Dépannage des tunnels IPsec et des problèmes courants de plan de contrôle avec les captures de paquets

Table des matières

Introduction

Ce document décrit comment les captures de paquets, d'autres outils, aident à résoudre les problèmes de plan de contrôle lors de la négociation d'un VPN de site à site sur les routeurs Cisco IOS® XE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de la configuration CLI de Cisco IOS®.
- Connaissances fondamentales des protocoles IKEv2 et IPsec.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CSR1000V - Logiciel Cisco IOS XE version 16.12.0.

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

Les captures de paquets sont un outil puissant qui vous aide à vérifier si des paquets sont envoyés/reçus entre des périphériques homologues VPN. Ils confirment également si le comportement observé avec les débogages IPsec s'aligne sur le résultat collecté sur les captures puisque les débogages sont une interprétation logique, et la capture représente l'interaction physique entre les homologues. De ce fait, vous pouvez confirmer ou ignorer les problèmes de connectivité.

Outils utiles

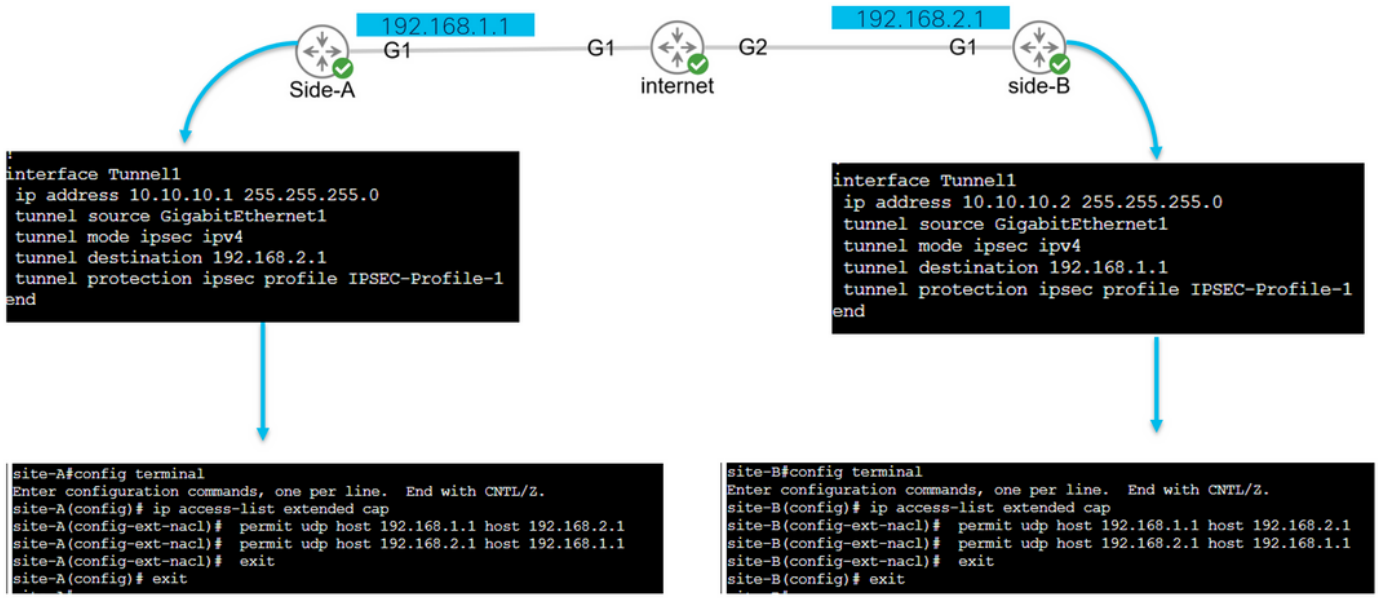
Il existe des outils utiles qui vous aident à configurer les captures, à extraire le résultat et à l'analyser plus en détail. Certaines d'entre elles sont :

- Wireshark : il s'agit d'un analyseur de paquets open source bien connu et utilisé.
- Captures de surveillance : fonctionnalité Cisco IOS XE sur les routeurs qui vous aide à collecter des captures et vous fournit une sortie lumineuse de ce à quoi ressemble le flux de trafic, le protocole collecté et ses horodatages.

Configuration des captures sur le routeur IOS XE

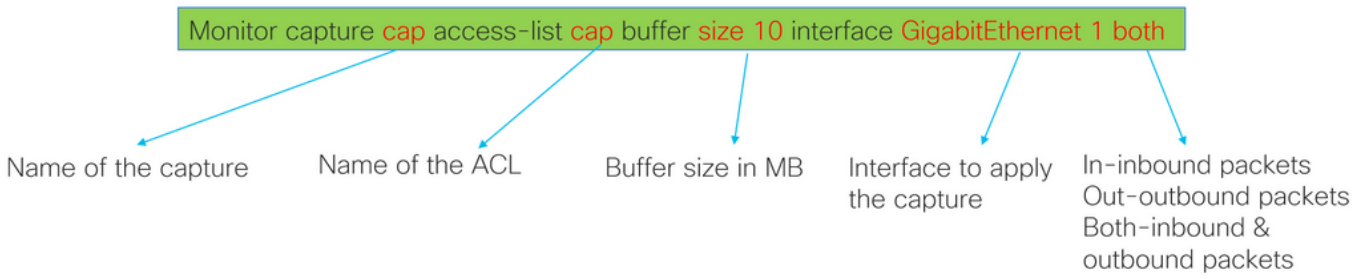
Une capture utilise une liste de contrôle d’accès étendue (ACL) qui définit le type de trafic à collecter, ainsi que les adresses source et de destination des homologues VPN ou des segments du trafic intéressant. Une négociation de tunnel utilise les ports UDP 500 et 4500 si NAT-T est activé le long du chemin. Une fois la négociation terminée et le tunnel établi, le trafic intéressant utilise le protocole IP 50 (ESP) ou UDP 4500 si NAT-T est activé.

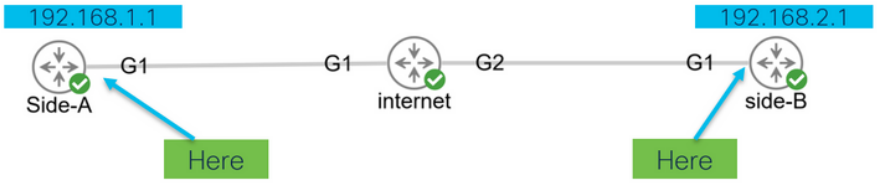
Afin de dépanner les problèmes liés au plan de contrôle, les adresses IP des homologues VPN doivent être utilisées pour capturer la façon dont le tunnel est négocié.




```
config terminal
ip access-list extended <ACL name>
permit udp host <local address> host <peer address>
permit udp host <peer address> host <source address>
exit
exit
```

La liste de contrôle d'accès configurée est utilisée pour restreindre le trafic capturé et elle est placée sur l'interface utilisée pour négocier le tunnel.






```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-A#
```

```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-B#
```

```
monitor capture <capture name> access-list <ACL name> buffer size <custom buffer size in MB> interface
```

Une fois la capture configurée, elle peut être manipulée pour l'arrêter, l'effacer ou extraire le trafic collecté à l'aide des commandes suivantes :

- Vérifiez les informations générales de capture : show monitor capture
- Démarrage/arrêt de la capture : surveillance début/arrêt du cap de capture
- Vérifiez que la capture collecte les paquets : show monitor capture cap buffer
- Voir un bref résultat du trafic : show monitor capture cap buffer brief
- Effacer la capture : effacer le cache de capture du moniteur
- Extrayez le résultat de la capture :
  - écran cap buff dump
  - monitor capture cap export bootflash:capture.pcap

Analyse de l’établissement du tunnel avec les captures de paquets

Comme mentionné précédemment, pour négocier le tunnel IPSec, les paquets sont envoyés sur UDP avec le port 500 et le port 4500 si NAT-T est activé. Avec les captures, davantage d'informations peuvent être vues à partir de ces paquets, telles que la phase en cours de négociation (phase 1 ou phase 2), le rôle de chaque périphérique (initiateur ou répondeur) ou les valeurs SPI qui viennent d'être créées.

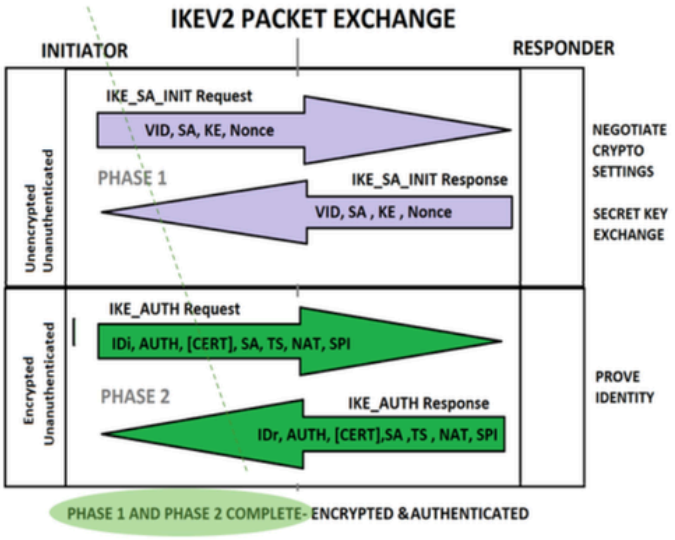
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

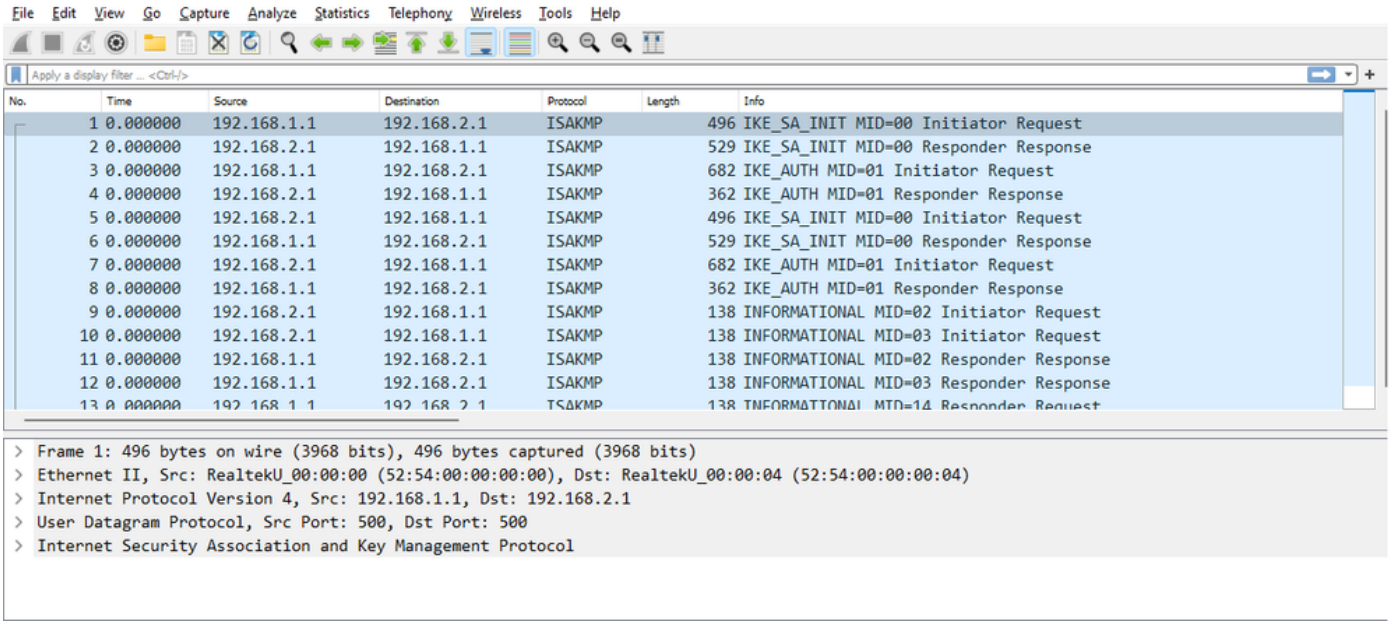
Phase 2 encrypted



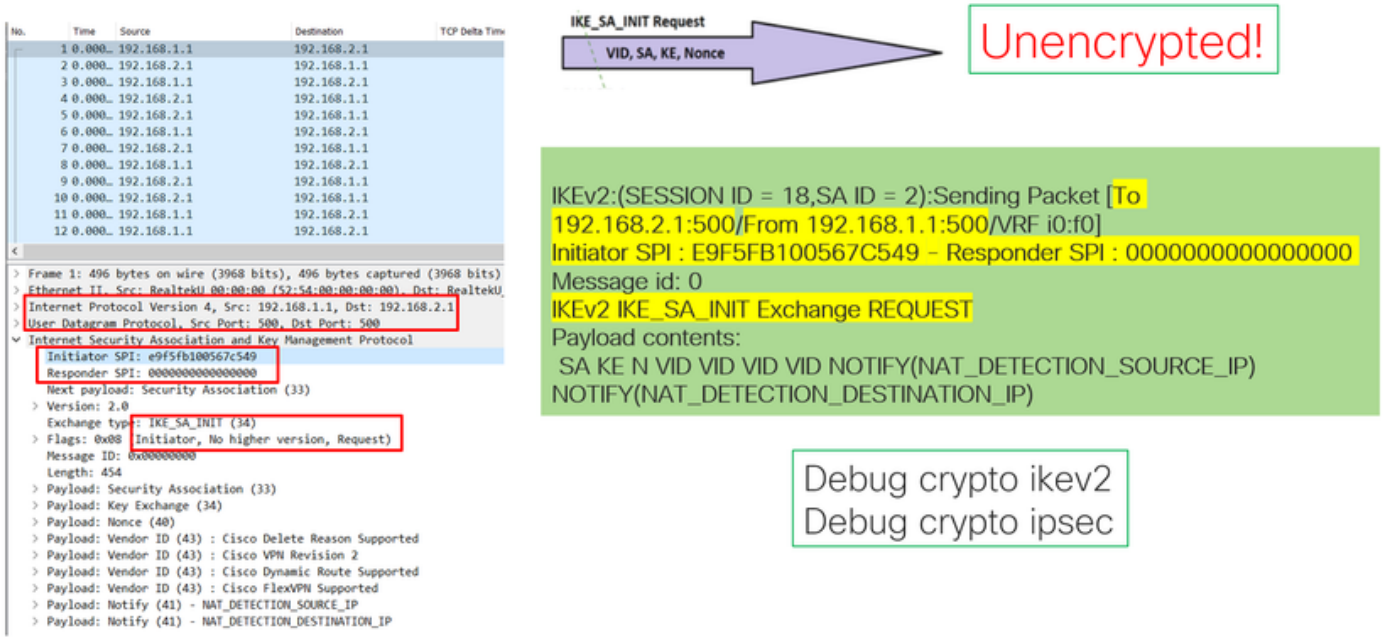
En affichant le bref résultat de la capture du routeur, l'interaction entre les homologues est visible, envoyant des paquets UDP.

```
site-A#show monitor cap cap buffer brief
 ------------------------------------------------------------------------------
 #   size   timestamp     source               destination      dscp    protocol
 ------------------------------------------------------------------------------
   0  496    0.000000    192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   1  529    0.011992    192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   2  682    0.026991    192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   3  362    0.035993    192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   4  496    0.579016    192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   5  529    0.593023    192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   6  682    0.610020    192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   7  362    0.616017    192.168.1.1       ->  192.168.2.1      48 CS6  UDP
   8  138    0.638019    192.168.2.1       ->  192.168.1.1      48 CS6  UDP
   9  138    0.638019    192.168.2.1       ->  192.168.1.1      48 CS6  UDP
  10  138    0.641009    192.168.1.1       ->  192.168.2.1      48 CS6  UDP
  11  138    0.655016    192.168.1.1       ->  192.168.2.1      48 CS6  UDP
```

Après avoir extrait le dump et exporté le fichier pcap du routeur, plus d'informations des paquets sont visibles à l'aide de wireshark.

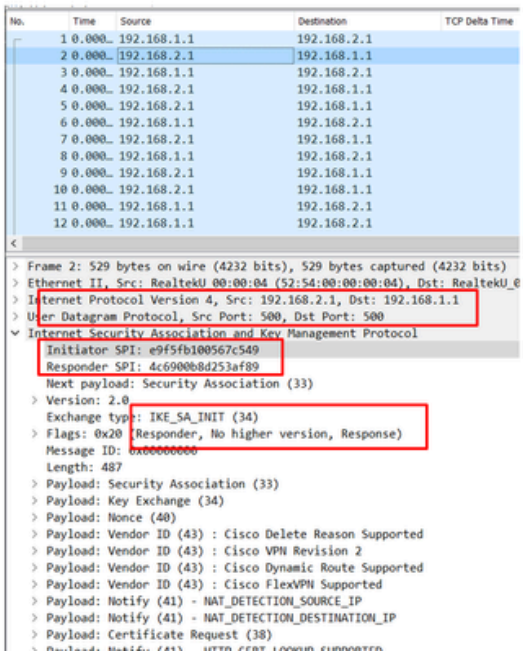


Dans la section Protocole Internet du premier paquet Exchange IKE_SA_INIT envoyé, les adresses source et de destination du paquet UDP sont localisées. Dans la section User Datagram Protocol, les ports utilisés et la section Internet Security Association and Key Management Protocol indiquent la version du protocole, le type de message échangé et le rôle du périphérique, ainsi que le SPI créé. Lors de la collecte des débogages IKEv2, les mêmes informations sont présentées dans les journaux de débogage.



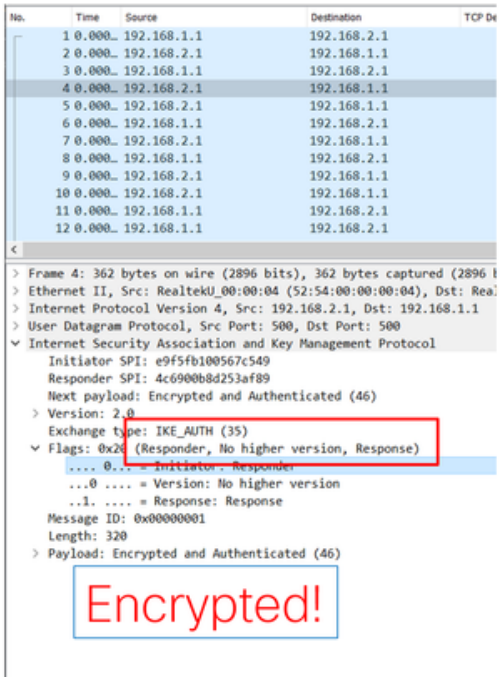
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

Unencrypted!



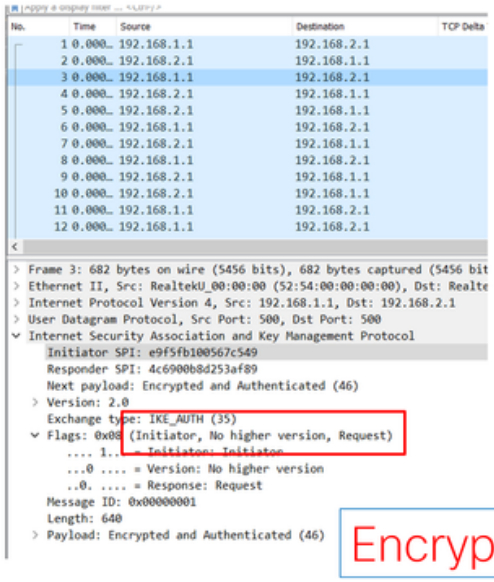
Lorsque la négociation d'échange IKE_AUTH a lieu, la charge utile est chiffrée, mais certaines informations sur la négociation sont visibles, telles que le SPI précédemment créé et le type de transaction effectuée.

IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE



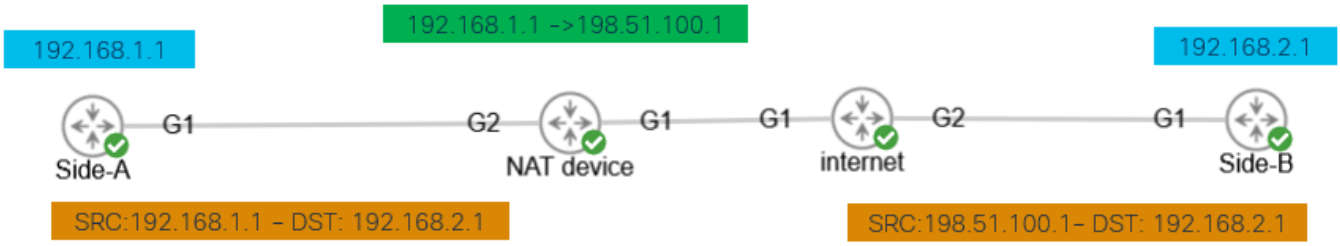
Encrypted!

Une fois le dernier paquet d'échange IKE_AUTH reçu, la négociation du tunnel est terminée.



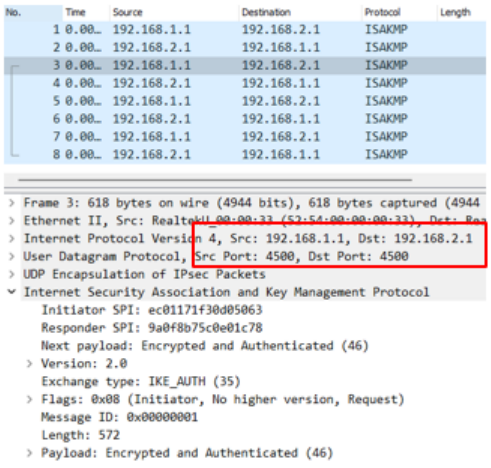
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Transaction lorsque NAT est entre



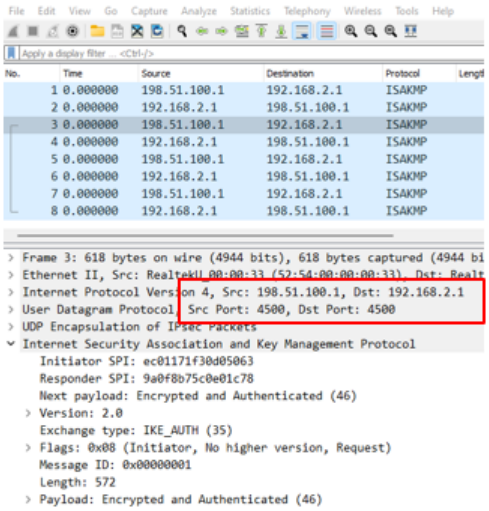
Nat-transversal est une autre fonctionnalité qui peut être vue lorsque la négociation de tunnel a lieu. Si un périphérique intermédiaire attribue une ou les deux adresses utilisées pour le tunnel, les périphériques changent le port UDP de 500 à 4500 lorsque la phase 2 (échange IKE_AUTH) est négociée.

Capture prise sur le côté A :



IKEv2:(SESSION ID = 10,SA ID = 1):Received Packet [From 192.168.1.1:4500/To 192.168.2.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
.....
IKEv2:(SESSION ID = 10,SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SESSION ID = 10,SA ID = 1):Checking NAT discovery
IKEv2:(SESSION ID = 10,SA ID = 1):NAT INSIDE found
IKEv2:(SESSION ID = 10,SA ID = 1):NAT detected float to init port 4500, resp port 4500

Capture prise sur la face B :



IKEv2:(SESSION ID = 11,SA ID = 1):Sending Packet [To 192.168.2.1:4500/From 198.51.100.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:

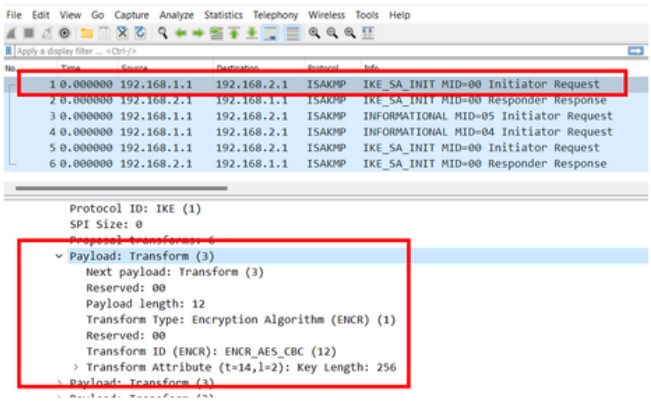
Problèmes courants liés au plan de contrôle

Il peut y avoir des facteurs locaux ou externes qui affectent la négociation de tunnel et peuvent être identifiés avec des captures aussi bien. Les scénarios suivants sont les plus courants.

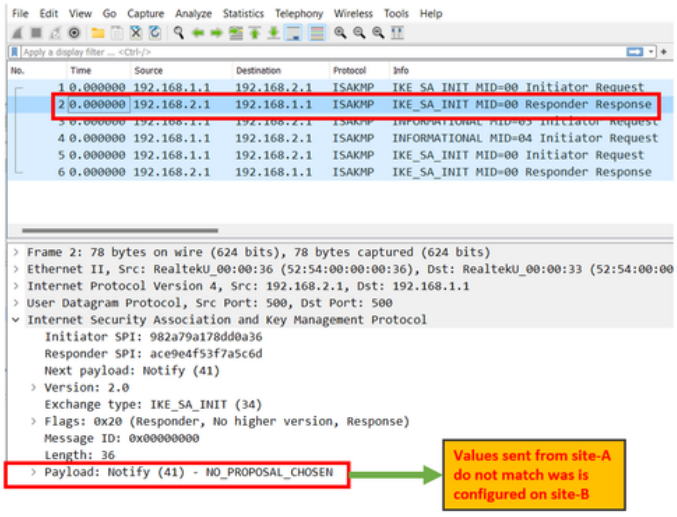
Non-concordance de configuration

Ce scénario peut être résolu en examinant chaque configuration des phases 1 et 2 du périphérique. Cependant, il peut y avoir des scénarios dans lesquels il n'y a pas d'accès à l'extrémité distante. Les captures aident à identifier le périphérique qui envoie un message NO_PROPOSAL_CHOSEN dans les paquets lors de la phase 1 ou 2. Cette réponse indique que la configuration peut présenter un problème et indique la phase à ajuster.

Side-A



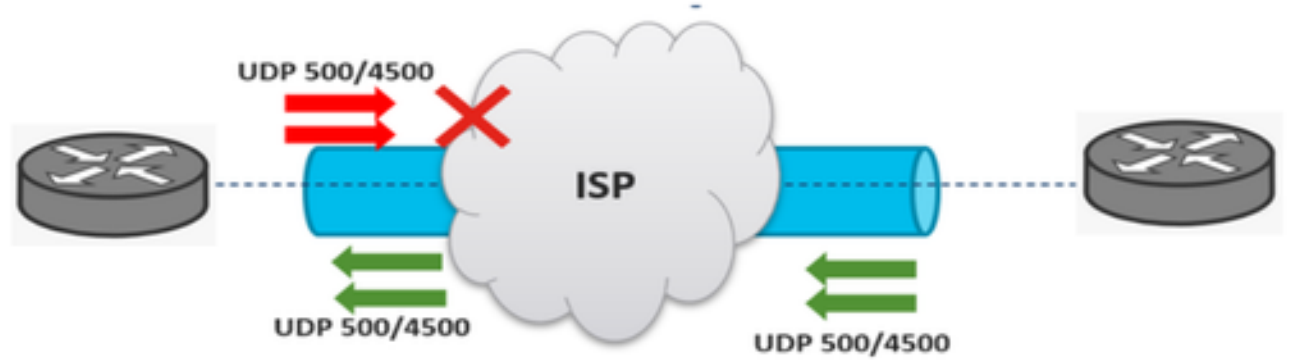
Side-B

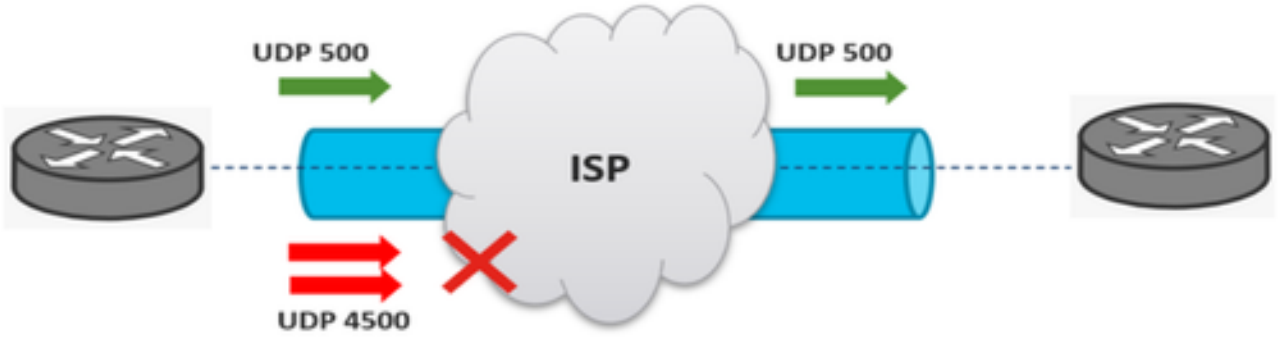


Retransmissions

Une négociation de tunnel IPSec peut échouer en raison de l'abandon des paquets de négociation sur le chemin entre les périphériques finaux. Les paquets abandonnés peuvent être des paquets de phase 1 ou de phase 2. Dans ce cas, le périphérique qui attend un paquet de réponse retransmet le dernier paquet, et s'il n'y a pas de réponse après 5 tentatives, le tunnel est terminé et redémarré depuis le début.

Les captures de chaque côté du tunnel aident à identifier ce qui pourrait bloquer le trafic et dans quelle direction il est affecté.





Side-A

Side-B

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response
4	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
7	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
8	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
9	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
3	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
4	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request

A device or service in between is blocking UDP packets that come from side-A

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.