

Troubleshoot IPsec Tunnels and Common Control-Plane Issues with Packet Captures

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Useful Tools](#)

[How to Configure Captures on IOS XE Router](#)

[Analyze the Tunnel Establishment with Packet Captures](#)

[Transaction When NAT is in Between](#)

[Common Control-Plane Issues](#)

[Configuration Mismatch](#)

[Retransmissions](#)

Introduction

This document describes how packet captures, other tools, help with control-plane issues when site-to-site VPN on Cisco IOS® XE routers is negotiated.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco IOS® CLI configuration.
- Fundamental knowledge of IKEv2 and IPsec.

Components Used

The information in this document is based on these software versions:

- CSR1000V - Cisco IOS XE Software running 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Packet captures are a powerful tool to help you verify whether packets are being sent/received between VPN peer devices. They also confirm if the behavior seen with IPsec debugs aligns to the output collected on the

captures since the debugs are a logical interpretation, and the capture represents the physical interaction between the peers. Because of that, you could confirm or discard connectivity issues.

Useful Tools

There are useful tools that help you configure the captures, extract the output, and analyze it further. Some of them are:

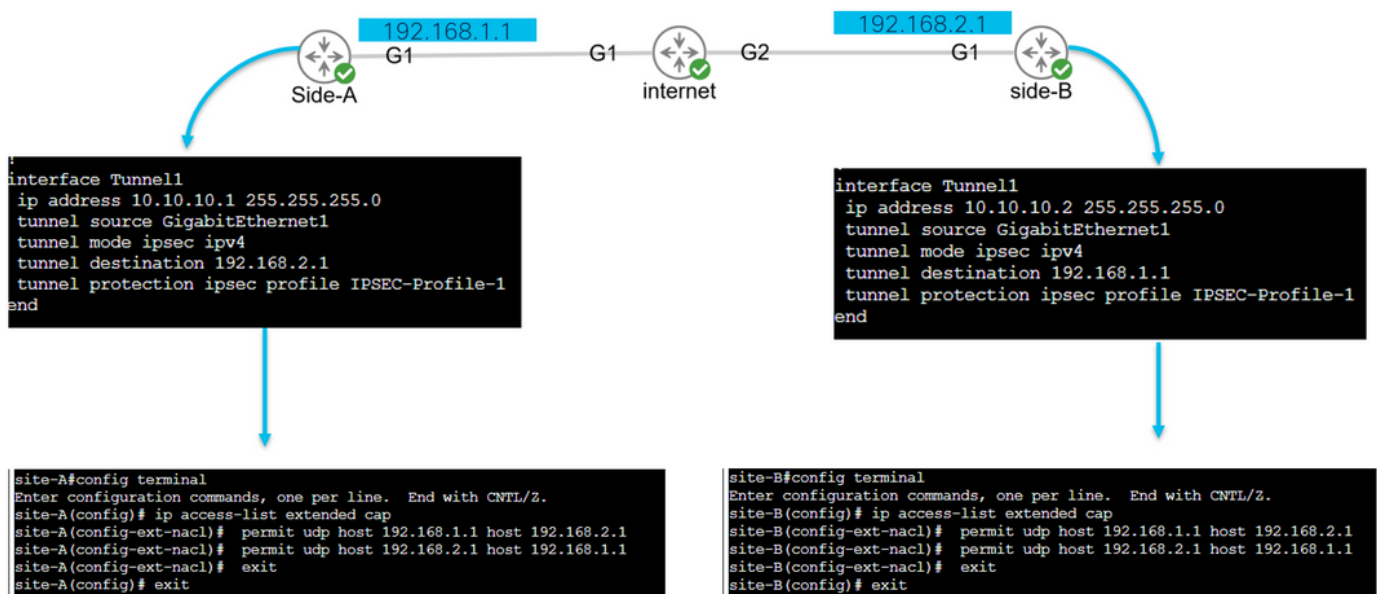
- Wireshark: This is a well-known and used open-source packet analyzer.
- Monitor captures: Cisco IOS XE feature on routers that help you collect captures and provide you a light output of what the traffic flow looks like, protocol collected, and its timestamps.

How to Configure Captures on IOS XE Router



A capture uses an extended access-list (ACL) that defines the type of traffic to be collected, and the source, and destination addresses of the VPN peers or segments of the interesting traffic. A tunnel negotiation uses the UDP port 500 and port 4500 if NAT-T is enabled along the path. Once the negotiation completes and the tunnel is established, the interesting traffic uses IP protocol 50 (ESP) or UDP 4500 if NAT-T is enabled.

In order to troubleshoot control-plane related issues, VPN peers IP addresses must be used to capture how the tunnel is negotiated.

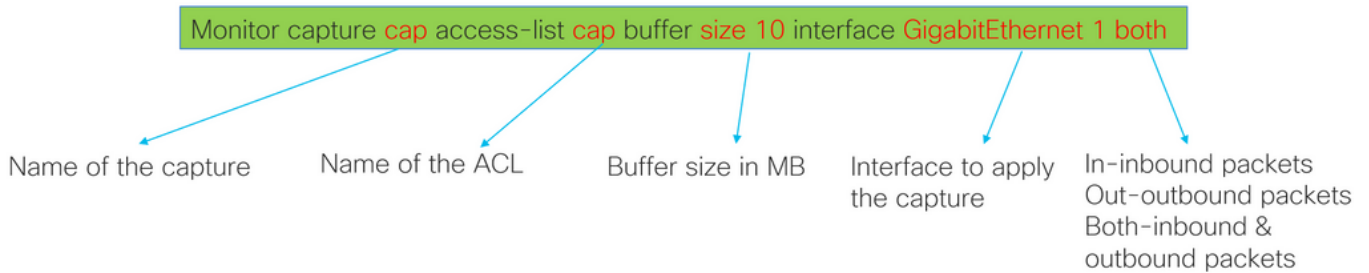


```

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

```

The configured ACL is used to narrow the captured traffic, and it is placed on the interface used to negotiate the tunnel.



```

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

Once the capture is configured, it can be manipulated to stop it, clear it, or extract the traffic collected with the next commands:

- **Check the general capture info:** show monitor capture
- **Start/stop the capture:** monitor capture cap start/stop
- **Verify the capture is collecting packets:** show monitor capture cap buffer

- **See a brief output of the traffic:** show monitor capture cap buffer brief
- **Clear the capture:** monitor capture cap clear
- **Extract the capture output:**
 - monitor cap cap buff dump
 - monitor capture cap export bootflash:capture.pcap

Analyze the Tunnel Establishment with Packet Captures

As mentioned earlier, to negotiate the IPsec tunnel, packets are sent over UDP with port 500 and port 4500 if NAT-T is enabled. With captures, more information can be seen from those packets such as the phase that is being negotiated (phase 1 or phase 2), the role of each device (initiator or responder), or the SPI values that were just created.

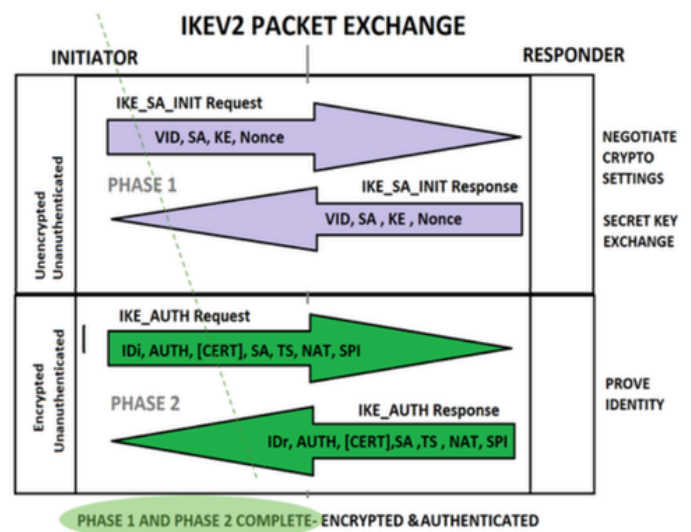
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

Phase 2 encrypted



Showing the brief output of the capture from the router, the interaction between the peers is seen, sending UDP packets.

```
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
```

After extracting the dump and exporting the pcap file from the router, more information from the packets is visible using Wireshark.

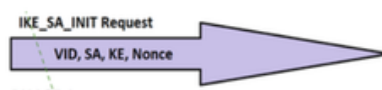
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	496	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	529	IKE_SA_INIT MID=00 Responder Response
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	682	IKE_AUTH MID=01 Initiator Request
4	0.000000	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=04 Responder Response

> 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

On the Internet Protocol section of the first IKE_SA_INIT Exchange packet sent, the source and destination addresses of the UDP packet are located. On the User Datagram Protocol section, the ports used and the Internet Security Association and Key Management Protocol section the version of the protocol, the type of message being exchanged, and the role of the device, as well as SPI created are seen. When collecting IKEv2 debugs, the same information is presented within the debug logs.

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	

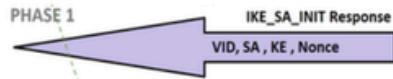
> Frame 1: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)
 > Ethernet II, Src: RealtekU_00:00:00 (52:54:00:00:00:00), Dst: RealtekU_00:00:04 (52:54:00:00:00:04)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
 > User Datagram Protocol, Src Port: 500, Dst Port: 500
 >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



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!

When the IKE_AUTH Exchange negotiation takes place, the payload is encrypted but, some information about the negotiation is visible, such as the SPI previously created, and the type of transaction being made.



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: Rea
> 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!

Once the last IKE_AUTH Exchange packet is received, the tunnel negotiation is completed.

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)

```



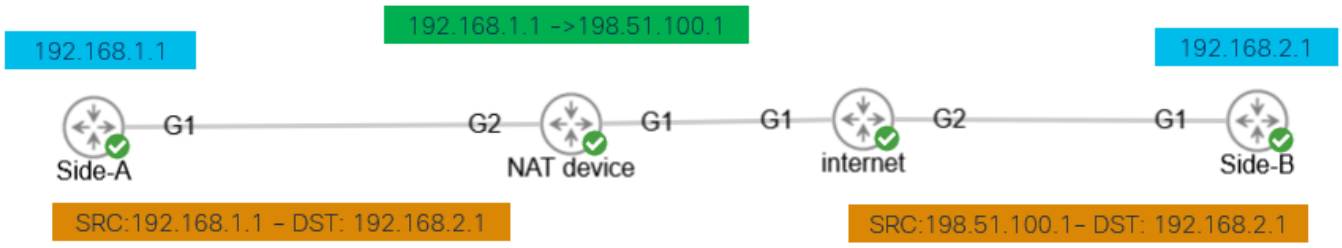
```

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!

Transaction When NAT is in Between



Nat-transversal is another feature that can be seen when the tunnel negotiation takes place. If an intermediate device is natting one or both addresses used for the tunnel, the devices change the UDP port from 500 to 4500 when phase 2 (IKE_AUTH Exchange) is negotiated.

Capture taken on Side-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

```

Capture taken on Side-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: Realte
> 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:

Common Control-Plane Issues

There could be local or external factors that affect the tunnel negotiation and can be identified with captures as well. The next scenarios are the most common.

Configuration Mismatch

This scenario can be resolved by looking at each device phase 1 and phase 2 configuration. However, there could be scenarios in which there is no access to the remote end. Captures help out by identifying which device sends a NO_PROPOSAL_CHOSEN within the packets either on phase 1 or 2. That response indicates something can be wrong with the configuration and which phase needs to be adjusted.

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: 6
  > 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
> 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: ace9e4f3f7a5c6d
  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

```

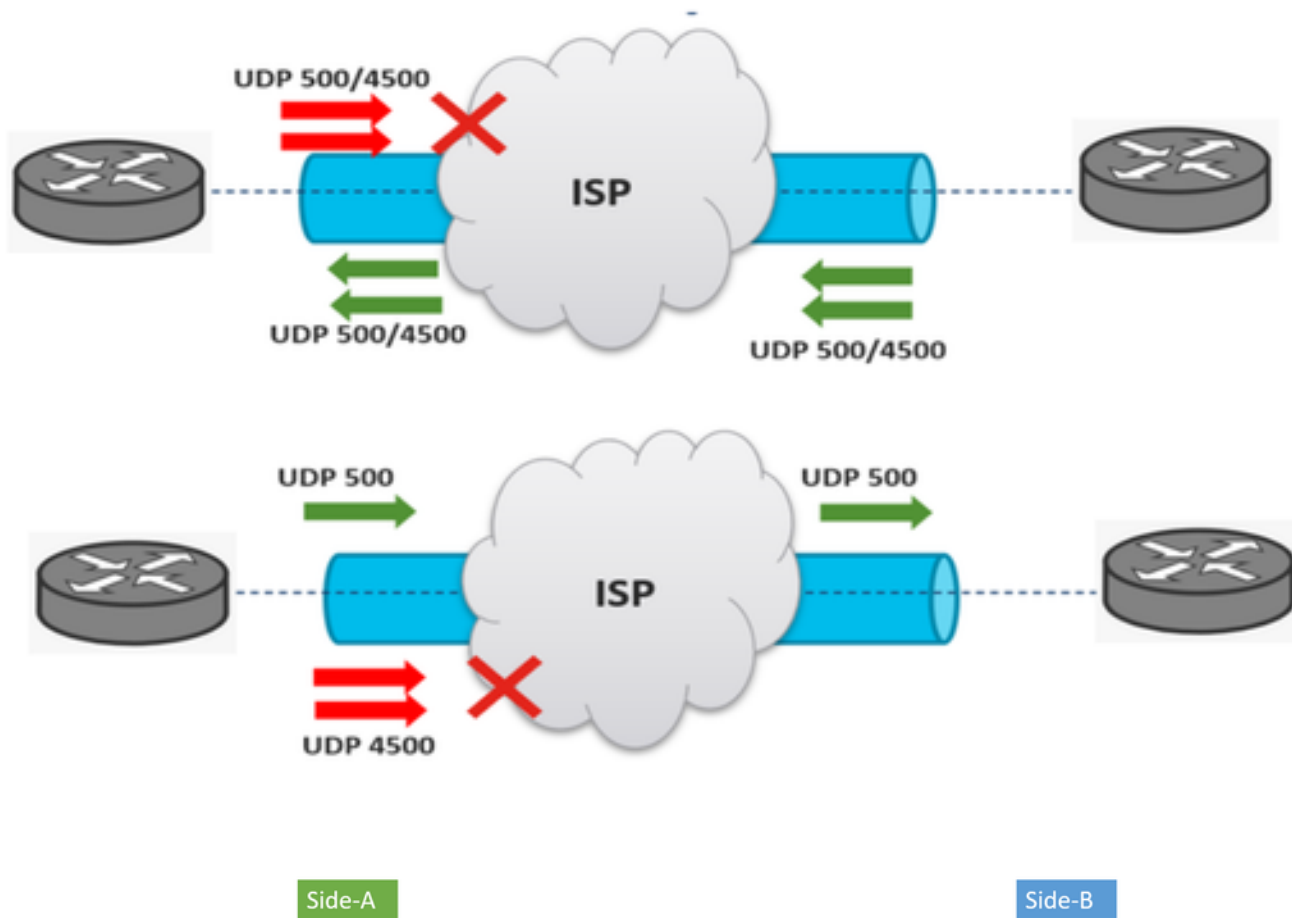
Values sent from site-A do not match what is configured on site-B

Retransmissions

An IPsec tunnel negotiation can fail due to the negotiation packets being dropped along the path between the end devices. The packets dropped can be phase 1 or phase 2 packets. When this is the case, the device that expects a response packet retransmits the last packet, and if there is no response after 5 attempts, the

tunnel is concluded and restarted from the beginning.

Captures on each side of the tunnel help by identifying what could possibly block the traffic and in which direction it is affected.



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