

Solucionar problemas de túneis IPsec e plano de controle comum com capturas de pacotes

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Ferramentas úteis](#)

[Como configurar capturas no roteador IOS XE](#)

[Analisar o estabelecimento de túnel com capturas de pacotes](#)

[Transação quando o NAT está entre](#)

[Problemas comuns do plano de controle](#)

[Incompatibilidade de configuração](#)

[Retransmissões](#)

Introdução

Este documento descreve como as capturas de pacotes, outras ferramentas, ajudam com problemas de plano de controle quando a VPN site a site nos roteadores Cisco IOS® XE é negociada.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração da CLI do Cisco IOS®.
- Conhecimento fundamental de IKEv2 e IPsec.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- CSR1000V - Software Cisco IOS XE executando a versão 16.12.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As capturas de pacotes são uma ferramenta poderosa para ajudá-lo a verificar se os pacotes estão sendo enviados/recebidos entre dispositivos pares de VPN. Eles também confirmam se o comportamento visto com depurações de IPsec se alinha à saída coletada nas capturas, já que as depurações são uma interpretação lógica, e a captura representa a interação física entre os correspondentes. Por causa disso, você pode confirmar ou descartar problemas de conectividade.

Ferramentas úteis

Existem ferramentas úteis que ajudam você a configurar as capturas, extrair a saída e analisá-la mais. Alguns deles são:

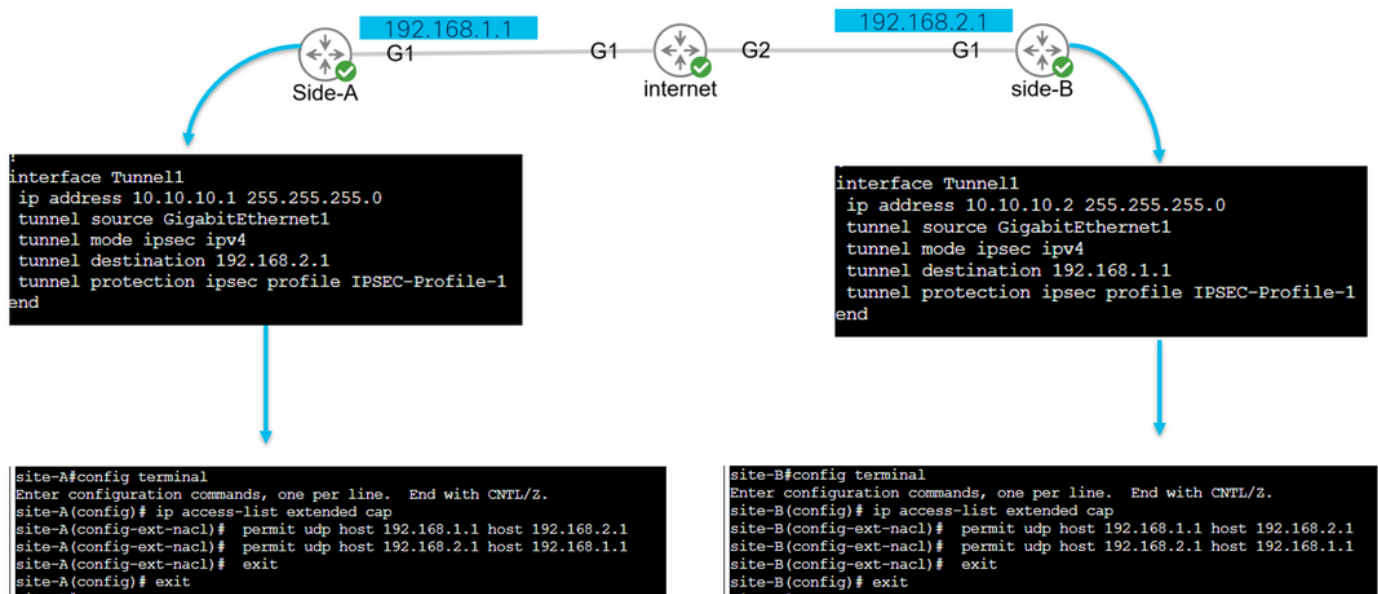
- Wireshark: Este é um analisador de pacotes de código aberto bem conhecido e usado.
- Monitorar capturas: recurso do Cisco IOS XE em roteadores que ajudam a coletar capturas e fornecem uma saída leve de como é o fluxo de tráfego, o protocolo coletado e seus timestamps.

Como configurar capturas no roteador IOS XE



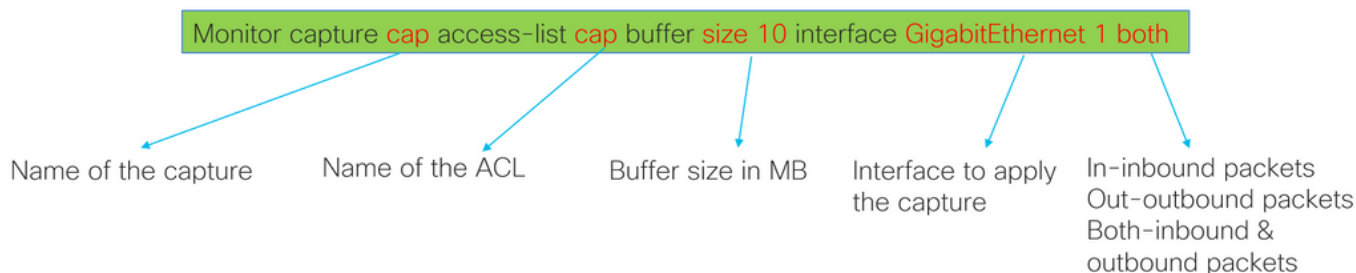
Uma captura usa uma lista de acesso estendida (ACL) que define o tipo de tráfego a ser coletado e os endereços origem e destino dos pares VPN ou segmentos do tráfego interessante. Uma negociação de túnel usa a porta UDP 500 e a porta 4500 se o NAT-T estiver habilitado ao longo do caminho. Quando a negociação for concluída e o túnel for estabelecido, o tráfego interessante usará o protocolo IP 50 (ESP) ou o UDP 4500 se o NAT-T estiver habilitado.

Para solucionar problemas relacionados ao plano de controle, os endereços IP dos pares de VPN devem ser usados para capturar como o túnel é negociado.



```
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
```

A ACL configurada é usada para restringir o tráfego capturado e é colocada na interface usada para negociar o 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

Uma vez configurada a captura, ela pode ser manipulada para interrompê-la, limpá-la ou extrair o tráfego coletado com os próximos comandos:

- Verifique as informações gerais de captura: show monitor capture
- Iniciar/parar a captura: iniciar/parar limite de captura do monitor
- Verifique se a captura está coletando pacotes: show monitor capture cap buffer
- Veja uma breve saída do tráfego: show monitor capture cap buffer brief
- Limpe a captura: limite de captura do monitor limpo
- Extraia a saída da captura:
 - dump buff da tampa do monitor
 - bootflash de exportação do cap de captura do monitor:capture.pcap

Analisar o estabelecimento de túnel com capturas de pacotes

Como mencionado anteriormente, para negociar o túnel IPsec, os pacotes são enviados por UDP com a porta 500 e a porta 4500 se o NAT-T estiver habilitado. Com as capturas, mais informações podem ser vistas desses pacotes, como a fase que está sendo negociada (fase 1 ou fase 2), a função de cada dispositivo (iniciador ou respondente) ou os valores SPI que acabaram de ser criados.

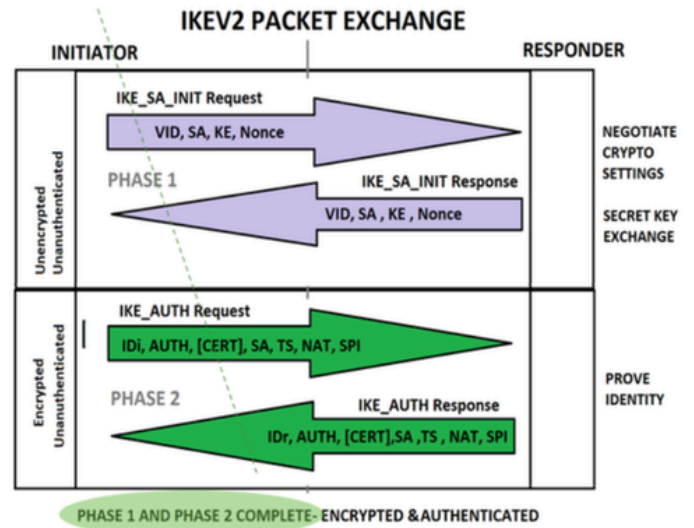
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

Phase 2 encrypted



Mostrando a breve saída da captura do roteador, a interação entre os peers é vista, enviando pacotes 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

Depois de extrair o dump e exportar o arquivo pcap do roteador, mais informações dos pacotes ficam visíveis usando o wireshark.

The image shows a Wireshark capture of an IKEv2 exchange. The packet list pane shows 13 packets. The packet details pane for the first packet (No. 1) shows the following structure:

- 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

Na seção Internet Protocol do primeiro pacote de troca IKE_SA_INIT enviado, os endereços de origem e destino do pacote UDP estão localizados. Na seção User Datagram Protocol, as portas usadas e a seção Internet Security Association and Key Management Protocol mostram a versão do protocolo, o tipo de mensagem que está sendo trocada e a função do dispositivo, bem como o SPI criado. Ao coletar depurações de IKEv2, as mesmas informações são apresentadas nos logs de depuração.

The image shows a Wireshark capture of an IKEv2 exchange with several annotations:

- A diagram shows a purple arrow labeled "IKE_SA_INIT Request" pointing to a box containing "VID, SA, KE, Nonce". A red box labeled "Unencrypted!" is positioned to the right of the arrow.
- The packet list pane shows 12 packets.
- The packet details pane for the first packet (No. 1) shows the following structure:
 - 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
 - Initiator SPI: e9f5fb100567c549
 - Responder SPI: 0000000000000000
 - Next payload: Security Association (33)
 - Version: 2.0
 - Exchange type: IKE_SA_INIT (34)
 - Flags: 0x08 Initiator, No higher version, Request
 - Message ID: 0x00000000
 - Length: 454
 - 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

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!

Quando ocorre a negociação de Intercâmbio IKE_AUTH, o payload é criptografado, mas algumas informações sobre a negociação são visíveis, como o SPI criado anteriormente e o tipo de transação que está sendo feita.



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!

Quando o último pacote IKE_AUTH Exchange for recebido, a negociação do túnel será concluída.

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: 0x00 (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)

```



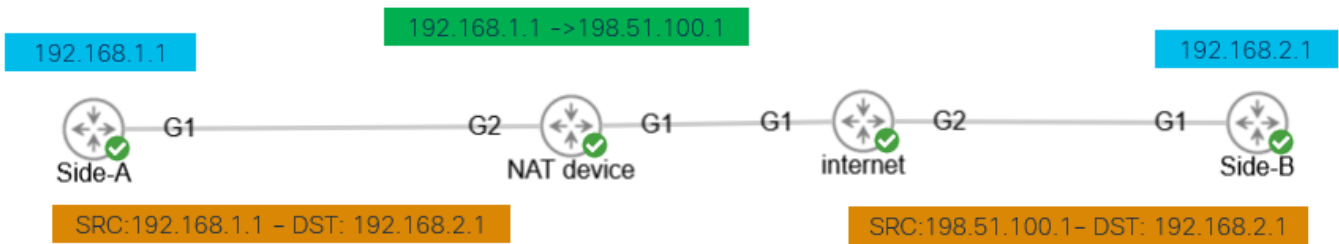
```

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!

Transação quando o NAT está entre



Nat-transversal é outra característica que pode ser vista quando a negociação do túnel ocorre. Se um dispositivo intermediário estiver vinculando um ou os dois endereços usados para o túnel, os dispositivos alterarão a porta UDP de 500 para 4500 quando a fase 2 (Intercâmbio IKE_AUTH) for negociada.

Captura realizada no 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: 0x00 (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 realizada no 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 (52:54:00:00:00:33), 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 comuns do plano de controle

Pode haver fatores locais ou externos que afetem a negociação do túnel e também podem ser identificados com capturas. Os próximos cenários são os mais comuns.

Incompatibilidade de configuração

Esse cenário pode ser resolvido observando-se a configuração das fases 1 e 2 de cada dispositivo. No entanto, pode haver situações em que não haja acesso à extremidade remota. Captura ajuda identificando qual dispositivo envia um NO_PROPOSAL_CHOSEN dentro dos pacotes na fase 1 ou 2. Essa resposta indica que algo pode estar errado com a configuração e que fase precisa ser ajustada.

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 Transform: 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 (52:54:00:00:00:36), Dst: RealtekU_00:00:33 (52:54:00:00:00:33)
> 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

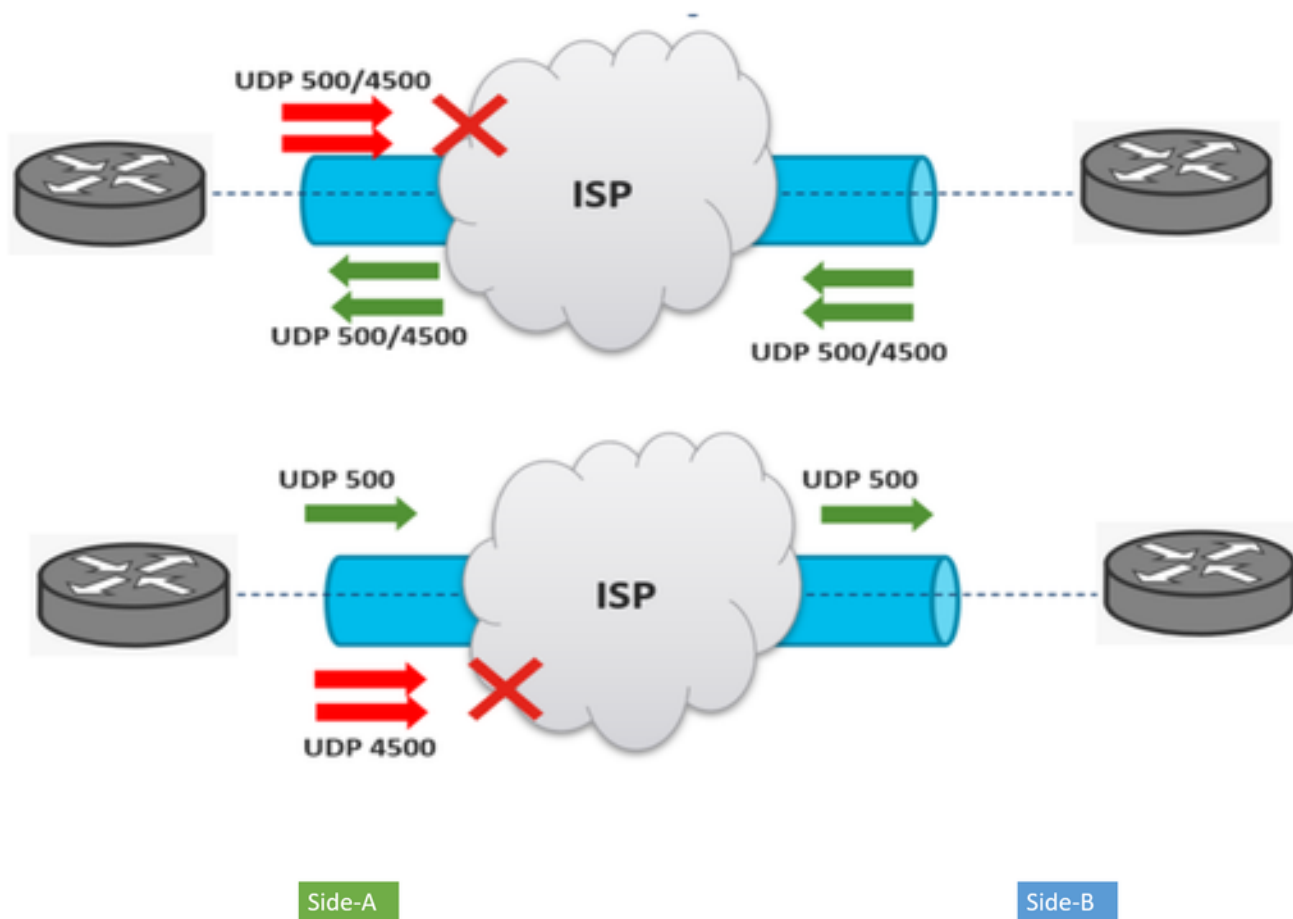
```

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

Retransmissões

Uma negociação de túnel IPsec pode falhar devido aos pacotes de negociação sendo descartados ao longo do caminho entre os dispositivos finais. Os pacotes descartados podem ser pacotes de fase 1 ou fase 2. Quando esse for o caso, o dispositivo que espera um pacote de resposta retransmite o último pacote e, se não houver resposta após 5 tentativas, o túnel é concluído e reiniciado desde o início.

As capturas em cada lado do túnel ajudam identificando o que poderia bloquear o tráfego e em que direção ele é afetado.



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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.