對資料包捕獲的IPsec隧道和常見控制平面問題進行故障排除

目錄

簡介

本檔案介紹在協商Cisco IOS® XE路由器上的站點到站點VPN時，封包擷取、其他工具如何協助解決控制平面問題。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS® CLI配置基礎知識。
- IKEv2和IPsec的基礎知識。

採用元件

本檔案中的資訊是根據以下軟體版本：

- CSR1000V — 運行版本16.12.0的Cisco IOS XE軟體。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

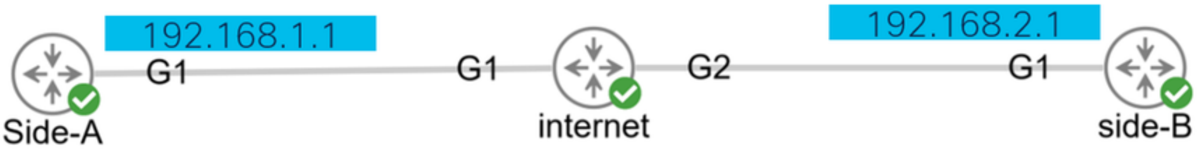
資料包捕獲是一個功能強大的工具，可幫助您驗證資料包是否在VPN對等裝置之間傳送/接收。它們還確認IPsec調試中看到的行為是否與捕獲上收集的輸出一致，因為調試是邏輯解釋，而捕獲表示對等體之間的物理互動。因此，您可以確認或放棄連線問題。

有用工具

有一些有用的工具可幫助您配置捕獲、提取輸出並對其進行進一步分析。其中一些是：

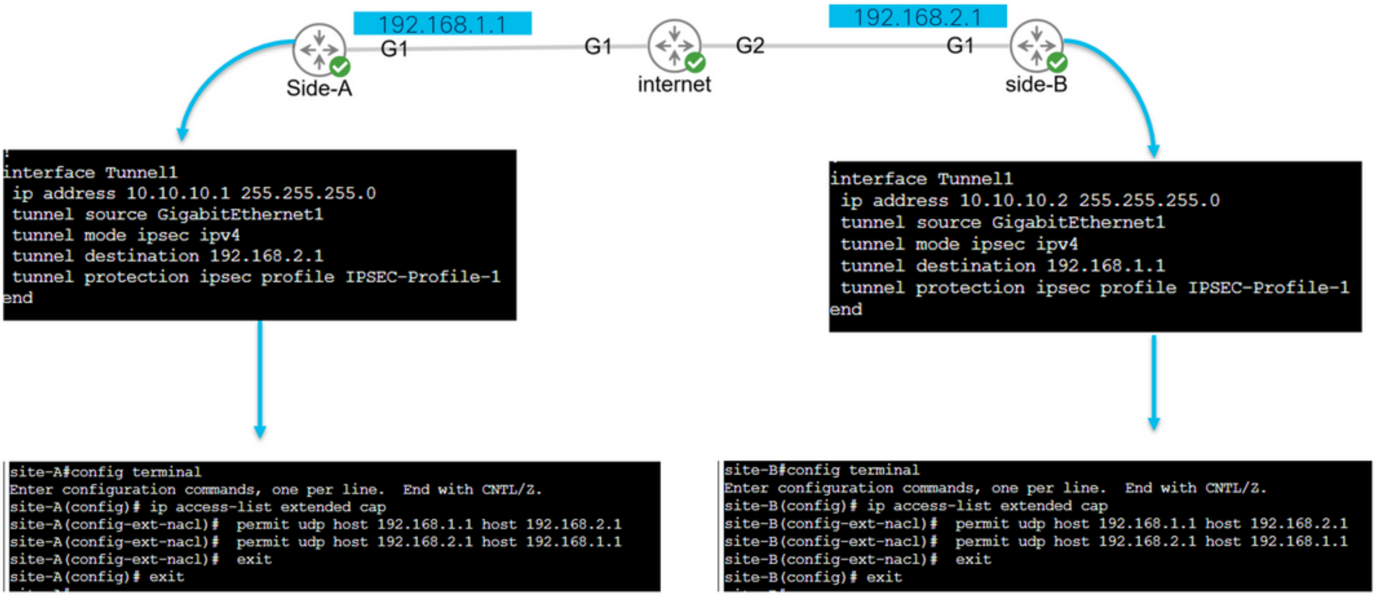
- Wireshark：這是一款眾所周知且使用的開源資料包分析器。
- 監控捕獲：路由器上的Cisco IOS XE功能，可幫助您收集捕獲，並提供流量外觀、收集的協定及其時間戳的簡單輸出。

如何在IOS XE路由器上配置捕獲



捕獲使用擴展訪問清單(ACL)，定義要收集的流量型別，以及VPN對等體或相關流量段的源地址和目的地址。如果路徑上啟用了NAT-T，則通道交涉會使用UDP連線埠500和連線埠4500。一旦協商完成且通道建立，如果啟用NAT-T，相關流量將使用IP協定50(ESP)或UDP 4500。

為了排查與控制平面相關的問題，必須使用VPN對等點IP位址來擷取通道交涉的方式。



```
!
interface Tunnel1
 ip address 10.10.10.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 192.168.2.1
 tunnel protection ipsec profile IPSEC-Profile-1
end
```

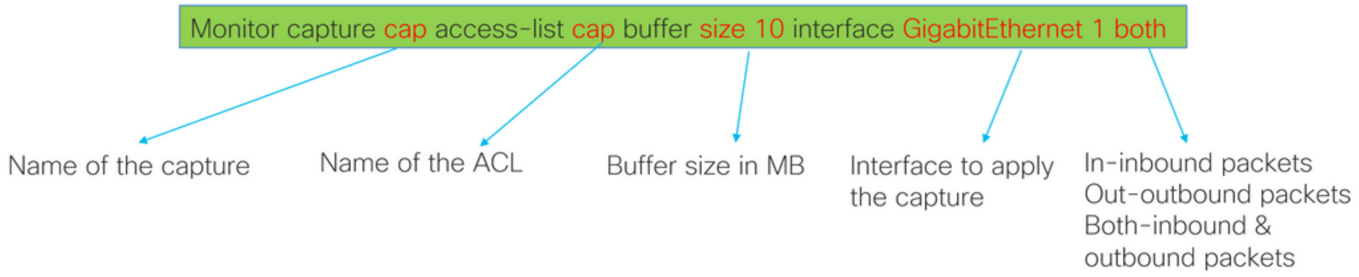
```
interface Tunnel1
 ip address 10.10.10.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 192.168.1.1
 tunnel protection ipsec profile IPSEC-Profile-1
end
```

```
site-A#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
site-A(config)# ip access-list extended cap
site-A(config-ext-nacl)#  permit udp host 192.168.1.1 host 192.168.2.1
site-A(config-ext-nacl)#  permit udp host 192.168.2.1 host 192.168.1.1
site-A(config-ext-nacl)#  exit
site-A(config)# exit
```

```
site-B#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
site-B(config)# ip access-list extended cap
site-B(config-ext-nacl)#  permit udp host 192.168.1.1 host 192.168.2.1
site-B(config-ext-nacl)#  permit udp host 192.168.2.1 host 192.168.1.1
site-B(config-ext-nacl)#  exit
site-B(config)# exit
```

```
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
```

設定的ACL是用來縮小擷取流量的範圍，且它放置於用來交涉通道的介面上。



Monitor capture cap access-list cap buffer size 10 interface GigabitEthernet 1 both

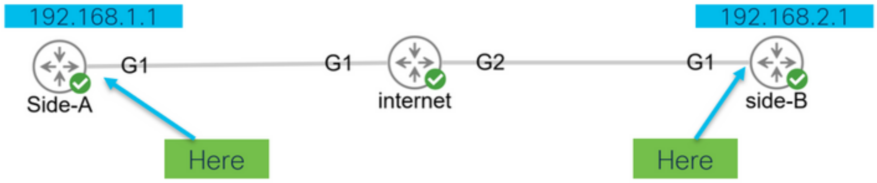
Name of the capture

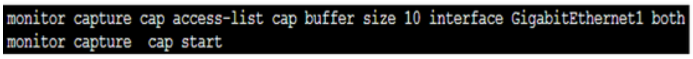
Name of the ACL

Buffer size in MB

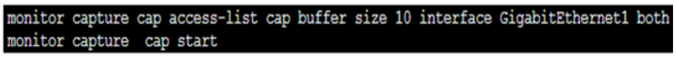
Interface to apply the capture

In-inbound packets
Out-outbound packets
Both-inbound & outbound packets

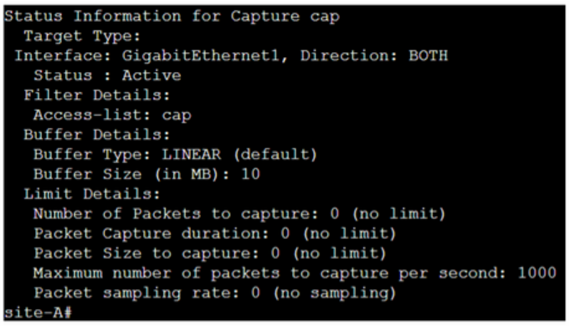




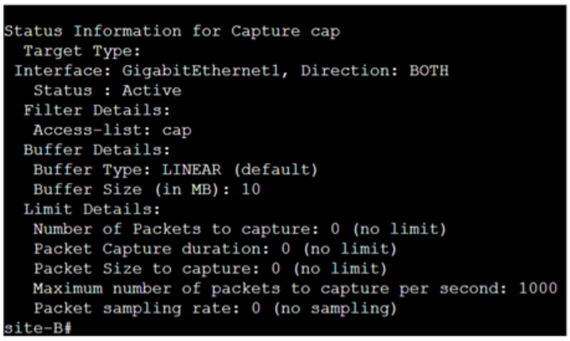
```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```



```
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
```

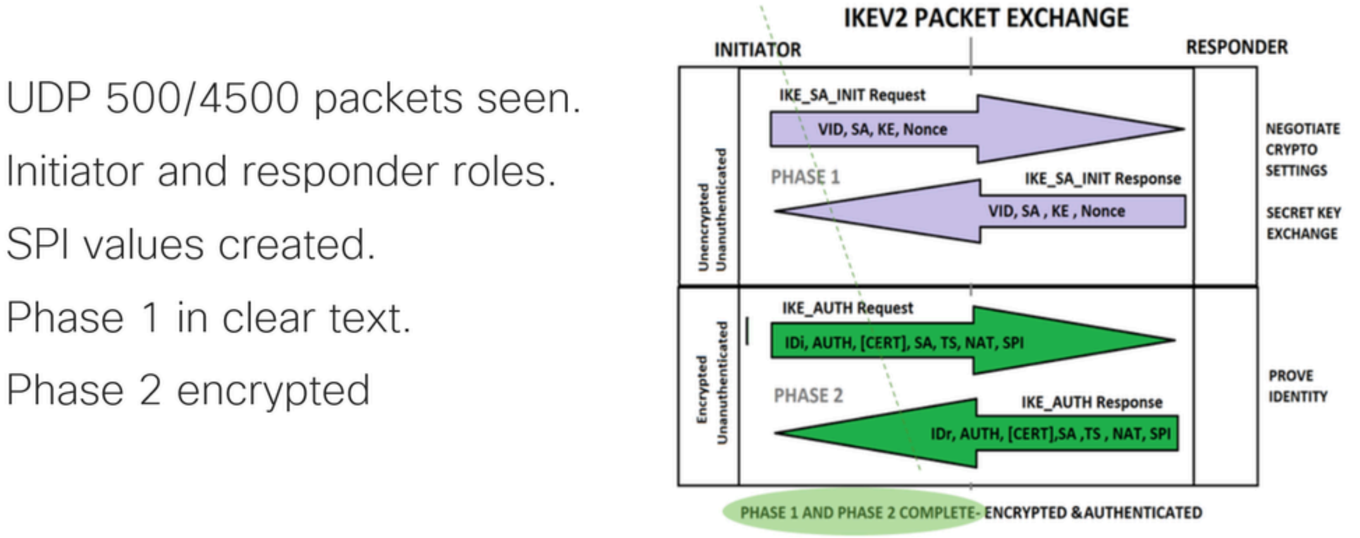
設定擷取後，可以操縱擷取停止、清除或擷取使用下列命令收集的流量：

- 檢查常規捕獲資訊：show monitor capture
- 啟動/停止捕獲：監控捕獲上限啟動/停止
- 驗證捕獲正在收集資料包: show monitor capture cap buffer

- 請參閱流量的簡短輸出：show monitor capture cap buffer brief
- 清除捕獲：監控捕獲封蓋清除
- 提取捕獲輸出：
  - 監控帽帽緩衝傾印
  - monitor capture cap export bootflash:capture.pcap

使用封包擷取分析通道建立

如前所述，要協商IPSec隧道，如果啟用NAT-T，則資料包將通過埠500和埠4500的UDP傳送。利用捕獲，可以從這些資料包中看到更多資訊，例如正在協商的階段（階段1或階段2）、每個裝置的角色（發起方或響應方），或者剛剛建立的SPI值。



UDP 500/4500 packets seen.

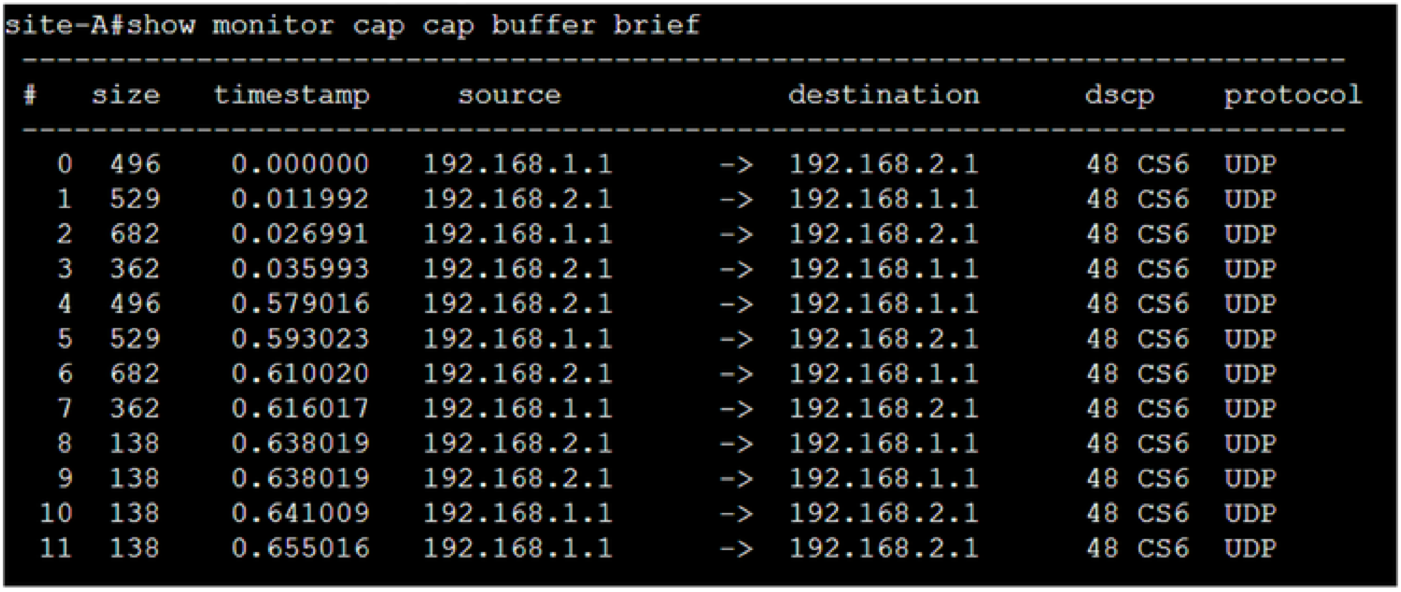
Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

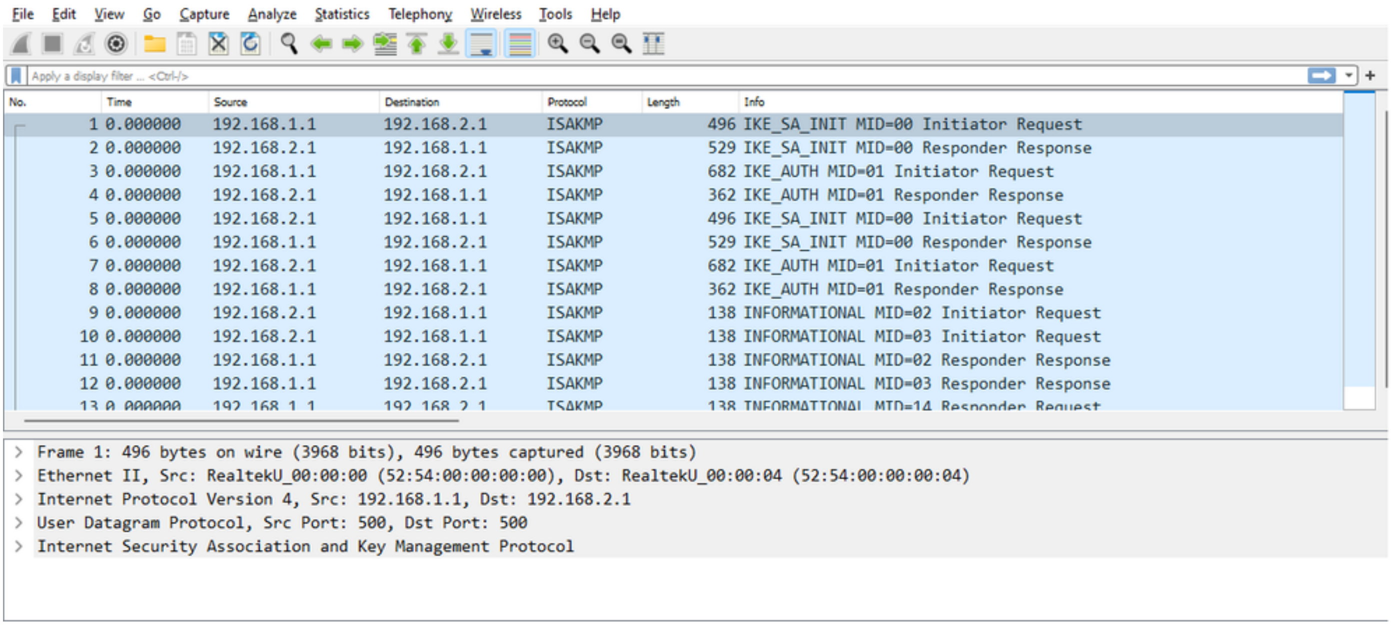
Phase 2 encrypted

顯示路由器捕獲的簡短輸出，即對等體之間的互動（傳送UDP資料包）。



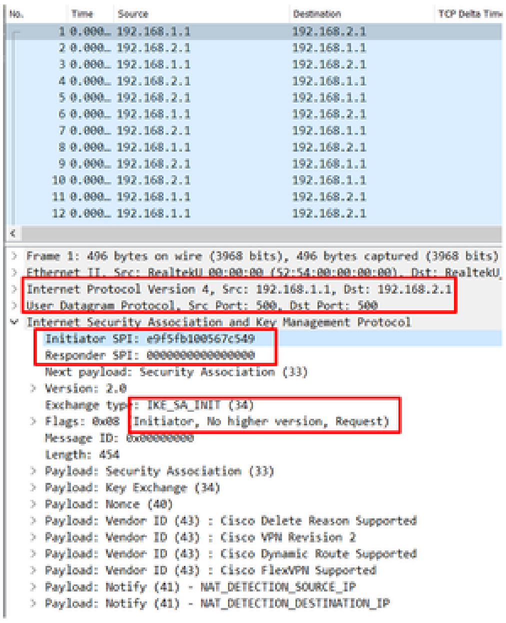
```
site-A#show monitor cap cap buffer brief
 ----------------------------------------------------------------------------
 #   size   timestamp     source             destination      dscp    protocol
 ----------------------------------------------------------------------------
   0  496    0.000000   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
```

提取轉儲並從路由器匯出pcap檔案後，可以使用wireshark檢視資料包中的詳細資訊。

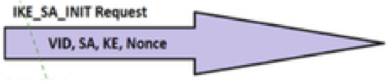


```
No.   Time      Source        Destination   Protocol  Length  Info
    1 0.000000  192.168.1.1   192.168.2.1   ISAKMP       496  IKE_SA_INIT MID=00 Initiator Request
    2 0.000000  192.168.2.1   192.168.1.1   ISAKMP       529  IKE_SA_INIT MID=00 Responder Response
    3 0.000000  192.168.1.1   192.168.2.1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

在傳送的第一個IKE_SA_INIT Exchange資料包的Internet協定部分上，找到UDP資料包的源地址和目的地址。在使用者資料包協定(User Datagram Protocol)部分中，顯示使用的埠，以及網際網路安全關聯和金鑰管理協定(Internet Security Association and Key Management Protocol)部分顯示協定的版本、正在交換的消息型別、裝置的角色以及建立的SPI。收集IKEv2調試時，調試日誌中會顯示相同的資訊。



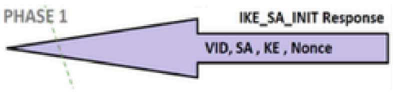
```
No.  Time      Source        Destination    TCP Delta Time
   1 0.000…  192.168.1.1   192.168.2.1
   2 0.000…  192.168.2.1   192.168.1.1
   3 0.000…  192.168.1.1   192.168.2.1
   4 0.000…  192.168.2.1   192.168.1.1
   5 0.000…  192.168.2.1   192.168.1.1
   6 0.000…  192.168.1.1   192.168.2.1
   7 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_
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v 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!

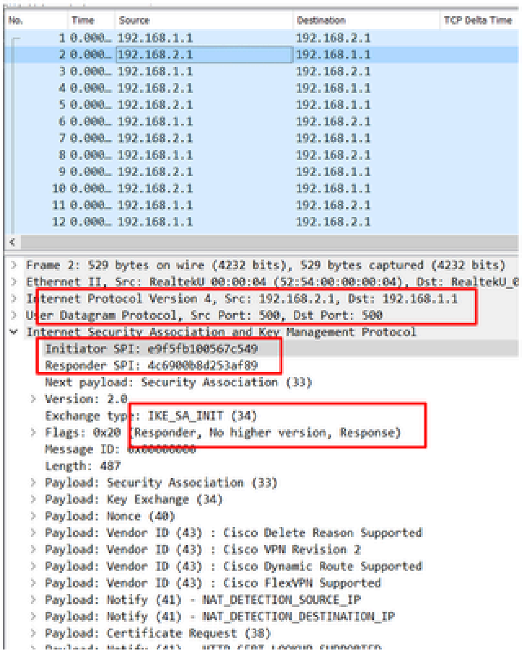
```
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To
192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 0000000000000000
Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)
```

```
Debug crypto ikev2
Debug crypto ipsec
```



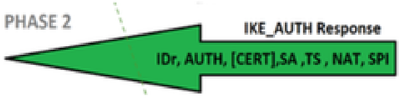
```
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From
192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
 SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ
NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)
```

Unencrypted!

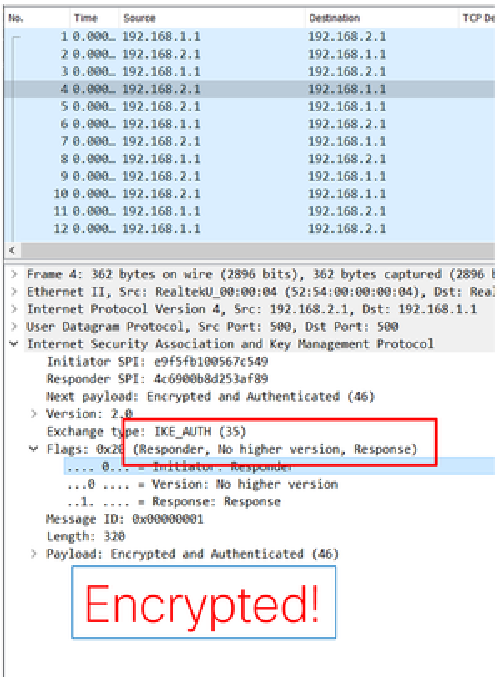


```
No.  Time      Source         Destination    TCP Delta Time
  1 0.000… 192.168.1.1    192.168.2.1
  2 0.000… 192.168.2.1    192.168.1.1
  3 0.000… 192.168.1.1    192.168.2.1
  4 0.000… 192.168.2.1    192.168.1.1
  5 0.000… 192.168.2.1    192.168.1.1
  6 0.000… 192.168.1.1    192.168.2.1
  7 0.000… 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 (52:54:00:00:00:04), 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
v 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)
  > Payload: Notify (41) - HTTP_CERT_LOOKUP_SUPPORTED
```

發生IKE_AUTH Exchange協商時，會加密負載，但可以看到一些有關協商的資訊，例如以前建立的SPI和正在進行的事務型別。



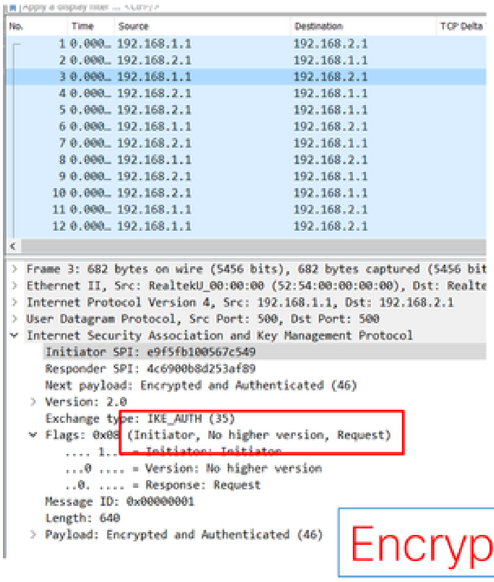
```
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From
192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
```



```
No.  Time      Source         Destination    TCP De
  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 (52:54:00:00:00:04), 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
v 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)
  v 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!

收到最後一個IKE_AUTH Exchange封包後，通道交涉完成。



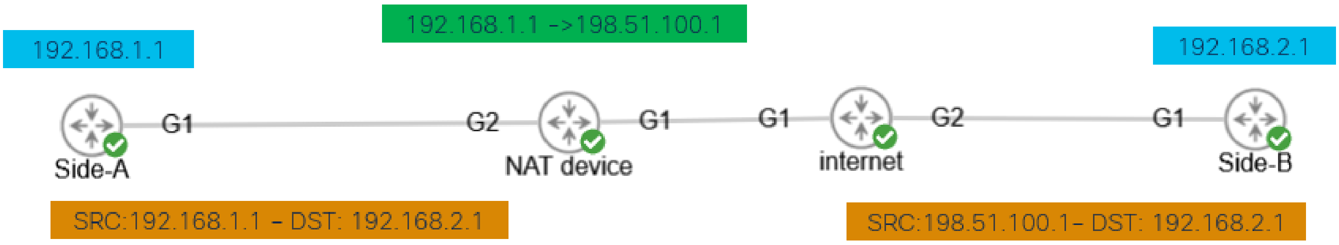
```
No.  Time      Source          Destination     TCP Delta
   1 0.000…  192.168.1.1      192.168.2.1
   2 0.000…  192.168.2.1      192.168.1.1
   3 0.000…  192.168.1.1      192.168.2.1
   4 0.000…  192.168.2.1      192.168.1.1
   5 0.000…  192.168.2.1      192.168.1.1
   6 0.000…  192.168.1.1      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
v 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)
  v Flags: 0x08 (Initiator, No higher version, Request)
      .... 1... = Initiator: Initiator
      ...0 .... = Version: No higher version
      ..0. .... = Response: Request
    Message ID: 0x00000001
    Length: 640
  > Payload: Encrypted and Authenticated (46)
```

Encrypted!

IKE_AUTH Request
IDi, AUTH, [CERT], SA, TS, NAT, SPI

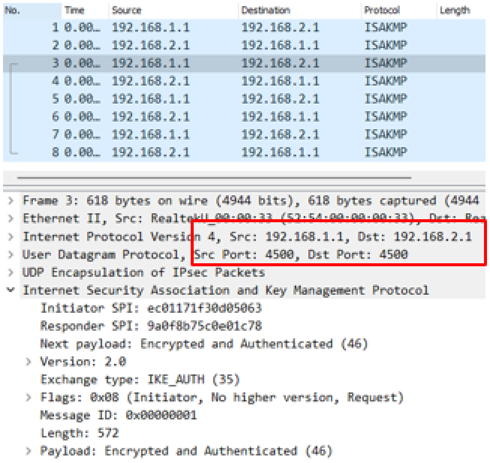
```
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To
192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
 ENCR
```

NAT介於兩者之間的事務



Nat-transversal是進行通道交涉時可以看到的另一個功能。如果中間裝置正在捨棄用於隧道的一個或兩個地址，則在協商第2階段(IKE_AUTH Exchange)時，裝置會將UDP埠從500更改為4500。

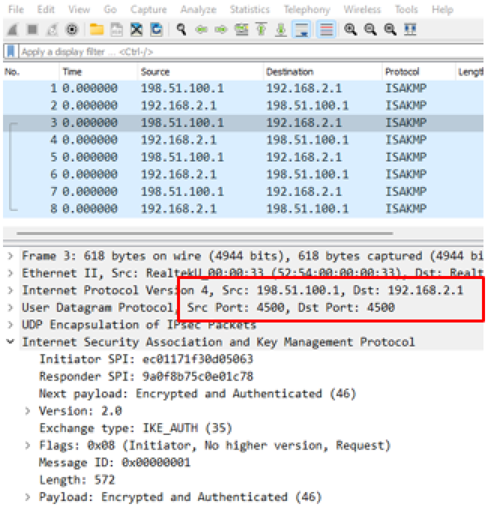
捕獲在A側：



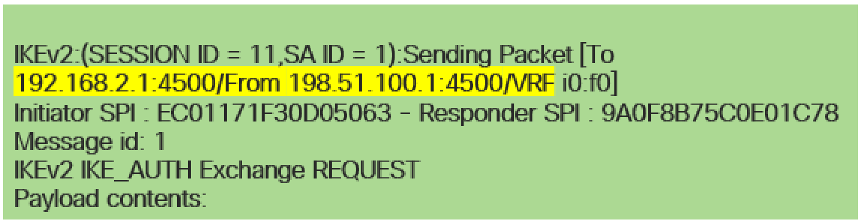
```
No.  Time     Source        Destination    Protocol  Length
   1 0.00…  192.168.1.1   192.168.2.1    ISAKMP
   2 0.00…  192.168.2.1   192.168.1.1    ISAKMP
   3 0.00…  192.168.1.1   192.168.2.1    ISAKMP
   4 0.00…  192.168.2.1   192.168.1.1    ISAKMP
   5 0.00…  192.168.1.1   192.168.2.1    ISAKMP
   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
v 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
```

在B端捕獲：



```
No.  Time      Source          Destination     Protocol  Lengt
   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 bi
> Ethernet II, Src: RealtekU_00:00:33 (52:54:00:00:00:33), Dst: Realt
> 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
v 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:
```

常見控制平面問題

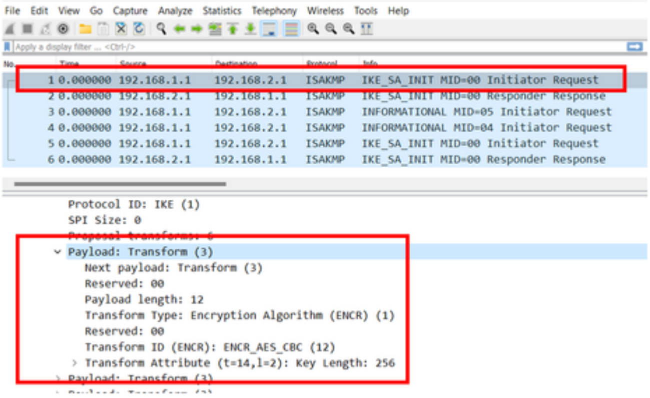
可能會有影響通道交涉的本地或外部因素，可以使用擷取進行識別。下一個場景最常見。

組態不相符

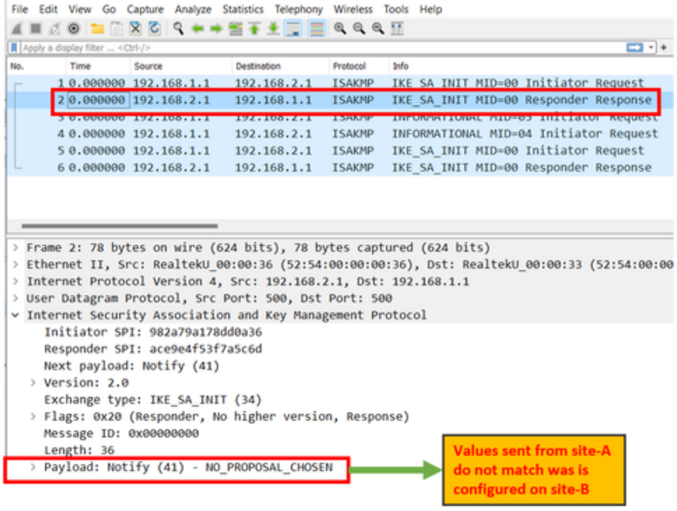
通過檢視每個裝置階段1和階段2的配置，可以解決此情況。但是，可能會出現無法訪問遠端端的情形。通過在階段1或階段2確定資料包中傳送NO_PROPOSAL_CHOSEN的裝置，捕獲幫助。該響應表示配置可能存在問題，需要調整哪個階段。

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
        Proposal transforms: 6
      v 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)
      > Payload: Transform (3)
```



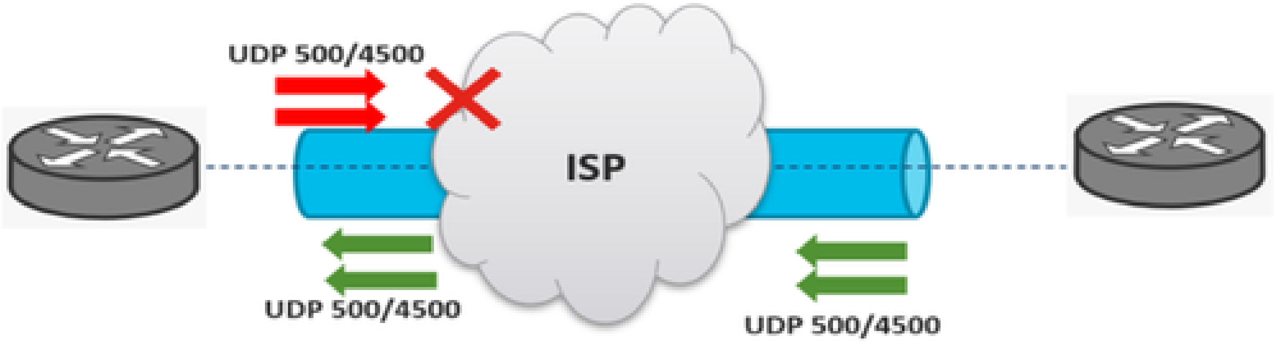
```
No.  Time      Source       Destination  Protocol  Info
   1 0.000000  192.168.1.1  192.168.2.1  ISAKMP    IKE_SA_INIT MID=00 Initiator Request
   2 0.000000  192.168.2.1  192.168.1.1  ISAKMP    IKE_SA_INIT MID=00 Responder Response
   3 0.000000  192.168.1.1  192.168.2.1  ISAKMP    INFORMATIONAL 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
v 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
```

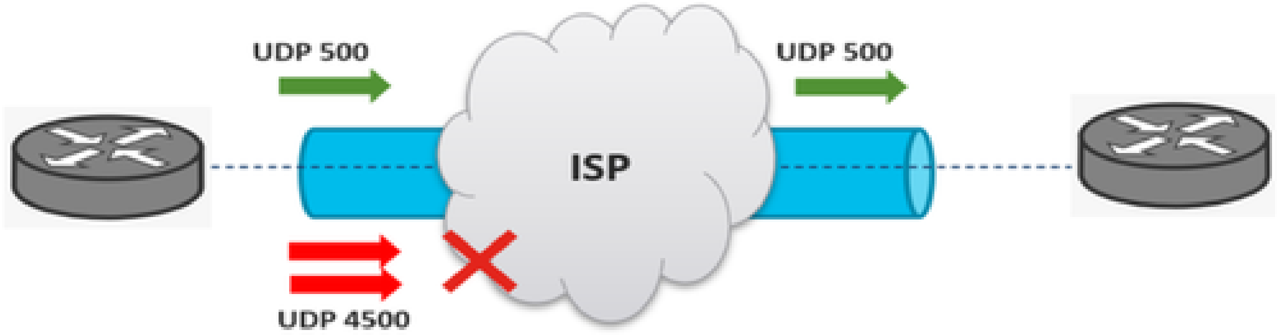
Values sent from site-A do not match was is configured on site-B

重新傳輸

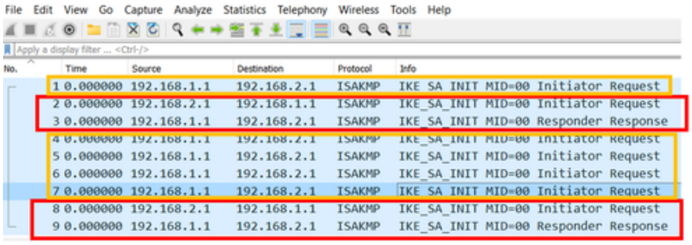
IPSec通道交涉可能會失敗，因為交涉封包是在終端裝置之間的路徑上遭捨棄的。丟棄的資料包可以是階段1或階段2資料包。在這種情況下，預期有響應封包的裝置會重新傳輸最後一個封包，如果嘗試了5次後沒有回應，通道就會結束，並從開始重新啟動。

在隧道每一端進行捕獲有助於確定哪些內容可能阻止流量以及流量受影響的方向。



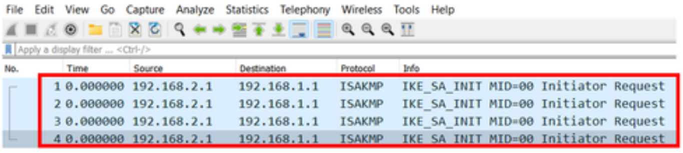


Side-A


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
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
```

Side-B


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。