

Resolución de problemas de túneles IPsec y planos de control comunes con capturas de paquetes

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Herramientas útiles](#)

[Cómo Configurar Capturas en el Router IOS XE](#)

[Análisis del establecimiento del túnel con capturas de paquetes](#)

[Transacción Cuando NAT está entre](#)

[Problemas comunes del plano de control](#)

[Discordancia de configuración](#)

[Retransmisiones](#)

Introducción

Este documento describe cómo las capturas de paquetes, otras herramientas, ayudan con los problemas del plano de control cuando se negocia la VPN de sitio a sitio en los routers Cisco IOS® XE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración CLI de Cisco IOS®.
- Conocimientos fundamentales de IKEv2 e IPsec.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CSR1000V: software Cisco IOS XE con versión 16.12.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las capturas de paquetes son una potente herramienta que le ayuda a verificar si los paquetes se están enviando o recibiendo entre dispositivos de pares VPN. También confirman si el comportamiento observado con las depuraciones IPsec se alinea con el resultado obtenido en las capturas, ya que las depuraciones son una interpretación lógica y la captura representa la interacción física entre los pares. Debido a esto, puede confirmar o descartar problemas de conectividad.

Herramientas útiles

Hay herramientas útiles que le ayudan a configurar las capturas, extraer el resultado y analizarlo más a fondo. Algunos de ellos son:

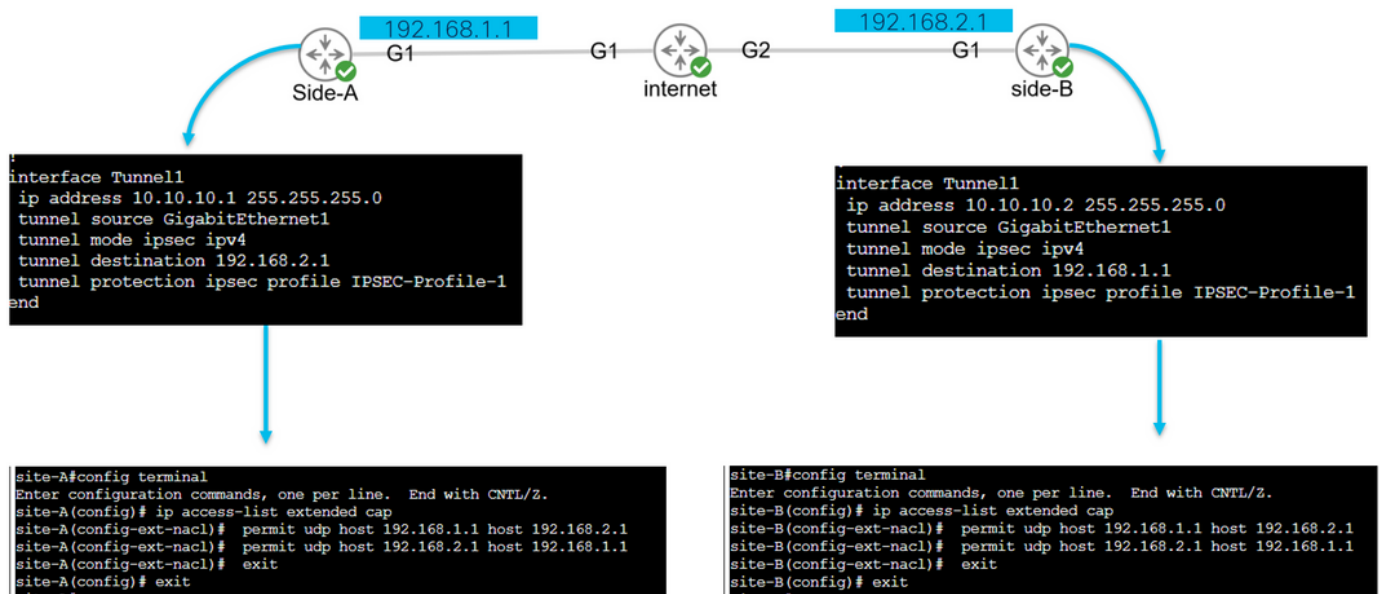
- Wireshark: se trata de un analizador de paquetes de código abierto conocido y utilizado.
- Supervisar capturas: la función Cisco IOS XE en los routers le ayuda a recopilar capturas y le proporciona una salida ligera del aspecto del flujo de tráfico, el protocolo recopilado y sus marcas de tiempo.

Cómo Configurar Capturas en el Router IOS XE



Una captura utiliza una lista de acceso ampliada (ACL) que define el tipo de tráfico que se va a recopilar, así como las direcciones de origen y destino de los pares VPN o los segmentos del tráfico interesante. Una negociación de túnel utiliza el puerto UDP 500 y el puerto 4500 si NAT-T está habilitado a lo largo de la trayectoria. Una vez que se completa la negociación y se establece el túnel, el tráfico interesante utiliza el protocolo IP 50 (ESP) o UDP 4500 si NAT-T está habilitado.

Para resolver problemas relacionados con el plano de control, se deben utilizar las direcciones IP de los pares VPN para capturar cómo se negocia el túnel.

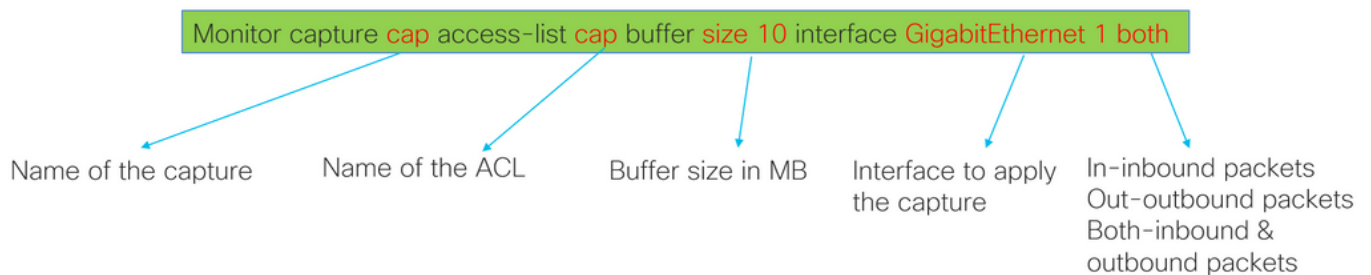


```

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 ACL configurada se utiliza para restringir el tráfico capturado y se coloca en la interfaz utilizada para negociar el túnel.





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

```
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#
```

```
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

Una vez configurada la captura, se puede manipular para detenerla, borrarla o extraer el tráfico recopilado con los siguientes comandos:

- Verifique la información general de captura: show monitor capture
- Iniciar/detener la captura: supervisor inicio/detención del límite de captura
- Verifique que la captura esté recopilando paquetes: show monitor capture cap buffer
- Vea una breve salida del tráfico: show monitor capture cap buffer brief
- Borrar la captura: monitor capture cap clear
- Extraiga el resultado de la captura:
 - monitor cap buff dump
 - monitor capture cap export bootflash:capture.pcap

Análisis del establecimiento del túnel con capturas de paquetes

Como se mencionó anteriormente, para negociar el túnel IPsec, los paquetes se envían a través de UDP con el puerto 500 y el puerto 4500 si NAT-T está habilitado. Con las capturas, se puede ver más información de esos paquetes, como la fase que se está negociando (fase 1 o fase 2), la función de cada dispositivo (iniciador o respondedor) o los valores SPI que se acaban de crear.

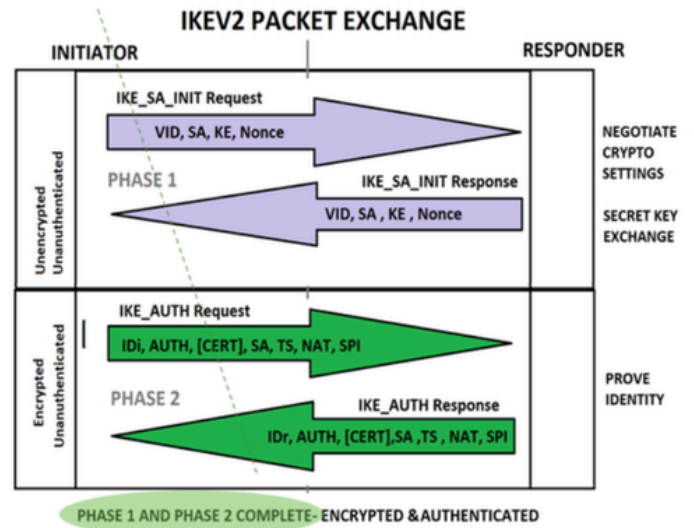
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

Phase 2 encrypted



Al mostrar el resultado breve de la captura del router, se observa la interacción entre los pares, que envían paquetes 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

Después de extraer el volcado y exportar el archivo pcap del router, se puede ver más información de los paquetes mediante wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	496	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	529	IKE_SA_INIT MID=00 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	682	IKE_AUTH MID=01 Initiator Request
4	0.000000	192.168.2.1	192.168.1.1	ISAKMP	362	IKE_AUTH MID=01 Responder Response
5	0.000000	192.168.2.1	192.168.1.1	ISAKMP	496	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.1.1	192.168.2.1	ISAKMP	529	IKE_SA_INIT MID=00 Responder Response
7	0.000000	192.168.2.1	192.168.1.1	ISAKMP	682	IKE_AUTH MID=01 Initiator Request
8	0.000000	192.168.1.1	192.168.2.1	ISAKMP	362	IKE_AUTH MID=01 Responder Response
9	0.000000	192.168.2.1	192.168.1.1	ISAKMP	138	INFORMATIONAL MID=02 Initiator Request
10	0.000000	192.168.2.1	192.168.1.1	ISAKMP	138	INFORMATIONAL MID=03 Initiator Request
11	0.000000	192.168.1.1	192.168.2.1	ISAKMP	138	INFORMATIONAL MID=02 Responder Response
12	0.000000	192.168.1.1	192.168.2.1	ISAKMP	138	INFORMATIONAL MID=03 Responder Response
13	0.000000	192.168.1.1	192.168.2.1	ISAKMP	138	INFORMATIONAL MID=14 Responder Request

```

> Frame 1: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)
> Ethernet II, Src: RealtekU_00:00:00 (52:54:00:00:00:00), Dst: RealtekU_00:00:04 (52:54:00:00:00:04)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
  
```

En la sección Internet Protocol (Protocolo de Internet) del primer paquete de intercambio IKE_SA_INIT enviado, se encuentran las direcciones de origen y destino del paquete UDP. En la sección User Datagram Protocol, se ven los puertos utilizados y la sección Internet Security Association and Key Management Protocol, la versión del protocolo, el tipo de mensaje que se intercambia y la función del dispositivo, así como el SPI creado. Cuando se recopilan depuraciones IKEv2, se presenta la misma información en los registros de depuración.

No.	Time	Source	Destination	TCP Delta Time
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	

IKE_SA_INIT Request
VID, SA, KE, Nonce

Unencrypted!

```

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 : 0000000000000000
Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)
  
```

Debug crypto ikev2
Debug crypto ipsec



No.	Time	Source	Destination	TCP Delta Time
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	

```

Frame 2: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits)
> Ethernet II, Src: RealtekU_00:00:04 (52:54:00:00:04), Dst: RealtekU_0
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
  > Internet Security Association and Key Management Protocol
    Initiator SPI: e9f5fb100567c549
    Responder SPI: 4c6900b8d253af89
    Next payload: Security Association (33)
  > Version: 2.0
  > Exchange type: IKE_SA_INIT (34)
  > Flags: 0x20 (Responder, No higher version, Response)
  > Message ID: 0x00000000
  > Length: 487
  > Payload: Security Association (33)
  > Payload: Key Exchange (34)
  > Payload: Nonce (40)
  > Payload: Vendor ID (43) : Cisco Delete Reason Supported
  > Payload: Vendor ID (43) : Cisco VPN Revision 2
  > Payload: Vendor ID (43) : Cisco Dynamic Route Supported
  > Payload: Vendor ID (43) : Cisco FlexVPN Supported
  > Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
  > Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
  > Payload: Certificate Request (38)
  
```

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!

Cuando se lleva a cabo la negociación de intercambio IKE_AUTH, la carga útil se cifra, pero se ve cierta información sobre la negociación, como el SPI creado anteriormente y el tipo de transacción que se está realizando.



No.	Time	Source	Destination	TCP Delta Time
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	

```

Frame 4: 362 bytes on wire (2896 bits), 362 bytes captured (2896 b
> Ethernet II, Src: RealtekU_00:00:04 (52:54:00:00:04), Dst: Real
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
  > Internet Security Association and Key Management Protocol
    Initiator SPI: e9f5fb100567c549
    Responder SPI: 4c6900b8d253af89
    Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x20 (Responder, No higher version, Response)
  > ... 0... = Initiator: Responder
  > ... 0... = Version: No higher version
  > ... 1... = Response: Response
  > Message ID: 0x00000001
  > Length: 320
  > Payload: Encrypted and Authenticated (46)
  
```

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!

Una vez que se recibe el último paquete de intercambio IKE_AUTH, se completa la negociación del túnel.

No.	Time	Source	Destination	TCP Delta
1	0.000	192.168.1.1	192.168.2.1	
2	0.000	192.168.2.1	192.168.1.1	
3	0.000	192.168.1.1	192.168.2.1	
4	0.000	192.168.2.1	192.168.1.1	
5	0.000	192.168.2.1	192.168.1.1	
6	0.000	192.168.1.1	192.168.2.1	
7	0.000	192.168.2.1	192.168.1.1	
8	0.000	192.168.1.1	192.168.2.1	
9	0.000	192.168.2.1	192.168.1.1	
10	0.000	192.168.2.1	192.168.1.1	
11	0.000	192.168.1.1	192.168.2.1	
12	0.000	192.168.1.1	192.168.2.1	


```

> Frame 3: 682 bytes on wire (5456 bits), 682 bytes captured (5456 bit
> Ethernet II, Src: RealtekU_00:00:00 (52:54:00:00:00:00), Dst: Realte
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
  Initiator SPI: e9f5fb100567c549
  Responder SPI: 4c6900b8d253af89
  Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x08 (Initiator, No higher version, Request)
    .... 1... = Initiator: Initiator
    .... 1... = Version: No higher version
    .... 0... = Response: Request
  Message ID: 0x00000001
  Length: 640
  > Payload: Encrypted and Authenticated (46)

```



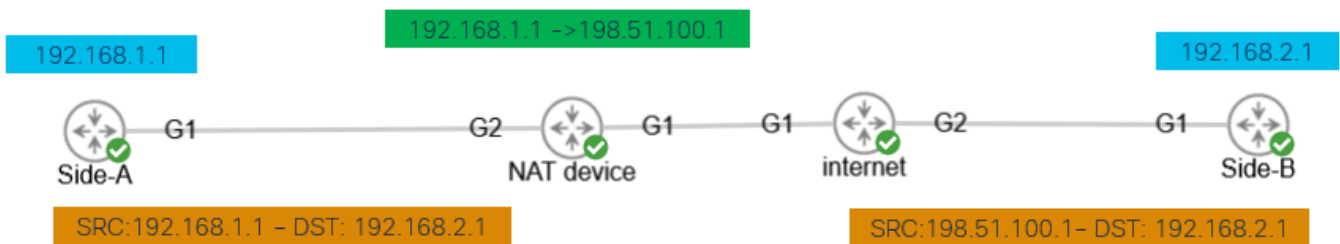
```

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

```

Encrypted!

Transacción Cuando NAT está entre



Nat-transversal es otra característica que se puede ver cuando se lleva a cabo la negociación de túnel. Si un dispositivo intermedio está navegando una o ambas direcciones utilizadas para el túnel, los dispositivos cambian el puerto UDP de 500 a 4500 cuando se negocia la fase 2 (IKE_AUTH Exchange).

Captura tomada en el lado A:

No.	Time	Source	Destination	Protocol	Length
1	0.00	192.168.1.1	192.168.2.1	ISAKMP	
2	0.00	192.168.2.1	192.168.1.1	ISAKMP	
3	0.00	192.168.1.1	192.168.2.1	ISAKMP	
4	0.00	192.168.2.1	192.168.1.1	ISAKMP	
5	0.00	192.168.1.1	192.168.2.1	ISAKMP	
6	0.00	192.168.2.1	192.168.1.1	ISAKMP	
7	0.00	192.168.1.1	192.168.2.1	ISAKMP	
8	0.00	192.168.2.1	192.168.1.1	ISAKMP	


```

> Frame 3: 618 bytes on wire (4944 bits), 618 bytes captured (4944
> Ethernet II, Src: RealtekU_00:00:33 (52:54:00:00:00:33), Dst: Rea
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
> Internet Security Association and Key Management Protocol
  Initiator SPI: ec01171f30d05063
  Responder SPI: 9a0f8b75c0e01c78
  Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x08 (Initiator, No higher version, Request)
  Message ID: 0x00000001
  Length: 572
  > Payload: Encrypted and Authenticated (46)

```

```

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

```

Captura tomada en el lado B:

No.	Time	Source	Destination	Protocol	Length
1	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
2	0.000000	192.168.2.1	198.51.100.1	ISAKMP	
3	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
4	0.000000	192.168.2.1	198.51.100.1	ISAKMP	
5	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
6	0.000000	192.168.2.1	198.51.100.1	ISAKMP	
7	0.000000	198.51.100.1	192.168.2.1	ISAKMP	
8	0.000000	192.168.2.1	198.51.100.1	ISAKMP	

```

> Frame 3: 618 bytes on wire (4944 bits), 618 bytes captured (4944 b)
> Ethernet II, Src: RealtekU_00:00:33 (52:54:00:00:33), Dst: Real
> Internet Protocol Version 4, Src: 198.51.100.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
> Internet Security Association and Key Management Protocol
  Initiator SPI: ec01171f30d05063
  Responder SPI: 9a0f8b75c0e01c78
  Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
  > Exchange type: IKE_AUTH (35)
  > Flags: 0x08 (Initiator, No higher version, Request)
  > Message ID: 0x00000001
  > Length: 572
  > Payload: Encrypted and Authenticated (46)

```

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:

Problemas comunes del plano de control

Puede haber factores locales o externos que afecten a la negociación del túnel y que también se puedan identificar con capturas. Los siguientes escenarios son los más comunes.

Discordancia de configuración

Este escenario se puede resolver observando cada configuración de fase 1 y fase 2 del dispositivo. Sin embargo, puede haber escenarios en los que no haya acceso al extremo remoto. Captura ayuda identificando qué dispositivo envía NO_PROPOSAL_CHOSEN dentro de los paquetes de la fase 1 o 2. Esa respuesta indica que algo puede estar mal con la configuración y qué fase debe ajustarse.

Side-A

Side-B

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 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=05 Initiator Request
4	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=04 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

```

Protocol ID: IKE (1)
SPI Size: 0
Proposed Transforms: 4
Payload: Transform (3)
  Next payload: Transform (3)
  Reserved: 00
  Payload length: 12
  Transform Type: Encryption Algorithm (ENCR) (1)
  Reserved: 00
  Transform ID (ENCR): ENCR_AES_CBC (12)
  > Transform Attribute (t=14,l=2): Key Length: 256
  > Payload: Transform (3)

```

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 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=05 Initiator Request
4	0.000000	192.168.1.1	192.168.2.1	ISAKMP	INFORMATIONAL MID=04 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

```

> Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: RealtekU_00:00:36 (52:54:00:00:36), Dst: RealtekU_00:00:33 (52:54:00:00:33)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
> Internet Security Association and Key Management Protocol
  Initiator SPI: 982a79a178dd0a36
  Responder SPI: ace9e4f53f7a5c6d
  Next payload: Notify (41)
  > Version: 2.0
  > Exchange type: IKE_SA_INIT (34)
  > Flags: 0x20 (Responder, No higher version, Response)
  > Message ID: 0x00000000
  > Length: 36
  > Payload: Notify (41) - NO_PROPOSAL_CHOSEN

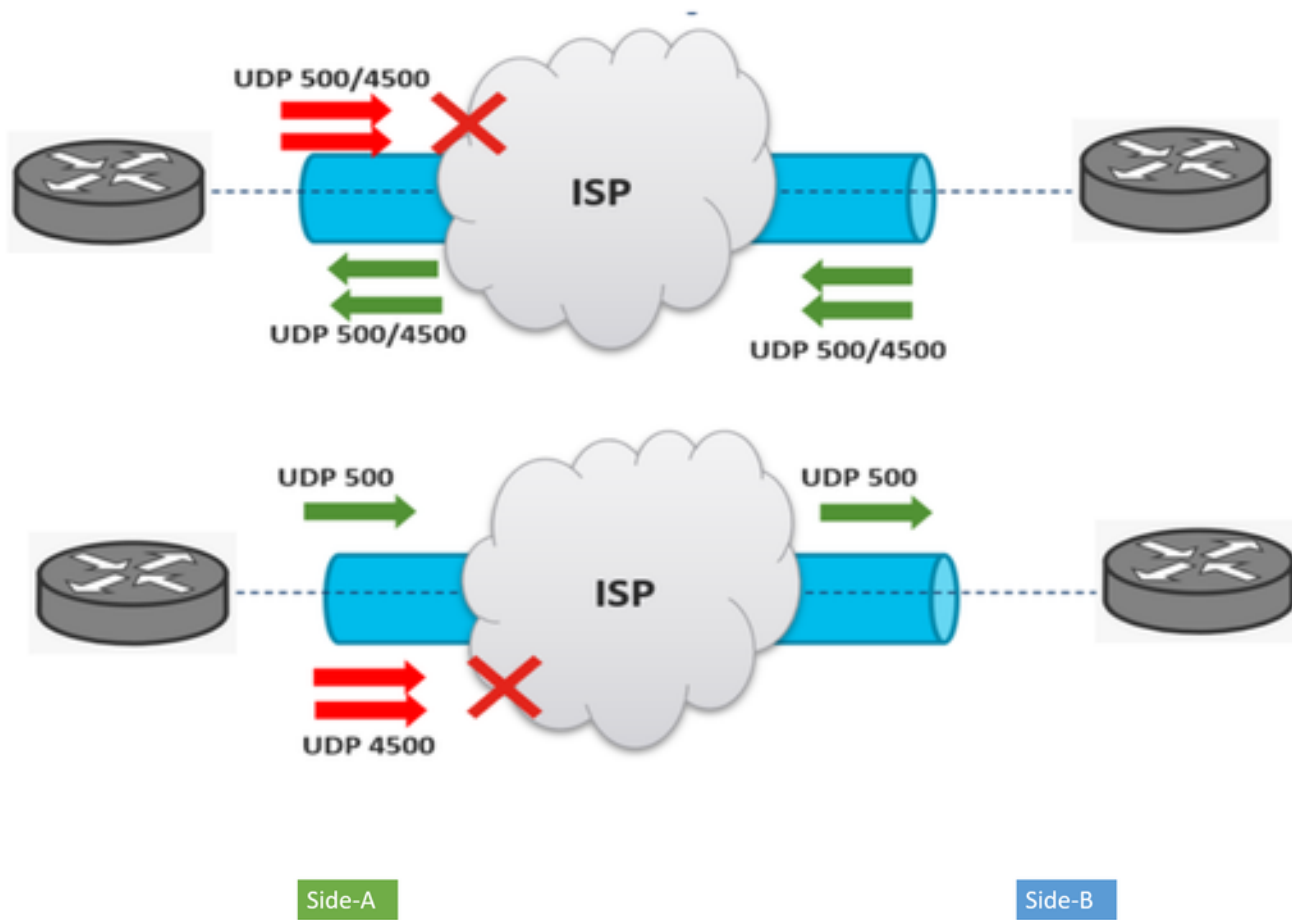
```

Values sent from site-A do not match as is configured on site-B

Retransmisiones

Una negociación de túnel IPsec puede fallar debido a que los paquetes de negociación se descartan a lo largo de la trayectoria entre los dispositivos finales. Los paquetes descartados pueden ser paquetes de fase 1 o fase 2. Cuando este es el caso, el dispositivo que espera un paquete de respuesta retransmite el último paquete, y si no hay respuesta después de 5 intentos, el túnel se concluye y se reinicia desde el principio.

Las capturas a cada lado del túnel ayudan a identificar qué podría bloquear el tráfico y en qué dirección se ve afectado.



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

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).