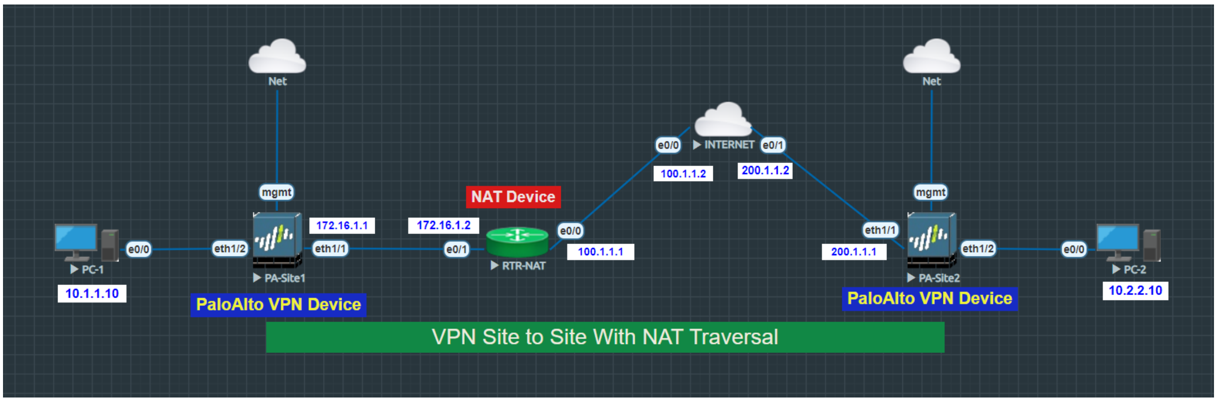
NAT Traversal on Palo Alto Firewall and NAT-D Payload Mismatch Demystified with Wireshark

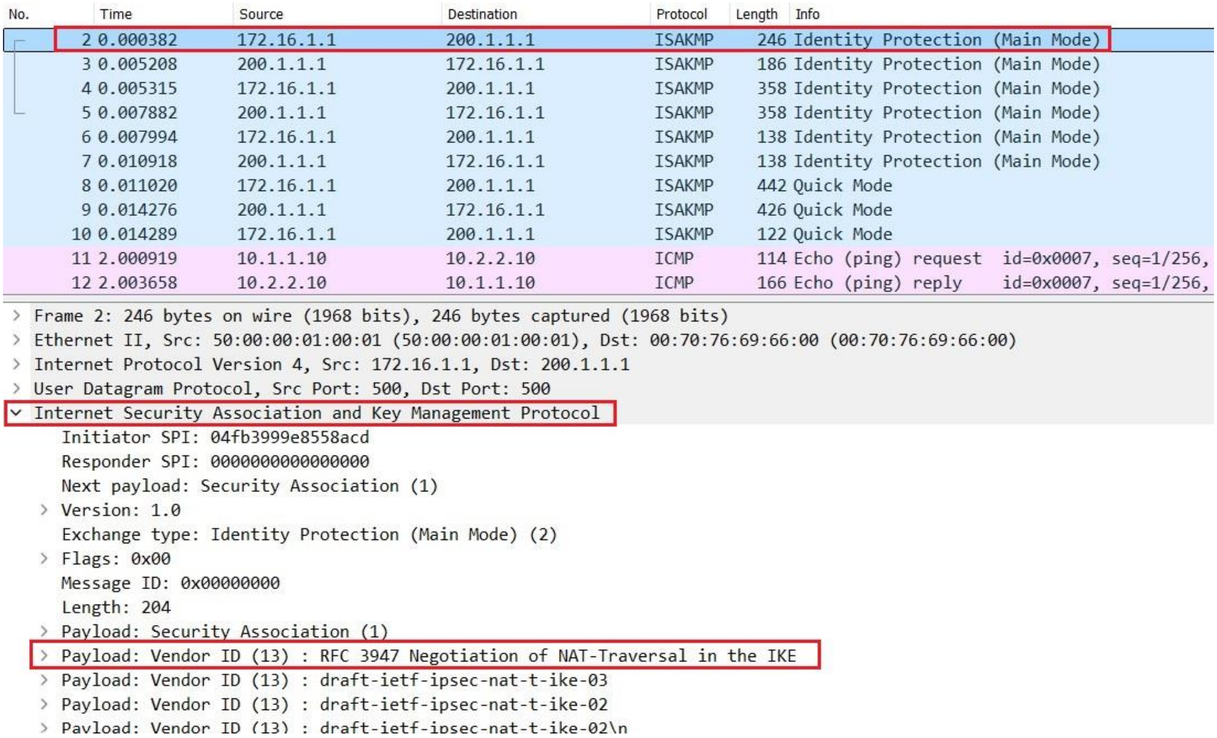


Redouane MEDDANE

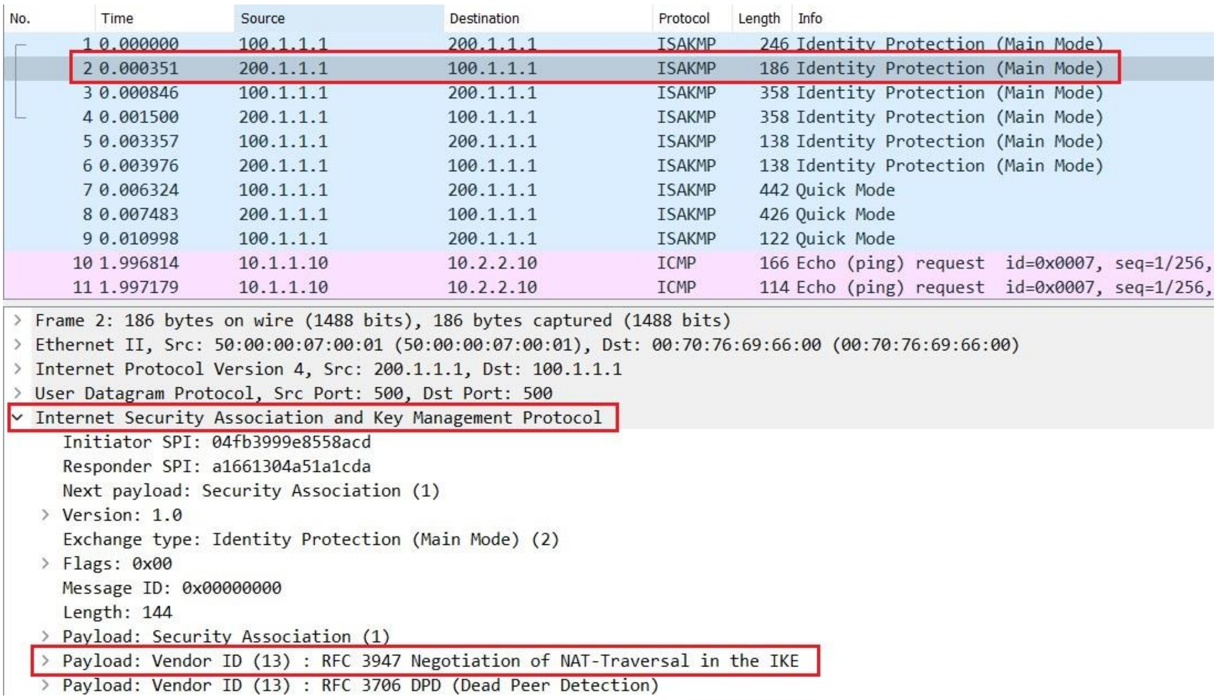
NAT Traversal performs two tasks:

Step-1: Detects if both VPN Devices PA-Site1 and PA-Site2 support NAT-T
Step-2: Detects if there is a NAT device along the path. It’s called NAT-Discovery.

Step-1 is performed in ISAKMP phase 1 (Main Mode) through the messages one and two as shown below between PA-Site1 172.16.1.1 and PA-Site-2 200.1.1.1.



```
No.   Time       Source       Destination  Protocol  Length Info
    2 0.000382   172.16.1.1   200.1.1.1    ISAKMP    246 Identity Protection (Main Mode)
    3 0.005208   200.1.1.1    172.16.1.1   ISAKMP    186 Identity Protection (Main Mode)
    4 0.005315   172.16.1.1   200.1.1.1    ISAKMP    358 Identity Protection (Main Mode)
    5 0.007882   200.1.1.1    172.16.1.1   ISAKMP    358 Identity Protection (Main Mode)
    6 0.007994   172.16.1.1   200.1.1.1    ISAKMP    138 Identity Protection (Main Mode)
    7 0.010918   200.1.1.1    172.16.1.1   ISAKMP    138 Identity Protection (Main Mode)
    8 0.011020   172.16.1.1   200.1.1.1    ISAKMP    442 Quick Mode
    9 0.014276   200.1.1.1    172.16.1.1   ISAKMP    426 Quick Mode
   10 0.014289   172.16.1.1   200.1.1.1    ISAKMP    122 Quick Mode
   11 2.000919   10.1.1.10    10.2.2.10    ICMP      114 Echo (ping) request  id=0x0007, seq=1/256,
   12 2.003658   10.2.2.10    10.1.1.10    ICMP      166 Echo (ping) reply    id=0x0007, seq=1/256,

> Frame 2: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: 0000000000000000
    Next payload: Security Association (1)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 204
  > Payload: Security Association (1)
  > Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
```



```
No.   Time       Source       Destination  Protocol  Length Info
    1 0.000000   100.1.1.1    200.1.1.1    ISAKMP    246 Identity Protection (Main Mode)
    2 0.000351   200.1.1.1    100.1.1.1    ISAKMP    186 Identity Protection (Main Mode)
    3 0.000846   100.1.1.1    200.1.1.1    ISAKMP    358 Identity Protection (Main Mode)
    4 0.001500   200.1.1.1    100.1.1.1    ISAKMP    358 Identity Protection (Main Mode)
    5 0.003357   100.1.1.1    200.1.1.1    ISAKMP    138 Identity Protection (Main Mode)
    6 0.003976   200.1.1.1    100.1.1.1    ISAKMP    138 Identity Protection (Main Mode)
    7 0.006324   100.1.1.1    200.1.1.1    ISAKMP    442 Quick Mode
    8 0.007483   200.1.1.1    100.1.1.1    ISAKMP    426 Quick Mode
    9 0.010998   100.1.1.1    200.1.1.1    ISAKMP    122 Quick Mode
   10 1.996814   10.1.1.10    10.2.2.10    ICMP      166 Echo (ping) request  id=0x0007, seq=1/256,
   11 1.997179   10.1.1.10    10.2.2.10    ICMP      114 Echo (ping) request  id=0x0007, seq=1/256,

> Frame 2: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)
> Ethernet II, Src: 50:00:00:07:00:01 (50:00:00:07:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 200.1.1.1, Dst: 100.1.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: a1661304a51a1cda
    Next payload: Security Association (1)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 144
  > Payload: Security Association (1)
  > Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
```

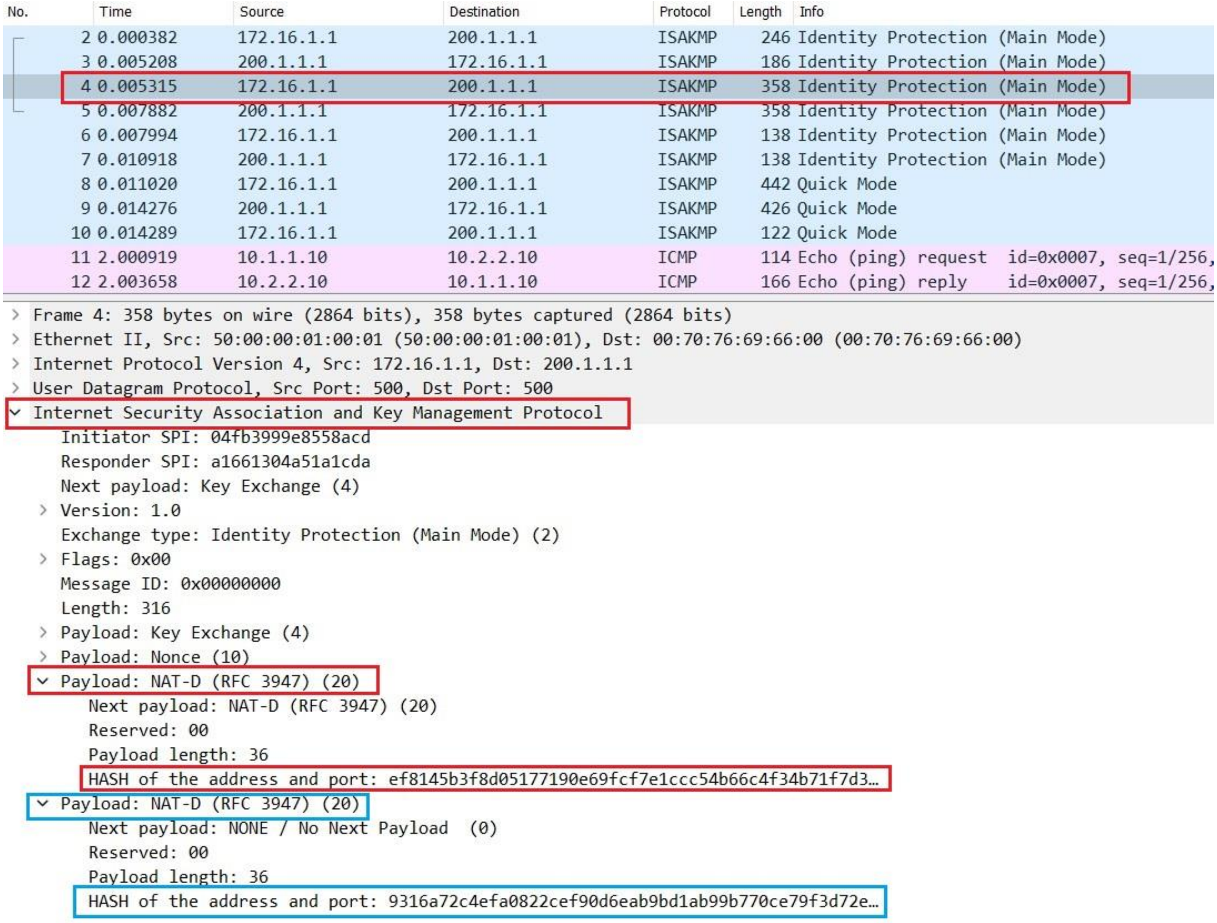
If both devices support NAT-T, then NAT-Discovery is performed in ISKAMP Phase 1 through messages three and four as shown below.

How do the VPN Devices PA-Site1 and PA-Site2 detect that there is a NAT device? The answer is NAT-D payload, the PA-Site1 device sent a NAD-ID payload, inside the NAT-ID payload there are a hash of the Source IP address and port (172.16.1.1 and 500) and a hash of the Destination IP address and port (200.1.1.1 and 500).

The PA-Site1 device (172.16.1.1) sends the following:

- A HASH of Source IP address and port (172.16.1.1 and 500): 9316a72c4efa0822cef90d6eab9bd1ab99b770ce79f3d72e

- A HASH of Destination IP address and port (200.1.1.1 and 500): ef8145b3f8d05177190e69fcf7e1ccc54b66c4f34b71f7d3

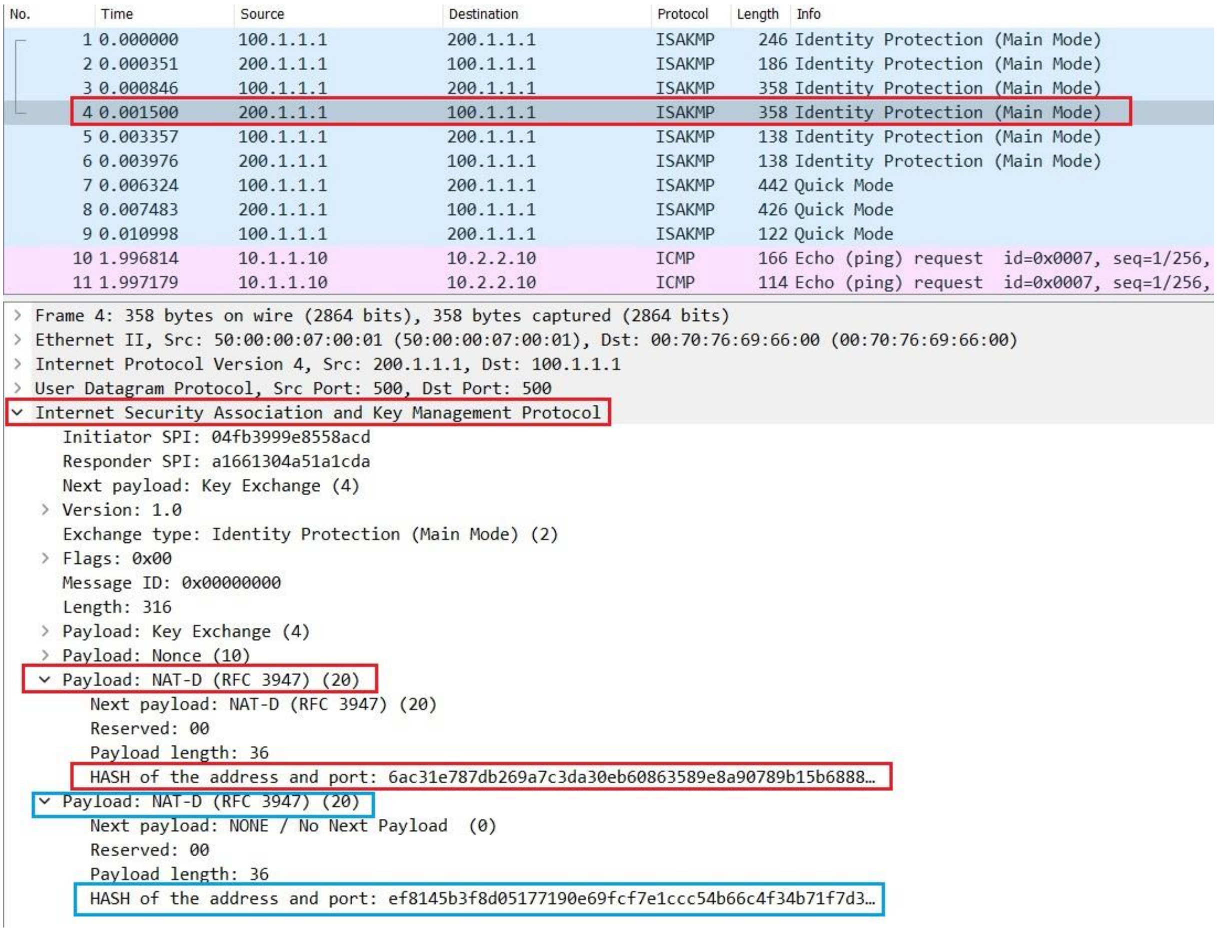


```
No.    Time        Source        Destination   Protocol   Length  Info
     2 0.000382    172.16.1.1    200.1.1.1     ISAKMP        246  Identity Protection (Main Mode)
     3 0.005208    200.1.1.1     172.16.1.1    ISAKMP        186  Identity Protection (Main Mode)
     4 0.005315    172.16.1.1    200.1.1.1     ISAKMP        358  Identity Protection (Main Mode)
     5 0.007882    200.1.1.1     172.16.1.1    ISAKMP        358  Identity Protection (Main Mode)
     6 0.007994    172.16.1.1    200.1.1.1     ISAKMP        138  Identity Protection (Main Mode)
     7 0.010918    200.1.1.1     172.16.1.1    ISAKMP        138  Identity Protection (Main Mode)
     8 0.011020    172.16.1.1    200.1.1.1     ISAKMP        442  Quick Mode
     9 0.014276    200.1.1.1     172.16.1.1    ISAKMP        426  Quick Mode
    10 0.014289    172.16.1.1    200.1.1.1     ISAKMP        122  Quick Mode
    11 2.000919    10.1.1.10     10.2.2.10     ICMP          114  Echo (ping) request  id=0x0007, seq=1/256,
    12 2.003658    10.2.2.10     10.1.1.10     ICMP          166  Echo (ping) reply    id=0x0007, seq=1/256,

> Frame 4: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits)
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: a1661304a51a1cda
    Next payload: Key Exchange (4)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 316
  > Payload: Key Exchange (4)
  > Payload: Nonce (10)
  v Payload: NAT-D (RFC 3947) (20)
      Next payload: NAT-D (RFC 3947) (20)
      Reserved: 00
      Payload length: 36
      HASH of the address and port: ef8145b3f8d05177190e69fcf7e1ccc54b66c4f34b71f7d3…
  v Payload: NAT-D (RFC 3947) (20)
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 36
      HASH of the address and port: 9316a72c4efa0822cef90d6eab9bd1ab99b770ce79f3d72e…
```

The PA-Site2 (200.1.1.1) device responds with the following:

- A HASH of Source IP address and port (200.1.1.1 and 500): ef8145b3f8d05177190e69fcf7e1ccc54b66c4f34b71f7d3

- A HASH of Destination IP address and port (100.1.1.1 and 500): 6ac31e787db269a7c3da30eb60863589e8a90789b15b6888

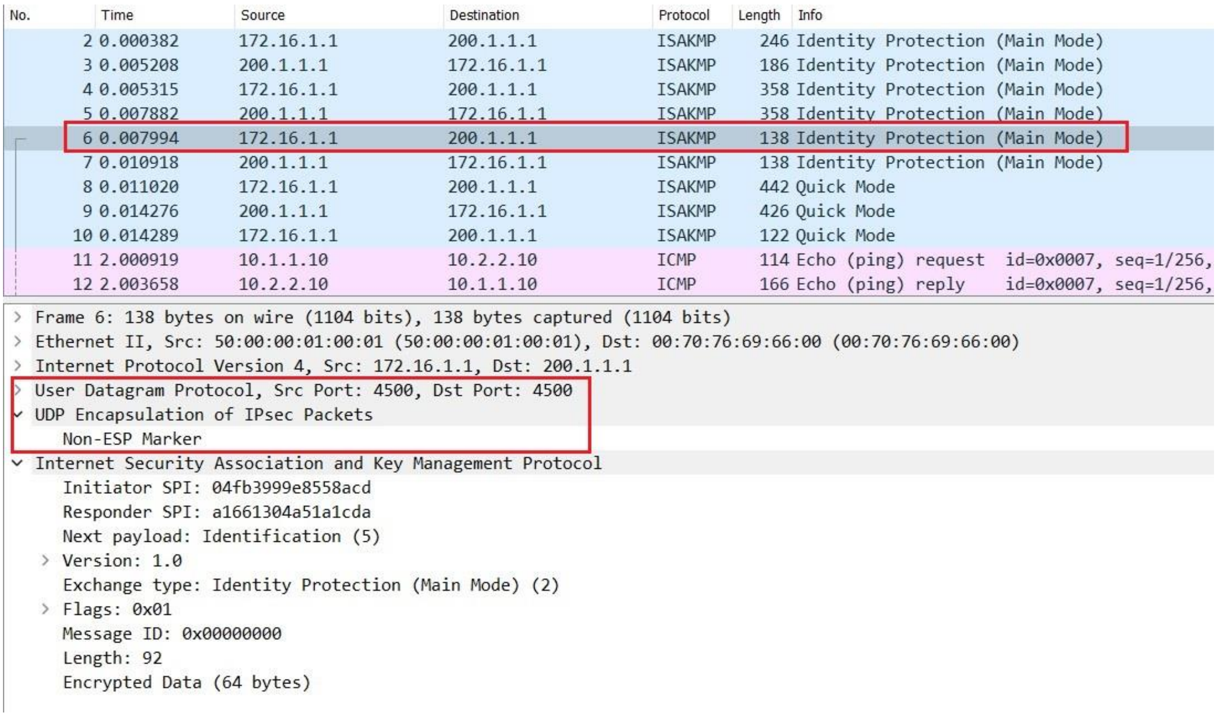


```
No.    Time        Source      Destination   Protocol   Length  Info
   1 0.000000     100.1.1.1    200.1.1.1     ISAKMP      246 Identity Protection (Main Mode)
   2 0.000351     200.1.1.1    100.1.1.1     ISAKMP      186 Identity Protection (Main Mode)
   3 0.000846     100.1.1.1    200.1.1.1     ISAKMP      358 Identity Protection (Main Mode)
   4 0.001500     200.1.1.1    100.1.1.1     ISAKMP      358 Identity Protection (Main Mode)
   5 0.003357     100.1.1.1    200.1.1.1     ISAKMP      138 Identity Protection (Main Mode)
   6 0.003976     200.1.1.1    100.1.1.1     ISAKMP      138 Identity Protection (Main Mode)
   7 0.006324     100.1.1.1    200.1.1.1     ISAKMP      442 Quick Mode
   8 0.007483     200.1.1.1    100.1.1.1     ISAKMP      426 Quick Mode
   9 0.010998     100.1.1.1    200.1.1.1     ISAKMP      122 Quick Mode
  10 1.996814     10.1.1.10    10.2.2.10     ICMP        166 Echo (ping) request  id=0x0007, seq=1/256,
  11 1.997179     10.1.1.10    10.2.2.10     ICMP        114 Echo (ping) request  id=0x0007, seq=1/256,

> Frame 4: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits)
> Ethernet II, Src: 50:00:00:07:00:01 (50:00:00:07:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 200.1.1.1, Dst: 100.1.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: a1661304a51a1cda
    Next payload: Key Exchange (4)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 316
  > Payload: Key Exchange (4)
  > Payload: Nonce (10)
  v Payload: NAT-D (RFC 3947) (20)
      Next payload: NAT-D (RFC 3947) (20)
      Reserved: 00
      Payload length: 36
      HASH of the address and port: 6ac31e787db269a7c3da30eb60863589e8a90789b15b6888…
  v Payload: NAT-D (RFC 3947) (20)
      Next payload: NONE / No Next Payload  (0)
      Reserved: 00
      Payload length: 36
      HASH of the address and port: ef8145b3f8d05177190e69fcf7e1ccc54b66c4f34b71f7d3…
```

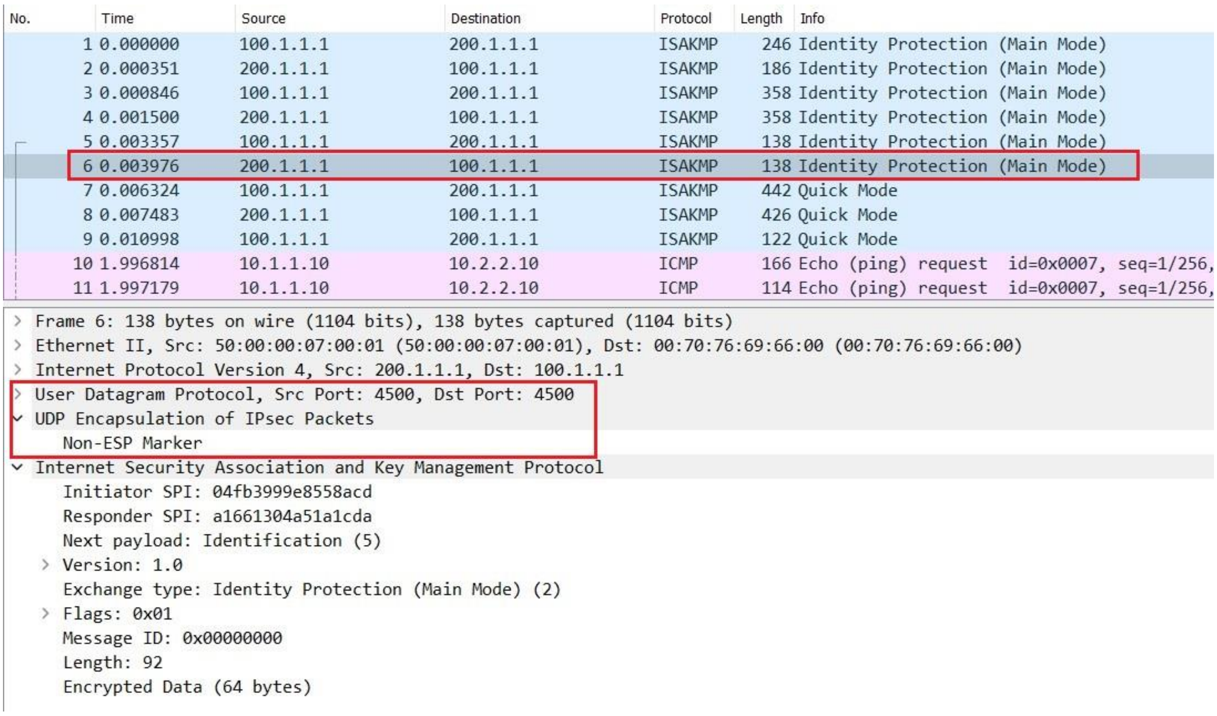
The result is that the receiving device PA-Site2 recalculates the hash based on the Destination Peer IP Address 100.1.1.1 and Port 500 which is **6ac31e787db269a7c3da30eb60863589e8a90789b15b6888** and compares it with the hash it received from PA-Site1 which is **9316a72c4efa0822cef90d6eab9bd1ab99b770ce79f3d72e**.

If they don't match a NAT device exists. This is the case in our scenario, the values are different.

Now PA-Site1 and PA-Site2 agree that a NAT Device exists along the path.
Now the NAT Device is discovered, still in the IKE 1 phase 1, PA-Site1 will change the UDP port 500 to UDP port 4500 as shown below in messages five and six.

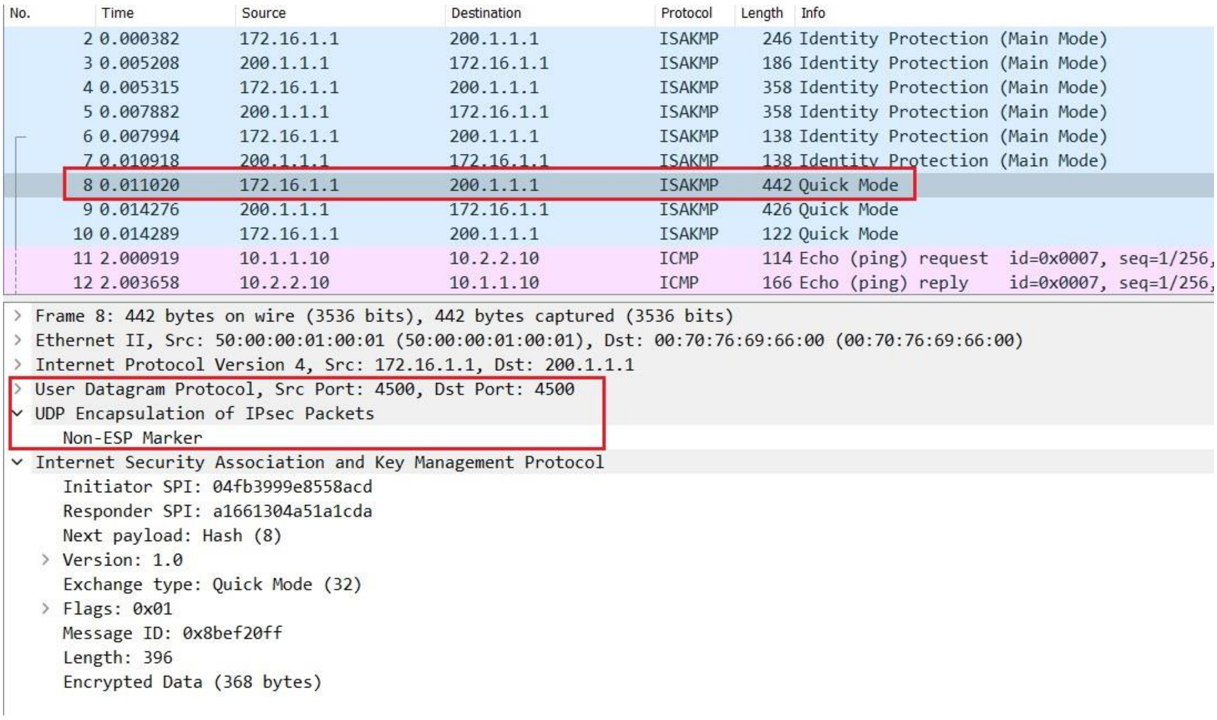


```
No.  Time       Source       Destination  Protocol  Length Info
   2 0.000382   172.16.1.1   200.1.1.1    ISAKMP    246 Identity Protection (Main Mode)
   3 0.005208   200.1.1.1    172.16.1.1   ISAKMP    186 Identity Protection (Main Mode)
   4 0.005315   172.16.1.1   200.1.1.1    ISAKMP    358 Identity Protection (Main Mode)
   5 0.007882   200.1.1.1    172.16.1.1   ISAKMP    358 Identity Protection (Main Mode)
   6 0.007994   172.16.1.1   200.1.1.1    ISAKMP    138 Identity Protection (Main Mode)
   7 0.010918   200.1.1.1    172.16.1.1   ISAKMP    138 Identity Protection (Main Mode)
   8 0.011020   172.16.1.1   200.1.1.1    ISAKMP    442 Quick Mode
   9 0.014276   200.1.1.1    172.16.1.1   ISAKMP    426 Quick Mode
  10 0.014289   172.16.1.1   200.1.1.1    ISAKMP    122 Quick Mode
  11 2.000919   10.1.1.10    10.2.2.10    ICMP      114 Echo (ping) request  id=0x0007, seq=1/256,
  12 2.003658   10.2.2.10    10.1.1.10    ICMP      166 Echo (ping) reply    id=0x0007, seq=1/256,

> Frame 6: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
v UDP Encapsulation of IPsec Packets
    Non-ESP Marker
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: a1661304a51a1cda
    Next payload: Identification (5)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x01
    Message ID: 0x00000000
    Length: 92
    Encrypted Data (64 bytes)
```



```
No.  Time       Source       Destination  Protocol  Length Info
   1 0.000000   100.1.1.1    200.1.1.1    ISAKMP    246 Identity Protection (Main Mode)
   2 0.000351   200.1.1.1    100.1.1.1    ISAKMP    186 Identity Protection (Main Mode)
   3 0.000846   100.1.1.1    200.1.1.1    ISAKMP    358 Identity Protection (Main Mode)
   4 0.001500   200.1.1.1    100.1.1.1    ISAKMP    358 Identity Protection (Main Mode)
   5 0.003357   100.1.1.1    200.1.1.1    ISAKMP    138 Identity Protection (Main Mode)
   6 0.003976   200.1.1.1    100.1.1.1    ISAKMP    138 Identity Protection (Main Mode)
   7 0.006324   100.1.1.1    200.1.1.1    ISAKMP    442 Quick Mode
   8 0.007483   200.1.1.1    100.1.1.1    ISAKMP    426 Quick Mode
   9 0.010998   100.1.1.1    200.1.1.1    ISAKMP    122 Quick Mode
  10 1.996814   10.1.1.10    10.2.2.10    ICMP      166 Echo (ping) request  id=0x0007, seq=1/256,
  11 1.997179   10.1.1.10    10.2.2.10    ICMP      114 Echo (ping) request  id=0x0007, seq=1/256,

> Frame 6: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
> Ethernet II, Src: 50:00:00:07:00:01 (50:00:00:07:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 200.1.1.1, Dst: 100.1.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
v UDP Encapsulation of IPsec Packets
    Non-ESP Marker
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: a1661304a51a1cda
    Next payload: Identification (5)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x01
    Message ID: 0x00000000
    Length: 92
    Encrypted Data (64 bytes)
```

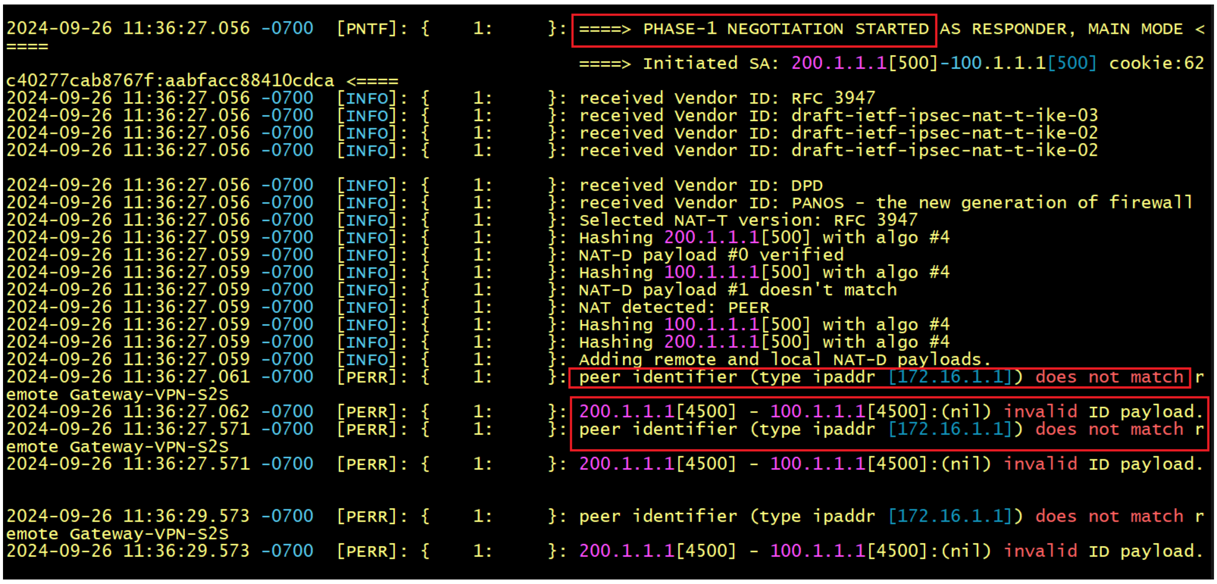
Because the NAT-T, in IKE Phase 2 (IPsec Quick Mode) encapsulates the Quick Mode (IPsec Phase 2) inside UDP 4500. After Quick Mode negociation is completed, Phase 2 is now ready to encrypt the data and ESP Packets are encapsulated inside UDP port 4500 as well, thus providing a port to be used in the NAT device to perform port address translation.



```
No.      Time       Source        Destination   Protocol  Length Info
       2 0.000382   172.16.1.1    200.1.1.1     ISAKMP     246 Identity Protection (Main Mode)
       3 0.005208   200.1.1.1     172.16.1.1    ISAKMP     186 Identity Protection (Main Mode)
       4 0.005315   172.16.1.1    200.1.1.1     ISAKMP     358 Identity Protection (Main Mode)
       5 0.007882   200.1.1.1     172.16.1.1    ISAKMP     358 Identity Protection (Main Mode)
       6 0.007994   172.16.1.1    200.1.1.1     ISAKMP     138 Identity Protection (Main Mode)
       7 0.010918   200.1.1.1     172.16.1.1    ISAKMP     138 Identity Protection (Main Mode)
       8 0.011020   172.16.1.1    200.1.1.1     ISAKMP     442 Quick Mode
       9 0.014276   200.1.1.1     172.16.1.1    ISAKMP     426 Quick Mode
      10 0.014289   172.16.1.1    200.1.1.1     ISAKMP     122 Quick Mode
      11 2.000919   10.1.1.10     10.2.2.10     ICMP       114 Echo (ping) request  id=0x0007, seq=1/256,
      12 2.003658   10.2.2.10     10.1.1.10     ICMP       166 Echo (ping) reply    id=0x0007, seq=1/256,

> Frame 8: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits)
> Ethernet II, Src: 50:00:00:01:00:01 (50:00:00:01:00:01), Dst: 00:70:76:69:66:00 (00:70:76:69:66:00)
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
v UDP Encapsulation of IPsec Packets
    Non-ESP Marker
v Internet Security Association and Key Management Protocol
    Initiator SPI: 04fb3999e8558acd
    Responder SPI: a1661304a51a1cda
    Next payload: Hash (8)
  > Version: 1.0
    Exchange type: Quick Mode (32)
  > Flags: 0x01
    Message ID: 0x8bef20ff
    Length: 396
    Encrypted Data (368 bytes)
```

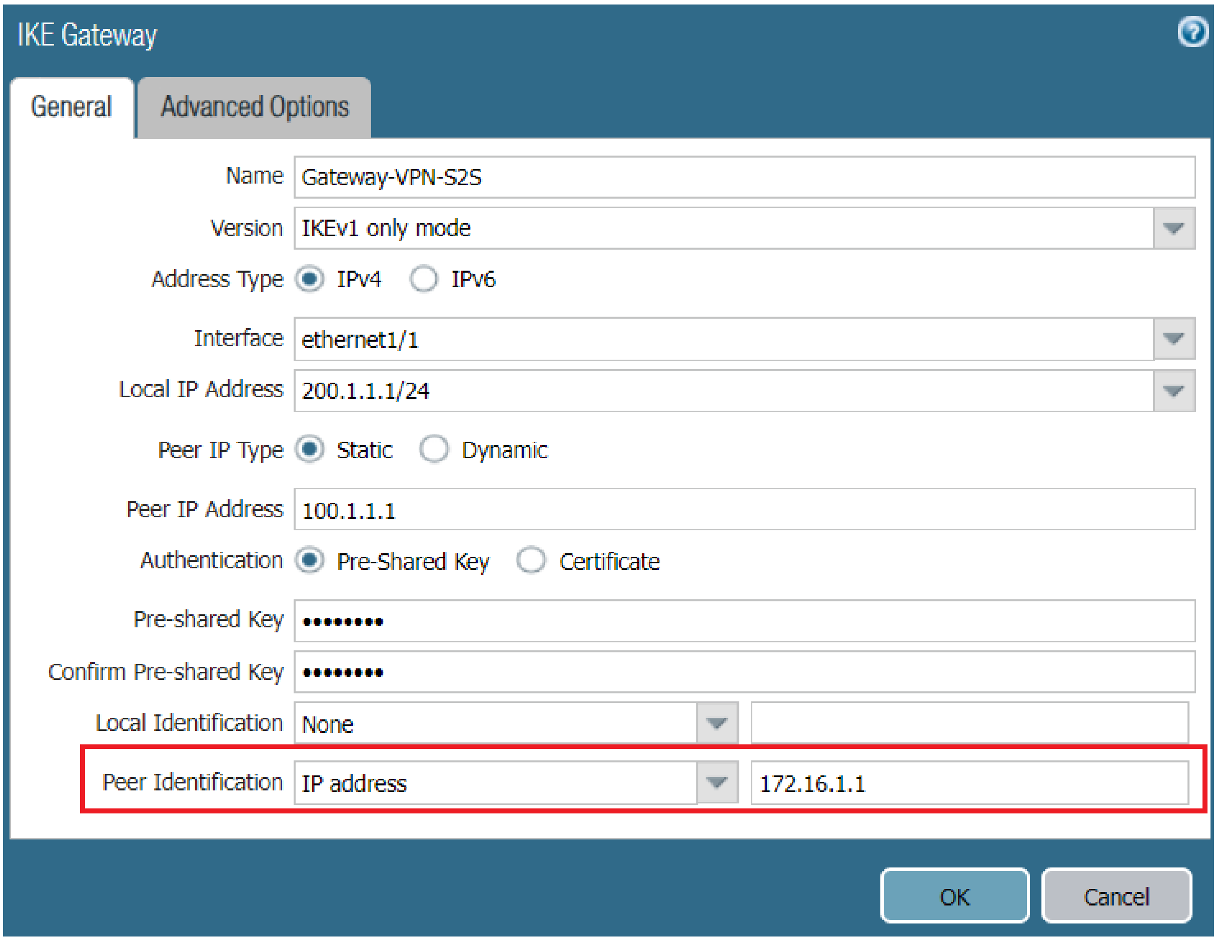
UDP encapsulation is used to hide the ESP packet behind the UDP header. So that the NAT Device processes the ESP packet as a normal UDP packet.
In other words, PA-Site1 encapsulates ESP packets inside UDP/4500 for Source and Destination Ports. After this encapsulation, NAT device can now translate the ESP packets. It will change the source port from 4500 to a random port and the source IP address from 172.16.1.1 to 100.1.1.1 and kept the destination port 4500
When a packet with source and destination port of 4500 is sent through a PAT device (from inside to outside), the PAT device will change the source port from 4500 to a random high port, while keeping the destination port of 4500.

The Palo Alto firewall does not accept the IKE Phase 1 negociation when the the NAT-D payload or the hash of the original IP address and port don't match as shown by the tail follow yes mp-log ikemgr.log command output, and finally the IPsec tunnel will not be established.



```
2024-09-26 11:36:27.056 -0700  [PNTF]: {     1:      }: ====> PHASE-1 NEGOTIATION STARTED AS RESPONDER, MAIN MODE <
====
                                                        ====> Initiated SA: 200.1.1.1[500]-100.1.1.1[500] cookie:62
c40277cab8767f:aabfacc88410cdca <====
2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: received Vendor ID: RFC 3947
2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: received Vendor ID: draft-ietf-ipsec-nat-t-ike-03
2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: received Vendor ID: draft-ietf-ipsec-nat-t-ike-02
2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: received Vendor ID: draft-ietf-ipsec-nat-t-ike-02

2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: received Vendor ID: DPD
2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: received Vendor ID: PANOS - the new generation of firewall
2024-09-26 11:36:27.056 -0700  [INFO]: {     1:      }: Selected NAT-T version: RFC 3947
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: Hashing 200.1.1.1[500] with algo #4
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: NAT-D payload #0 verified
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: Hashing 100.1.1.1[500] with algo #4
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: NAT-D payload #1 doesn't match
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: NAT detected: PEER
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: Hashing 100.1.1.1[500] with algo #4
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: Hashing 200.1.1.1[500] with algo #4
2024-09-26 11:36:27.059 -0700  [INFO]: {     1:      }: Adding remote and local NAT-D payloads.
2024-09-26 11:36:27.061 -0700  [PERR]: {     1:      }: peer identifier (type ipaddr [172.16.1.1]) does not match r
emote Gateway-VPN-S2S
2024-09-26 11:36:27.062 -0700  [PERR]: {     1:      }: 200.1.1.1[4500] - 100.1.1.1[4500]:(nil) invalid ID payload.
2024-09-26 11:36:27.571 -0700  [PERR]: {     1:      }: peer identifier (type ipaddr [172.16.1.1]) does not match r
emote Gateway-VPN-S2S
2024-09-26 11:36:27.571 -0700  [PERR]: {     1:      }: 200.1.1.1[4500] - 100.1.1.1[4500]:(nil) invalid ID payload.


2024-09-26 11:36:29.573 -0700  [PERR]: {     1:      }: peer identifier (type ipaddr [172.16.1.1]) does not match r
emote Gateway-VPN-S2S
2024-09-26 11:36:29.573 -0700  [PERR]: {     1:      }: 200.1.1.1[4500] - 100.1.1.1[4500]:(nil) invalid ID payload.
```

To solve this issue, on PA-Site2, configure Peer Identification with the private IP address of PA-Site1.



Name: Gateway-VPN-S2S

Version: IKEv1 only mode

Address Type: ● IPv4 ○ IPv6

Interface: ethernet1/1

Local IP Address: 200.1.1.1/24

Peer IP Type: ● Static ○ Dynamic

Peer IP Address: 100.1.1.1

Authentication: ● Pre-Shared Key ○ Certificate

Pre-shared Key: ••••••••

Confirm Pre-shared Key: ••••••••

Local Identification: None

Peer Identification: IP address 172.16.1.1