Problemen met IPsec-tunnels en gemeenschappelijke besturingsplane bij pakketvastlegging oplossen

Inhoud

Inleiding

Dit document beschrijft hoe het pakket, andere hulpmiddelen, hulp met controle-vlakke kwesties opneemt wanneer plaats-aan-plaats VPN op Cisco IOS® XE routers wordt besproken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de configuratie van Cisco IOS® CLI.
- Fundamentele kennis van IKEv2 en IPsec.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- CSR100V - Cisco IOS XE-softwarerelease 16.12.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrondinformatie

Packet Captures zijn een krachtig hulpmiddel om u te helpen verifiëren of pakketten worden verzonden/ontvangen tussen VPN-peer apparaten. Zij bevestigen ook als het gedrag dat met IPsec-debuggen wordt gezien, uitgelijnd is met de output die op de opnamen is verzameld, aangezien de debuggen een logische interpretatie zijn en de opname de fysieke interactie tussen de peers vertegenwoordigt. Hierdoor kunt u connectiviteitsproblemen bevestigen of weggooien.

Handige tools

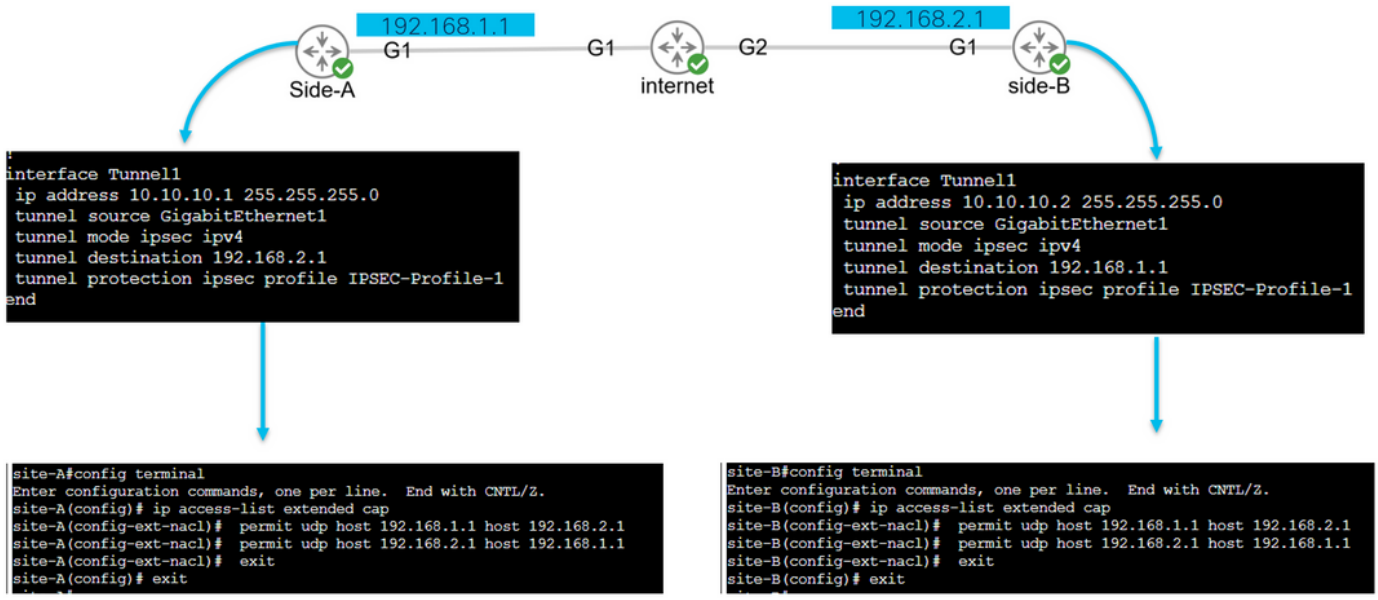
Er zijn handige tools die u helpen om de opnamen te configureren, de uitvoer te extraheren en verder te analyseren. Enkele van deze zijn:

- Wireshark: Dit is een bekende en gebruikte open-source pakketanalyzer.
- De monitor vangt: Cisco IOS XE eigenschap op routers die u helpen vangt en verstrekt u een lichte output van wat de verkeersstroom als kijkt, verzameld protocol, en zijn tijdstempels.

Opnamen op IOS XE router configureren

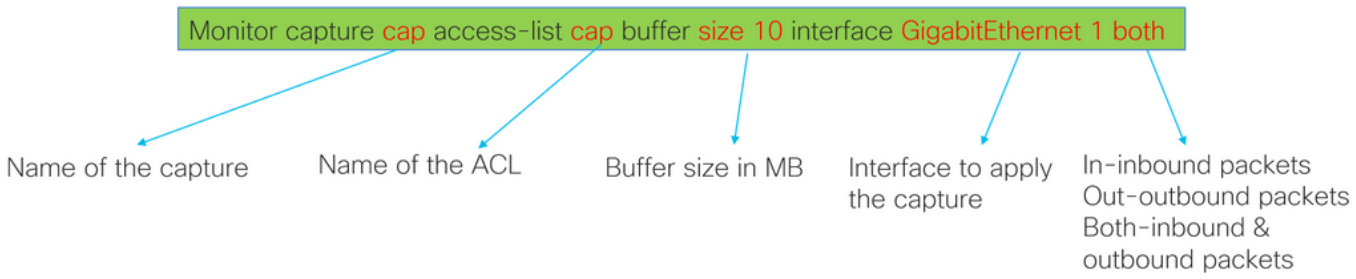
Een opname gebruikt een uitgebreide toegangslijst (ACL) die het te verzamelen type verkeer definieert, en de bron- en doeladressen van de VPN-peers of segmenten van het interessante verkeer. In een tunnelonderhandeling worden de UDP-poort 500 en de poort 4500 gebruikt als NAT-T langs het pad is ingeschakeld. Zodra de onderhandeling voltooid is en de tunnel tot stand is gebracht, maakt het interessante verkeer gebruik van IP-protocol 50 (ESP) of UDP 4500 als NAT-T is ingeschakeld.

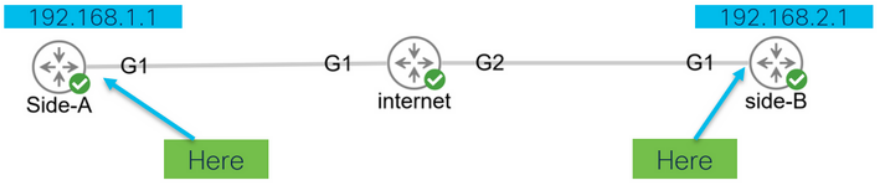
Om problemen met de besturingsplane op te lossen, moeten IP-adressen van VPN-peers worden gebruikt om vast te leggen hoe de tunnel wordt onderhandeld.




```
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
```

De geconfigureerde ACL wordt gebruikt om het opgenomen verkeer te beperken en wordt op de interface geplaatst die wordt gebruikt om over de tunnel te onderhandelen.






```
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
```

Zodra de opname is geconfigureerd, kan deze worden gemanipuleerd om de opname te stoppen, te wissen of het verkeer te extraheren dat met de volgende opdrachten is verzameld:

- Controleer de algemene opnameinformatie: toon monitoropname
- Opname starten/stoppen: monitoropnamekap start/stop
- Controleer of de opnamepakketten worden verzameld: toon monitor Capture cap buffer
- Bekijk een korte output van het verkeer: toon monitor Capture cap buffer kort
- Schakel de opname uit: monitor opnamekap wissen
- Extraheert de opnameoutput:
  - afvoerslang monitordop
  - monitor Capture cap export bootflash:capture.pcap

De tunnelinrichting analyseren met pakketvastlegging

Zoals eerder vermeld, om de IPSec-tunnel te onderhandelen, worden pakketten via UDP verzonden met poort 500 en poort 4500 als NAT-T is ingeschakeld. Met opnamen, kan meer informatie worden gezien van die pakketten zoals de fase die wordt besproken (fase 1 of fase 2), de rol van elk apparaat (initiator of antwoordapparaat), of de waarden van SPI die enkel werden gecreëerd.

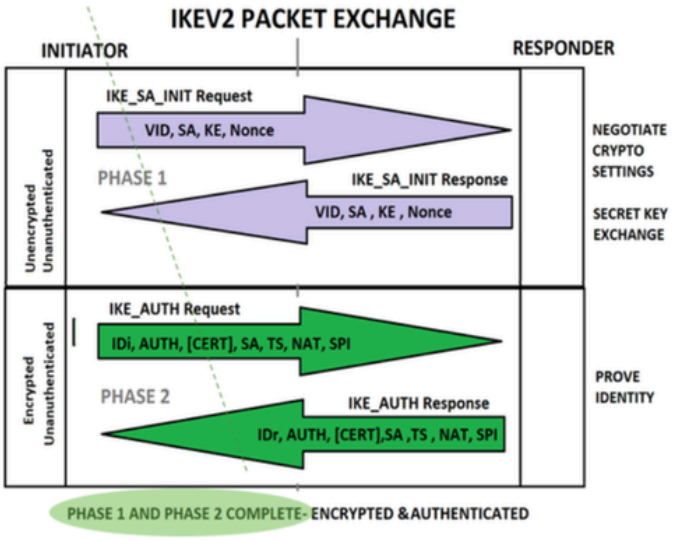
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

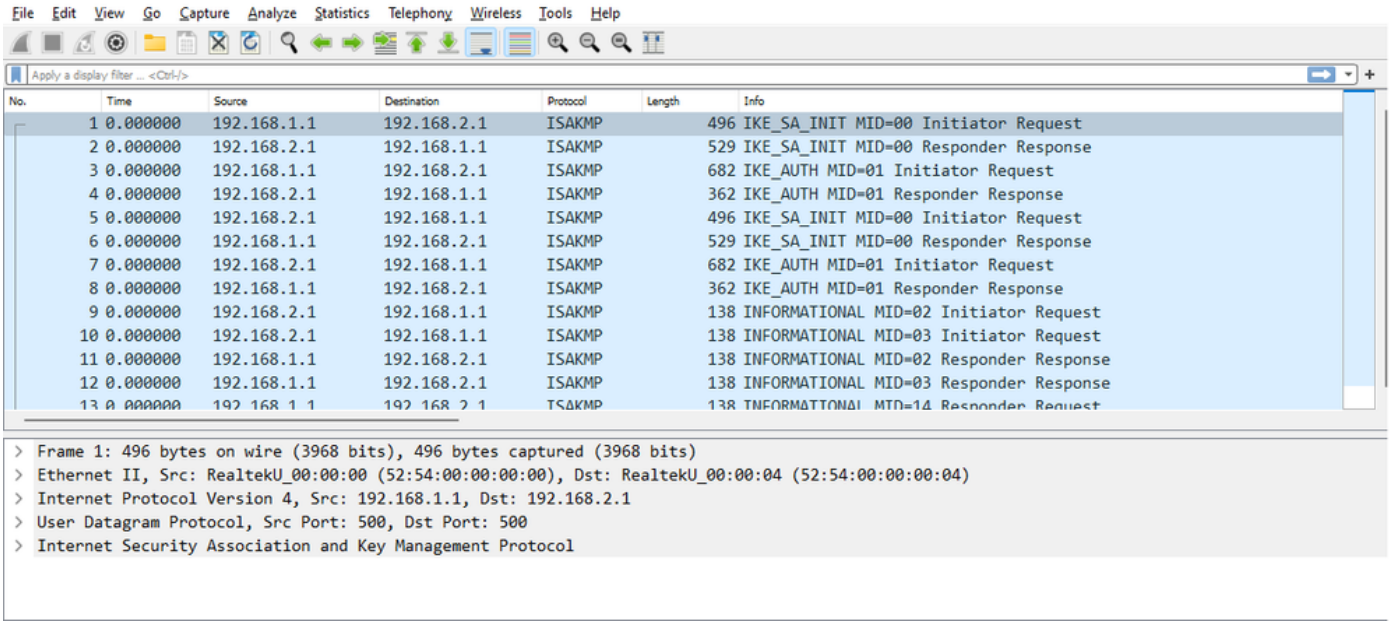
Phase 2 encrypted



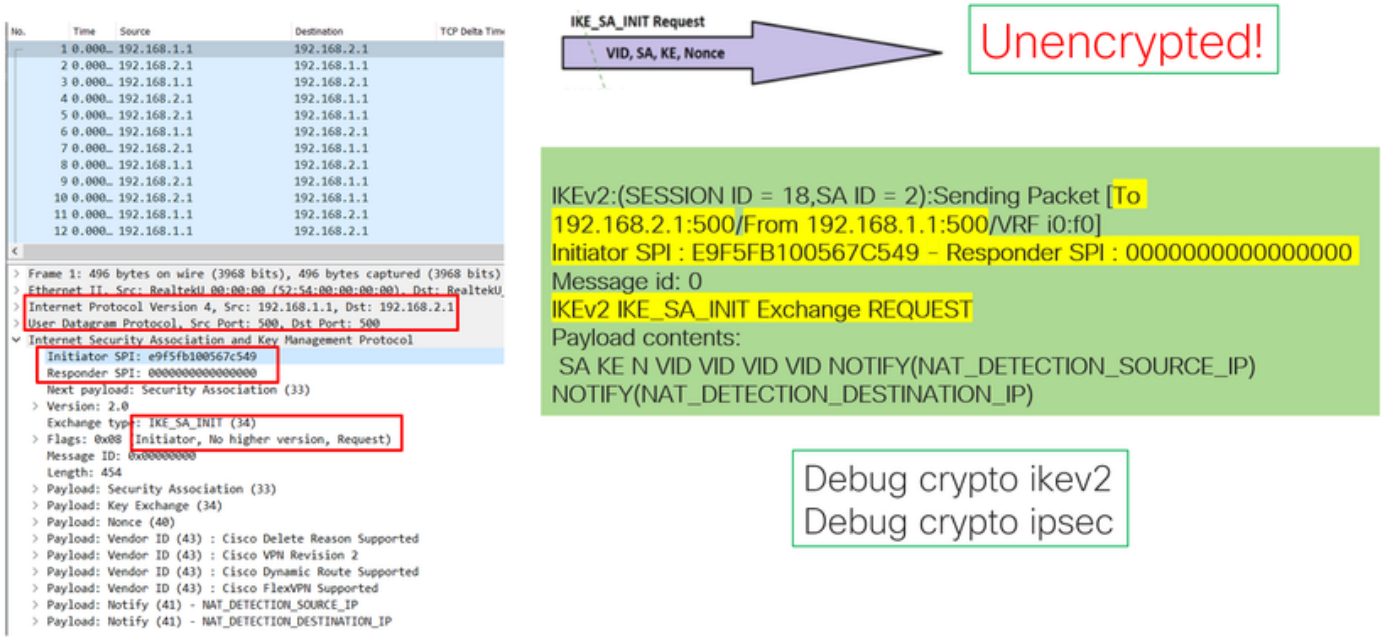
Wanneer de korte output van de opname van de router wordt weergegeven, wordt de interactie tussen de peers gezien en worden UDP-pakketten verzonden.

```
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
```

Na het uitnemen van de stortplaats en het exporteren van het pcap-bestand van de router, is meer informatie uit de pakketten zichtbaar met behulp van wireshark.

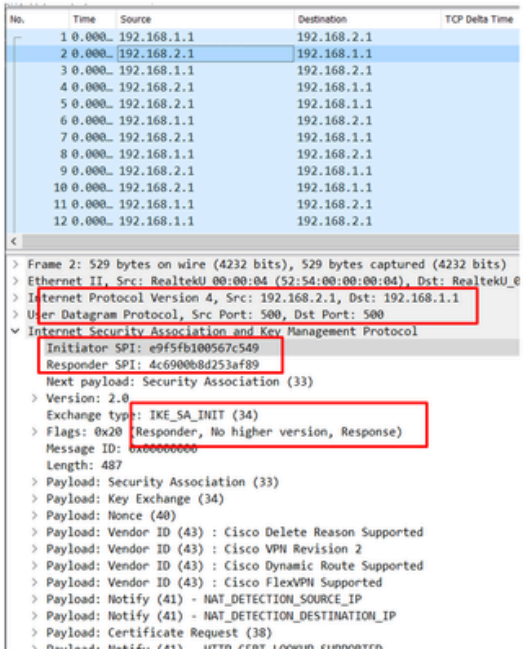


In het gedeelte Internet Protocol van het eerste verzonden IKE_SA_INIT Exchange-pakket bevinden zich de bron- en doeladressen van het UDP-pakket. In het gedeelte User Datagram Protocol worden de gebruikte poorten en de sectie Internet Security Association and Key Management Protocol weergegeven met de versie van het protocol, het type bericht dat wordt uitgewisseld en de rol van het apparaat en de SPI die is gemaakt. Wanneer het verzamelen van IKEv2 debugs, wordt dezelfde informatie gepresenteerd binnen de debug logs.



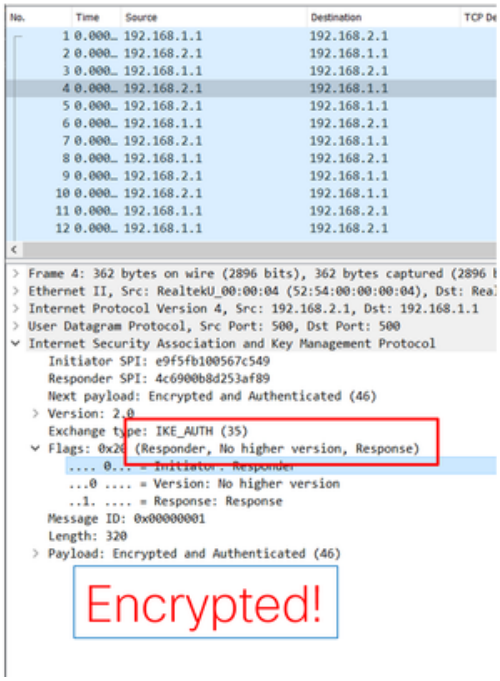
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)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

Unencrypted!



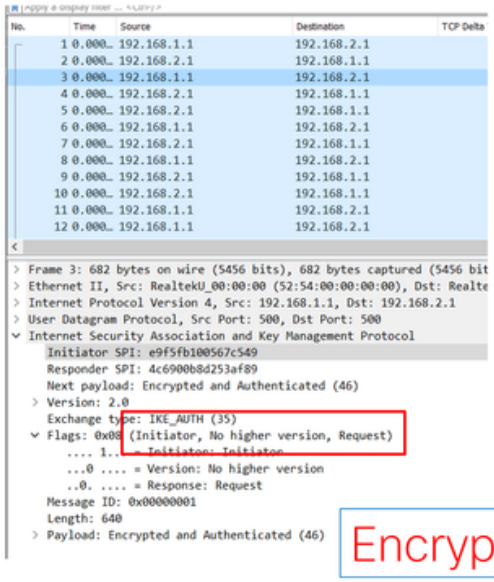
Wanneer de IKE_AUTH Exchange onderhandeling plaatsvindt, wordt de payload versleuteld, maar is er enige informatie over de onderhandeling zichtbaar, zoals de eerder gemaakte SPI, en het type transactie dat wordt uitgevoerd.

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



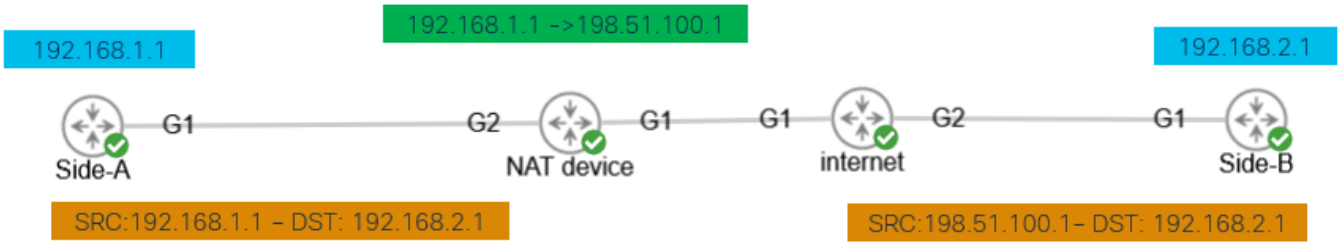
Encrypted!

Zodra het laatste IKE_AUTH Exchange-pakket is ontvangen, is de tunnelonderhandeling voltooid.



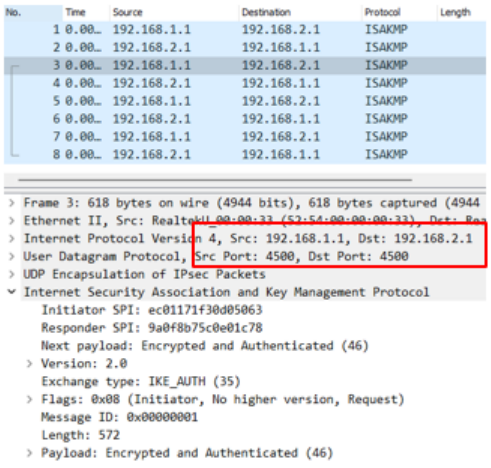
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Transactie wanneer NAT ertussen zit



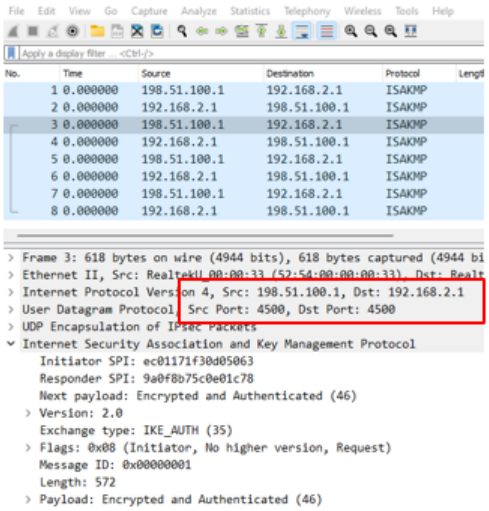
Nat-transversale is een andere eigenschap die kan worden gezien wanneer de tunnelonderhandeling plaatsvindt. Als een intermediair apparaat één of beide adressen die voor de tunnel worden gebruikt in de weg staat, veranderen de apparaten de UDP poort van 500 naar 4500 wanneer fase 2 (IKE_AUTH Exchange) wordt onderhandeld.

Opname op kant-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

Opname op kant-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:

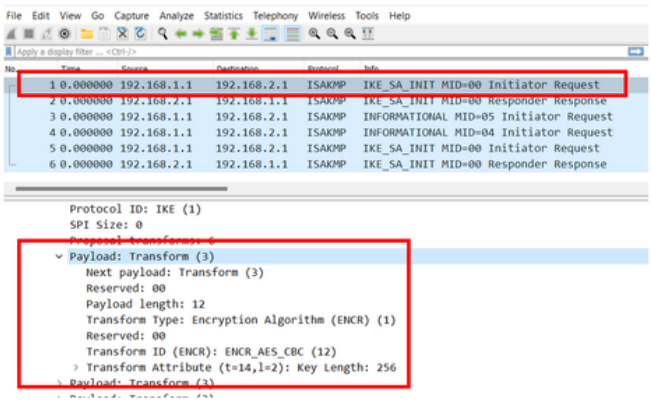
Veelvoorkomende problemen met controlevliegtuigen

Er zouden lokale of externe factoren kunnen zijn die de tunnelonderhandeling beïnvloeden en ook met opnamen kunnen worden geïdentificeerd. De volgende scenario's zijn de meest voorkomende.

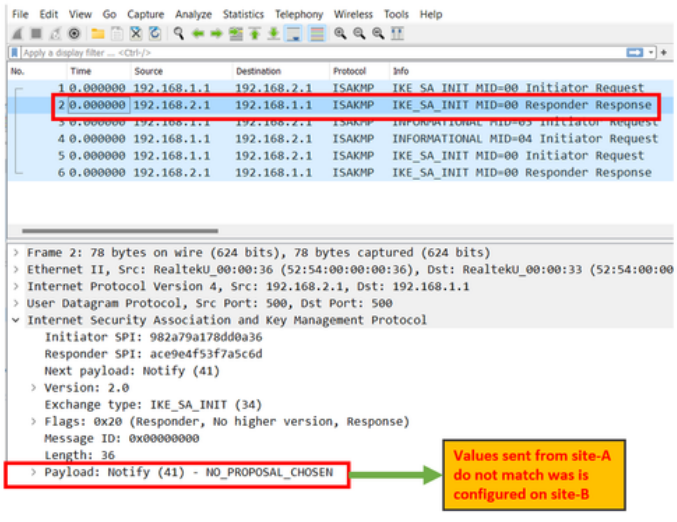
Configuratie-wanverhouding

Dit scenario kan worden opgelost door elke configuratie van de apparaatfase 1 en fase 2 te bekijken. Er kunnen echter scenario's zijn waarin er geen toegang is tot het verre eind. Leg de help-out vast door vast te stellen welk apparaat in fase 1 of 2 een NO_OFFER_CHOSEN verstuurt binnen de pakketten. Die respons geeft aan dat er iets mis kan zijn met de configuratie en welke fase moet worden aangepast.

Side-A



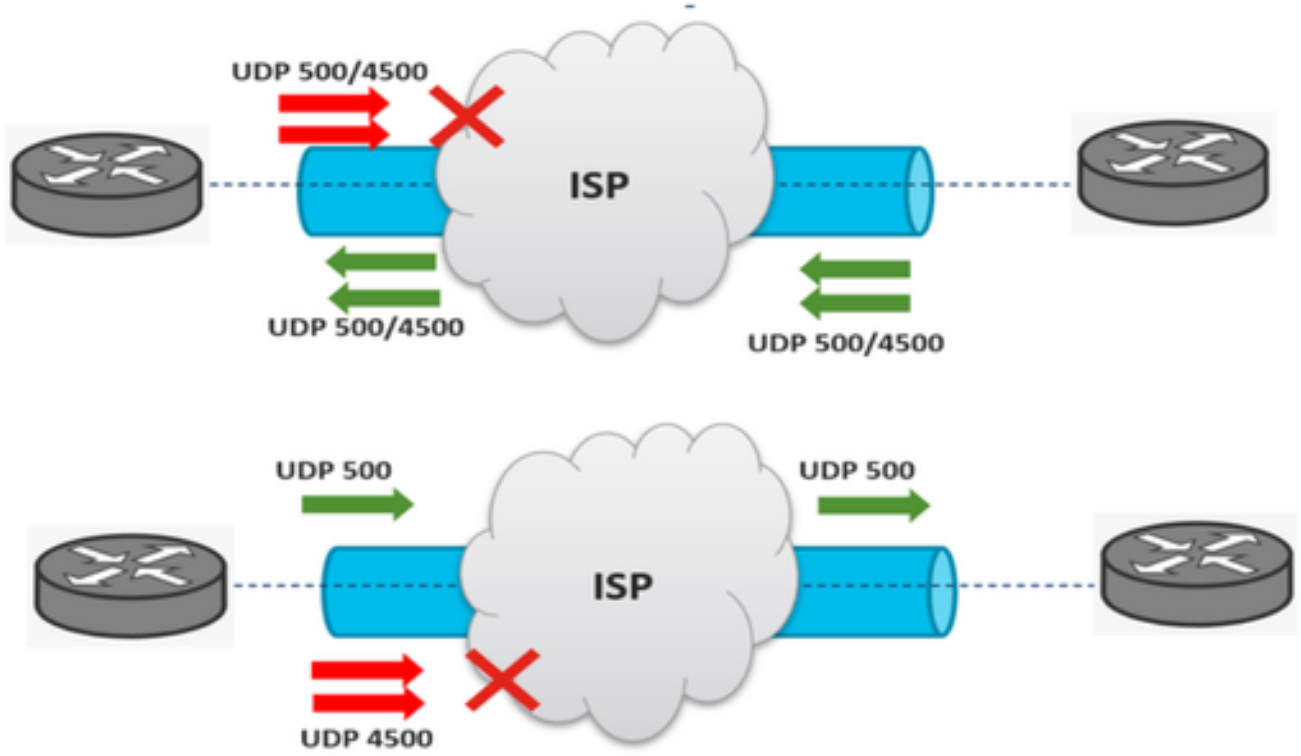
Side-B



Heruitzendingen

Een IPSec-tunnelonderhandeling kan mislukken als gevolg van de onderhandelingspakketten die worden gedropt langs het pad tussen de eindapparaten. De gedropte pakketten kunnen fase 1 of fase 2 pakketten zijn. Wanneer dit het geval is, brengt het apparaat dat een reactiepakket verwacht het laatste pakket opnieuw over, en als er geen reactie na 5 pogingen is, wordt de tunnel gesloten en van bij het begin opnieuw begonnen.

Vangt aan elke kant van de tunnel door te identificeren wat het verkeer zou kunnen blokkeren en in welke richting het wordt beïnvloed.



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	192.168.1.1	192.168.2.1	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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.