

Dépannage des problèmes IPsec pour les tunnels de service sur les vEdge avec IKEv2

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Glossaire IKE](#)

[Échange de paquets IKEv2](#)

[Dépannage](#)

[Activer les débogages IKE](#)

[Conseils pour démarrer le processus de dépannage des problèmes IPsec](#)

[Symptôme 1. Le tunnel IPsec n'est pas établi](#)

[Symptôme 2. Le tunnel IPsec s'est arrêté et a été rétabli de lui-même](#)

[Retransmissions DPD](#)

[Symptôme 3. Le tunnel IPsec s'est arrêté et reste à l'état d'arrêt](#)

[Non-concordance PFS](#)

[Tunnel vEdge IPsec/Ikev2 non relancé après avoir été arrêté en raison d'un événement DELETE](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner les problèmes les plus courants pour les tunnels de sécurité du protocole Internet (IPsec) vers des périphériques tiers avec Internet Key Exchange version 2 (IKEv2) configuré. La documentation Cisco SD-WAN fait généralement référence aux tunnels de service/transport. Ce document explique également comment activer et lire les débogages IKE et les associer à l'échange de paquets pour comprendre le point d'échec sur une négociation IPsec.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEv2
- Négociation IPsec
- SD-WAN Cisco

Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

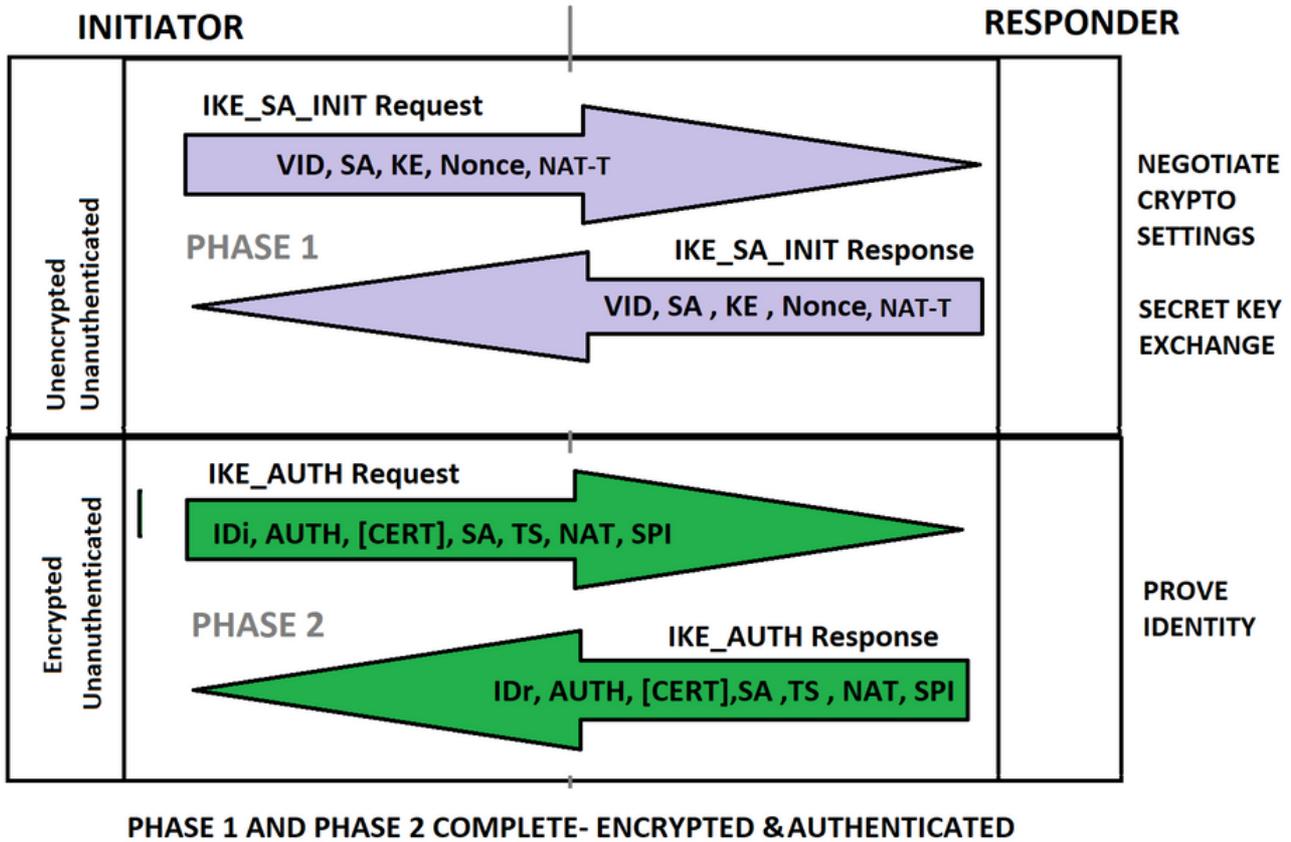
Glossaire IKE

- IPsec (Internet Protocol security) est une suite standard de protocoles entre deux points de communication sur le réseau IP qui fournit l'authentification, l'intégrité et la confidentialité des données.
- IKEv2 (Internet Key Exchange version 2) est le protocole utilisé pour configurer une association de sécurité (SA) dans la suite de protocoles IPsec.
- Une association de sécurité (SA) est l'établissement d'attributs de sécurité partagés entre deux entités réseau pour prendre en charge des communications sécurisées. Une SA peut inclure des attributs tels que l'algorithme et le mode cryptographiques ; clé de cryptage du trafic ; et les paramètres des données réseau à transmettre sur la connexion.
- Les ID de fournisseur (VID) sont utilisés pour identifier les périphériques homologues avec la même implémentation de fournisseur afin de prendre en charge des fonctionnalités spécifiques au fournisseur.
- Nonce : valeurs aléatoires créées dans l'échange pour ajouter du caractère aléatoire et empêcher les attaques de relecture.
- Informations Key-exchange (KE) pour le processus d'échange de clés sécurisé Diffie-Hellman (DH).
- L'identité de l'initiateur/répondeur (IDi/IDr) est utilisée pour envoyer des renseignements d'authentification à l'homologue. Ces informations sont transmises sous la protection du secret partagé commun.
- La clé partagée IPsec peut être dérivée avec l'utilisation de DH à nouveau pour assurer Perfect Forward Secrecy (PFS) ou avec une actualisation du secret partagé dérivé de l'échange DH original.
- L'échange de clés Diffie-Hellman (DH) est une méthode d'échange sécurisé d'algorithmes cryptographiques sur un canal public.
- Les sélecteurs de trafic (TS) sont les identités de proxy ou le trafic échangé lors de la négociation IPsec pour passer à travers le tunnel chiffré.

Échange de paquets IKEv2

Chaque paquet IKE contient des informations de charge utile pour l'établissement du tunnel. Le glossaire IKE explique les abréviations indiquées sur cette image dans le contenu de la charge utile pour l'échange de paquets.

IKEV2 PACKET EXCHANGE



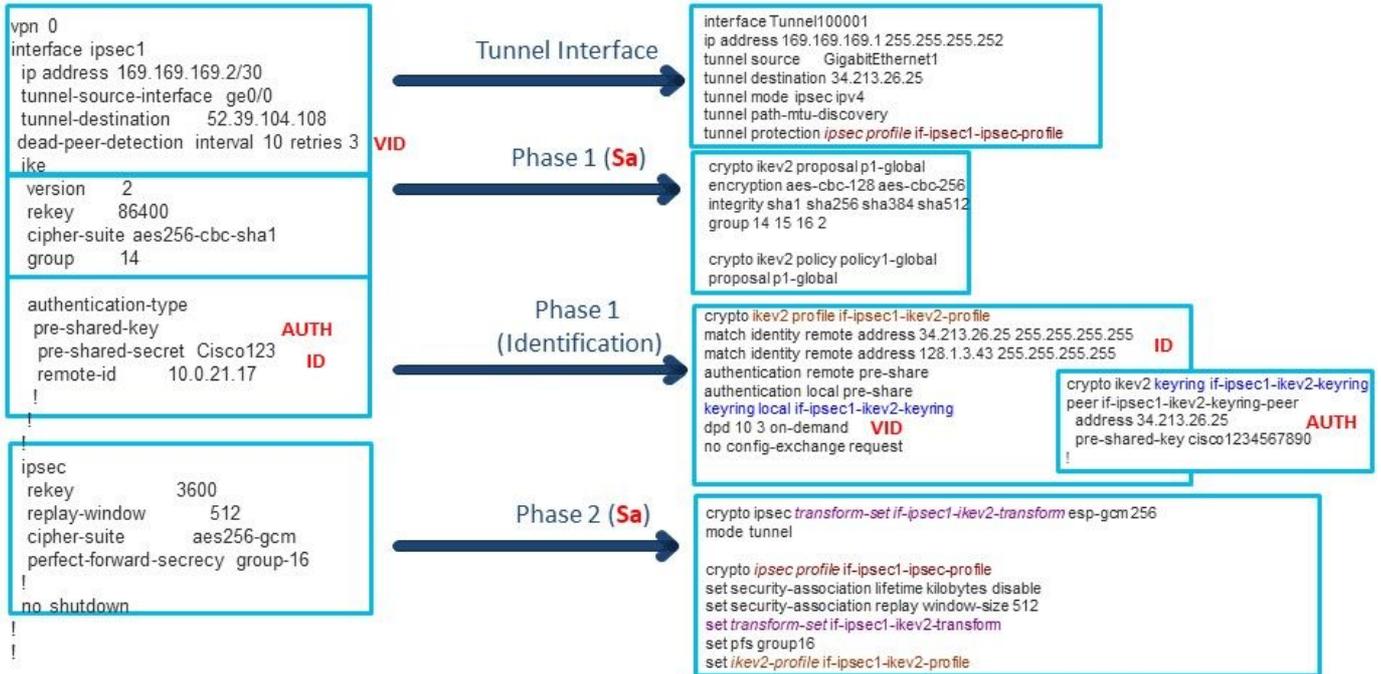
IKEV2-Exchange

✎ Remarque : Il est important de vérifier sur quel échange de paquets de la négociation IKE le tunnel IPsec ne parvient pas à analyser rapidement quelle configuration est impliquée pour résoudre efficacement le problème.

✎ Remarque : Ce document ne décrit pas plus en détail l'échange de paquets IKEv2. Pour plus de références, accédez à [IKEv2 Packet Exchange and Protocol Level Debugging](#)

Il est nécessaire de corréler la configuration vEdge avec la configuration Cisco IOS® XE. Il est également utile de faire correspondre les concepts IPsec et le contenu de la charge utile pour les échanges de paquets IKEv2, comme illustré dans l'image.

Vedge and IOS-XE Config.



Remarque : Chaque partie de la configuration modifie un aspect de l'échange de négociation IKE. Il est important de corréliser les commandes avec la négociation de protocole d'IPsec.

Dépannage

Activer les débogages IKE

Sur vEdge debug iked active les informations de niveau de débogage IKEv1 ou IKEv2.

```
debug iked misc high
debug iked event high
```

Il est possible d'afficher les informations de débogage actuelles dans vshell et d'exécuter la commande `tail -f <chemin de débogage>`.

```
vshell
tail -f /var/log/message
```

Dans CLI, il est également possible d'afficher les journaux/informations de débogage actuels pour le chemin spécifié.

```
monitor start /var/log/messages
```

Conseils pour démarrer le processus de dépannage des problèmes IPsec

Il est possible de séparer trois scénarios IPsec différents. C'est un bon point de référence pour identifier le symptôme d'avoir une meilleure approche pour savoir comment commencer.

1. Le tunnel IPsec ne s'établit pas.
2. Le tunnel IPsec s'est arrêté et il a été rétabli tout seul. (Rabat)
3. Le tunnel IPsec est tombé en panne et il reste à l'état down.

Pour le tunnel IPsec n'établit pas de symptômes, il est nécessaire de déboguer en temps réel pour vérifier quel est le comportement actuel sur la négociation IKE.

Pour IPsec tunnel est tombé en panne et il a rétabli sur ses propres symptômes, plus communément connu sous le nom de tunnel Flapped et l'analyse de la cause première (RCA) est nécessaire. Il est indispensable de connaître l'horodatage de la panne du tunnel ou d'avoir une estimation du temps pour examiner les débogages.

Pour le tunnel IPsec est tombé en panne et il reste sur les symptômes d'état d'arrêt, cela signifie que le tunnel a fonctionné avant, mais pour une raison quelconque, il est tombé et nous devons connaître la raison de démontage et le comportement actuel qui empêche le tunnel d'être établi avec succès à nouveau.

Identifiez les points avant le début du dépannage :

1. Tunnel IPsec (numéro) avec problèmes et configuration.
2. Horodatage de la panne du tunnel (le cas échéant).
3. Adresse IP de l'homologue IPsec (destination du tunnel).

Tous les débogages et les journaux sont enregistrés sur les fichiers /var/log/messages, pour les journaux actuels, ils sont enregistrés sur les fichiers messages mais pour ce symptôme spécifique, le flap pourrait être identifié des heures/jours après le problème, très probablement les débogages liés seraient sur les messages 1,2,3..etc. Il est important de connaître l'horodatage pour regarder le bon fichier de message et analyser les débogages (charon) pour la négociation IKE du tunnel IPsec associé.

La plupart des débogages n'impriment pas le numéro du tunnel IPsec. La façon la plus fréquente d'identifier la négociation et les paquets est avec l'adresse IP de l'homologue distant et l'adresse IP d'où le tunnel provient sur le bord. Quelques exemples de débogages IKE imprimés :

```
<#root>
```

```
Jun 18 00:31:22 vedge01
```

```
charon:
```

```
09[CFG] vici initiate '
```

```
child_IPsec2_1
```

```
,  
Jun 18 00:31:22 vedge01
```

```
charon:
```

```
16[IKE] initiating
```

```
IKE_SA ipsec2_1
```

```
[223798] to 10.10.10.1  
Jun 18 00:31:22 vedge01
```

```
charon:
```

```
16[IKE] initiating
```

```
IKE_SA ipsec2_1
```

```
[223798] to 10.10.10.1
```

Les débogages de la négociation IKE INIT indiquent le numéro du tunnel IPsec. Cependant, les informations suivantes pour l'échange de paquets utilisent uniquement les adresses IP du tunnel IPsec.

```
<#root>
```

```
Jun 18 00:31:22 vedge01 charon: 09[CFG] vici initiate 'child_ipsec2_1'  
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1  
Jun 18 00:31:22 vedge01 charon: 16[IKE] initiating IKE_SA ipsec2_1[223798] to 10.10.10.1  
Jun 18 00:31:22 vedge01 charon: 16[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]  
Jun 18 00:31:22 vedge01 charon: 16[NET] sending packet:
```

```
from 10.132.3.92[500] to 10.10.10.1[500]
```

```
(464 bytes)
```

```
Jun 18 00:31:22 vedge01 charon: 12[NET] received packet:
```

```
from 10.10.10.1[500] to 10.132.3.92[500]
```

```
(468 bytes)
```

```
Jun 18 00:31:22 vedge01 charon: 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]  
Jun 18 00:31:22 vedge01 charon: 12[ENC] received unknown vendor ID: 4f:85:58:17:1d:21:a0:8d:69:cb:5f:60  
Jun 18 00:31:22 vedge01 charon: 12[IKE] local host is behind NAT, sending keep alives
```

Configuration du tunnel IPsec :

```
interface ipsec2  
 ip address 192.168.1.9/30  
 tunnel-source 10.132.3.92  
 tunnel-destination 10.10.10.1  
 dead-peer-detection interval 30  
 ike
```

```

version      2
rekey        86400
cipher-suite aes256-cbc-sha1
group        14
authentication-type
pre-shared-key
pre-shared-secret $8$wgrs/Cw6tX0na34yF4Fga0B62mGBpHFd0zFaRmoYfnBioWV03s3efFPBbkaZqvoN
!
!
!
ipsec
rekey          3600
replay-window  512
cipher-suite   aes256-gcm
perfect-forward-secrecy group-14
!

```

Symptôme 1. Le tunnel IPsec n'est pas établi

Comme le problème peut être la première implémentation du tunnel, il n'a pas été activé et les débogages IKE sont la meilleure option.

Symptôme 2. Le tunnel IPsec s'est arrêté et a été rétabli de lui-même

Comme mentionné précédemment, ce symptôme est généralement adressé pour connaître la cause première de la panne du tunnel. Lorsque l'analyse de la cause première est connue, l'administrateur du réseau empêche parfois d'autres problèmes.

Identifiez les points avant le début du dépannage :

1. Tunnel IPsec (numéro) avec problèmes et configuration.
2. Horodatage de la panne du tunnel.
3. Adresse IP de l'homologue IPsec (destination du tunnel)

Retransmissions DPD

Dans cet exemple, le tunnel est tombé le 18 juin à 00:31:17.

```
<#root>
```

```
Jun 18 00:31:17 vedge01 FTMD[1472]:
```

```
%Viptela-vedge01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec2 DOWN
```

```
Jun 18 00:31:17 vedge01 FTMD[1472]:
```

```
%Viptela-vedge01-ftmd-6-INFO-1400002:
```

```
Notification: interface-state-change severity-level:major host-name:"vedge01" system-ip:4.0.5.1 vpn-id
```

 Remarque : Les journaux pour la désactivation du tunnel IPsec ne font pas partie des débogages liés, ce sont des journaux FTMD. Par conséquent, ni charon ni IKE ne seraient imprimés.

 Remarque : Les journaux associés ne sont généralement pas imprimés ensemble, il y a plus d'informations entre eux non liés au même processus.

Étape 1. Une fois l'horodatage identifié et l'heure et les journaux mis en corrélation, commencez à examiner les journaux de bas en haut.

```
Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
```

<#root>

```
Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with
```

```
message ID 543
```

```
(tries=3, timeout=30, exchange=37, state=2)
```

```
Jun 18 00:28:22 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

<#root>

```
Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with
```

```
message ID 543
```

```
(tries=3, timeout=30, exchange=37, state=2)
```

```
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

<#root>

```
Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
```

```
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL
```

```
request 543
```

```
[ ]
```

```
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3, timeout=30
```

```
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

Le dernier échange de paquets DPD réussi est décrit comme la demande 542.

<#root>

```
Jun 18 00:24:08 vedge01 charon: 11[ENC]
```

```
generating INFORMATIONAL request 542 [ ]
```

```
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 13.51.17.190[4500] to 10.10.10.1[4500] (7
```

```
Jun 18 00:24:08 vedge01 charon: 07[ENC]
```

```
parsed INFORMATIONAL response 542
```

```
[ ]
```

Étape 2. Rassemblez toutes les informations dans le bon ordre :

```
Jun 18 00:24:08 vedge01 charon: 11[ENC] generating INFORMATIONAL request 542 [ ]
```

```
Jun 18 00:24:08 vedge01 charon: 11[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:24:08 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to 10.132.3.92[4500] (76
```

```
Jun 18 00:24:08 vedge01 charon: 07[ENC] parsed INFORMATIONAL response 542 [ ]
```

```
Jun 18 00:25:21 vedge01 charon: 08[IKE] sending DPD request
```

```
Jun 18 00:25:21 vedge01 charon: 08[ENC] generating INFORMATIONAL request 543 [ ]
```

```
Jun 18 00:25:21 vedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:25:51 vedge01 charon: 05[IKE] retransmit 1 of request with message ID 543 (tries=3, timeout=3
```

```
Jun 18 00:25:51 vedge01 charon: 05[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:26:45 vedge01 charon: 06[IKE] retransmit 2 of request with message ID 543 (tries=3, timeout=3
```

```
Jun 18 00:26:45 vedge01 charon: 06[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:28:22 vedge01 charon: 08[IKE] retransmit 3 of request with message ID 543 (tries=3, timeout=3
```

```
Jun 18 00:28:22 Lvedge01 charon: 08[NET] sending packet: from 10.132.3.92[4500] to 10.10.10.1[4500] (76
```

```
Jun 18 00:31:17 vedge01 charon: 11[IKE] giving up after 3 retransmits
```

```
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec2 DOWN
```

```
Jun 18 00:31:17 vedge01 FTMD[1472]: %Viptela-LONDSR01-ftmd-6-INFO-1400002: Notification: interface-stat
```

Pour l'exemple décrit, le tunnel s'arrête parce que vEdge01 ne reçoit pas les paquets DPD de 10.10.10.1. Il est attendu après 3 retransmissions DPD que l'homologue IPsec est défini comme « perdu » et que le tunnel s'arrête. Il existe plusieurs raisons à ce comportement, généralement, il est lié au FAI où les paquets sont perdus ou abandonnés dans le chemin. Si le problème se produit une seule fois, il n'y a aucun moyen de suivre le trafic perdu. Toutefois, si le problème persiste, le paquet peut être suivi à l'aide de captures sur vEdge, l'homologue IPsec distant et le FAI.

Symptôme 3. Le tunnel IPsec s'est arrêté et reste à l'état d'arrêt

Comme mentionné précédemment dans ce symptôme, le tunnel fonctionnait bien auparavant, mais pour une raison quelconque, il est tombé et le tunnel n'a pas pu être établi avec succès à nouveau. Dans ce scénario, il y a une affectation au réseau.

identifiez les points avant le début du dépannage :

1. Tunnel IPsec (numéro) avec problèmes et configuration.
2. Horodatage de la panne du tunnel.
3. Adresse IP de l'homologue IPsec (destination du tunnel)

Non-concordance PFS

Dans cet exemple, le dépannage ne commence pas par l'horodatage lorsque le tunnel tombe en panne. Comme le problème persiste, les débogages IKE sont la meilleure option.

```
interface ipsec1
  description          VWAN_VPN
  ip address 192.168.0.101/30
  tunnel-source-interface ge0/0
  tunnel-destination   10.10.10.1
  ike
    version           2
    rekey              28800
    cipher-suite      aes256-cbc-sha1
    group              2
    authentication-type
      pre-shared-key
        pre-shared-secret "$8$jK2pLLjgKWNQu0KecNtY3+fo3hbTs0/7iJy6unNtersmCGjGB38kIPjsoqqXZdVmtizLu79\naq
      !
    !
  ipsec
    rekey              3600
    replay-window      512
    cipher-suite      aes256-cbc-sha1
    perfect-forward-secrecy group-16
    !
  mtu                  1400
  no shutdown
```

Le lien de débogage est activé et la négociation s'affiche.

<#root>

```
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] received packet: from 10.10.10.1[4500] to 172.28.0
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] parsed CREATE_CHILD_SA request 557 [ SA No TSi TSr
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] received proposals: ESP:AES_GCM_16_256/NO_EXT_SEQ,
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] no acceptable proposal found
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[IKE] failed to establish CHILD_SA, keeping IKE_SA
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[ENC] generating CREATE_CHILD_SA response 557 [ N(NO_PRO
daemon.info: Apr 27 05:12:56 vedge01 charon: 16[NET] sending packet: from 172.28.0.36[4500] to 10.10.10

daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] received packet: from 10.10.10.1[4500] to 172.28.0
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] parsed INFORMATIONAL request 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[ENC] generating INFORMATIONAL response 558 [ ]
daemon.info: Apr 27 05:12:57 vedge01 charon: 08[NET] sending packet: from 172.28.0.36[4500] to 10.10.10
```

```
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[NET] received packet: from 10.10.10.1[4500] to 172.28.0
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[ENC] parsed CREATE_CHILD_SA request 559 [ SA No TSi TSr
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG]
```

```
received proposals: ESP:AES_GCM_16_256/NO_EXT_SEQ, ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ, ESP:3DES_CBC
```

```
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[CFG]
```

```
configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
```

```
daemon.info: Apr 27 05:12:58 Avedge01 charon: 07[IKE]
```

```
no acceptable proposal found
```

```
daemon.info: Apr 27 05:12:58 vedge01 charon: 07[IKE] failed to establish CHILD_SA, keeping IKE_SA
```

 Remarque : Les paquets CREATE_CHILD_SA sont échangés pour chaque nouvelle clé ou nouvelle SA. Pour plus de références, accédez à [Présentation de IKEv2 Packet Exchange](#)

Les débogages IKE présentent le même comportement et il est constamment répété, de sorte qu'il est possible de prendre une partie des informations et de les analyser :

CREATE_CHILD_SA signifie une nouvelle clé, dans le but de générer et d'échanger les nouveaux SPIS entre les terminaux IPsec.

- Le périmètre reçoit le paquet de requête CREATE_CHILD_SA de 10.10.10.1.
- Le serveur Edge traite la demande et vérifie les propositions (SA) envoyées par l'homologue 10.10.10.1
- Le serveur Edge compare la proposition reçue envoyée par l'homologue à ses propositions configurées.
- L'échange CREATE_CHILD_SA échoue avec « aucune proposition acceptable trouvée ».

À ce stade, la question est la suivante : Pourquoi y a-t-il une erreur de correspondance de configuration si le tunnel a fonctionné précédemment et qu'aucune modification n'a été effectuée ?

Analysez en profondeur, il y a un champ supplémentaire sur les propositions configurées que l'homologue n'envoie pas.

```
propositions configurées : ESP : AES_CBC_256/HMAC_SHA1_96/MODP_4096/NO_EXT_SEQ
```

Demandes reçues :

```
ESP : AES_GCM_16_256/NO_EXT_SEQ,
ESP : AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ,
ESP : 3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ,
ESP : AES_CBC_256/HMAC_SHA2_256_128/NO_EXT_SEQ,
ESP : AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ,
ESP : 3DES_CBC/HMAC_SHA2_256_128/NO_EXT_SEQ
```

MODP_4096 est le groupe DH 16, que vedges a configuré pour PFS (Perfect-Forward-Secrecy)

sur la phase 2 (section IPsec).

PFS est la seule configuration non concordante dans laquelle le tunnel peut être établi avec succès ou non selon qui est l'initiateur ou le répondeur dans la négociation IKE. Cependant, lorsque la nouvelle clé démarre, le tunnel ne peut pas continuer et ce symptôme peut être présenté ou associé à.

Tunnel vEdge IPsec/Ikev2 non relancé après avoir été arrêté en raison d'un événement DELETE

Consultez l'ID de bogue Cisco [CSCvx86427](#) pour plus d'informations sur ce comportement.

Au fur et à mesure que le problème persiste, les débogages IKE sont les meilleures options. Cependant, pour ce bogue particulier, si les débogages sont activés, aucune information n'est affichée, ni le terminal ni le fichier de message.

Pour réduire ce problème et vérifier si vEdge atteint l'ID de bogue Cisco [CSCvx86427](#), il est nécessaire de trouver le moment où le tunnel tombe en panne.

identifiez les points avant le début du dépannage :

1. Tunnel IPsec (numéro) avec problèmes et configuration.
2. Horodatage de la panne du tunnel.
3. Adresse IP de l'homologue IPsec (destination du tunnel)

Une fois l'horodatage identifié et la corrélation entre l'heure et les journaux effectuée, consultez les journaux juste avant que le tunnel ne s'arrête.

<#root>

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] received DELETE for IKE_SA ipsec1_1[217]
```

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between 10.16.0.5[10.16.0.5]...10
```

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] deleting IKE_SA ipsec1_1[217] between 10.16.0.5[10.16.0.5]...10
```

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
```

```
Apr 13 22:05:21 vedge01 charon: 12[IKE] IKE_SA deleted
```

```
Apr 13 22:05:21 vedge01 charon: 12[ENC] generating INFORMATIONAL response 4586 [ ]
```

```
Apr 13 22:05:21 vedge01 charon: 12[NET] sending packet: from 10.16.0.5[4500] to 10.10.10.1[4500] (80 by
```

```
Apr 13 22:05:21 vedge01 charon: 12[KNL] Deleting SAD entry with SPI 00000e77
```

```
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-FTMD-6-INFO-1000001: VPN 1 Interface ipsec1 DOWN
```

```
Apr 13 22:05:21 vedge01 FTMD[1269]: %Viptela-AZGDSR01-ftmd-6-INFO-1400002: Notification: interface-state
```

 Remarque : Il y a plusieurs paquets DELETES sur une négociation IPsec, et le DELETE pour CHILD_SA est un DELETE attendu pour un processus REKEY, ce problème est vu quand un paquet IKE_SA DELETE pur est reçu sans aucune négociation IPsec particulière. Cette suppression supprime tous les tunnels IPsec/IKE.

Informations connexes

- [Échange de paquets KEv2 et débogage au niveau du protocole](#)
- [Internet Key Exchange \(IKE\) – RFC 2409](#)
- [IKEv2 - RFC 7296](#)
- [IPSec de LAN à LAN de site à site entre vEdge et Cisco IOS](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.