabilité introduit avec la vérification anti-relecture qui est ajoutée pour les messages du plan de contrôle. Plus précisément, un KS qui exécute l'ancien code réinitialisera le numéro de séquence de la clé KEK à 1, et cette valeur sera supprimée par l'GM qui exécute le nouveau code lorsqu'il l'interprète comme un paquet de nouvelle clé rejoué. Pour plus de détails, voir l'ID de bogue Cisco CSCta05809 (GETVPN : Plan de contrôle GETVPN raisonnable pour la réexécution), et restrictions de configuration GETVPN.

Fond

Avec GETVPN, les messages du plan de contrôle peuvent transporter des informations sensibles au temps afin de fournir le service de contrôle anti-relecture basé sur le temps. Par conséquent, ces messages ont besoin d'une protection contre les rediffusions afin d'assurer l'accélération du temps. Ces messages sont les suivants :

- **Rekey Messages** de KS à GM
- **Messages d'annonce COOP** entre KS

Dans le cadre de cette mise en oeuvre de la protection anti-relecture, des vérifications des numéros de séquence ont été ajoutées afin de protéger les messages rejoués, ainsi qu'une vérification pseudo-temporelle lorsque TBAR est activé.

Solution

Afin de résoudre ce problème, la GM et le KS doivent être mis à niveau vers les versions de Cisco IOS après la fonctionnalité de vérification de la relecture du plan de contrôle. Avec le nouveau code Cisco IOS, KS ne réinitialise pas le numéro de séquence à 1 pour une clé KEK, mais continue à utiliser le numéro de séquence actuel et réinitialise uniquement le numéro de séquence pour les clés TEK.

Ces versions de Cisco IOS disposent des fonctions de vérification de relecture :

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M et ultérieur

Autres problèmes liés à la relecture

- Échec COOP en raison d'un échec de vérification de la relecture des messages ANN (ID de bogue Cisco CSCtc52655)

Échecs de relecture du plan de contrôle de débogage

Pour les autres échecs de relecture du plan de contrôle, collectez ces informations et assurez-vous que les heures sont synchronisées entre le KS et le GM.

- Syslog de GM et KS
- Débogues ISAKMP
- Débogues GDOI (rekey and replay) de KS et GM

Problèmes de fragmentation de paquets du plan de contrôle

Avec GETVPN, la fragmentation des paquets du plan de contrôle est un problème courant, et elle peut se manifester dans l'un de ces deux scénarios lorsque les paquets du plan de contrôle sont suffisamment volumineux pour nécessiter une fragmentation IP :

- Paquets d'annonce GETVPN COOP
- Paquets de nouvelle clé GETVPN

Paquets d'annonce COOP

Les paquets d'annonce COOP transportent les informations de la base de données GM, et peuvent donc prendre de l'ampleur dans un déploiement GETVPN important. D'après l'expérience passée, un réseau GETVPN composé de plus de 1 500 GM produira des paquets d'annonce de plus de 1 8024 octets, soit la taille de tampon énorme par défaut de Cisco IOS. Dans ce cas, le KS ne parvient pas à allouer une mémoire tampon suffisamment grande pour transmettre les paquets ANN avec cette erreur :

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 18872 -Process= "Crypto IKMP", ipl= 0, pid= 183
```

Afin de corriger cette condition, ce réglage de la mémoire tampon est recommandé :

```
buffers huge permanent 10
buffers huge size 65535
```

Rekey Packets

Les paquets de nouvelle clé GETVPN peuvent également dépasser la taille de MTU (Maximum Transition Unit) 1500 IP standard lorsque la stratégie de cryptage est importante, par exemple une politique qui comprend plus de 8 lignes d'entrées de contrôle d'accès (ACE) dans la liste de contrôle d'accès de cryptage.

Problème de fragmentation et identification

Dans les deux scénarios précédents, GETVPN doit être en mesure de transmettre et de recevoir correctement les paquets UDP fragmentés afin que la clé COOP ou GDOI fonctionne correctement. La fragmentation IP peut poser problème dans certains environnements réseau. Par exemple, un réseau constitué d'un plan de transfert ECMP (Equal Cost Multi Path) et de certains périphériques du plan de transfert nécessitent un réassemblage virtuel des paquets IP fragmentés, tels que le réassemblage de fragmentation virtuelle (VFR).

Afin d'identifier le problème, vérifiez les erreurs de réassemblage sur le périphérique où il est suspecté que les paquets UDP 848 fragmentés ne sont pas correctement reçus :

```
KS1#show ip traffic | section Frags
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

Si les délais de réassemblage continuent à s'incrémenter, utilisez la commande **debug ip error** afin de confirmer si la suppression fait partie du flux de paquets rekey/COOP. Une fois confirmée, le dépannage normal de transfert IP doit être effectué afin d'isoler le périphérique exact dans le plan de transfert qui aurait pu abandonner les paquets. Voici quelques outils couramment utilisés :

- Capture de paquets
- Statistiques de transfert de trafic
- Statistiques des fonctions de sécurité (pare-feu, IPS)
- Statistiques VFR

Problèmes d'interopérabilité GDOI

Divers problèmes d'interopérabilité ont été détectés avec GETVPN au fil des ans, et il est essentiel de noter les versions de Cisco IOS entre KS et GM et parmi les KS pour les problèmes d'interopérabilité.

D'autres problèmes d'interopérabilité connus de GETVPN sont les suivants :

- Contrôle du relais du plan de contrôle
- Changement de comportement de la clé GETVPN KEK
- ID de bogue Cisco CSCub42920 (GETVPN : KS ne parvient pas à valider le hachage dans rekey ACK des versions GM précédentes)
- ID de bogue Cisco CSCuw48400 (GetVPN GM n'a pas pu s'enregistrer ou la clé échoue - sig-hash > SHA-1 par défaut)
- ID de bogue Cisco CSCvg19281 (plantages multiples de GETVPN GM après la migration vers une nouvelle paire KS ; si une version GM est antérieure à la version 3.16 et que KS est mis à niveau d'un code antérieur à la version 3.16 ou ultérieure, ce problème peut se produire)

Procédure de mise à niveau de GETVPN IOS

Cette procédure de mise à niveau de Cisco IOS doit être suivie lorsqu'une mise à niveau de code Cisco IOS doit être effectuée dans un environnement GETVPN :

1. Mettez d'abord à niveau un KS secondaire et attendez que la sélection COOP KS soit terminée.
2. Répétez l'étape 1 pour tous les KS secondaires.
3. Mettre à niveau le KS principal.
4. Mettre à niveau les GM.

Dépannage des problèmes de plan de données GETVPN

Par rapport aux problèmes liés au plan de contrôle, les problèmes liés au plan de données GETVPN sont des problèmes dans lesquels le GM a la politique et les clés pour effectuer le chiffrement et le déchiffrement du plan de données, mais pour une raison quelconque, le flux de trafic de bout en bout ne fonctionne pas. La plupart des problèmes de plan de données pour GETVPN concernent le transfert IPsec générique et ne sont pas spécifiques à GETVPN. La plupart des méthodes de dépannage décrites ici s'appliquent donc également aux problèmes de plan de données IPsec générique.

Avec les problèmes de cryptage (tunnels basés sur des groupes ou des paires), il est important de dépanner le problème et d'isoler le problème à une partie particulière du chemin de données. Plus précisément, l'approche de dépannage décrite ici a pour but de vous aider à répondre à ces questions :

- Quel périphérique est responsable du chiffrement du routeur ou du déchiffrement du routeur ?
- Dans quelle direction le problème se produit-il - en entrée ou en sortie ?

Outils de dépannage du plan de données GETVPN

Le dépannage du plan de données IPsec est très différent de celui du plan de contrôle. Avec le plan de données, il n'y a généralement aucun débogage que vous pouvez exécuter, ou du moins exécuter en toute sécurité dans un environnement de production. Le dépannage repose donc sur différents compteurs et statistiques de trafic qui peuvent aider à suivre le paquet le long d'un chemin de transmission. L'idée est de pouvoir développer un ensemble de points de contrôle afin d'aider à isoler les endroits où les paquets peuvent être abandonnés, comme indiqué ici :

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)

Les points de contrôle du chemin de données de l'image précédente peuvent être validés à l'aide des outils suivants :

Cryptage GM

- Interface LAN entrante
  - ACL d'entrée
  - Débit net entrant
  - Capture de paquets intégrée
  - Comptabilité de priorité d'entrée

- Moteur de chiffrement
  - **show crypto ipsec sa**
  - **show crypto ipsec sa detail**
  - **show crypto engine accélération statistics**

- Interface WAN de sortie
    - Débit net de sortie
    - Capture de paquets intégrée
    - Comptabilité de priorité de sortie

Décryptage des OGM

- Interface WAN entrante
    - ACL d'entrée
    - Débit net entrant
    - Capture de paquets intégrée
    - Comptabilité de priorité d'entrée

- Moteur de chiffrement
    - **show crypto ipsec sa**
    - **show crypto ipsec sa detail**
    - **show crypto engine accélération statistics**

- Interface LAN de sortie
    - Débit net de sortie
    - Capture de paquets intégrée

Le chemin de retour suit le même flux de trafic. Les sections suivantes présentent quelques exemples de ces outils de plan de données utilisés.

Compteurs de chiffrement/déchiffrement

Les compteurs de chiffrement/déchiffrement sur un routeur sont basés sur un flux IPsec. Malheureusement, cela ne fonctionne pas bien avec GETVPN, car GETVPN déploie généralement une politique de cryptage « permit ip any any » qui chiffre tout. Donc si le problème ne se produit que pour certains flux et pas tous, ces compteurs peuvent être un peu difficiles à utiliser afin d'évaluer correctement si les paquets sont chiffrés ou décryptés quand il y a suffisamment de trafic de fond significatif qui fonctionne.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

Netflow

Netflow peut être utilisé afin de surveiller le trafic d'entrée et de sortie sur les deux GM. Notez que la stratégie **permit ip any any** GETVPN, le trafic chiffré sera agrégé et ne fournit pas les informations par flux. Les informations par flux devront ensuite être collectées avec le marquage DSCP/priorité décrit plus loin.

Dans cet exemple, le flux réseau d'une requête ping de 100 comptes d'un hôte derrière GM1 vers un hôte derrière GM2 est affiché aux différents points de contrôle.

Cryptage GM

Configuration de Netflow :

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

Sortie Netflow :

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

> **Note**: Dans le résultat précédent, * indique le trafic de sortie. La première ligne indique le trafic chiffré de sortie (avec le protocole 0x32 = ESP) hors de l'interface WAN, et la seconde ligne le trafic ICMP d'entrée qui touche l'interface LAN.

Décryptage des OGM

Configuration:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

Sortie Netflow :

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

Marquage de priorité DSCP/IP

Le problème avec le dépannage d'un problème de cryptage est qu'une fois le paquet chiffré, vous perdez de la visibilité sur la charge utile, ce que le cryptage est censé faire, ce qui rend difficile le suivi du paquet pour un flux IP particulier. Il y a deux façons de résoudre cette limite en matière de dépannage d'un problème IPsec :

- Utilisez ESP-NULL comme transformation IPsec. IPsec effectue toujours l'encapsulation ESP mais aucun chiffrement n'est appliqué à la charge utile, de sorte qu'ils sont visibles dans une capture de paquets.
- Marquer un flux IP avec un marquage DSCP (Differentiated Services Code Point)/priorité unique en fonction de leurs caractéristiques L3/L4.

ESP-NULL nécessite des modifications sur les deux points d'extrémité du tunnel et n'est souvent pas autorisé en fonction de la stratégie de sécurité du client. Par conséquent, Cisco recommande généralement l'utilisation du marquage DSCP/priorité à la place.

Tableau de référence DSCP/Precedence

ToS (hexadécimal)	ToS (décimal)	Priorité IP	DSCP	Binaire
0xE0	224	7 Contrôle du réseau	56 CS7	11100000
0xC0	192	6 Contrôle interréseau	48 CS6	11000000
0xB8	184	5 Critique	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4 Remplacement Flash	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	3 Flash	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2 Immédiat	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1 Priorité	8 CS1	00100000
0x00	0	0 Routine	0 DFT	00000000

Marquer les paquets avec DSCP/Precedence

Ces méthodes sont généralement utilisées pour marquer les paquets avec les marquages DSCP/Precedence spécifiques.

PBR

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
match ip address 150
set ip precedence flash-override
```

MQC

```
class-map match-all my_flow
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

Router Ping

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

> **Note**: Il est toujours recommandé de surveiller le flux de trafic normal et le profil DSCP/priorité avant d'appliquer le marquage afin que le flux de trafic marqué soit unique.

Surveiller les paquets marqués

Comptabilité de priorité IP

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
```

```
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

ACL d'interface

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

Capture de paquets intégrée

Embedded Packet Capture (EPC) est un outil utile pour capturer des paquets au niveau de l'interface afin d'identifier si un paquet a atteint un périphérique spécifique. Rappelez-vous qu'EPC fonctionne bien pour le trafic de texte clair, mais cela peut être difficile lorsque les paquets capturés sont chiffrés. Par conséquent, des techniques telles que le marquage DSCP/priorité dont il a été question précédemment ou d'autres caractères IP, tels que la longueur du paquet IP, doivent être utilisées avec EPC afin de rendre le dépannage plus efficace.

Cisco IOS-XE Packet Trace

Il s'agit d'une fonctionnalité utile pour suivre le chemin de transfert des fonctionnalités sur toutes

les plates-formes qui exécutent Cisco IOS-XE, telles que CSR1000v, ASR1000 et ISR4451-X.

Problèmes courants du plan de données GETVPN

Le dépannage du plan de données IPsec pour GETVPN n'est généralement pas différent du dépannage des problèmes de plan de données IPsec point à point traditionnels, avec deux exceptions dues à ces propriétés uniques de plan de données de GETVPN.

Échec de l'anti-relecture basé sur l'heure

Dans un réseau GETVPN, les pannes TBAR peuvent être difficiles à dépanner car il n'existe plus de tunnels par paire. Afin de dépanner les défaillances de la BARRE TBAR GETVPN, procédez comme suit :

1. Identifiez le paquet abandonné en raison d'une défaillance TBAR et identifiez ensuite le mécanisme de chiffrement GM.

   Avant la version 15.3(2)T, le syslog d'échec TBAR n'imprimait pas l'adresse source du paquet défaillant, ce qui rend très difficile l'identification du paquet qui a échoué. Ceci a été considérablement amélioré dans les versions 15.3(2)T et ultérieures, où Cisco IOS imprime ceci :

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=13, sequence number=1

%GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in group G1:
my_pseudotime = 620051.84 secs, peer_pseudotime = 619767.09 secs, replay_window =
4 (sec), src_ip = 192.168.13.2, dst_ip = 192.168.14.2
```

   Un historique TBAR a également été mis en oeuvre dans cette version :

```
GM2#show crypto gdoi gm replay
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs


TBAR Error History (sampled at 10pak/min):
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

   Note: Les améliorations mentionnées précédemment ont depuis été mises en oeuvre dans Cisco IOS-XE par l'ID de bogue Cisco CSCun49335 et dans Cisco IOS par l'ID de bogue Cisco CSCub91811.
   Pour les versions de Cisco IOS qui n'avaient pas cette fonctionnalité, **debug crypto gdoi gm replay detail** peut également fournir ces informations, bien que ce débogage imprime les informations TBAR pour tout le trafic (pas seulement les paquets abandonnés en raison d'une défaillance TBAR), il peut être impossible de s'exécuter dans un environnement de

production.

```
GDOI:GM REPLAY:DET:(0):my_pseudotime is 621602.30 (secs), peer_pseudotime is 621561.14
(secs), replay_window is 4 (secs), src_addr = 192.168.14.2, dest_addr = 192.168.13.2
```

2. Une fois que la source du paquet est identifiée, vous devez être en mesure de trouver le mécanisme de chiffrement GM. Ensuite, le pseudotimestamp sur les OGM chiffrant et décryptant devrait être surveillé pour détecter toute dérive pseudotemporelle potentielle. La meilleure façon d'y parvenir serait de synchroniser à la fois les OGM et les KS avec NTP et de recueillir périodiquement les pseudo-informations à l'aide d'une horloge système de référence sur tous ces systèmes afin de déterminer si le problème est causé par le décalage de l'horloge sur les GM.

GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.26 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

GM2

```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

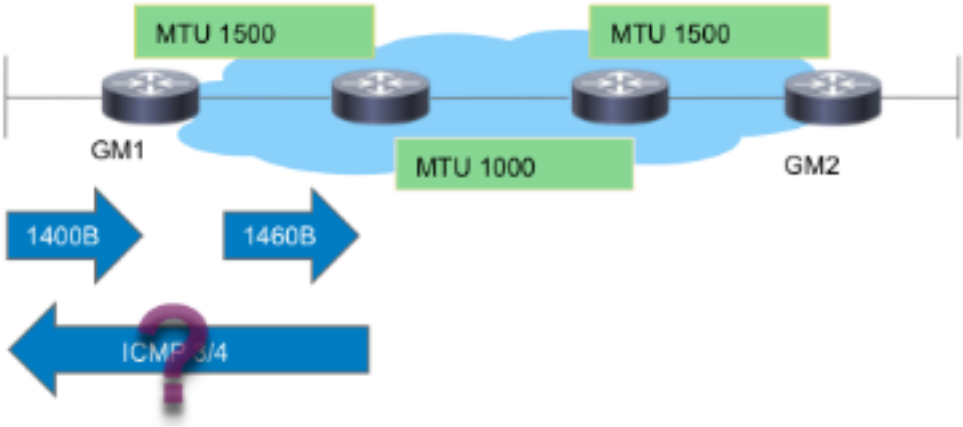
Dans l'exemple précédent, si le pseudo-temps (tel qu'indiqué par la valeur de relecture) est sensiblement différent entre les GM lorsque les sorties sont capturées avec le même temps de référence, alors le problème peut être attribué à la distorsion de l'horloge.

> **Note**: Sur la plate-forme de la gamme Cisco Aggregated Services Router 1000, en raison de l'architecture de la plate-forme, le chemin de données sur le processeur de flux Quantum (QFP) fait référence à l'horloge murale pour le comptage des graduations pseudotemporelles. Cela a créé des problèmes avec TBAR lorsque l'heure de l'horloge murale change en raison de la synchronisation NTP. Ce problème est documenté avec l'ID de bogue Cisco CSCum37911.

Préservation des en-têtes PMTUD et GETVPN

Avec GETVPN, la découverte de MTU de chemin (PMTUD) ne fonctionne pas entre les GM de chiffrement et de déchiffrement, et les paquets volumineux avec le bit DF (Don't Fragment) défini peuvent être mis en veille. La raison pour laquelle cela ne fonctionne pas est due à la préservation

de l'en-tête GETVPN où les adresses source/destination de données sont conservées dans l'en-tête d'encapsulation ESP. Cette image est représentée :



Comme le montre l'image, PMTUD se décompose avec GETVPN avec ce flux :

1. Un paquet de données volumineux arrive sur le module GM1 de chiffrement.
2. Le paquet ESP post-cryptage est transféré de GM1 et transmis vers la destination.
3. S'il existe une liaison de transit avec une MTU IP de 1 400 octets, le paquet ESP sera abandonné et un message ICMP 3/4 de paquet trop grand sera envoyé vers la source du paquet, qui est la source du paquet de données.
4. Le paquet ICMP3/4 est soit abandonné en raison d'ICMP qui n'est pas exclu de la stratégie de chiffrement GETVPN, soit abandonné par l'hôte final car il ne connaît rien au paquet ESP (charge utile non authentifiée).

En résumé, PMTUD ne fonctionne pas avec GETVPN aujourd'hui. Afin de résoudre ce problème, Cisco recommande les étapes suivantes :

1. Implémenter « ip tcp adjust-mss » afin de réduire la taille de segment de paquet TCP afin de prendre en charge la surcharge de cryptage et le MTU de chemin minimal dans le réseau de transit.
2. Effacez le bit DF dans le paquet de données lorsqu'il arrive sur le module GM de chiffrement afin d'éviter la PMTUD.

Problèmes de plan de données IPsec générique

La plupart du dépannage du plan de données IPsec est similaire au dépannage des tunnels IPsec point à point traditionnels. L'un des problèmes courants est %CRYPTO-4-RECVD_PKT_MAC_ERR. Voir Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR : » Message d'erreur avec perte de Ping sur le tunnel IPsec Dépannage pour plus de détails de dépannage.

Problèmes identifiés

Ce message peut être généré lorsqu'un paquet IPsec est reçu qui ne correspond pas à un SPI dans la SADB. Reportez-vous à l'ID de bogue Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC signalé pour pkt non correspondant au flux. Voici un exemple :

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
```

```
vrf/dest_addr= /192.168.14.2, src_addr= 192.168.13.2, prot= 50
```

Ce message doit être %CRYPTO-4-RECVD_PKT_INV_SPI, qui est ce qui est signalé pour IPsec traditionnel ainsi que sur certaines plates-formes matérielles telles que ASR. Ce problème cosmétique a été corrigé par l'ID de bogue Cisco CSCup80547 : Erreur lors de la génération du rapport CRYPTO-4-RECVD_PKT_NOT_IPSEC pour le pak ESP.

> **Note**: Ces messages peuvent parfois apparaître en raison d'un autre bogue GETVPN CSCup34371 : GETVPN GM arrête de déchiffrer le trafic après la nouvelle clé TEK.

Dans ce cas, le GM ne peut pas décrypter le trafic GETVPN, bien qu'il ait une SA IPsec valide dans la SADB (l'SA en cours de requalification). Le problème disparaît dès que la SA expire et est supprimée de la SADB. Ce problème provoque une panne importante, car la retouche TEK est effectuée à l'avance. Par exemple, la panne peut être de 22 minutes dans le cas d'une durée de vie TEK de 7 200 secondes. Consultez la description du bogue pour connaître la condition exacte qui doit être remplie afin de rencontrer ce bogue.

Dépannage de GETVPN sur les plates-formes qui exécutent Cisco IOS-XE

Dépannage des commandes

Les plates-formes qui exécutent Cisco IOS-XE ont des implémentations spécifiques à la plate-forme et nécessitent souvent un débogage spécifique à la plate-forme pour les problèmes GETVPN. Voici une liste des commandes généralement utilisées pour dépanner GETVPN sur ces plates-formes :

show crypto eli all

show platform software ipsec policy statistics

show platform software ipsec fp active Inventory

show platform hardware qfp active feature ipsec spd all

show platform hardware qfp active statistics drop clear

show platform hardware qfp active feature ipsec data drop clear

show crypto ipsec sa

show crypto gdoi

show crypto ipsec internal

debug crypto ipsec

debug crypto ipsec error

debug crypto ipsec states

debug crypto ipsec message

debug crypto ipsec hw-req

debug crypto gdoi gm infra detail

debug crypto gdoi gm rekey detail

Problèmes courants de l'ASR1000

Échec de l'installation de la stratégie IPsec (réenregistrement continu)

Un module GM ASR1000 peut continuer à s'enregistrer sur le serveur de clés si le moteur de chiffrement ne prend pas en charge la stratégie ou l'algorithme IPsec reçu. Par exemple, sur les plates-formes ASR basées sur Nitrox (telles que ASR1002), les politiques Suite-B ou SHA2 ne sont pas prises en charge et cela peut provoquer des symptômes de réenregistrement continu.

Problèmes courants de migration/mise à niveau

Limitation de TBAR ASR1000

Sur la plate-forme ASR1000, le bogue Cisco ID CSCum37911 a introduit une limitation sur cette plate-forme où le temps TBAR de moins de 20 secondes n'est pas pris en charge. Voir Restrictions pour GETVPN sur IOS-XE.

Ce bogue d'amélioration a été ouvert pour lever cette restriction, le bogue Cisco ID CSCuq25476 - ASR1k doit prendre en charge une taille de fenêtre TBAR GETVPN inférieure à 20 secondes.

Mise à jour: Cette restriction a depuis été levée avec le correctif pour l'ID de bogue Cisco CSCur57558 , et elle n'est plus une limitation dans le code XE3.10.5, XE3.13.2 et ultérieur.

Notez également que pour un GM qui fonctionne sur des plates-formes Cisco IOS-XE (ASR1k ou ISR4k), il est fortement recommandé que le périphérique exécute une version avec correction pour ce problème si TBAR est activé ; ID de bogue Cisco CSCut91647 - GETVPN sur IOS-XE : GM supprime incorrectement les paquets en raison d'une défaillance TBAR.

Problème de classification ISR4x00

Une régression a été trouvée sur la plate-forme ISR4x00 où les stratégies de refus sont ignorées. Pour plus de détails, voir l'ID de bogue Cisco CSCut14355 - GETVPN - ISR4300 GM ignore la politique de refus.

Informations connexes

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