

# تالكشمو IPsec قافناً ءاطخاً فاشكتسأ طاقتلا تايلمع عم ةعئاشلا مكحتلا يوتسم اهحالصإو مزحلا

## تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةديفملا تاودألا](#)

[IOS XE هجوم ىلع طاق، تلالا نيوكت ةيفيكي](#)

[مزحلا طاق، تلالا مادختساب قف، نلا عاش، نلا ليحت](#)

[ن.ب. NAT، نوكي امدة عة كرحلا](#)

[ةعئاشلا مكحتلا يوتسم لكاشم](#)

[قباطتم ريغ نيوكتلا](#)

[لباسبالا ةداعا تايلمع](#)

## ةمدقملا

يوتسم لكاشم يف ةدعاسملاو، ىرخألا تاودألاو، ةمزحلا طاق، تلالا ةيفيكي دنتسملا اذه فصوي  
Cisco IOS® XE تاهجوم ىلع عقوم ىلا عقوم نم VPN ةكبش ىلع ضوافتلا دنع مكحتلا

## ةيساسألا تابلطتملا

[تابلطتملا](#)

ةيلالتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- Cisco IOS® CLI نيوكت بةيساسأ ةفرعم
- IPsec و IKEv2 بةيساسأ ةفرعم

## ةمدختسملا تانوكملا

ةيلالتلا جماربلا تارادصا ىلا دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Cisco IOS XE رادصا 16.12.0 جم انرب - CSR1000V

ةصاخة يلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت  
تناك اذا. (يضا رتفا) حوسمم نيوكت بةيساسأ دنتسملا اذه يف ةمدختسملا ةزهجالا عيمج تادب  
رما يال لم تحملا ريثا تلال كم هف نم دكأتف، ليغشتلا دي قكتك بش

## ةيساسأ تامولعم

م تي مزحلل تناك اذا ام ققحتللا يف كدعاسمل ةيوق ةادأ يه مزحلل تاطقل  
م تي يذلا كولسلل ناك اذا ام دكؤت اهنأ امك. VPN ريظن ةزهجأ نيپ اهلابقتسا/اهلاسرا  
تايللمع ىلع هعيميحت م تي يذلا جارخاللا عم قفاوت يي IPsec ءاطخأ حيحصت عم هتدهاشم  
لعافتلا طاقتللالا لثمي و، يقطنم ريسفت يه ءاطخألا حيحصت تايللمع نأل ارظن طاقتللالا  
اهلهاجت وأ لاصتالا لكاشم ديكتأت كنكمي، ببسلل اذهل و. ةريظنللا ةزهجالا نيپ يداملا

## ةديفملا تاودالا

رثكأ اهليلحت و، تاجرخلل جارختسا و، طاقتللالا نيوكت ىلع كدعاست ةديفم تاودا كانه  
اهضعب:

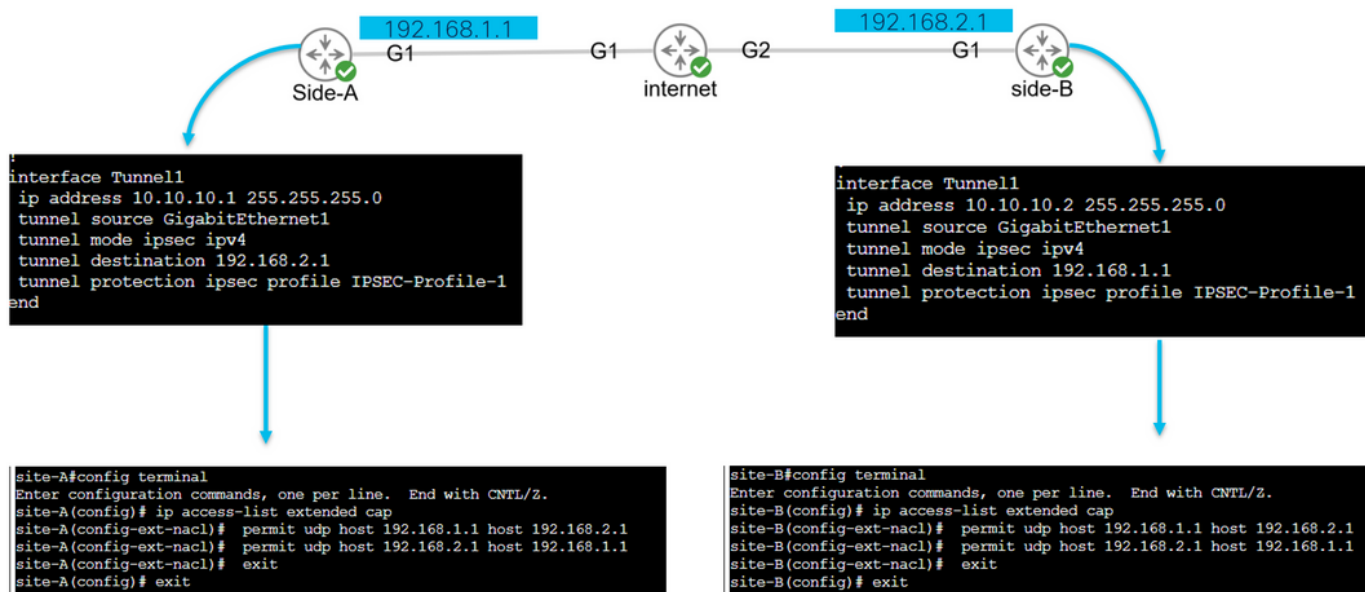
- م دختسم و اديج فورعم رصملا حوتفم مزحلل لحه اذه: Wireshark.
- طاقتللالا عمج ىلع تاهجوملا ىلع Cisco IOS XE ةزيم كدعاست: ةشاشلا ضبق ىلع  
م تي يذلا لوكوتوربللا و، رورملا ةكرح قفدت هيلع و دب يامل يئوض جرخم ريفوت و  
هبة صاخلا ةينمزللا عباوطللا و، هعيميحت.

## IOS XE هجوم ىلع طاقتللالا نيوكت ةيفيك



م تيس يتلا رورملا ةكرح عون ددحت يتلا (ACL) ةعسوملا لوصوللا ةمئاق طاقتللالا مدختسي  
ةديفملا رورملا ةكرح عطاقم و VPN ءارظن بة صاخلا ةهجوملا و رصملا نيوانعو، اهعيميحت  
راسملا ىلع تنكم نوكي NAT-T نأ 4500 ءاني و 500 ءاني م UDP ل قفن ضوافت لمعتسي  
IP 50 لوكوتورب ةديفملا رورملا ةكرح مدختست، قفنللا ءاشن و ضوافتلا لامتكأ درجمب  
NAT-T. ةنيكمت مت اذا UDP 4500 و (ESP)

نيوانع مادختسا بجي، اهالصللا و محتللا ءحولب ةقلعتملا لكاشملا ءاطخأ فاشكتسا لجأ نم  
قفنللا لوح ضوافتلا ةيفيك طاقتللالا VPN ءارظن بة صاخلا IP

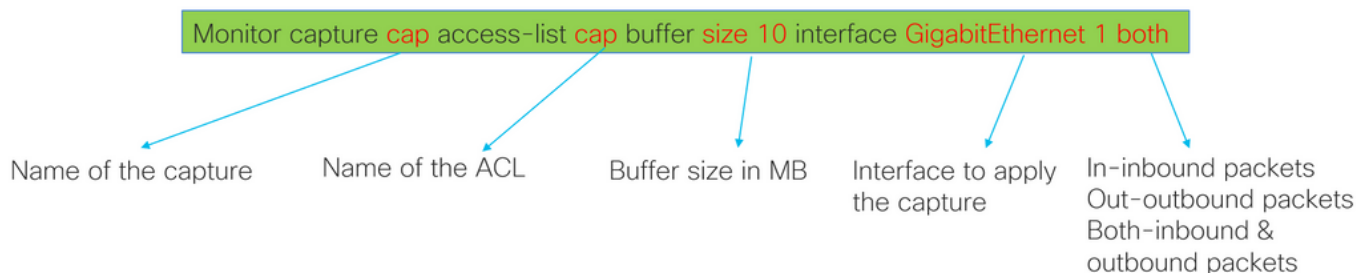


```

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

```

رورملا ةكرح قي ي ضتل انه نيوكت مت يتي التا (ACL) لوصولها في مكحت التا ةمئاق مادختسا متي قف نلا يلع ضوافتل ل ةمدختس مالا ةهجاو لا يلع اهعضو متي و، اه يلع ءاليتسالا مت يتي التا





```
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

رورم لا ءك رح صالختسا وأ ،هحسم وأ ،هفاقيإل هب بعالتلا نكمي ،طاقتلالا نيوكت درجمب  
ةيالتلا رماوأل مادختساب اهعيجمت مت يتلا

- show monitor capture :ةمإعلا طاقتلالا تامولعم نم ققحت
- ءشاشلا طاقتلا فاقيا/ءدب :طاقتلالا فاقيا/ءدب
- show monitor capture cap buffer :مزل عمجي طاقتلالا نأ نم ققحت
- show monitor capture cap buffer :رورملا ءكرجل زجوم جارخا عجار
- ءشاشلا طاقتلا فرح حسم :طاقتلالا حسم
- طاقتلالا جارخا جارختسا:
  - ءشاشلا ءاطغ غيرفت ءيلمع
  - bootflash:capture.pcap ريءصت فرط طاقتلا بردم

## مزل طاقتلا مادختساب قفنلا ءاشنإ ليلحت

عم UDP ربع مزل لاسرا متي ،IPSec قفن يلع ضوافتلل ،اقبسم ءراشإلا تمت امكو  
نم ءيزمة يور نكمي ،طاقتلالا تايلمع عم . NAT-T نيكمت مت اذا 4500 ذفنملاو 500 ذفنملا  
وأ ،(2 ءلحرملا وأ 1 ءلحرملا) اه يلع ضوافتلا متي يتلا ءلحرملا لثم مزللا كلت نم تامولعمل  
وتلل اهؤاشنإ مت يتلا SPI ميقي وأ ،(بيجتسمللا وأ ئءابللا) زاك لك رود

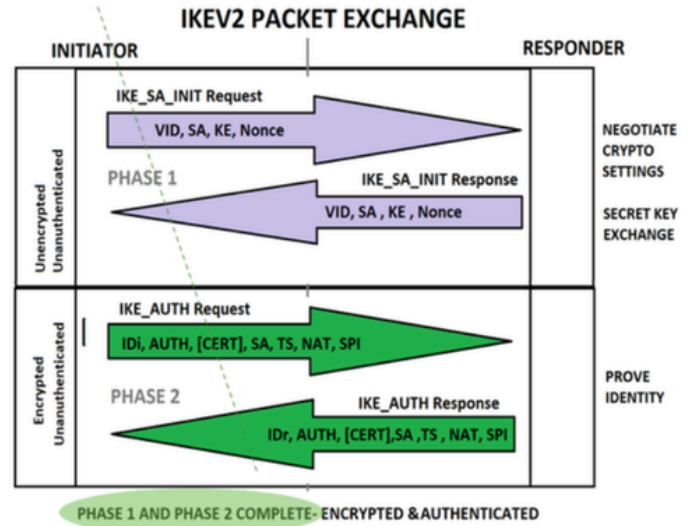
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

Phase 2 encrypted



UDP مزج لاسررا عم ،نارقألانېب لعافتال رهظي ،هجومال نم طاقتلالال نم زجومال جارخالال راهظا

```
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

مزجال نم تامولعملال نم ديزمال نإف ،هجومال نم PCAP فلم ري دصت و غيرفتال جارختسا دعب  
مادختساب ةيئرم نوكت wireshark.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

متي، اهل اسرار متي يتل الى وال IKE\_SA\_INIT لدابت ةمزح نم تنرتن الى لوكوتورب مسق يلى  
 تانايب ططخم لوكوتورب مسق يف. UDP ةمزحل ةهچول او رصم الى وانع عقوم ديدحت  
 ةراد لوكوتوربو تنرتن الى نام ارتقا مسق و ةمدختس م الى ذف انم الى رهظت، مدختس م الى  
 الى ةفاض الى اب، زاهچ الى رودو، اهل دابت متي يتل الى اسر الى عونو، لوكوتورب الى رادص الى حيتاف م الى  
 لىخاد اهسفن تامول عمل ضرع متي، IKEv2 ةاطخ الى حيصت عي مچت دنع. هؤاشن الى مت يذلى SPI  
 ةاطخ الى حيصت الى لچس.

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	

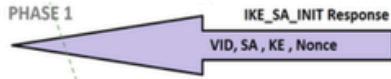
> Frame 1: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)  
 > Ethernet II, Src: RealtekU\_00:00:00 (52:54:00:00:00:00), Dst: RealtekU\_00:00:04 (52:54:00:00:00:04)  
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1  
 > User Datagram Protocol, Src Port: 500, Dst Port: 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



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_
> 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!

تامولعمل اضعب نوكت، نكلو ةلومحلل ريفشت متي، IKE\_AUTH لدابت تاضوافم ءارج دنع  
 اءارج متي يتل ءكحلل عونو، اقبس م هؤاشن مت يذل SPI لثم، ةيئرم ضوافتل لوج



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)
  
```

Encrypted!

قفنل ضوافت لامك متي، IKE\_AUTH لدابت ةمزح رخأ يقلت درجمب

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)

```



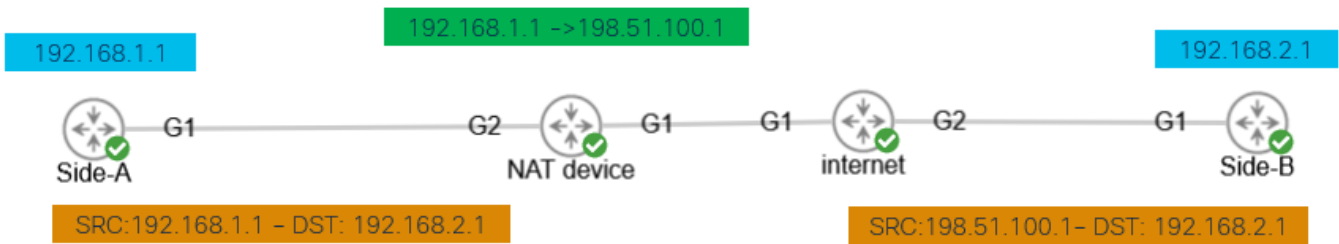
```

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!

## نېب NAT نوکي ام دنع ةكرحلا



طسوت م زاهج ناك اذا. قفنلا ضوافت متي ام دنع اهتيور نكمي رخأ ةزيم وه nat-transversal  
 ىل 500 نم UDP ذفنم ريغت ةزهجالا ناف، قفنلا نامدختسي نيناونع الك وأ اناونع لمحي  
 4500 (IKE\_AUTH Exchange) ةلحرملا ىلع ضوافتلا دنع

أ: بنجالا ىلع ذوخام رسأ

No.	Time	Source	Destination	Protocol	Length
1	0.000	192.168.1.1	192.168.2.1	ISAKMP	
2	0.000	192.168.2.1	192.168.1.1	ISAKMP	
3	0.000	192.168.1.1	192.168.2.1	ISAKMP	
4	0.000	192.168.2.1	192.168.1.1	ISAKMP	
5	0.000	192.168.1.1	192.168.2.1	ISAKMP	
6	0.000	192.168.2.1	192.168.1.1	ISAKMP	
7	0.000	192.168.1.1	192.168.2.1	ISAKMP	
8	0.000	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

```

ب: بنجالا ىلع ذوخام رسأ



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:

## ةعئاشلال مكحتلال يوتسم لكاشم

طاقتلال عم اهديحت نكميوقفلالضوافتلىع رثؤتةيجراخوأةيلحملمواعكانه نوكتدق اعويش رثكألالهةةيلتلالتاهوييرانيسلالاضيا.

### قباطتم ريغ نيوكتلال

عمو 2.ةلحرملاو 1.ةلحرملايف زاهج لك نيوكتيف رظنلاللالخ نم وييرانيسلالاذه لح نكميولع.ديعبلالفرطلاللىلوصولالةينكالم اهيف رفوتتال تاهوييرانيسلكانه نوكتدق،لكلذ اما مزحلاللخاد NO\_PROPOSAL\_CHOSEN لسرييذل زاهجالديحتقيرطنع ةدعاسمضبق وأونيوكتلاليف ائطاخنوكي نأ نكميام عيشلىلإباجتسالالاهذريشت 2.وأ 1.ةلحرملايف اهلديعت مزليةلحرم

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 (52:54:00:00:00:36), 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

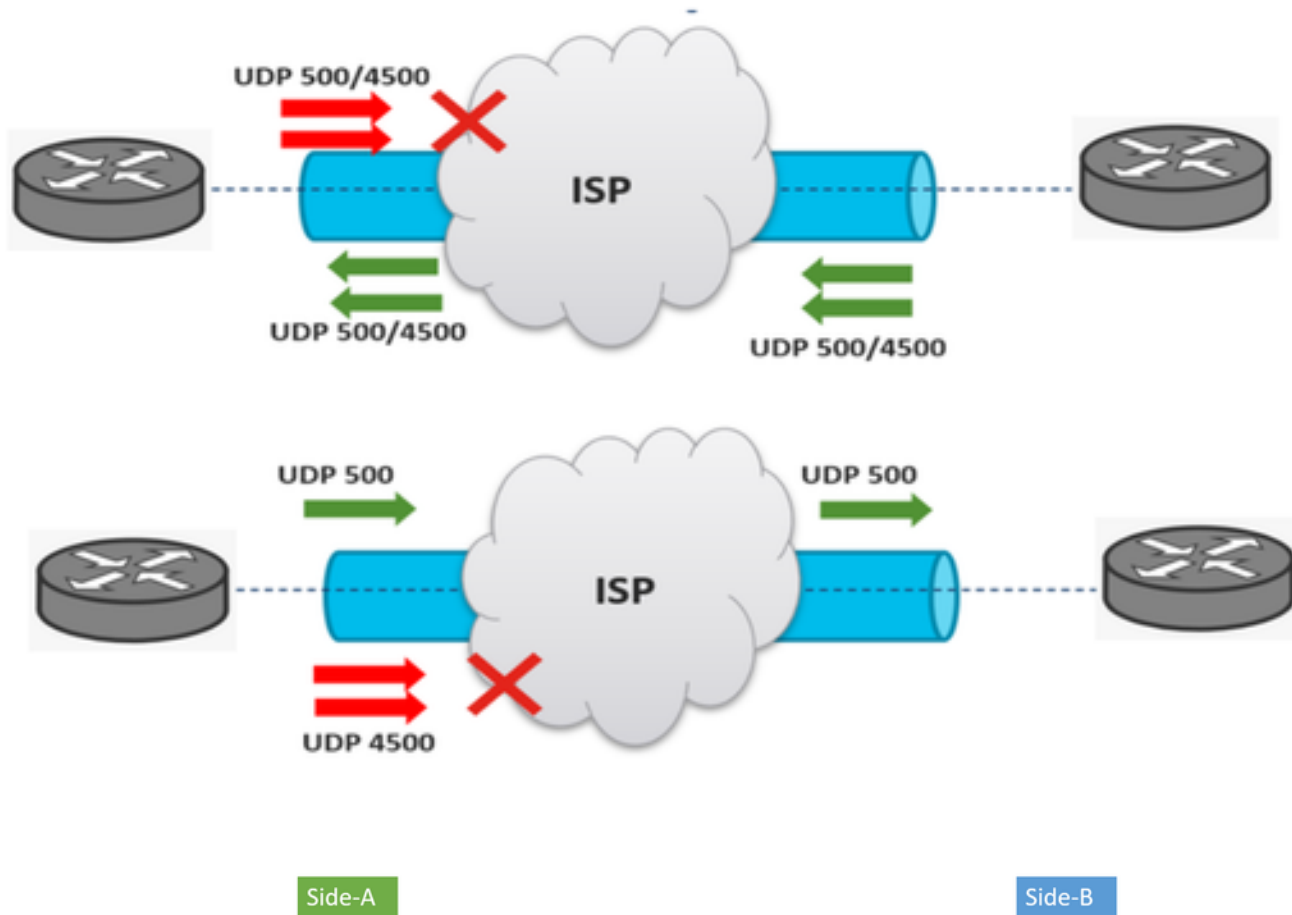
```

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

### لاسزالا ةداعإ تايلمع

راسم لى لى ع اطاقس ا متي يتل ا ضوافت ل مزح ب بسب IPsec ق فن ضوافت ل شفي ن ا نكمي ام دن ع 2 ة ل حرمل ا و ا 1 ة ل حرمل ا متي يتل ا مزحل ا نوكت ن ا نكمي . ةي فرطلا ةزه ج ا ل ني ب كانه نكمي مل اذ ا و ، ةري خ ا ل ا ة مزح ع قوت ي ي ذل ا زا ج ل ل سر ي ، ة ل ا ج ل ا وه ا ذه نو ك ي ةي ا د ب ل ا نم هل ي غ ش ت ة د ا ع ا و ق فن ل ا م ا ت ت خ ا متي ، ت ا ل و ا ح م 5 د ع ب ة ب ا ج ت س ا

ي ا ي ف و ر و ر م ل ا ة ك ر ح ق ي ع ي ن ا نكمي ا م د ي د ح ت ب ة د ع ا س م ل ا ق فن ل ا نم ب ن ا ج ل ك لى ع ط ق ت ل ي ر ث ا ت ه ا ج ت ا



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

