

IPSecトンネルとパケットキャプチャに関する一般的なコントロールプレーンの問題のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[便利なツール](#)

[IOS XEルータでのキャプチャの設定方法](#)

[パケットキャプチャによるトンネル確立の分析](#)

[NATが中間にある場合のトランザクション](#)

[コントロールプレーンのよくある問題](#)

[設定の不一致](#)

[再送信](#)

はじめに

このドキュメントでは、Cisco IOS® XEルータのサイト間VPNがネゴシエートされる際に、パケットキャプチャなどのツールがコントロールプレーンの問題にどのように役立つかについて説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco IOS® CLI設定に関する基本的な知識。
- IKEv2およびIPsecに関する基礎知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- CSR1000V : バージョン16.12.0を実行するCisco IOS XEソフトウェア。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

パケットキャプチャは、VPNピアデバイス間でパケットが送受信されているかどうかを確認するのに役立つ強力なツールです。また、デバッグは論理的な解釈であり、キャプチャはピア間の物理的なインタラクションを表すため、IPSecデバッグで確認される動作がキャプチャで収集された出力と一致するかどうかも確認されます。そのため、接続の問題を確認したり、破棄したりできます。

便利なツール

キャプチャの設定、出力の抽出、および詳細な分析に役立つ便利なツールがあります。次のその一例を示します。

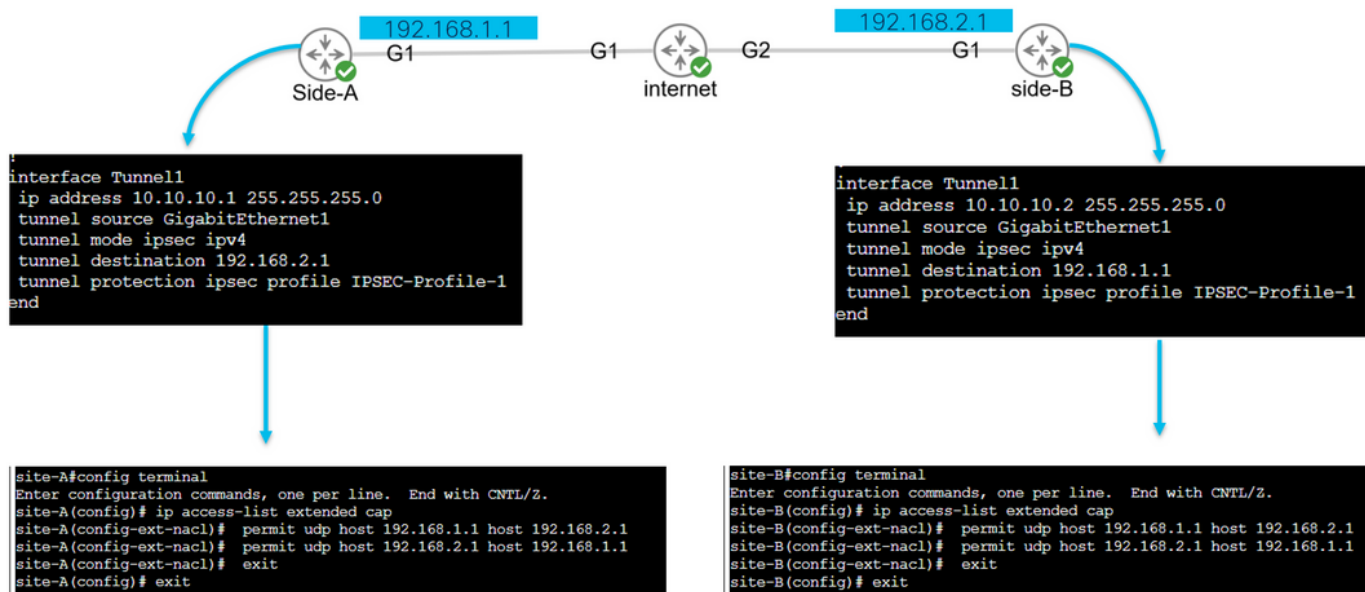
- Wireshark : これは広く知られ、使用されているオープンソースパケットアナライザです。
- キャプチャの監視 : ルータ上のCisco IOS XE機能。キャプチャの収集に役立ち、トラフィックフローの状態、収集されたプロトコル、およびタイムスタンプの光出力を提供します。

IOS XEルータでのキャプチャの設定方法



キャプチャは、収集するトラフィックのタイプと、対象トラフィックのVPNピアまたはセグメントの送信元アドレスおよび宛先アドレスを定義する拡張アクセスリスト(ACL)を使用します。パス上でNAT-Tが有効になっている場合、トンネルネゴシエーションではUDPポート500とポート4500が使用されます。ネゴシエーションが完了してトンネルが確立されると、NAT-Tが有効な場合、対象トラフィックはIPプロトコル50(ESP)またはUDP 4500を使用します。

コントロールプレーンに関連する問題をトラブルシューティングするには、トンネルのネゴシエーション方法をキャプチャするためにVPNピアのIPアドレスを使用する必要があります。

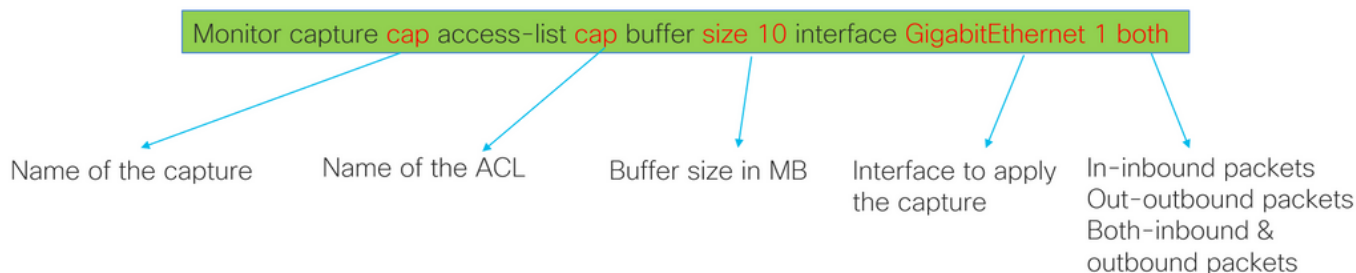


```

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

```

設定されたACLは、キャプチャされたトラフィックを絞り込むために使用され、トンネルのネゴシエーションに使用されるインターフェイスに配置されます。





```
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

キャプチャを設定したら、キャプチャを操作して停止したり、クリアしたり、次のコマンドで収集したトラフィックを抽出したりできます。

- 一般的なキャプチャ情報を確認します。 show monitor capture
- キャプチャの開始/停止 : monitor capture cap start/stop
- キャプチャがパケットを収集していることを確認します。 show monitor capture cap buffer
- トラフィックの簡単な出力を参照してください: show monitor capture cap buffer brief
- キャプチャのクリア : monitor capture cap clear
- キャプチャ出力を抽出します。
 - キャップキャップバフダンプの監視
 - monitor capture cap export bootflash:capture.pcap

パケットキャプチャによるトンネル確立の分析

前述のように、IPSecトンネルをネゴシエートするには、NAT-Tが有効になっている場合、ポート500およびポート4500を使用してパケットがUDP経由で送信されます。キャプチャを使用すると、ネゴシエートされるフェーズ（フェーズ1またはフェーズ2）、各デバイスの役割（イニシエータまたはレスポンド）、作成されたSPI値などの詳細な情報をパケットから確認できます。

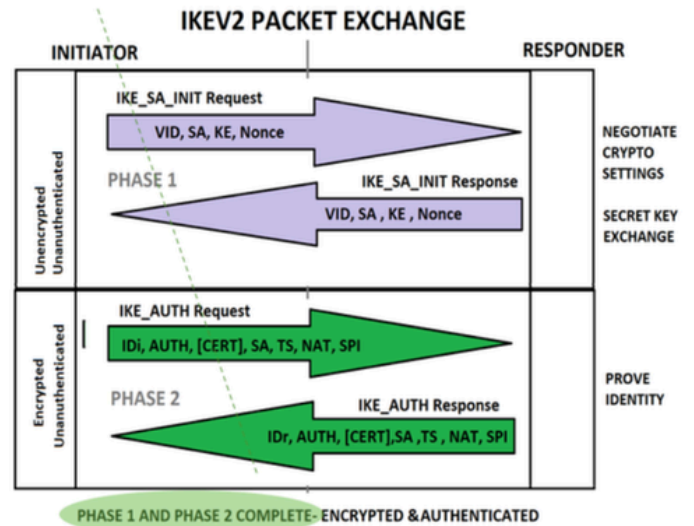
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

Phase 2 encrypted



ルータからのキャプチャの簡単な出力を示すと、ピア間のインタラクションが確認され、UDPパケットが送信されます。

```
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

ダンプを抽出し、pcapファイルをルータからエクスポートした後、Wiresharkを使用してパケットの詳細情報を表示できます。

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
  
```

送信された最初のIKE_SA_INIT ExchangeパケットのInternet Protocolセクションに、UDPパケットの送信元アドレスと宛先アドレスがあります。User Datagram Protocol (UDP ; ユーザデータグラムプロトコル) セクションには、使用されているポートとInternet Security Association and Key Management Protocol(ISAKMP)セクション、プロトコルのバージョン、交換されるメッセージのタイプ、デバイスのロール、および作成されるSPIが表示されます。IKEv2デバッグを収集すると、同じ情報がデバッグログに表示されます。

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!

IKE_AUTH交換ネゴシエーションが行われると、ペイロードは暗号化されますが、前に作成されたSPIや作成されたトランザクションのタイプなど、ネゴシエーションに関する一部の情報が表示されます。



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!

最後のIKE_AUTH交換パッケージが受信されると、トンネルネゴシエーションが完了します。

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)
  
```

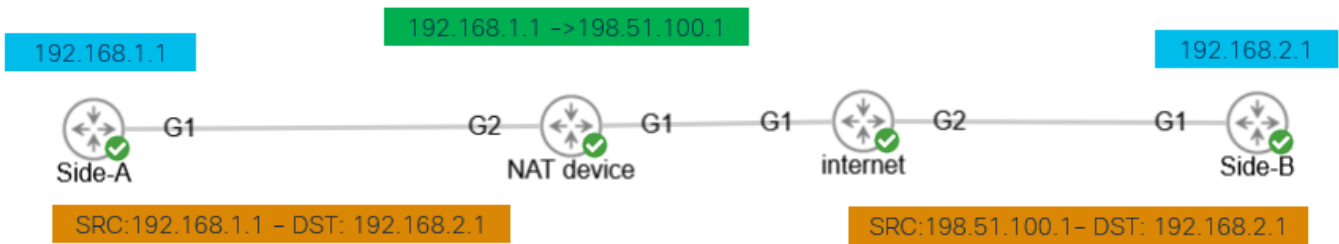


```

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!

NATが中間にある場合のトランザクション



Nat-transversalは、トンネルネゴシエーションが行われるときに表示されるもう1つの機能です。中間デバイスがトンネルに使用される一方または両方のアドレスをnat処理している場合、フェーズ2 (IKE_AUTH交換) がネゴシエートされると、デバイスはUDPポートを500から4500に変更します。

サイドAで取得されたキャプチャ :

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: Re
> 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
  
```

サイドBで取得されたキャプチャ :

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:

コントロールプレーンのよくある問題

トンネルネゴシエーションに影響を与えるローカルまたは外部の要因があり、キャプチャで特定することもできます。次に、最も一般的なシナリオを示します。

設定の不一致

このシナリオは、各デバイスフェーズ1およびフェーズ2の設定を確認することで解決できます。ただし、リモートエンドにアクセスできないシナリオが存在する可能性があります。どのデバイスがフェーズ1または2のいずれかでパケット内でNO_PROPOSAL_CHOSENを送信するかを特定することによって、ヘルプをキャプチャします。この応答は、設定に何らかの問題がある可能性があります。どのフェーズを調整する必要があるかを示しています。

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: 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

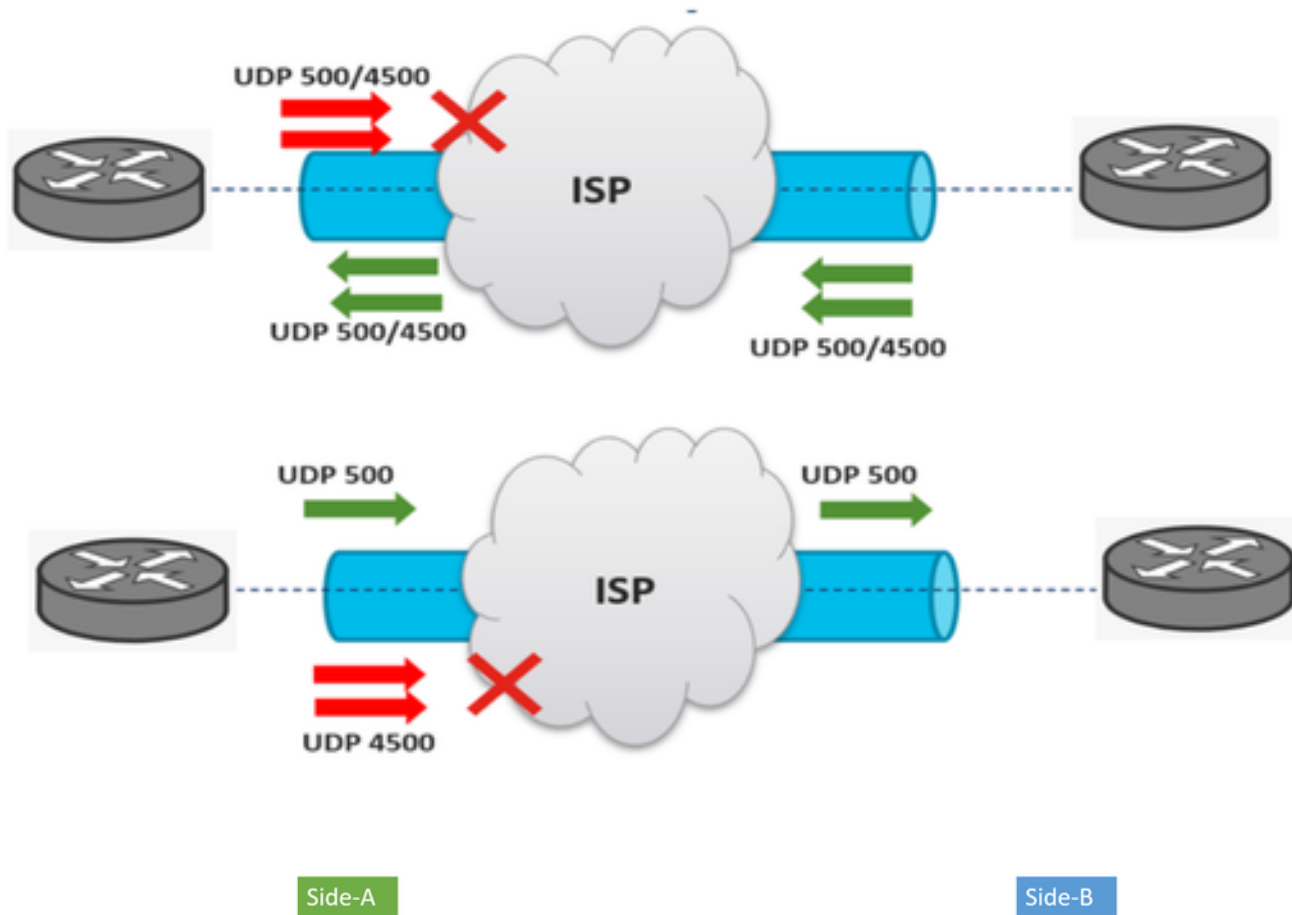
```

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

再送信

IPSecトンネルネゴシエーションは、エンドデバイス間のパス上でネゴシエーション packets がドロップされているために失敗する可能性があります。廃棄される packets は、フェーズ1またはフェーズ2の packets です。この場合、応答 packets を期待するデバイスは最後の packets を再送信し、5回試行しても応答がない場合、トンネルは終了し、最初から再開されます。

トンネルの両側のキャプチャは、トラフィックをブロックしている可能性のある要素と、トラフィックが影響を受ける方向を特定することによって役立ちます。



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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。