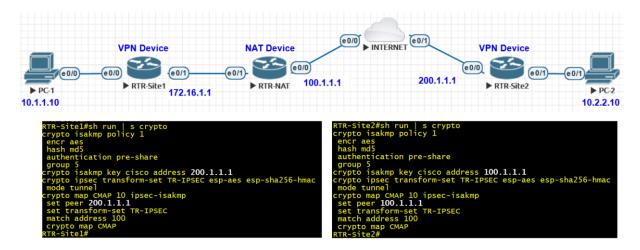
## NAT Traversal NAT-T in IPSEC VPN explained with wireshark

## By Redouane MEDDANE



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.

| No. | Time                 | Source                 | Destination            | Protocol  | Length Info   |
|-----|----------------------|------------------------|------------------------|-----------|---|
|     | 10.000000            | aa:bb:cc:00:30:10      | aa:bb:cc:00:30:10      | LOOP      | 60 Reply  |
|     | 2 1.498940           | aa:bb:cc:00:10:10      | aa:bb:cc:00:10:10      | LOOP      | 60 Reply  |
| 5   | 3 8.864732           | 10.1.1.10              | 10.2.2.10              | TCP       | 114 30206 → 23 [SYN] Seq=0 Win=4128 Len=0 MSS=536   |
|     | 4 8.866726           | 200.1.1.1              | 172.16.1.1             | ESP       | 114 ESP (SPI=0x2cf80587)  |
|     | 5 8.867551           | 10.1.1.10              | 10.2.2.10              | TCP       | 110 30206 → 23 [ACK] Seq=1 Ack=1 Win=4128 Len=0   |
|     | 6 8.867565           | 10.1.1.10              | 10.2.2.10              | TELNET    | 122 Telnet Data   |
|     | 7 8,867568           | 10.1.1.10              | 10.2.2.10              |           | 110 [TCP Dup ACK 5#1] 30206 → 23 [ACK] Seq=13 Ack=1 Win=4128 Len=0                          |
| 1   | 8 8,868752           | 200.1.1.1              | 172.16.1.1             | ESP       | 110 ESP (SPI=0x2cf80587)  |
|     | 9 8.931580           | 200.1.1.1              | 172.16.1.1             | ESP       | 122 ESP (SPI=0x2cf80587)  |
|     | 10 8.931626          | 200.1.1.1              | 172.16.1.1             | ESP       | 150 ESP (SPI=0x2cf80587)  |
|     | 11 8.932286          | 10.1.1.10              | 10.2.2.10              | TCP       | 110 30206 → 23 [ACK] Seq=13 Ack=55 Win=4074 Len=0   |
| >   | Frame 6: 122 bytes   | on wire (976 bits), 1  | 122 bytes captured (97 | 6 bits) c | n interface 0   |
| >   | Ethernet II, Src: a  | a:bb:cc:00:10:10 (aa:  | bb:cc:00:10:10), Dst:  | aa:bb:co  | :00:30:10 (aa:bb:cc:00:30:10)   |
| >   | Internet Protocol \  | Version 4, Src: 172.16 | 5.1.1, Dst: 200.1.1.1  |           |   |
| >   | Jser Datagram Proto  | col, Src Port: 4500,   | Dst Port: 4500         | Wit       | n NAT Traversal, NAT Device can translate te Source Port 4500 as it's UDP Packet            |
| _   | JDP Encapsulation of | of IPsec Packets       |                        |           |   |
| >   | Encapsulating Secur  | ity Payload            |                        |           |   |
| >   | Internet Protocol N  | Version 4, Src: 10.1.1 | L.10, Dst: 10.2.2.10   |           |   |
| >   | Transmission Contro  | 1 Protocol, Src Port:  | : 30206, Dst Port: 23, | Seq: 1,   | Ack: 1, Len: 12 Encrypted, NAT Device cannot decrypt to perform PAT Translation at L4 Lever |
|     | Telnet               | ,                      |                        |           |   |
|     |                      |                        |                        |           |   |

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.

| 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 Conso  | ble   |
|   | 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)   |
| L                                       | 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  | <pre>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre>   |
| > F                                     | name 5: 210 bytes   | on wire (1680 bits),   | 210 bytes cantured (1)   | 580 hits)   | on interface 0   |   |
|   |   |  |  |   | ::00:30:10 (aa:bb:cc:00:30:  | 10)   |
|   |   | /ersion 4, Src: 172.16   |  | 00.00.00  |  |   |
|   |   | ocol, Src Port: 500, D   |  |   |  |   |
|   |   | Association and Key Ma   |  |   |  |   |
| • 1                                     | Initiator SPI: 6  |  | hagement Protocol  |   |  |   |
|   | Responder SPI: 0  |  |  |   |  |   |
|   |   | curity Association (1  | )  |   |  |   |
|   | Version: 1.0  | curry Association (1   | /  |   |  |   |
|   |   | dentity Protection (M  | ain Mode) (2)  |   |  |   |
|   | Flags: 0x00   | denercy recection (n   | u111 Houe) (2)   |   |  |   |
|   | Message ID: 0x00  | 000000   |  |   |  |   |
|   | Length: 168   | 000000   |  |   |  |   |
|   | Payload: Securit  | w Association (1)  |  |   |  |   |
|   |   | ID (13) : RFC 3947 Ne  | notistion of NAT Trave   | uncal in  | the TKE  |   |
|   |   | ID (13) : draft-ietf-  |  | 1.201 10  | the IKE  |   |
|   |   | ID (13) : draft-ietf-<br>ID (13) : draft-ietf-   |  |   |  |   |
|   |   | ID (13) : draft-ietf-<br>ID (13) : draft-ietf-   |  |   |  |   |
|   | Fayload. Venuor   | 10 (13) : unart-lett-  | ipsec-nac-c-ike-02 (n  |   |  |   |
|   |   |  |  |   |  |   |
|   |   |  |  |   |  |   |
| No                                      | Time  | Course   | Dectination  | Protocol  | length Info  |   |
| No.                                     | Time  | Source   | Destination  | Protocol  | Length Info  | ale   |
| No.                                     | 4 14.179353   | aa:bb:cc:00:30:10  | DEC-MOP-Remote-Cons.   | 0x6002  | 77 DEC DNA Remote Conse  |   |
| No.                                     | 4 14.179353<br>5 14.366759  | aa:bb:cc:00:30:10<br>172.16.1.1  | DEC-MOP-Remote-Cons<br>200.1.1.1   | 0x6002<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection   | (Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171   | aa:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1   | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1  | 0x6002<br>ISAKMP<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>150 Identity Protection  | (Main Mode)<br>(Main Mode)  |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505  | aa:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1   | DEC-MOP-Remote-Cons<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>150 Identity Protection<br>382 Identity Protection   | (Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676   | aa:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>200.1.1.1   | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1   | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>150 Identity Protection<br>382 Identity Protection<br>402 Identity Protection  | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)  |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222  | aa:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1  | DEC-MOP-Remote-Cons<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1   | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>150 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection   | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222<br>10 14.402622  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>150 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection<br>122 Identity Protection  | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1  | DEC-MOP-Remote-Cons.<br>2001.1.1<br>172.16.1.1<br>2001.1.1<br>172.16.1.1<br>172.16.1.1<br>2001.1.1<br>172.16.1.1<br>2001.1.1   | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode   | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378595<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.409821  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>200.1.1.1  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1<br>172.16.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1   | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP                                  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode   | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.409821<br>13 14.410792  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1  | Ox6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP                                  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>138 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode   | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| No.                                     | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378595<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.409821  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>200.1.1.1  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1<br>172.16.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1   | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP                                  | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>138 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode   | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
|   | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.396676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.409821<br>13 14.410792<br>14 16.368026  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10  | Ox6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP                        | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection<br>138 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request  | (Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)<br>(Main Mode)   |
| F                                       | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.4089821<br>13 14.410792<br>14 16.368026<br>Trame 6: 150 bytes  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1   | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection<br>138 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> F                              | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet II, Src: 4  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I                       | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet II, Src: 4<br>atternet Protocol N  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>pa:bb:cc:00:30:10 (as:  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U                | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.396676<br>9 14.401222<br>10 14.40622<br>10 14.40622<br>11 14.408116<br>12 14.409821<br>13 14.410792<br>14 16.368026<br>thernet II, Src: 4<br>thernet II, Src: 4<br>thernet II, Src: 4<br>thernet II, Src: 4<br>thernet Protocol V<br>ser Datagram Protocol V   | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>a:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>19.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>st Port: 500  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U                | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.396676<br>9 14.401222<br>10 14.40622<br>10 14.40622<br>11 14.408116<br>12 14.409821<br>13 14.410792<br>14 16.368026<br>thernet II, Src: 4<br>thernet II, Src: 4<br>thernet II, Src: 4<br>thernet II, Src: 4<br>thernet Protocol V<br>ser Datagram Protocol V   | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>pa:bb:cc:00:30:10 (pa:<br>/ersion 4, Src: 200.1.<br>pcol, Src Port: 500.1<br>Association and Key Ma   | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>19.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>st Port: 500  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U                | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398505<br>8 14.402622<br>10 14.402622<br>11 14.408116<br>12 14.408126<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet II, Src: 4<br>ser Datagram Protocol V<br>thernet Scurity /  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>10.1.1.1<br>0 on wire (1200 bits),<br>0 a:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>Scol, Src Port: 500, D<br>Association and Key Ma<br>3998ee5d0f0d8426  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>19.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>st Port: 500  | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U                | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>13 14.410792<br>14 16.368026<br>150 bytes<br>thernet II, Src: 4<br>hternet Protocol V<br>ser Datagram Proty<br>thernet Security /<br>Initiator SPI: 6<br>Responder SPI: 6   | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>10.1.1.1<br>0 on wire (1200 bits),<br>0 a:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>Scol, Src Port: 500, D<br>Association and Key Ma<br>3998ee5d0f0d8426  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>st Port: 500<br>nagement Protocol                     | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U<br>Y I         | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.390676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>13 14.410792<br>14 16.368026<br>150 bytes<br>thernet II, Src: 4<br>hternet Protocol V<br>ser Datagram Proty<br>thernet Security /<br>Initiator SPI: 6<br>Responder SPI: 6   | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>aa:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>ccol, Src Port: 500, D<br>Association and Key Ma<br>099ResEd0Fd0d8426<br>12bb20f5ba3e602   | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>st Port: 500<br>nagement Protocol                     | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U<br>Y I         | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet Protocol V<br>iser Datagram Proto<br>ternet Security /<br>Initiator SPI: 6<br>Responder SPI: 6<br>Responder SPI: 6<br>Next payload: Se<br>Version: 1.0  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>aa:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>ccol, Src Port: 500, D<br>Association and Key Ma<br>099ResEd0Fd0d8426<br>12bb20f5ba3e602   | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>ist Port: 500<br>nagement Protocol                    | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U<br>V<br>V      | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet Protocol V<br>iser Datagram Proto<br>ternet Security /<br>Initiator SPI: 6<br>Responder SPI: 6<br>Responder SPI: 6<br>Next payload: Se<br>Version: 1.0  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>a:bb:cc:00:30:10 (as:<br>4ersion 4, Src: 200.1.<br>occl, Src Port: 500, D<br>sociation and Key Ma<br>9998e5d0f0d8426<br>1:2bb20f5ba3e602<br>scurity Association (1  | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>ist Port: 500<br>nagement Protocol                    | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> U<br>> U                | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet II, Src: 4<br>hternet Protocol V<br>ser Datagram Protocol V<br>ser Datagram Protocol V<br>ternet Security /<br>Initiator SPI: 6<br>Responder SPI: 6<br>Next payload: set   | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>aa:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>cool, Src Port: 500. D<br>Association and Key Ma<br>5998ee5d0f0d8426<br>:12bb20f5ba3e602<br>ecurity Association (1<br>identity Protection (M          | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>ist Port: 500<br>nagement Protocol                    | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> U<br>> U                | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.409821<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet II, Src: a<br>otternet Protocol N<br>ser Datagram Protocol N<br>ser Datagram Protocol N<br>thernet Security /<br>Initiator SPI: 6<br>Next payload: Se<br>Version: 1.0<br>Exchange type: 1<br>Flags: 0x00  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>aa:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>cool, Src Port: 500. D<br>Association and Key Ma<br>5998ee5d0f0d8426<br>:12bb20f5ba3e602<br>ecurity Association (1<br>identity Protection (M          | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>ist Port: 500<br>nagement Protocol                    | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U<br>V<br>V<br>V | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408121<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet Protocol V<br>Initiator SPI: 6<br>Responder SPI: 6<br>Next payload: Se<br>Version: 1.0<br>Exchange type: 1<br>Flags: 0x00<br>Message ID: 0x06<br>Length: 108  | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>172.16.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>aa:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>cool, Src Port: 500. D<br>Association and Key Ma<br>5998ee5d0f0d8426<br>:12bb20f5ba3e602<br>ecurity Association (1<br>identity Protection (M          | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>ist Port: 500<br>nagement Protocol                    | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP                | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>482 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>on interface 0                                  | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |
| > F<br>> E<br>> I<br>> U<br>V<br>V<br>V | 4 14.179353<br>5 14.366759<br>6 14.373171<br>7 14.378505<br>8 14.398505<br>8 14.398505<br>8 14.398676<br>9 14.401222<br>10 14.402622<br>11 14.408116<br>12 14.408126<br>13 14.410792<br>14 16.368026<br>rame 6: 150 bytes<br>thernet Ir, Src: a<br>thernet Protocol N<br>ser Datagram | a:bb:cc:00:30:10<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.1.1.10<br>on wire (1200 bits),<br>aa:bb:cc:00:30:10 (aa:<br>/ersion 4, Src: 200.1.<br>Scol, Src Port: 500, D<br>Sesociation and Key Ma<br>9998ee5d0f0d8426<br>1:2bb20f5ba3e602<br>scurity Association (1<br>dentity Protection (M<br>0000000 | DEC-MOP-Remote-Cons.<br>200.1.1.1<br>172.16.1.1<br>200.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>172.16.1.1<br>200.1.1.1<br>10.2.2.10<br>150 bytes captured (1<br>bb:cc:00:30:10), Dst:<br>1.1, Dst: 172.16.1.1<br>st Port: 500<br>nagement Protocol<br>)<br>ain Mode) (2) | 0x6002<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ISAKMP<br>ICMP<br>200 bits)<br>aa:bb:cc | 77 DEC DNA Remote Conso<br>210 Identity Protection<br>382 Identity Protection<br>402 Identity Protection<br>138 Identity Protection<br>122 Identity Protection<br>218 Quick Mode<br>218 Quick Mode<br>106 Quick Mode<br>170 Echo (ping) request<br>0 on interface 0<br>::00:10:10 (aa:bb:cc:00:10: | <pre>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>(Main Mode)<br/>id=0x000d, seq=1/256, ttl=254 (no response found!)</pre> |

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

|        | 4 14.179353   | aa:bb:cc:00:30:10      | DEC-MOP-Remote-Cons    | 0x6002  | 77 DEC DNA Remote Conso | le          |            |             |                  |  |
|--------|---|------------------------|------------------------|---------|-------------------------|-------------|------------|-------------|------------------|--|
| Г      | 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) |            |             |                  |  |
| L      | 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!) |  |
|        | <pre>&gt; Internet Protocol Version 4, Src: 172.16.1.1, Dst: 200.1.1.1 &gt; User Datagram Protocol, Src Port: 500 V Internet Security Association and Key Management Protocol Initiator SPI: 6998ee500608426 Responder SPI: e12bb20f5ba3e602 Next payload: Key Exchange (4)</pre> |                        |                        |         |                         |             |            |             |                  |  |
| >      | Version: 1.0  | .,                     |                        |         |                         |             |            |             |                  |  |
|        | Exchange type: I  | [dentity Protection (M | ain Mode) (2)          |         |                         |             |            |             |                  |  |
| >      | Flags: 0x00   |                        |                        |         |                         |             |            |             |                  |  |
|        | Message ID: 0x00  | 000000                 |                        |         |                         |             |            |             |                  |  |
|        | Length: 340   |                        |                        |         |                         |             |            |             |                  |  |
| >      | Payload: Key Exc  | change (4)             |                        |         |                         |             |            |             |                  |  |
| >      | Payload: Nonce (  | (10)                   |                        |         |                         |             |            |             |                  |  |
| >      | Payload: Vendor   | ID (13) : RFC 3706 DP  | D (Dead Peer Detection | n)      |                         |             |            |             |                  |  |
| >      | Payload: Vendor   | ID (13) : Unknown Ven  | dor ID                 |         |                         |             |            |             |                  |  |
| >      | Payload: Vendor   | ID (13) : XAUTH        |                        |         |                         |             |            |             |                  |  |
| ~      | Payload: NAT-D (  | (RFC 3947) (20)        |                        |         |                         |             |            |             |                  |  |
|        | Next payload:   | NAT-D (RFC 3947) (20   | )                      |         |                         |             |            |             |                  |  |
|        | Reserved: 00  |                        |                        |         |                         |             |            |             |                  |  |
|        | Pavload lengt   |                        |                        |         |                         |             |            |             |                  |  |
| _      |   |                        | b859631968ceeb26b61430 | 0014fc6 |                         |             |            |             |                  |  |
| $\sim$ | Payload: NAT-D (  |                        |                        |         |                         |             |            |             |                  |  |
|        |   | NONE / No Next Paylo   | ad (0)                 |         |                         |             |            |             |                  |  |
|        | Reserved: 00  |                        |                        |         |                         |             |            |             |                  |  |
|        | Payload lengt   |                        |                        |         |                         |             |            |             |                  |  |
|        | HASH of the a   | ddress and port: ab18  | c4efb950c61f568a636561 | 1764e6f |                         |             |            |             |                  |  |
|        |   |                        |                        |         |                         |             |            |             |                  |  |

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

|     | 4 14.179353        | aa:bb:cc:00:30:10      | DEC-MOP-Remote-Cons.   | 0x6002  | 77 DEC DNA Remote Conso | ole         |            |                     |            |
|-----|--------------------|------------------------|------------------------|---------|-------------------------|-------------|------------|---------------------|------------|
|     | 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              | TSAKMP  | 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 respons | se found!) |
| > 1 | nternet Protocol \ | Version 4, Src: 200.1. | 1.1. Dst: 172.16.1.1   |         |                         |             |            |                     |            |
|     |                    | ocol, Src Port: 500, [ |                        |         |                         |             |            |                     |            |
|     |                    | Association and Key Ma |                        |         |                         |             |            |                     |            |
|     | Initiator SPI: 6   | 5998ee5d0f0d8426       |                        |         |                         |             |            |                     |            |
|     | Responder SPI: e   | e12bb20f5ba3e602       |                        |         |                         |             |            |                     |            |
|     | Next payload: Ke   | ey Exchange (4)        |                        |         |                         |             |            |                     |            |
| 2   | Version: 1.0       |                        |                        |         |                         |             |            |                     |            |
|     |                    | [dentity Protection (M | lain Mode) (2)         |         |                         |             |            |                     |            |
| 2   | Flags: 0x00        |                        |                        |         |                         |             |            |                     |            |
|     | Message ID: 0x00   | 000000                 |                        |         |                         |             |            |                     |            |
|     | Length: 360        |                        |                        |         |                         |             |            |                     |            |
| 2   | Payload: Key Exc   | change (4)             |                        |         |                         |             |            |                     |            |
| 2   | Payload: Nonce (   | (10)                   |                        |         |                         |             |            |                     |            |
| 2   | Payload: Vendor    | ID (13) : CISCO-UNITY  | 1.0                    |         |                         |             |            |                     |            |
| 2   | Payload: Vendor    | ID (13) : RFC 3706 DF  | D (Dead Peer Detection | n)      |                         |             |            |                     |            |
| 2   | Payload: Vendor    | ID (13) : Unknown Ver  | dor ID                 |         |                         |             |            |                     |            |
| _   | Payload: Vendor    | ID (13) : XAUTH        |                        |         |                         |             |            |                     |            |
| ·   | ∕ Payload: NAT-D ( |                        |                        |         |                         |             |            |                     |            |
|     |                    | NAT-D (RFC 3947) (20   | )                      |         |                         |             |            |                     |            |
|     | Reserved: 00       |                        |                        |         |                         |             |            |                     |            |
|     | Payload lengt      |                        |                        |         |                         |             |            |                     |            |
| _   |                    |                        | 8a3d26322b74c7de2c87fb | o1ff4c9 | ]                       |             |            |                     |            |
| 2   | ✓ Payload: NAT-D ( |                        |                        |         |                         |             |            |                     |            |
|     |                    | NONE / No Next Paylo   | ad (0)                 |         |                         |             |            |                     |            |
|     | Reserved: 00       |                        |                        |         |                         |             |            |                     |            |
|     | Pavload lengt      |                        |                        |         |                         |             |            |                     |            |
|     | HASH of the a      | ddress and port: 8b44  | b859631968ceeb26b61430 | 0014fc6 |                         |             |            |                     |            |
|     |                    |                        |                        |         |                         |             |            |                     |            |

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.

| N  | b. 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)  |  |  |  |  |
| r. | 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!) |  |  |  |  |
| _  | Ename 0, 120 hutes on wine (1104 hits) 120 hutes contured (1104 hits) on intenface 0 |                   |                     |          |  |  |  |  |  |

Frame 9: 138 bytes on wire (1104 bits), 138 bytes captured (1104 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

- Internet Security Association and Key Management Protocol Initiator SPI: 6998ee5d0f0d8426 Responder SPI: e12bb20f5ba3e602
- Next pavload: Identification (5)
- > Version: 1.0
- Exchange type: Identity Protection (Main Mode) (2)
- > Flags: 0x01 Message ID: 0x00000000 Length: 92
- Encrypted Data (64 bytes)

| N   | o. 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)  |
| ſ   | 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 byte | s on wire (976 bits),  | 122 bytes captured (97 | 76 bits) | on interface 0   |
| >   | Ethernet II, Src:  | aa:bb:cc:00:30:10 (aa: | bb:cc:00:30:10), Dst:  | aa:bb:c  | c: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 Prot | ocol, Src Port: 4500,  | Dst Port: 4500         |          |  |
| >   | UDP Encapsulation  | of IPsec Packets       |                        |          |  |
| ~   | Internet Security  | Association and Key Ma | nagement Protocol      |          |  |
|     | Initiator SPI:     | 6998ee5d0f0d8426       |                        |          |  |
|     | Responder SPI:     | e12bb20f5ba3e602       |                        |          |  |
|     | Next payload: I    | dentification (5)      |                        |          |  |
|     | > Version: 1.0     |                        |                        |          |  |
|     | Exchange type:     | Identity Protection (M | lain Mode) (2)         |          |  |
|     | > Flags: 0x01      |                        |                        |          |  |
|     | Message ID: 0x0    | 000000                 |                        |          |  |
|     | 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 Re | mote Conso | le          |            |         |              |         |
|    | 5 14.366759        | 172.16.1.1             | 200.1.1.1             | ISAKMP   | 210     | Identity P | rotection  | (Main Mode) |            |         |              |         |
|    | 6 14.373171        | 200.1.1.1              | 172.16.1.1            | ISAKMP   | 150     | Identity P | rotection  | (Main Mode) |            |         |              |         |
|    | 7 14.378505        | 172.16.1.1             | 200.1.1.1             | ISAKMP   | 382     | Identity P | rotection  | (Main Mode) |            |         |              |         |
|    | 8 14.390676        | 200.1.1.1              | 172.16.1.1            | ISAKMP   | 402     | Identity P | rotection  | (Main Mode) |            |         |              |         |
|    | 9 14.401222        | 172.16.1.1             | 200.1.1.1             | ISAKMP   | 138     | Identity P | rotection  | (Main Mode) |            |         |              |         |
|    | 10 14.402622       | 200.1.1.1              | 172.16.1.1            | ISAKMP   | 122     | Identity P | rotection  | (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, | tt1=254 | (no response | found!) |
| >  | Frame 11: 218 byte | s on wire (1744 bits), | 218 bytes captured (1 | 744 bits | s) on i | nterface Ø |            |             |            |         |              |         |
|    |                    | aa:bb:cc:00:10:10 (aa: |                       |          |         |            |            | 10)         |            |         |              |         |
| >  | Internet Protocol  | Version 4, Src: 172.16 | .1.1, Dst: 200.1.1.1  |          |         |            |            | -           |            |         |              |         |
| >  | User Datagram Prot | ocol, Src Port: 4500,  | Dst Port: 4500        |          |         |            |            |             |            |         |              |         |
| >  | UDP Encapsulation  | of IPsec Packets       |                       |          |         |            |            |             |            |         |              |         |
| ~  | Internet Security  | Association and Key Ma | nagement Protocol     |          |         |            |            |             |            |         |              |         |
|    | Initiator SPI: 6   | 5998ee5d0f0d8426       |                       |          |         |            |            |             |            |         |              |         |
|    | Responder SPI: e   | e12bb20f5ba3e602       |                       |          |         |            |            |             |            |         |              |         |
|    | Next payload: Ha   | ash (8)                |                       |          |         |            |            |             |            |         |              |         |
|    | > Version: 1.0     |                        |                       |          |         |            |            |             |            |         |              |         |
|    | Exchange type: (   | Quick Mode (32)        |                       |          |         |            |            |             |            |         |              |         |
|    | > Flags: 0x01      |                        |                       |          |         |            |            |             |            |         |              |         |
|    | Message ID: 0x70   | :d96d10                |                       |          |         |            |            |             |            |         |              |         |
|    | 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.

| No | Time       | 2           | Source                | Destination           | Protocol L | 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 (1 | 360 hits)  | ) on interface 0  |
| 5  |            |             |                       |                       |            | :00:30:10 (aa:bb:cc:00:30:10)   |
| 5  |            |             | rsion 4, Src: 172.16. |                       |            | ······  |
| >  |            |             | ol, Src Port: 4500, D |                       | <u> </u>   | he NAT Device uses the new L4 informations to perform PAT or Source NAT |
|    | UDP Encaps | sulation of | IPsec Packets         |                       |            | he har bevice uses the new L4 mornations to perform PAT of Source har   |
| 2  | Encapsulat | ting Securi | ty Pavload            |                       |            |   |
| -  | ESP SPI    | : 0x902a8f  | e6 (2418708454)       |                       |            |   |
|    | ESP Seg    | uence: 1    |                       |                       |            |   |
|    |            |             |                       |                       |            |   |