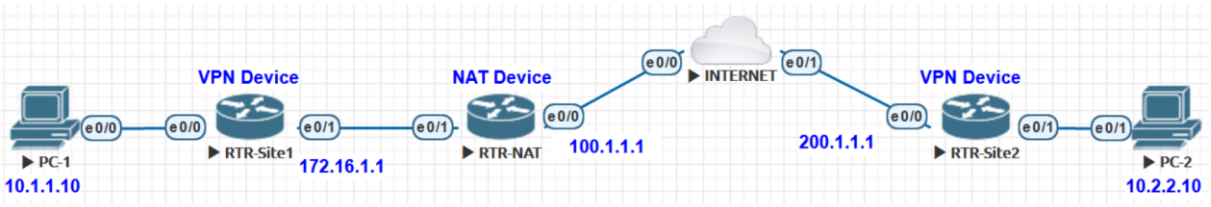
NAT Traversal NAT-T in IPSEC VPN explained with wireshark

By Redouane MEDDANE




```
RTR-Site1#sh run | s crypto
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco address 200.1.1.1
crypto ipsec transform-set TR-IPSEC esp-aes esp-sha256-hmac
 mode tunnel
crypto map CMAP 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set TR-IPSEC
 match address 100
 crypto map CMAP
RTR-Site1#
```

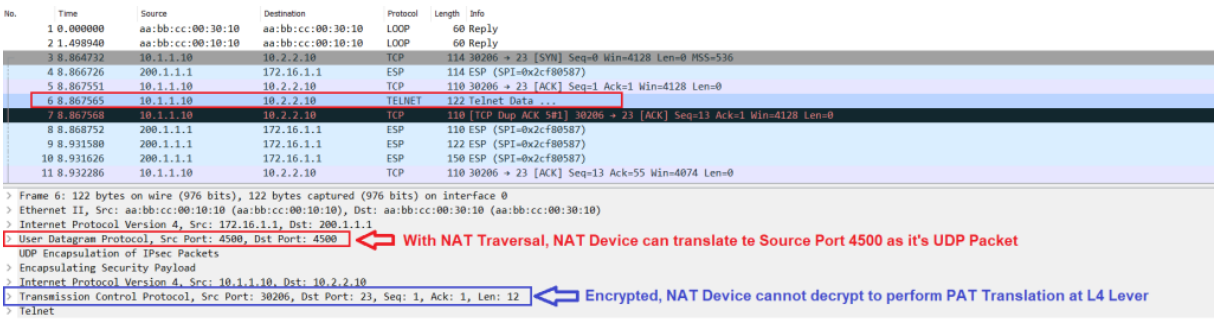
```
RTR-Site2#sh run | s crypto
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco address 100.1.1.1
crypto ipsec transform-set TR-IPSEC esp-aes esp-sha256-hmac
 mode tunnel
crypto map CMAP 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set TR-IPSEC
 match address 100
 crypto map CMAP
RTR-Site2#
```

One of the biggest concept in VPN Technologies is NAT Traversal, like NAT Traversal in VOIP deployment with SIP Protocol, the history is always inside the payload to solve the Incompatibility between NAT and IPSEC like the Incompatibility between SIP protocol and NAT.

IPsec uses ESP to encrypt all packet, encapsulating the L3/L4 headers within an ESP header. ESP is an IP pro
tocol but there is no port number (Layer 4). This is a difference from ISAKMP which uses UDP port 500 as its UDP layer 4.

Because ESP is a protocol without ports and at the other side the L4 information the , The NAT device cannot change these encrypted headers and cannot perform PAT translation at the L4 level.

Below the telnet packet captured from PC-1 to PC-2, the Source port 30206 and the Destination Port 23 are encapsulated by ESP and both are encrypted. (I decrypted the packet to see how it looks inside ESP after decryption at the RTR-Site2.



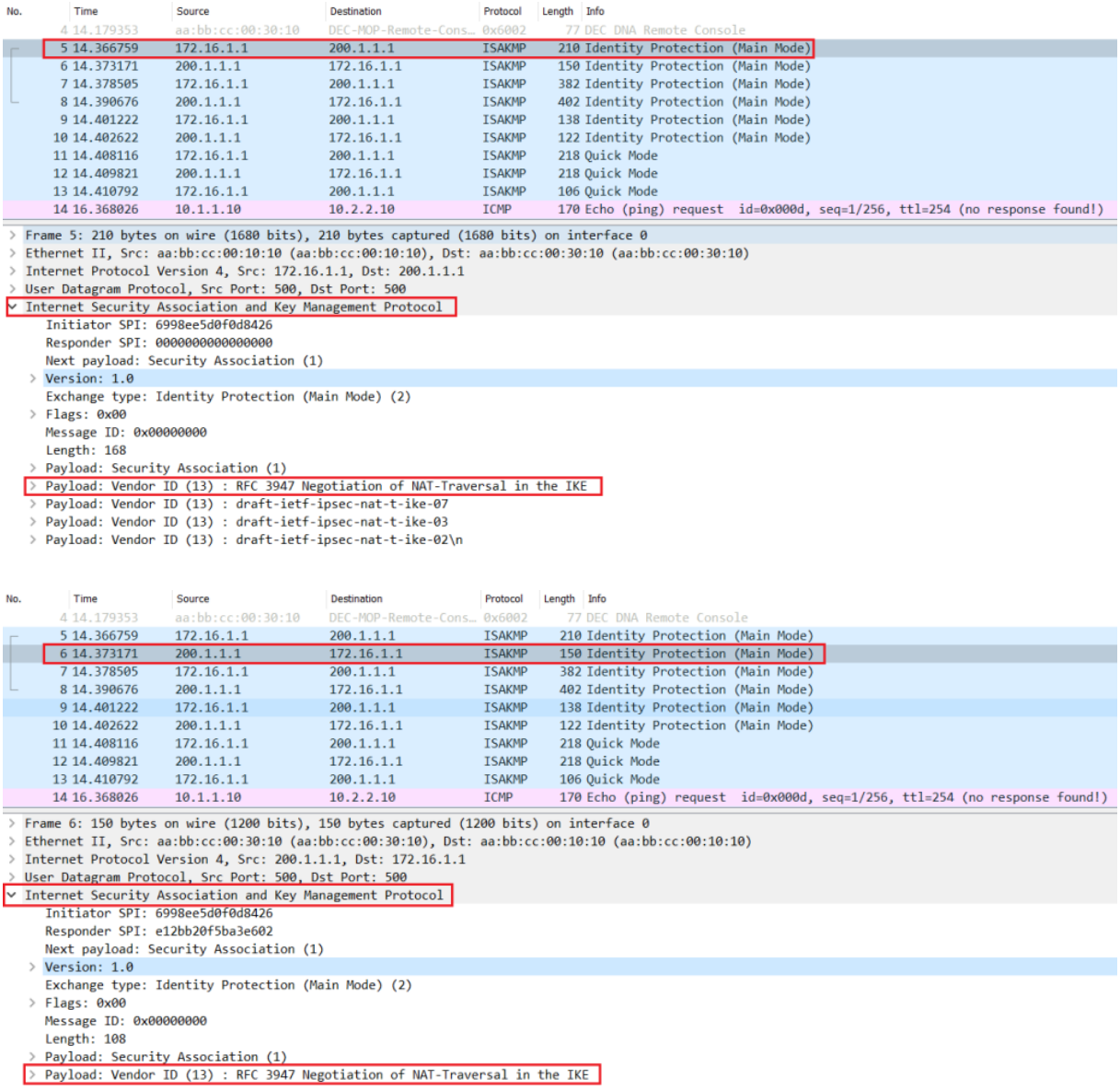
Without NAT Traversal and new UDP Encapsulation of ESP packets with source port 4500 and destination 4500, the NAT Device cannot do anything.

It is clear NAT and IPSec are incompatible with each other, and to resolve this NAT Traversal was developed. NAT Traversal adds a UDP header which encapsulates the IPSec ESP header. As this new UDP header is NOT encrypted and is treated as just like a normal UDP packet, the NAT device can make the required changes and process the message,

NAT Traversal performs two tasks:

Step-1: Detects if both VPN Devices RTR-Site1 and RTR-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 RTR-Site1 172.16.1.1 and RTR-Site-2 200.1.1.1.

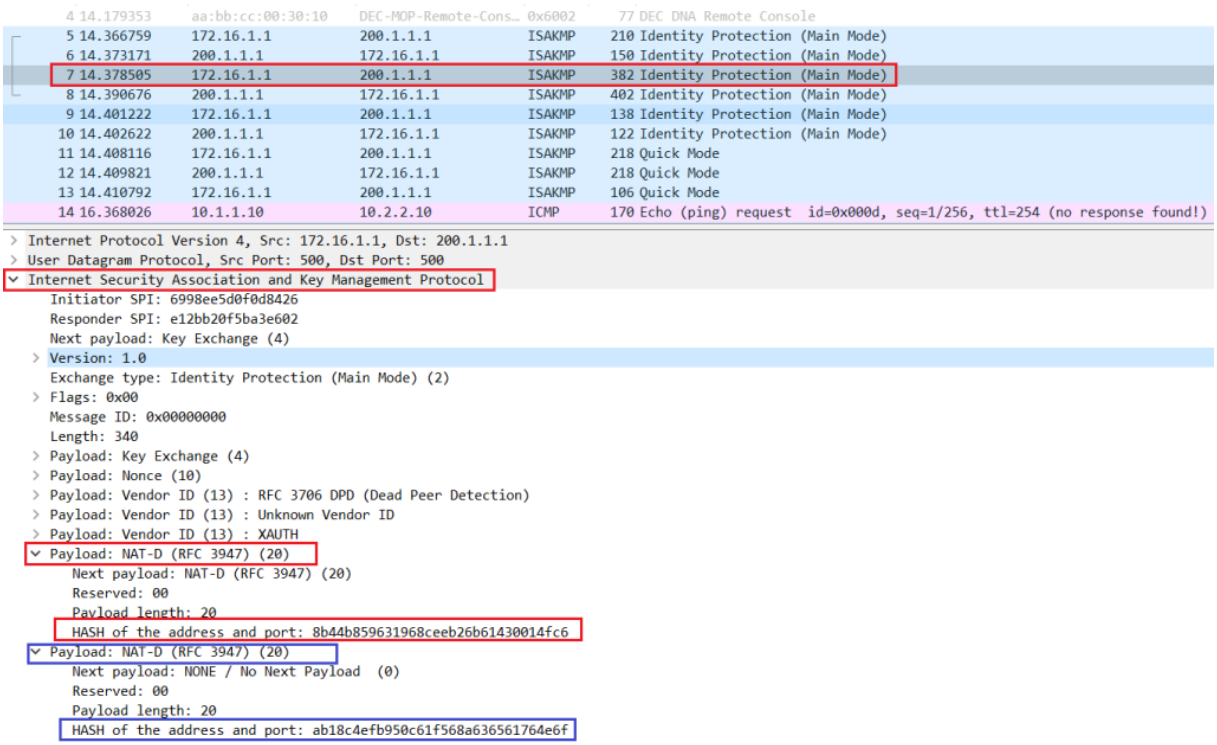


If both devices support NAT-T, then NAT-Discovery is performed in ISKAMP Phase 1 through messages three and four as shown below.

How do the VPN Devices RTR-Site1 and RTR-Site2 detect that there is a NAT device?
The answer is NAT-D payload, the RTR-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).

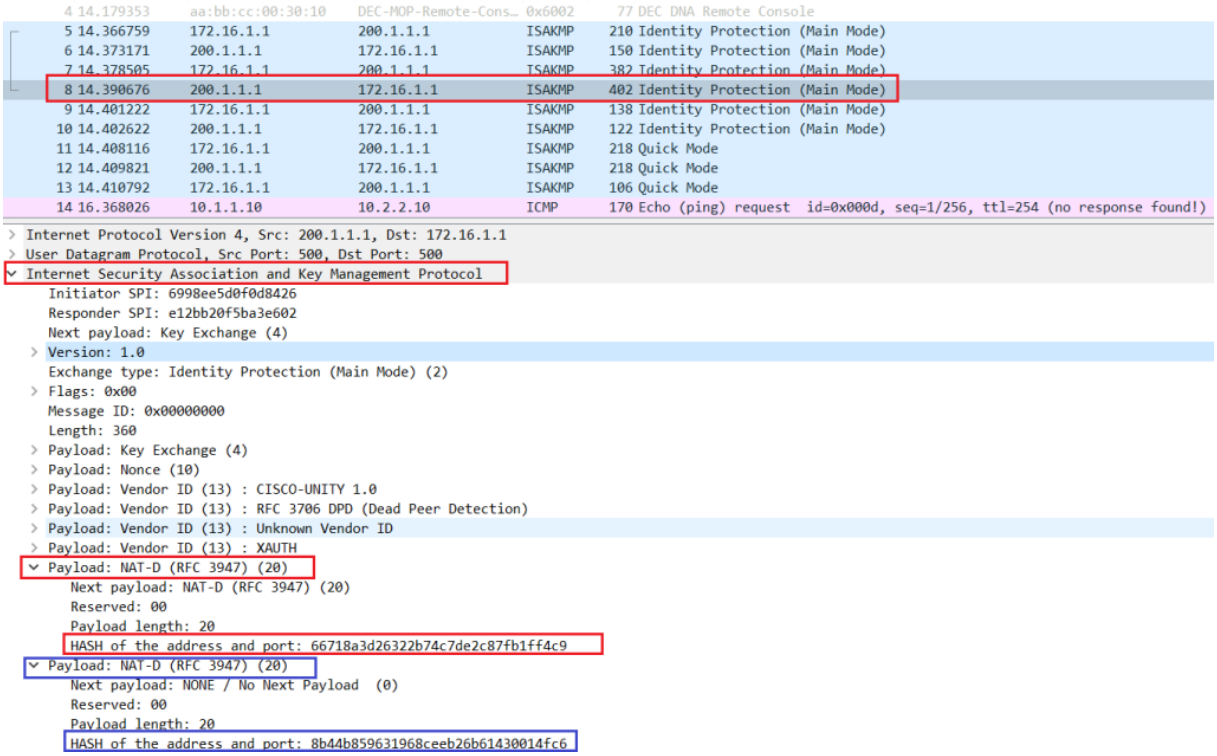
The RTR-Site1 device (172.16.1.1) sends the following:

- A HASH of Source IP address and port (172.16.1.1 and 500): ab18C4efb950c61f568a636561764e6f
- A HASH of Destination IP address and port (200.1.1.1 and 500): 8b44b859631968ceeb26b61430014fc6



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

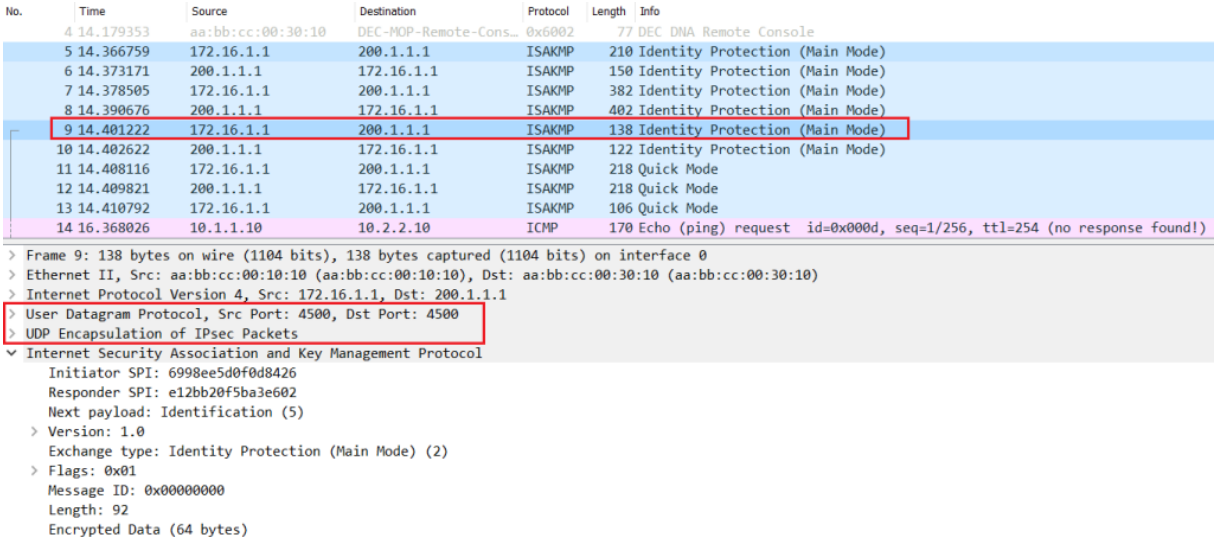
- A HASH of Source IP address and port (200.1.1.1 and 500): 8b44b859631968ceeb26b61430014fc6
- A HASH of Destination IP address and port (100.1.1.1 and 500): 66718a3d26322b74c7de2c87fb1ff4c9

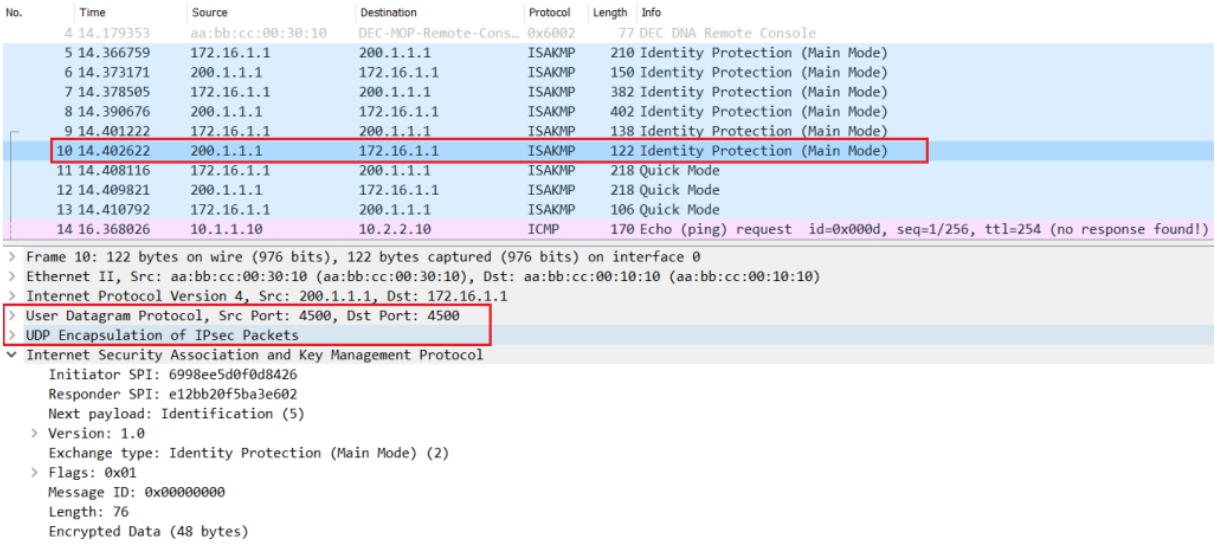


The result is that the receiving device RTR-Site2 recalculates the hash based on the Destination Peer IP Address 100.1.1.1 and Port 500 which is **66718a3d26322b74c7de2c87fb1ff4c9** and compares it with the hash it received from RTR-Site1 which is **ab18C4efb950c61f568a636561764e6f**.

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

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

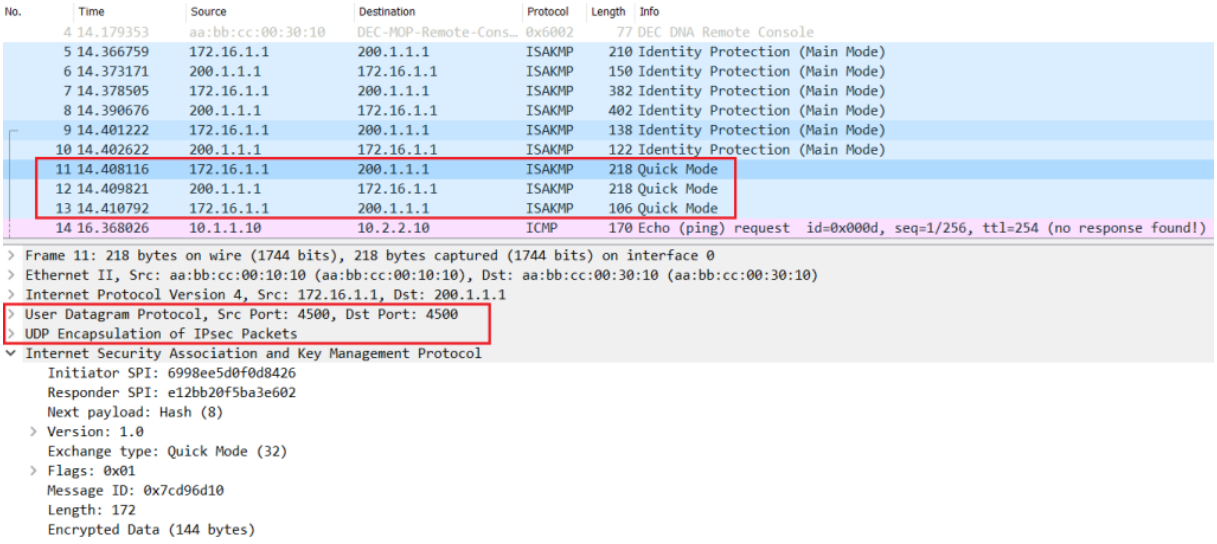




No.	Time	Source	Destination	Protocol	Length	Info
4	14.179353	aa:bb:cc:00:30:10	DEC-MOP-Remote-Cons…	0x6002	77	DEC DNA Remote Console
5	14.366759	172.16.1.1	200.1.1.1	ISAKMP	210	Identity Protection (Main Mode)
6	14.373171	200.1.1.1	172.16.1.1	ISAKMP	150	Identity Protection (Main Mode)
7	14.378505	172.16.1.1	200.1.1.1	ISAKMP	382	Identity Protection (Main Mode)
8	14.390676	200.1.1.1	172.16.1.1	ISAKMP	402	Identity Protection (Main Mode)
9	14.401222	172.16.1.1	200.1.1.1	ISAKMP	138	Identity Protection (Main Mode)
10	14.402622	200.1.1.1	172.16.1.1	ISAKMP	122	Identity Protection (Main Mode)
11	14.408116	172.16.1.1	200.1.1.1	ISAKMP	218	Quick Mode
12	14.409821	200.1.1.1	172.16.1.1	ISAKMP	218	Quick Mode
13	14.410792	172.16.1.1	200.1.1.1	ISAKMP	106	Quick Mode
14	16.368026	10.1.1.10	10.2.2.10	ICMP	170	Echo (ping) request id=0x000d, seq=1/256, ttl=254 (no response found!)

```
> Frame 10: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Ethernet II, Src: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10), Dst: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10)
> Internet Protocol Version 4, Src: 200.1.1.1, Dst: 172.16.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6998ee5d0f0d8426
    Responder SPI: e12bb20f5ba3e602
    Next payload: Identification (5)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x01
    Message ID: 0x00000000
    Length: 76
    Encrypted Data (48 bytes)
```

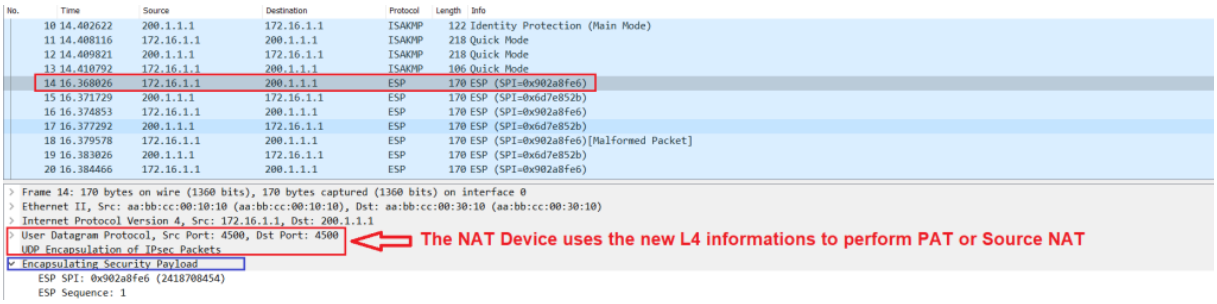
Because the NAT-T, in IKE Phase 2 (IPsec Quick Mode) encapsulates the Quick Mode (IPsec Phase 2) inside UDP 4500. After Quick Mode negociation is completed, Phase 2 is now ready to encrypt the data and ESP Packets are encapsulated inside UDP port 4500 as well, thus providing a port to be used in the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



No.	Time	Source	Destination	Protocol	Length	Info
4	14.179353	aa:bb:cc:00:30:10	DEC-MOP-Remote-Cons…	0x6002	77	DEC DNA Remote Console
5	14.366759	172.16.1.1	200.1.1.1	ISAKMP	210	Identity Protection (Main Mode)
6	14.373171	200.1.1.1	172.16.1.1	ISAKMP	150	Identity Protection (Main Mode)
7	14.378505	172.16.1.1	200.1.1.1	ISAKMP	382	Identity Protection (Main Mode)
8	14.390676	200.1.1.1	172.16.1.1	ISAKMP	402	Identity Protection (Main Mode)
9	14.401222	172.16.1.1	200.1.1.1	ISAKMP	138	Identity Protection (Main Mode)
10	14.402622	200.1.1.1	172.16.1.1	ISAKMP	122	Identity Protection (Main Mode)
11	14.408116	172.16.1.1	200.1.1.1	ISAKMP	218	Quick Mode
12	14.409821	200.1.1.1	172.16.1.1	ISAKMP	218	Quick Mode
13	14.410792	172.16.1.1	200.1.1.1	ISAKMP	106	Quick Mode
14	16.368026	10.1.1.10	10.2.2.10	ICMP	170	Echo (ping) request id=0x000d, seq=1/256, ttl=254 (no response found!)

```
> Frame 11: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
> Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10)
> Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6998ee5d0f0d8426
    Responder SPI: e12bb20f5ba3e602
    Next payload: Hash (8)
  > Version: 1.0
    Exchange type: Quick Mode (32)
  > Flags: 0x01
    Message ID: 0x7cd96d10
    Length: 172
    Encrypted Data (144 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, RTR-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.


No. Time Source Destination Protocol Length Info
10 14.402622 200.1.1.1 172.16.1.1 ISAKMP 122 Identity Protection (Main Mode)
11 14.408116 172.16.1.1 200.1.1.1 ISAKMP 218 Quick Mode
12 14.409821 200.1.1.1 172.16.1.1 ISAKMP 218 Quick Mode
13 14.410792 172.16.1.1 200.1.1.1 ISAKMP 106 Quick Mode
14 16.368026 172.16.1.1 200.1.1.1 ESP 170 ESP (SPI=0x902a8fe6)
15 16.371729 200.1.1.1 172.16.1.1 ESP 170 ESP (SPI=0x6d7e852b)
16 16.374853 172.16.1.1 200.1.1.1 ESP 170 ESP (SPI=0x902a8fe6)
17 16.377292 200.1.1.1 172.16.1.1 ESP 170 ESP (SPI=0x6d7e852b)
18 16.379578 172.16.1.1 200.1.1.1 ESP 170 ESP (SPI=0x902a8fe6)[Malformed Packet]
19 16.383026 200.1.1.1 172.16.1.1 ESP 170 ESP (SPI=0x6d7e852b)
20 16.384466 172.16.1.1 200.1.1.1 ESP 170 ESP (SPI=0x902a8fe6)
Frame 14: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: aa:bb:cc:00:30:10 (aa:bb:cc:00:30:10)
Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
ESP SPI: 0x902a8fe6 (2418708454)
ESP Sequence: 1
The NAT Device uses the new L4 informations to perform PAT or Source NAT