GETVPN dépannent le guide

Contenu

Introduction

Ce document est destiné pour présenter dépannage d'une méthodologie structurée et des outils utiles pour aider à identifier et isoler des problèmes du Group Encrypted Transport VPN (GETVPN) et à fournir les solutions possibles.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- GETVPN
  Guide de configuration officiel GETVPN
  Guide officiel de conception et réalisation 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.

Méthodologie de dépannage GETVPN

Comme avec la plupart de dépannage des problèmes de technologie complexe, la clé est de pouvoir localiser le problème dans une caractéristique spécifique, un sous-système, ou un composant. La solution GETVPN est composée d'un certain nombre de composants de caractéristique, spécifiquement :

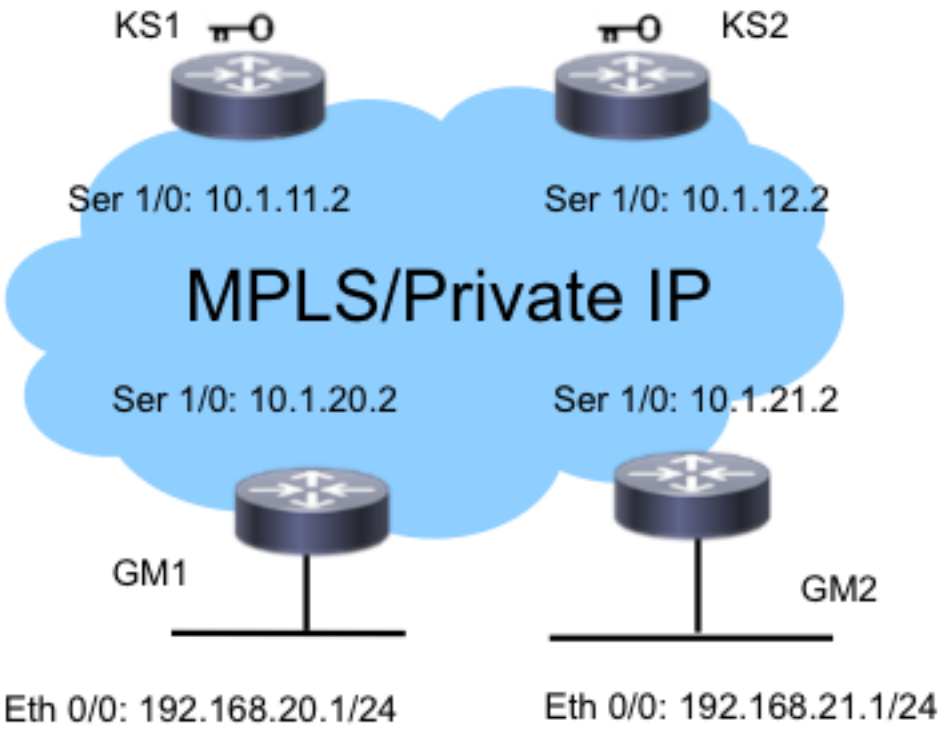
- Échange de clés Internet (IKE) - Utilisé entre le membre du groupe (GM) et le serveur principal (KS), et parmi Protocol coopératif (CAGE) KSs afin d'authentifier et protéger l'avion de contrôle.
- Groupez le domaine de la traduction (GDOI) - Protocol utilisé pour le KS afin de distribuer des clés de groupe et fournir le service principal tel que le rekey à tout le GMs.
- CAGE - Protocol l'a utilisé pour le KSs afin de communiquer les uns avec les autres et fournir la Redondance.
- Conservation d'en-tête - IPsec dans le tunnel mode qui préserve l'en-tête de paquet de données d'origine pour la livraison de bout en bout du trafic.

- Le temps a basé l'anti-relecture (TBAR) - Mécanisme de détection de rediffusion utilisé dans un environnement de clé de groupe.

Il fournit également 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. La clé à ce dépannage structuré est de pouvoir décomposer le problème à un contrôle ou à la question de plan de données. Vous pouvez faire ceci si vous suivez le protocole ou le flux de données et utilisez les divers outils présentés ici point de reprise les.

Topologie de référence

Ces topologie GETVPN et système d'adressage est utilisée dans tout 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 par souci de concision.

Terminologie

- **KS** - Serveur principal
- **GM** - Membre du groupe
- **CAGE** - Protocol coopératif
- **TBAR** - Le temps a basé l'anti-relecture
- **KEK** - Clé de chiffrement à clé
- **TEK** - Clé de cryptage du trafic

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 de** GMs et de KSs affectés, 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 :

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

- 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 les questions d'avion de contrôle GETVPN

Contrôlez l'avion signifie tous les événements de protocole qui ont amené à la stratégie et à la création de l'association de sécurité (SA) sur le GM de sorte qu'ils soient prêts à chiffrer et déchiffrer le trafic de plan de données. Certains des points de reprise principaux dans l'avion de contrôle GETVPN sont :

Contrôlez les pratiques recommandées plates d'élimination des imperfections

Ces pratiques recommandées de dépannage ne sont pas particularité GETVPN ; ils s'appliquent à presque n'importe quelle élimination des imperfections d'avion de contrôle. Il est essentiel de suivre ces pratiques recommandées afin d'assurer le dépannage le plus efficace :

- Arrêtez la journalisation console et utilisez le tampon de journalisation ou le Syslog afin de collecter met au point.
- Utilisez les horloges de routeur de sync de NTP sur tous les périphériques qui sont mis au point.
- Activez l'horodatage milliseconde pour mettent au point et les messages de log :

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

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

```
terminal exec prompt timestamp
```

- Utilisez l'élimination des imperfections conditionnelle dans un environnement d'échelle si possible.

Outils de dépannage d'avion de contrôle GETVPN

Commandes show GETVPN

En règle générale, ce sont les sorties de commande que vous devriez 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 de Syslog GETVPN

GETVPN fournit un ensemble étendu de messages de Syslog pour des événements et des conditions d'erreurs significatifs de protocole. Le Syslog devrait toujours être le premier endroit à regarder quand vous exécutez le dépannage GETVPN.

Messages communs de Syslog KS

Messages de Syslog	Explication
COOP_CONFIG_MISMATCH	La configuration le serveur entre le serveur de clé primaire et clé secondai mal adaptée.
COOP_KS_ELECTION	Le serveur principal local a écrit le processus d'élection dans un groupe.
COOP_KS_REACH	L'accessibilité entre les serveurs principaux coopératifs configurés est restaurée.
COOP_KS_TRANS_TO_PRI	Le serveur principal local transitioned à un rôle primaire d'être un serveur secondaire dans un groupe.
COOP_KS_UNAUTH	Un serveur distant autorisé jugé pour contacter le serveur principal local da un groupe, qui pourrait être considéré un événement hostile.
COOP_KS_UNREACH	L'accessibilité entre les serveurs principaux coopératifs configurés est perc qui pourraient être considérés un événement hostile.
KS_GM_REVOKED	Pendant le protocole de rekey, un membre non autorisé jugé pour joindre groupe, qui pourrait être considéré un événement hostile.
KS_SEND_MCAST_REKEY	Envoi du rekey de Multidiffusion.
KS_SEND_UNICAST_REKEY	Envoi du rekey d'unicast.
KS_UNAUTHORIZED	Pendant le protocole d'enregistrement GDOI, un membre non autorisé jug pour joindre un groupe, qui pourrait être considéré un événement hostile.
UNAUTHORIZED_IPADDR	La demande d'enregistrement a été abandonnée parce que le périphériqu demandeur n'a pas été autorisé à joindre le groupe.

Messages communs de Syslog GM

Messages de Syslog	Explication
GM_CLEAR_REGISTER	La commande de **clear crypto gdoi** a été exécutée par le membre du gr local.
GM_CM_ATTACH	Un crypto map a été relié pour le membre du groupe local.
GM_CM_DETACH	Un crypto map a été détaché pour le groupe local member.&
GM_RE_REGISTER	IPsec SA créé pour un groupe pourrait avoir été expiré ou autorisé. Le b

	de reregister au serveur principal.
GM_RECV_REKEY	Rekey reçu.
GM_REGS_COMPL	Enregistrement complet.
GM_REKEY_TRANS_2_MULTI	Le membre du groupe transitioned d'utiliser un mécanisme de rekey d'u à utiliser un mécanisme de Multidiffusion.
GM_REKEY_TRANS_2_UNI	Le membre du groupe transitioned d'utiliser un mécanisme de rekey de Multidiffusion à utiliser un mécanisme d'unicast.
PSEUDO_TIME_LARGE	Un membre du groupe a reçu un pseudotime avec une valeur qui est en grande partie différente de son propre pseudotime.
REPLAY_FAILED	Un membre du groupe ou un serveur de clé a manqué un contrôle d'ant relecture.

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

Debugs globaux cryptos et GDOI

GETVPN met au point est divisé :

1. D'abord par le périphérique sur lequel vous dépannez.
```
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. En second lieu par le type de problème 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. Tiers par le niveau de l'élimination des imperfections qui doit être activée. Dans la version 15.1(3)T et ultérieures, toute la caractéristique GDOI met au point ont été normalisées pour faire mettre au point ces derniers des niveaux. Ceci a été conçu afin d'aider à dépanner les environnements de grande puissance GETVPN avec assez de finesse d'élimination des imperfections. Quand vous mettez au point des problèmes GETVPN, il est important d'utiliser l'approprié mettent au point de niveau. En règle générale, le début avec le plus bas mettent au point de niveau, c'est le niveau d'erreur, et augmente la finesse d'élimination des imperfections une fois 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
```

Élimination des imperfections conditionnelle GDOI

Dans la version 15.1(3)T et ultérieures de Cisco IOS®, l'élimination des imperfections conditionnelle GDOI a été ajoutée afin d'aider à dépanner GETVPN dans un environnement de grande puissance. Tellement tous les Protocole ISAKMP (Internet Security Association and Key

Management Protocol) et GDOI met au point peuvent maintenant être déclenchés avec un filtre conditionnel basé sur le groupe ou l'adresse IP de pair. Pour la plupart des problèmes GETVPN, il est bon d'activer l'ISAKMP et GDOI met au point avec le filtre conditionnel approprié, puisque GDOI met au point seulement des exécutions de GDOI-particularité d'exposition. Afin d'utiliser l'ISAKMP et le GDOI conditionnels met au point, se termine ces deux étapes simples :

1. Placez le filtre conditionnel.
2. Activez l'ISAKMP et le 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 l'ISAKMP et le GDOI conditionnels met au point, afin d'attraper les messages de débogage qui ne pourraient pas avoir les informations conditionnelles de filtre, par exemple l'adresse IP dans le chemin de débogage, l'indicateur **inégalé** peut être activée. Cependant, ceci doit être utilisé avec prudence parce qu'il peut produire l'un grand nombre mettent au point les informations.

Suivis d'événement GDOI

Ceci a été ajouté 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. Les suivis d'événement peuvent fournir plus d'informations de historique d'événement GETVPN que des Syslog traditionnels.

Des suivis d'événement GDOI sont activés par défaut et peuvent être récupérés de la mémoire tampon de suivi avec la commande d'égal-**suivi de show monitor**.

```
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
```

Le repère de conduit de sortie fournit les informations détaillées au sujet du chemin de sortie, cela est exception et conditions d'erreurs, avec l'option de retour arrière activée par défaut. Les retours arrière peuvent alors être utilisés afin de décoder l'ordre précis de code qui a mené à l'état de chemin de sortie. Employez l'option de **détail** afin de récupérer les retours arrière de la mémoire tampon de suivi :

```
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 de mémoire tampon par défaut de suivi est 512 entrées, et ceci ne pourrait pas être assez si le problème est intermittent. Afin d'augmenter cette taille par défaut d'entrée de suivi, les paramètres de configuration de suivi d'événement peuvent être changés comme affiché 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 reprise et problèmes courants d'avion de contrôle GETVPN

Voici certaines des questions d'avion de contrôle commun pour GETVPN. Pour réitérer, l'avion de contrôle est défini en tant que tous les composants de caractéristique GETVPN exigés afin d'activer le cryptage et le déchiffrement de dataplane sur le GMs. À un haut niveau, ceci exige l'enregistrement réussi GM, la stratégie de sécurité et le téléchargement SA/installent, et rekey ultérieur KEK/TEK.

Création d'installation et de stratégie de CAGE

Afin de vérifier et vérifier que le KS a avec succès créé la stratégie de sécurité et le KEK/TEK associé, entrent :

```
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 l'installation de stratégie KS est quand il y a différentes stratégies configurées entre le KSs primaire et secondaire. Ceci peut avoir comme conséquence le comportement imprévisible KS et cette erreur sera signalée :

```
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
```

Actuellement il n'y a aucun sync de configuration automatique entre KSs primaire et secondaire, ainsi ceux-ci doivent être manuellement rectifiés.

Puisque la CAGE est une configuration essentielle (et presque toujours obligatoire) pour GETVPN, elle est principale pour s'assurer que des travaux de CAGE correctement et les rôles de la CAGE KS sont correcte :

```
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 installation fonctionnelle de CAGE, on devrait observer cet écoulement de protocole :

L'échange d'IKE > l'annonce avec des priorités de CAGE ont permuté > élection de CAGE > annonce de primaire à KS secondaire (stratégie, base de données GM, et clés)

Quand la CAGE ne fonctionne pas correctement, ou s'il y a un fractionnement de CAGE, tel que plusieurs KSs deviennent les KS primaires, ceux-ci mettent au point 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
```

Installation d'IKE

L'échange réussi d'IKE est exigé pour GETVPN afin de sécuriser le canal de contrôle pour la stratégie ultérieure et le téléchargement SA. À la fin de l'échange réussi d'IKE, GDOI_REKEY SA est créé.

Dans les versions plus tôt que le Cisco IOS 15.4(1)T, le GDOI_REKEY peut être affiché avec la commande de **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 le Cisco IOS 15.4(1)T et plus tard, ce GDOI_REKEY SA est affiché avec la commande de **rekey SA de show crypto gdoi** :

```
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 initial d'IKE se termine, des stratégies ultérieures et des clés **seront poussées du** KS au GM avec l'utilisation de GDOI_REKEY SA. Donc il n'y a aucun rekey pour GDOI_IDLE SA quand ils expirent ; ils disparaissent quand leurs vies expirent. Cependant, il devrait toujours y avoir de GDOI_REKEY SA sur le GM pour qu'il reçoive des rekeys.

L'échange d'IKE pour GETVPN n'est pas différent de l'IKE utilisé dans des tunnels point par point traditionnels d'IPsec, ainsi la méthode de dépannage demeure la même. Ceux-ci met au point doivent être collectés afin de dépanner des questions d'authentification d'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)
```

L'enregistrement, le téléchargement de stratégie, et la SA installent

Une fois que l'authentification d'IKE réussit, le GM s'inscrit au KS. On s'attend à ce que ces messages de Syslog soient vus quand ceci 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 avec 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 l'utilisation GETVPN, d'arrivée et sortante SAS le même SPI.

Avec GETVPN l'enregistrement et la stratégie installent le type de problèmes, ceux-ci met au point sont nécessaires afin de dépanner :

```
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: Supplémentaire met au point peut être exigé selon les résultats de ces sorties.

Puisque l'enregistrement GETVPN se produit typiquement juste après la recharge GM, ce script

EEM pourrait être utile afin de collecter ces derniers met au point :

```
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)
```

Rekey

Une fois que le GMs sont enregistrés au KS et le réseau GETVPN est correctement installé, le KS primaire est responsable d'envoyer des messages de rekey à tout le GMs enregistré à lui. Les messages de rekey sont utilisés afin de synchroniser tous les stratégies, clés, et pseudotimes sur le GMs. Les messages de rekey peuvent être envoyés par un unicast ou une méthode de Multidiffusion.

Ce message de Syslog est vu sur le KS quand le message de rekey est envoyé :

```
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)
```

Sur le GMs, c'est le Syslog qui est vu quand il reçoit le rekey :

```
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)
```

Condition requise de paire de clés RSA pour le rekey sur KS

La fonctionnalité de rekey exige la présence des clés RSA sur le KS. Le KS fournit la clé publique de la paire de clés RSA au GM par ce canal de sécuriser pendant l'enregistrement. Le KS signe alors les messages GDOI envoyés au GM avec la clé RSA privée dans la charge utile GDOI SIG. Le GM reçoit les messages GDOI et utilise la clé publique RSA afin de vérifier le message. Les messages entre le KS et le GM sont chiffrés avec le KEK, qui est également distribué au GM pendant l'enregistrement. Une fois que l'enregistrement est complet, des rekeys ultérieurs sont chiffrés avec le KEK et signés avec la clé RSA privée.

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

```
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)
```

Quand les clés ne sont pas présentes sur le KS, le GM s'enregistre pour la première fois, mais le prochain rekey échoue du KS. Par la suite les clés existantes sur le GM expirent, et il reregisters de nouveau.

```
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)
```

Puisque la paire de clés RSA est utilisée afin de signer les messages de rekey, ils **DOIVENT** être identiques entre le KSs primaire et tout le secondaire. Ceci s'assure que pendant une panne primaire KS, les rekeys envoyés par un KS secondaire (le nouveau KS primaire) peuvent encore être correctement validés par le GMs. Quand il génère la paire de clés RSA sur le KS primaire, la paire de clés doit être créée avec l'option **exportable** de sorte qu'ils puissent être exportés à tout le KSs secondaire afin de répondre à cette exigence.

Dépannage de rekey

La panne de rekey KEK/TEK est l'un des problèmes GETVPN les plus communs produits dans des déploiements de client. Le dépannage des questions de rekey devrait suivre les étapes de rekey comme tracé les grandes lignes ici :

1. Les rekeys ont-ils obtenu envoyé par le KS ?

   Ceci peut être vérifié par un observion du message de Syslog %GDOI-5-KS_SEND_UNICAST_REKEY ou plus exactement avec 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 rekeys retransmis est indicatif des paquets d'accusé de réception de rekey non reçus par le KS et donc les questions possibles de rekey. Maintenez dans l'esprit que le rekey GDOI utilise l'UDP comme mécanisme de transport peu fiable, ainsi quelques baisses de rekey pourraient être prévues selon la fiabilité du réseau de transport sous-jacent, mais une tendance des retransmissions croissantes de rekey devrait toujours être étudiée.

   Des statistiques plus détaillées du rekey par-GM peuvent également être obtenues. C'est typiquement le premier endroit pour rechercher les questions potentielles de rekey.

```
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 rekey ont-ils obtenu livré dans le réseau sous-jacent d'infrastructure ?

   Le dépannage standard IP le long du chemin de transfert de rekey devrait être suivi afin de s'assurer que les paquets de rekey ne sont pas lâchés dans le transit network entre KS et GM. Quelques outils communs de dépannage utilisés ici sont Listes de contrôle d'accès (ACL) d'entrée/sortie, NetFlow, et capture de paquet dans le transit network.

3. Les paquets de rekey ont-ils atteint le procédé GDOI pour le traitement de rekey ?

   Vérifiez les statistiques de rekey 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 rekey est-il revenu au KS ?

   Suivez les étapes 1 à 3 afin de tracer le paquet d'accusé de réception de rekey du GM de nouveau au KS.

Rekey de Muticast

Le rekey de Multidiffusion est différent du rekey d'unicast dans ces aspects :

- Puisque la Multidiffusion est utilisée afin de transporter ces paquets de rekey du KS au GMs, le KS n'a pas besoin de répliquer les paquets de rekey lui-même. Le KS envoie seulement une copie du paquet de rekey, et ils sont répliqués dans le réseau Multidiffusion-activé.
- Il n'y a aucun mécanisme d'accusé de réception pour le rekey de Multidiffusion, ainsi si un GM n'étaient pas de recevoir le paquet de rekey, le KS n'aurait aucune connaissance de lui, et donc ne retirera jamais un GM de sa base de données GM. Et parce qu'il n'y a aucun accusé de réception, le KS retransmettra toujours les paquets de rekey basés sur sa configuration de retransmission de rekey.

Le plus généralement - le problème vu de rekey de Multidiffusion est quand le rekey n'est pas reçu sur le GM. Il a pu y avoir un certain nombre de causes possibles pour ceci, comme :

- Question de la livraison de paquet dans l'infrastructure de routage de Multidiffusion
- Le routage de bout en bout de Multidiffusion n'est pas activé dans le réseau

La première étape pour dépanner une question avec le rekey de Multidiffusion est de voir si des travaux de rekey une fois commutée de la Multidiffusion à la méthode d'unicast.

Une fois que vous identifiez que la question est spécifique au rekey de Multidiffusion, vérifiez que KS envoie le rekey à l'adresse de multidiffusion spécifiée.

```
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
```

Testez la connectivité multicast entre le KS et le GM avec une demande de Protocole ICMP (Internet Control Message Protocol) à l'adresse de multidiffusion. Tout le GMs qui font partie du groupe de multidiffusion devrait répondre au ping. Assurez-vous que l'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 de ping de Multidiffusion échoue, alors le dépannage de Multidiffusion doit être exécuté, qui est en dehors de la portée de ce document.

Contrôlez le contrôle plat de relais

Symptôme

Quand les clients améliorent leur GM à une nouvelle version de Cisco IOS, ils pourraient éprouver des pannes de rekey KEK avec ce message observé dans le Syslog :

```
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
```

Ce comportement est provoqué par par un problème d'interopérabilité introduit avec le contrôle d'anti-relecture qui est ajouté pour des messages d'avion de contrôle. Spécifiquement, un KS qui exécute le code plus ancien remettra à l'état initial le numéro de séquence de rekey KEK à 1, et ceci sera relâché par le GM qui exécute le nouveau code quand il interprète qui comme paquet rejoué de rekey. Pour plus de détails, voir l'ID de bogue Cisco CSCta05809 (GETVPN : Contrôle-avion GETVPN raisonnable pour rejouer), et restrictions de configuration GETVPN.

Fond

Avec GETVPN, les messages d'avion de contrôle peuvent diffuser les informations sensibles au temps afin de fournir le service basé sur temps de contrôle d'anti-relecture. Par conséquent, ces messages exigent de la protection d'anti-relecture eux-mêmes afin d'assurer l'accruracy de temps. Ces messages sont :

- **Messages de rekey de** KS au GM
- **Messages d'annonce de CAGE** entre KSs

En tant qu'élément de cette implémentation de protection d'anti-relecture, des contrôles de numéro de séquence ont été ajoutés afin de protéger des messages rejoués, aussi bien qu'un contrôle de pseudotime quand TBAR est activé.

Solution

Afin de résoudre ce problème, le GM et KS doivent être mis à jour aux versions de Cisco IOS après que la caractéristique de contrôle de rediffusion d'avion de contrôle. Avec nouveau code de Cisco IOS, KS ne remet pas à l'état initial le numéro de séquence de nouveau au 1par un rekey KEK, mais à la place il continue à utiliser le numéro de séquence en cours et remet à l'état initial seulement le numéro de séquence pour des rekeys TEK.

Ces versions de Cisco IOS ont les caractéristiques de contrôle de rediffusion :

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

Autre rejouent des questions connexes

- La panne de CAGE due à la rediffusion manquante de messages annonce vérifient (ID de bogue Cisco CSCtc52655)

Pannes de rediffusion d'avion de contrôle de debug

Pour d'autres pannes de rediffusion d'avion de contrôle, collectez ces informations et assurez-vous que les temps synched entre le KS et le GM.

- Syslog de GM et de KS
- L'ISAKMP met au point
- GDOI met au point (rekey et rediffusion) de KS et de GM

Contrôlez les questions plates de fragmentation de paquets

Avec GETVPN, la fragmentation de paquets plate de contrôle est un problème courant, et elle peut se manifester dans un de ces deux scénarios quand les paquets d'avion de contrôle sont assez grands qu'ils exigeront la fragmentation IP :

- Paquets d'annonce de CAGE GETVPN
- Paquets de rekey GETVPN

Paquets d'annonce de CAGE

Les paquets d'annonce de CAGE diffusent les informations de base de données GM, et peuvent se développer ainsi grands dans un grand déploiement GETVPN. De l'expérience passée, un réseau GETVPN qui se compose de 1500+ GMs produira des paquets d'annonce plus grands que 18024 octets, qui est la taille de tampon énorme par défaut de Cisco IOS. Quand ceci se produit, le KS n'alloue pas une mémoire tampon assez grande pour transmettre les paquets annonce avec cette erreur :

```
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
```

Afin de rectifier cette condition, cet ajustement de mémoire tampon est recommandé :

```
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
```

Paquets de rekey

Les paquets de rekey GETVPN peuvent également dépasser la taille maximum typique d'unité de transition IP 1500 (MTU) quand la stratégie de chiffrement est grande, comme une stratégie qui se compose des lignes 8+ des entrées de contrôle d'accès (as) dans l'ACL de cryptage.

Problème et identification de fragmentation

Dans chacun des deux scénarios précédents, GETVPN doit pouvoir correctement transmettre et recevoir les paquets UDP fragmentés pour que le rekey de CAGE ou GDOI fonctionne correctement. La fragmentation IP peut être un problème dans quelques environnements de réseau. Par exemple, un réseau qui se compose de l'avion multi d'expédition du chemin de coût égal (ECMP), et quelques périphériques dans l'avion d'expédition exigent le réassemblage virtuel des paquets IP fragmentés, tels que le réassemblage virtuel de fragmentation (VFR).

Afin d'identifier le problème, vérifiez les erreurs de réassemblage sur le périphérique où on le suspecte que l'UDP fragmenté 848 paquets ne soient 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 d'attente de réassemblage continuent à incrémenter, employez la commande de **debug ip error** afin de confirmer si la baisse fait partie de l'écoulement de paquet rekey/COOP. Une fois que confirmé, le dépannage normal d'expédition IP devrait être exécuté afin d'isoler le périphérique précis dans l'avion d'expédition qui pourrait avoir relâché les paquets. Quelques outils utilisés généralement incluent :

- Capture de paquet
- Statistiques d'expédition du trafic
- Statistiques de fonctionnalité de sécurité (Pare-feu, IPS)

- Statistiques VFR

Problèmes d'interopérabilité GDOI

De divers problèmes d'interopérabilité ont été trouvés avec GETVPN au cours des années, et il est essentiel de noter les versions de Cisco IOS entre KS et GM et parmi le KSs pour des problèmes d'interopérabilité.

D'autres problèmes d'interopérabilité réputés GETVPN sont :

- Contrôlez le contrôle plat de relais
- Modification de comportement de rekey GETVPN KEK
- ID de bogue Cisco CSCub42920 (GETVPN : KS ne valide pas des informations parasites dans le rekey ACK des versions précédentes GM)
- ID de bogue Cisco CSCuw48400 (le GM de GetVPN incapable de s'enregistrer ou le rekey échoue - des Sig-informations parasites > le par défaut SHA-1)
- ID de bogue Cisco CSCvg19281 (GM de multiple GETVPN tombe en panne après transfert à de nouvelles paires KS ; si une version GM est plus tôt que 3.16, et KS est mis à jour de code antérieur à 3.16 ou plus tard, cette question peut se produire)

Procédure de mise à niveau d'IOS GETVPN

Cette procédure de mise à niveau de Cisco IOS devrait être suivie quand une mise à jour de code de Cisco IOS doit être exécutée dans un environnement GETVPN :

1. Améliorez un KS secondaire d'abord et attendez jusqu'à ce que l'élection de la CAGE KS soit terminée.
2. Répétition Step1 pour tout le KSs secondaire.
3. Améliorez le KS primaire.
4. Mise à jour GMs.

Dépannez les questions de plan de données GETVPN

Comparé pour contrôler des problèmes plats, les questions de plan de données GETVPN sont des problèmes où le GM a la stratégie et les clés pour exécuter le cryptage et le déchiffrement de dataplane, mais pour quelque raison la circulation de bout en bout ne fonctionne pas. La plupart des questions de dataplane pour GETVPN associent à l'expédition générique d'IPsec, et ne sont pas particularité GETVPN. Ainsi la majeure partie de l'approche de dépannage décrite ici s'applique aux questions génériques de dataplane d'IPsec aussi bien.

Avec des problèmes de cryptage (basé sur groupe ou par paires des tunnels), il est important de dépanner le problème et de localiser le problème dans une partie particulière du datapath. Spécifiquement, l'approche de dépannage décrite ici est destinée pour vous aider à répondre à ces questions :

- Quel périphérique est le coupable - routeur de cryptage ou routeur de déchiffrage ?
- Dans quelle direction est-il le problème se produisant - d'entrée ou de sortie ?

Outils de dépannage de plan de données GETVPN

Le dépannage de dataplane d'IPsec est très différent de celui pour l'avion de contrôle. Avec le dataplane, il y a habituellement aucun met au point que vous pouvez s'exécuter, ou s'exécute au moins sans risque dans un environnement de production. Ainsi le dépannage se fonde fortement sur les différents compteurs et statistiques de trafic qui peuvent aider à tracer le paquet le long d'un chemin de transfert. L'idée est de pouvoir développer un ensemble de points de reprise afin d'aider à isoler où des paquets pourraient être lâchés comme affiché ici :

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)

Les points de reprise dans le datapath dans l'image précédente peuvent être validés avec ces outils :

Chiffrer le GM

- Interface de RÉSEAU LOCAL d'entrée
  - ACL d'entrée
  - NetFlow d'entrée
  - Capture incluse de paquet
  - Comptabilité de priorité d'entrée

- Moteur de chiffrement
  - show crypto ipsec sa
  - **détail de show crypto ipsec sa**
  - **shows crypto engine accelerator statistics**

- Interface WAN de sortie
  - NetFlow de sortie
  - Capture incluse de paquet
  - Comptabilité de priorité de sortie

GM de déchiffrage

- Interface WAN d'entrée
  - ACL d'entrée

NetFlow d'entrée
Capture incluse de paquet
Comptabilité de priorité d'entrée

- Moteur de chiffrement
  show crypto ipsec sa
  détail de show crypto ipsec sa
  shows crypto engine accelerator statistics

- Interface de RÉSEAU LOCAL de sortie
  NetFlow de sortie
  Capture incluse de paquet

Le chemin de retour suit la même circulation. Les sections suivantes ont quelques exemples de ces outils de dataplane en service.

Compteurs de cryptage/déchiffrement

Les compteurs de cryptage/déchiffrement sur un routeur sont basés sur un écoulement d'IPsec. Malheureusement ceci ne fonctionne pas bien avec GETVPN puisque GETVPN déploie typiquement un « IP d'autorisation n'importe quelle n'importe quelle » stratégie de chiffrement qui chiffre tout. Ainsi si le problème se produit seulement pour certains des écoulements et pas de tous, il peut être quelque peu difficiles les utiliser ces compteurs afin d'évaluer correctement si les paquets sont chiffrés ou déchiffrés quand il y a assez de trafic significatif de fond 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

Le NetFlow peut être utilisé afin de surveiller le d'entrée et le trafic en sortie sur des les deux GMs. La note avec l'**IP d'autorisation** GETVPN **n'importe quelle n'importe quelle** stratégie, le trafic enrypted sera agrégat et ne fournit pas les informations de par-écoulement. les informations de Par-écoulement devront alors être collectées avec le marquage DSCP/precedence décrit plus tard.

Dans cet exemple, le NetFlow pour un ping de 100 comptes d'un hôte derrière GM1 à un hôte derrière GM2 est affiché aux divers points de reprise.

Chiffrer le 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
```

NetFlow sorti :

```
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 la sortie précédente, * dénote le trafic en sortie. La première ligne le trafic chiffré par de sortie d'expositions (avec le protocole 0x32 = l'ESP) hors de l'interface WAN, et la deuxième ligne le trafic d'ICMP d'entrée frappant l'interface de RÉSEAU LOCAL.

GM de déchiffrage

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
```

NetFlow sorti :

```
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 défi avec dépanner un problème de cryptage est qu'une fois que le paquet est chiffré vous perdent la visibilité dans la charge utile, est qui ce que le cryptage est censé pour faire, et cela le rend difficile de tracer le paquet pour un ip flow particulier. Il y a deux manières d'adresser cette limite quand il s'agit de dépanner un problème d'IPsec :

- L'utilisation ESP-NULL comme IPsec transforment. IPsec effectue toujours l'encapsulation de l'ESP mais aucun cryptage n'est appliqué à la charge utile, ainsi ils sont visibles dans une capture de paquet.
- Marquez un ip flow avec un seul marquage de Differentiated Services Code Point (DSCP) /precedence basé sur leurs caractéristiques L3/L4.

ESP-NULL exigent des modifications sur des points d'extrémité de tunnel et souvent ne sont pas laissés basé sur la stratégie de sécurité de client. Par conséquent, Cisco recommande

typiquement l'utilisation de DSCP/precedence marquant à la place.

Tableau de référence DSCP/Precedence

Tos (hexa)	ToS(Decimal)	Priorité IP	DSCP	Binaire
0xE0	224	Network Control 7	56 CS7	11100000
0xC0	192	Contrôle de l'interréseau 6	48 CS6	11000000
0xB8	184	5 essentiel	46 E-F	10111000
0xA0	160		40 CS5	10100000
0x88	136	Dépassement 4 instantané	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	Éclair 3	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 routines	0 Dflt	00000000

Marquez les paquets avec DSCP/Precedence

Ces méthodes sont typiquement utilisées afin de marquer des paquets avec les marquages de la particularité DSCP/Precedence.

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
```

Ping de routeur

```
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**: C'est toujours une bonne idée de surveiller la circulation normale et profil DSCP/precedence avant que vous appliquiez le marquage de sorte que la circulation marquée soit seule.

Surveillez 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 incluse de paquet

La capture incluse de paquet (CPE) est un outil utile pour capturer des paquets au niveau d'interface afin d'identifier si un paquet a atteint un appareil spécifique. Souvenez-vous que les travaux CPE bien pour le trafic des textes clairs, mais ce peuvent être un défi quand les paquets capturés sont chiffrés. Par conséquent des techniques comme le marquage DSCP/precedence discuté précédemment ou d'autres caractères IP, tels que la longueur du paquet IP, doivent être utilisés ainsi que la CPE afin de faire le dépannage de plus efficace.

Tracé de paquets de Cisco IOS XE

C'est une fonctionnalité utile pour tracer le chemin de transfert de caractéristique sur toutes les Plateformes qui exécutent le Cisco IOS XE, tel que CSR1000v, ASR1000, et ISR4451-X.

Problèmes courants de plan de données GETVPN

Le dépannage du dataplane d'IPsec pour GETVPN n'est en grande partie pas différent de dépanner les questions point par point traditionnelles de dataplane d'IPsec, à deux exceptions

dues à ces seules propriétés de dataplane de GETVPN.

Le temps a basé la panne d'anti-relecture

Dans un réseau GETVPN, il peut souvent être difficiles dépanner des pannes TBAR puisqu'il n'y a plus par paires des tunnels. Afin de dépanner des pannes GETVPN TBAR, terminez-vous ces étapes :

1. Identifiez quel paquet est dû lâché à la panne TBAR et identifiez ultérieurement le GM chiffrant.

   Avant la version 15.3(2)T, le Syslog de panne TBAR n'a pas imprimé l'adresse de source du paquet défectueux, ainsi ceci le rend très difficile d'identifier quel paquet a manqué. Ceci a été sensiblement amélioré dans la version 15.3(2)T et ultérieures, où le Cisco IOS imprime ceci :

```
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
```

   Un historique TBAR a été également mis en application 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 été depuis mises en application dans le Cisco IOS XE par l'ID de bogue Cisco CSCun49335 et dans le Cisco IOS par l'ID de bogue Cisco CSCub91811.
   Pour les versions de Cisco IOS qui n'ont pas eu cette caractéristique, le **détail de rediffusion GM de debug crypto gdoi** peut également fournir ces informations, bien que ceci mettent au point des copies les informations TBAR pour tout le trafic (non seulement en raison relâché par paquets de la panne TBAR), ainsi il ne pourrait pas être faisable de s'exécuter dans un environnement de production.

```
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
```

2. Une fois la source du paquet est identifiée, vous devrait pouvoir trouver le GM chiffrant. Puis, le pseudotimestamp sur le GMs chiffrant et de déchiffrage devrait être surveillé pour n'importe quelle dérive potentielle de pseudotime. La meilleure manière de faire ceci serait de synchroniser GMs et le KS au NTP et de collecter périodiquement les informations de pseudotime avec une horloge système de référence sur tous afin de déterminer si le problème est provoqué par par distorsion d'horloge sur le GMs.

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

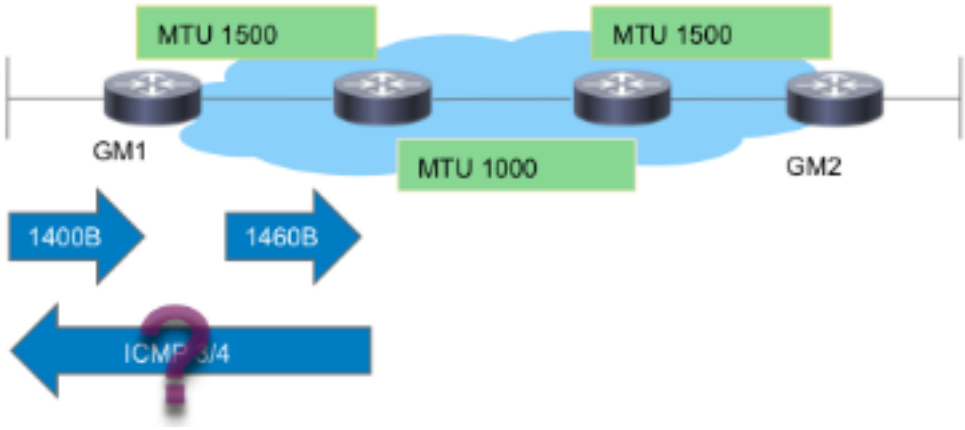
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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 pseudotime (comme indiqué par valeur de rediffusion) est sensiblement différent entre le GMs quand les sorties sont capturées avec du même temps de référence, alors le problème peut être attribué pour synchroniser la distorsion.

> **Note**: Sur Cisco la plate-forme agrégée de gamme 1000 de routeur de services, due à l'architecture de plate-forme, le datapath sur le processeur d'écoulement de Quantum (QFP) se rapporte réellement à l'horloge de mur pour compter des coutils de pseudotime. Ceci a créé des problèmes avec TBAR quand les modifications de temps d'horloge murale dues au sync de NTP. Ce problème est documenté avec l'ID de bogue Cisco CSCum37911.

Conservation d'en-tête PMTUD et GETVPN

Avec GETVPN, la découverte de MTU de chemin (PMTUD) ne fonctionne pas entre le GMs chiffrant et de déchiffrage, et de grands paquets avec le positionnement de bit du Don't Fragment (DF) peut obtenir blackholed. La raison pour laquelle ceci ne fonctionne pas est due à la conservation d'en-tête GETVPN où le point d'émission de données/adresses de destination sont préservés en ESP encapsulant l'en-tête. Ceci est dépeint dans cette image :



Pendant que l'image affiche, PMTUD décompose avec GETVPN avec cet écoulement :

1. Le grand paquet de données arrive sur le GM1 chiffrant.
2. Le paquet de l'ESP de POST-cryptage est expédié hors de GM1 et livré vers la destination.
3. S'il y a une liaison de transit avec l'IP MTU de 1400 octets, le paquet de l'ESP sera lâché, et un ICMP 3/4 message trop grand de paquet sera envoyé vers la source de paquet, qui est la source du paquet de données.
4. Le paquet ICMP3/4 est vers la fin hôte dû à l'ICMP non exclu de la stratégie de chiffrement GETVPN et ou lâché lâché puisqu'il ne connaît rien le paquet de l'ESP (charge utile unauthenticated).

En résumé, PMTUD ne fonctionne pas avec GETVPN aujourd'hui. Afin de fonctionner autour de cette question, Cisco recommande ces étapes :

1. La mise en place « ip tcp adjust-mss » afin de réduire la commande o de bidon de taille de segment de paquet TCP facilitent le MTU de chemin de temps système et de minimum de cryptage dans le transit network.
2. Effacez le bit DF dans le paquet de données comme ils arrivent sur le GM chiffrant afin d'éviter PMTUD.

Questions génériques d'IPsec Dataplane

La majeure partie du dépannage de dataplane d'IPsec est comme dépanner les tunnels point par point traditionnels d'IPsec. Un des problèmes courants est %CRYPTO-4-RECVD_PKT_MAC_ERR. Voir le message d'erreur du Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" avec la perte de ping au-dessus du dépannage de tunnel d'IPsec pour plus de détails de dépannage.

Problèmes identifiés

Ce message peut être généré quand on reçoit un paquet d'IPsec qui n'apparie pas un SPI dans le SADB. Voir l'ID de bogue Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC

signalé pour le paquet n'appariant pas l'écoulement. Un exemple est :

```
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
```

Ce message devrait être %CRYPTO-4-RECVD_PKT_INV_SPI, qui est ce qui obtient signalé pour IPsec traditionnel aussi bien que sur certaines plates-formes matérielles telles que l'ASR. Cette question cosmétique a été réparée par l'ID de bogue Cisco CSCup80547 : Erreur en signalant CRYPTO-4-RECVD_PKT_NOT_IPSEC pour l'ESP PAK.

> **Note**: Ces messages peuvent parfois sembler dus à une autre bogue CSCup34371 GETVPN : Arrêts GM GETVPN decrytping le trafic après rekey TEK.

Dans ce cas, le GM ne peut pas déchiffrer le trafic GETVPN, bien qu'il ait IPsec valide SA dans le SADB (SA étant réintroduite). Le problème disparaît dès que SA expirera et est retirée du SADB. Cette question entraîne la panne significative, parce que le rekey TEK est exécuté à l'avance. Par exemple, la panne peut être de 22 minutes dans le cas d'une vie TEK de 7200 secondes. Voyez la description de bogue pour la condition précise qui devrait être remplie afin de rencontrer cette bogue.

Dépannez GETVPN sur les Plateformes qui exécutent le Cisco IOS XE

Dépannage des commandes

Les Plateformes qui exécutent le Cisco IOS XE ont des réalisations de plateforme spécifique, et exigent souvent le plateforme spécifique mettant au point pour des questions GETVPN. Voici une liste des commandes typiquement utilisée afin de dépanner GETVPN sur ces Plateformes :

show crypto eli tout

statistiques de stratégie d'ipsec de logiciel de show platform

inventaire d'active point de gel d'ipsec de logiciel de show platform

ipsec actif SPD tout de caractéristique de qfp de matériel de show platform

baisse de statistiques actives de qfp de matériel de show platform claire

les données actives d'ipsec de caractéristique de qfp de matériel de show platform chutent clairement

show crypto ipsec sa

show crypto gdoi

affichez le crypto ipsec interne

debug crypto ipsec

erreur de debug crypto ipsec

états de debug crypto ipsec

message de debug crypto ipsec

hw-req de debug crypto ipsec

de debug crypto gdoi GM détail infra

détail de rekey GM de debug crypto gdoi

Problèmes courants ASR1000

La stratégie d'IPsec installent la panne (le Re-enregistrement continu)

Un GM ASR1000 pourrait continuer à s'enregistrer au serveur principal si le moteur de chiffrement ne prend en charge pas la stratégie ou l'algorithme d'IPsec reçu. Par exemple, sur le Nitrox a basé des Plateformes ASR (telles qu'ASR1002), suite-b ou les stratégies SHA2 ne sont pas prises en charge et ceci peut entraîner les symptômes continus de re-enregistrement.

Questions communes de transfert/mise à jour

Limite ASR1000 TBAR

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

Cette bogue d'amélioration a été ouverte pour lever cette restriction, l'ID de bogue Cisco CSCuq25476 - ASR1k doit prendre en charge une taille de la fenêtre GETVPN TBAR de moins de 20 secondes.

Mise à jour : Cette restriction a été depuis levée avec la difficulté pour l'ID de bogue Cisco CSCur57558, et ce n'est plus une limite en XE3.10.5, XE3.13.2 et code postérieur.

Notez-également, pour un GM qui fonctionne sur des Plateformes de Cisco IOS XE (ASR1k ou ISR4k), l'est fortement recommandé que le périphérique exécute une version avec la difficulté pour cette question si TBAR est activé ; ID de bogue Cisco CSCut91647 - GETVPN sur IOS-XE : Le GM relâche inexactement des paquets dus à la panne TBAR.

Question de la classification ISR4x00

Une régression a été trouvée sur la plate-forme ISR4x00 où les stratégies de refuser sont

ignorées. Pour des détails, voir l'ID de bogue Cisco CSCut14355 - GETVPN - Le GM ISR4300 ignore refusent la stratégie.

Informations connexes

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