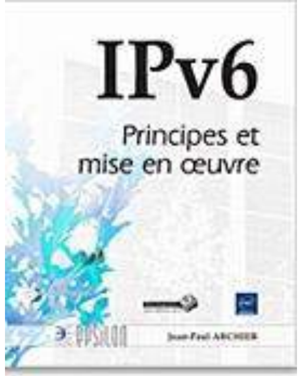
Analysis and troubleshooting of IPsec VPNs

Jean-Paul ARCHIER
contact@jpaconseil.com

Let me introduce myself

I am Jean-Paul ARCHIER

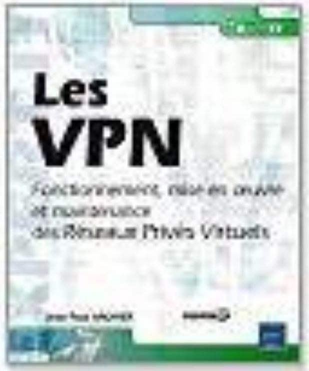
- Network & System Engineer since 1982
- Independant Consultant & Trainer since 2010
- Author for the French publisher ENI
- **You can reach me at : jean-paul@jpaconseil.com**



IPv6

Principes et mise en œuvre

Jean-Paul ARCHIER



Les VPN

Fonctionnement, mise en œuvre et maintenance des Réseaux Privés Virtuels

Agenda

- Analysis of Site to Site IPsec VPN with encrypted packets
    - IKEv2 without NAT
    - IKEv2 with NAT
- Analysis of Remote to Site Ipsec VPN
- Troubleshooting of some common cases
- Overview of how to decrypt IKE and ESP packets (when possible)

Capture files and profiles

- Files used for this presentation are available at

https://tinyurl.com/ipsec-2024

- Content :
  - Several capture files
  - Profile folders

Analysing IPsec without decryption

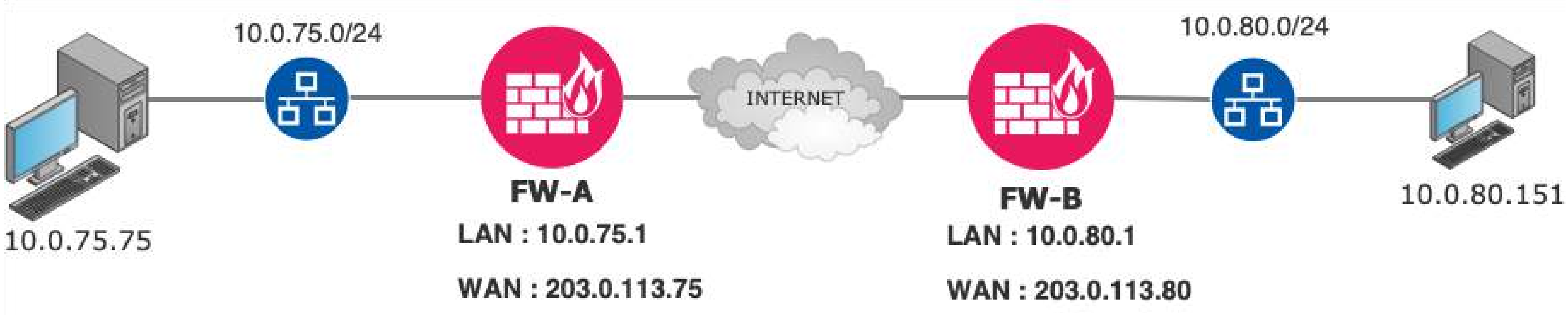
- Obviously only a part of the exchanges are visible in plain text

- We can still find enough information in the visible part and, sometimes, make some guessing from the encrypted exchanges
- We will only study the IKEv2 version (IKEv1 has been deprecated by RFC 9395 in April 2023 as well as algorithms like MD5-128, SHA1_160)

Example 1 - Site to Site VPN – No NAT

- Firewall A : Fortigate 40
  - WAN IP : 203.0.113.75/24
  - LAN IP : 10.0.75.1/24
- Firewall B :   WatchGuard
  - WAN IP : 203.0.113.80/24
  - LAN : 10.0.80.1/24

File : EXAMPLE1.pcap
Profile : VPN-simple



What can we observe 1/3 ?

- Creation of IKE SA (Parent SA)
- Creation of IPsec Sas (Child SAs)
- Two roles : Initiator and Responder
- All messages in pairs : request and response

What can we observe 2/3 ?

- ISAKMP/IKE : commonly 4 messages
    - 2 unencrypted : IKE_SA_INIT
        - Security parameters (cryptographic suites)
        - Nonces
        - DH values
    - 2 encrypted : IKE_AUTH
        - Identities
        - Secrets
        - Creation of first Child SA

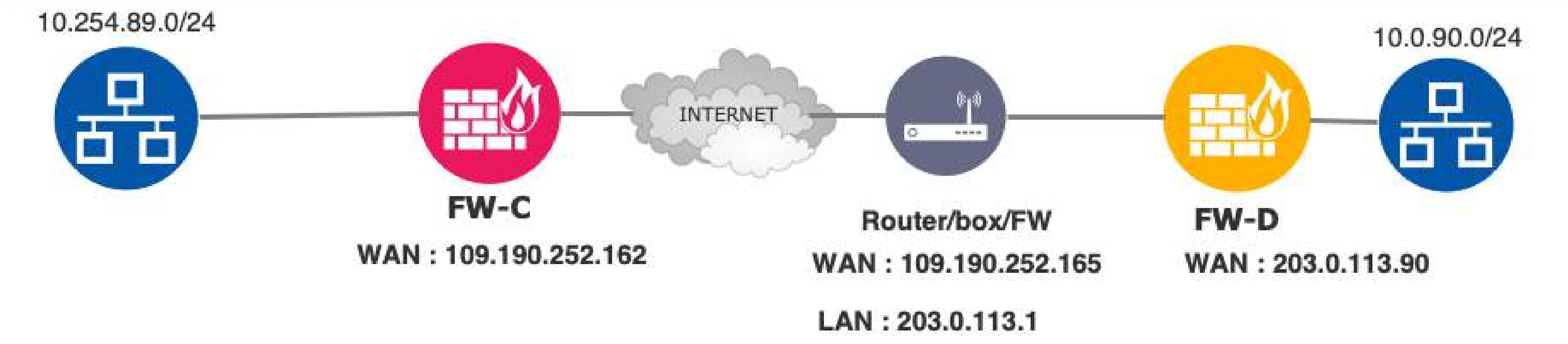
What can we observe 3/3 ?

- ESP : encrypted
  - Only fields in clear : SPI and sequence number

Site to Site VPN – Example2 -NAT

- Context :
  - NAT (on Router/FW) between Firewall-C and Firewall-D

- File : EXAMPLE2.pcap



Site to Site VPN – Example2 -NAT

- Differences with previous example (without NAT)
  - Use of port 500 for IKE_SA_INIT
  - Use of port 4500 after IKE_SA_INIT
  - ESP uses also port 4500

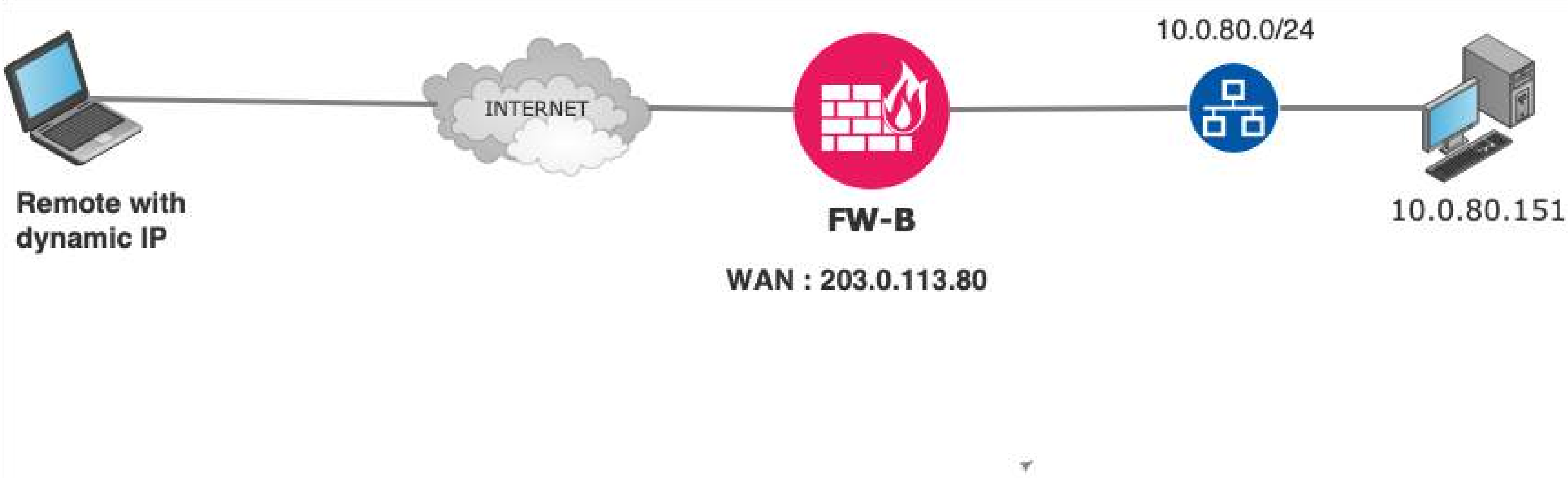
- Each IKE packet on port 4500 includes a four bytes zeros prefix

Remote PC to Main Site

- Main caracteristics
  - Use of port 500 for IKE_SA_INIT
  - Use of port 4500 after IKE_SA_INIT
  - ESP uses also port 4500
  - But source ports are random

File : EXAMPLE3.pcap

- Each IKE packet on port 4500 includes a four bytes zeros prefix



When something goes wrong …

- … It's time to do some troubleshooting

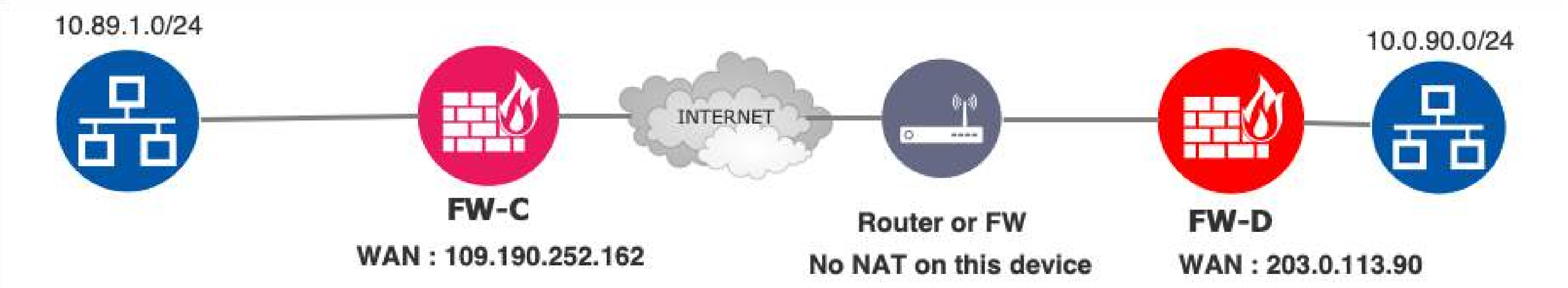
Troubleshooting of IPsec VPNs

Troubleshooting Case 1

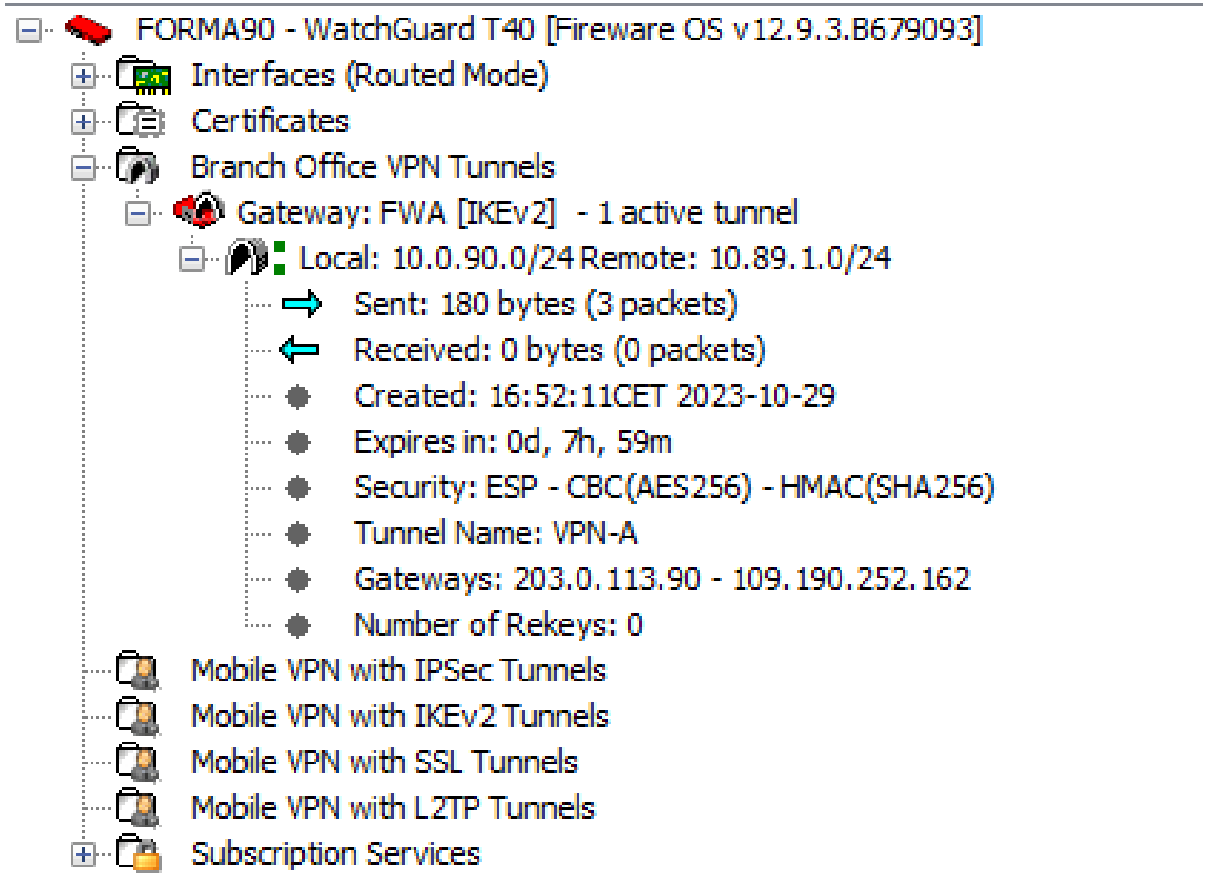
- Context
  - Site 1 : Firewall-C
  - Site 2 : Firewall-D

Files :
Case1_FirewallC_KO,
Case1_FirewallD_KO

- Symptoms :
  - VPN established according to the log and the status
  - When available outgoing counters increment
  - But no ping (or whatever protocol) possible between the two LANs



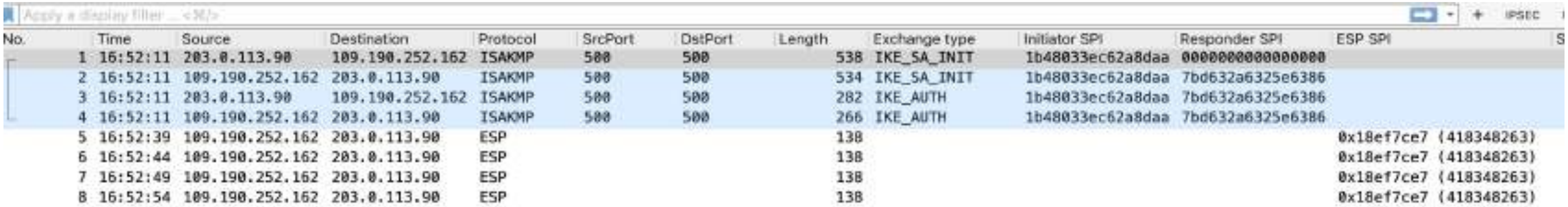
Case 1



```
⊟ FORMA90 - WatchGuard T40 [Fireware OS v12.9.3.B679093]
    ⊞ Interfaces (Routed Mode)
    ⊞ Certificates
    ⊟ Branch Office VPN Tunnels
        ⊟ Gateway: FWA [IKEv2]  - 1 active tunnel
            ⊟ Local: 10.0.90.0/24 Remote: 10.89.1.0/24
                ⇨ Sent: 180 bytes (3 packets)
                ⇦ Received: 0 bytes (0 packets)
                ● Created: 16:52:11CET 2023-10-29
                ● Expires in: 0d, 7h, 59m
                ● Security: ESP - CBC(AES256) - HMAC(SHA256)
                ● Tunnel Name: VPN-A
                ● Gateways: 203.0.113.90 - 109.190.252.162
                ● Number of Rekeys: 0
    Mobile VPN with IPSec Tunnels
    Mobile VPN with IKEv2 Tunnels
    Mobile VPN with SSL Tunnels
    Mobile VPN with L2TP Tunnels
    ⊞ Subscription Services
```

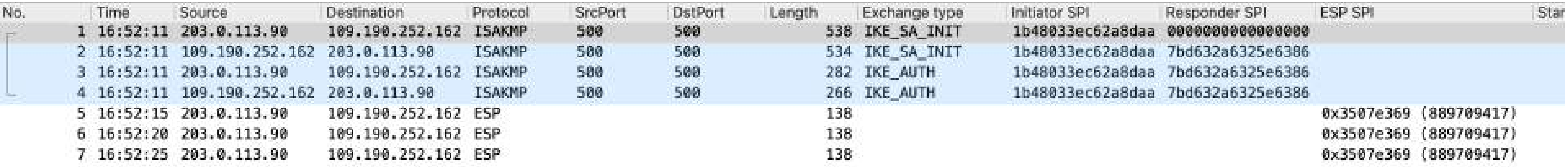
Case 1 -What we see in Wireshark

- On site C



No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Length	Exchange type	Initiator SPI	Responder SPI	ESP SPI	S
1	16:52:11	203.0.113.90	109.190.252.162	ISAKMP	500	500	538	IKE_SA_INIT	1b48033ec62a8daa	0000000000000000		
2	16:52:11	109.190.252.162	203.0.113.90	ISAKMP	500	500	534	IKE_SA_INIT	1b48033ec62a8daa	7bd632a6325e6386		
3	16:52:11	203.0.113.90	109.190.252.162	ISAKMP	500	500	282	IKE_AUTH	1b48033ec62a8daa	7bd632a6325e6386		
4	16:52:11	109.190.252.162	203.0.113.90	ISAKMP	500	500	266	IKE_AUTH	1b48033ec62a8daa	7bd632a6325e6386		
5	16:52:39	109.190.252.162	203.0.113.90	ESP			138				0x18ef7ce7 (418348263)	
6	16:52:44	109.190.252.162	203.0.113.90	ESP			138				0x18ef7ce7 (418348263)	
7	16:52:49	109.190.252.162	203.0.113.90	ESP			138				0x18ef7ce7 (418348263)	
8	16:52:54	109.190.252.162	203.0.113.90	ESP			138				0x18ef7ce7 (418348263)	

- On site D (no NAT between 203.0.113.90 and 109.190.252.162)



No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Length	Exchange type	Initiator SPI	Responder SPI	ESP SPI	Star
1	16:52:11	203.0.113.90	109.190.252.162	ISAKMP	500	500	538	IKE_SA_INIT	1b48033ec62a8daa	0000000000000000		
2	16:52:11	109.190.252.162	203.0.113.90	ISAKMP	500	500	534	IKE_SA_INIT	1b48033ec62a8daa	7bd632a6325e6386		
3	16:52:11	203.0.113.90	109.190.252.162	ISAKMP	500	500	282	IKE_AUTH	1b48033ec62a8daa	7bd632a6325e6386		
4	16:52:11	109.190.252.162	203.0.113.90	ISAKMP	500	500	266	IKE_AUTH	1b48033ec62a8daa	7bd632a6325e6386		
5	16:52:15	203.0.113.90	109.190.252.162	ESP			138				0x3507e369 (889709417)	
6	16:52:20	203.0.113.90	109.190.252.162	ESP			138				0x3507e369 (889709417)	
7	16:52:25	203.0.113.90	109.190.252.162	ESP			138				0x3507e369 (889709417)	

Case 1 - What we see in Wireshark

- No need to decrypt anything
- Capture on Firewall C :
  - Both incoming and outgoing ISAKMP trafic between the two firewalls
  - Only outgoing ESP trafic from B

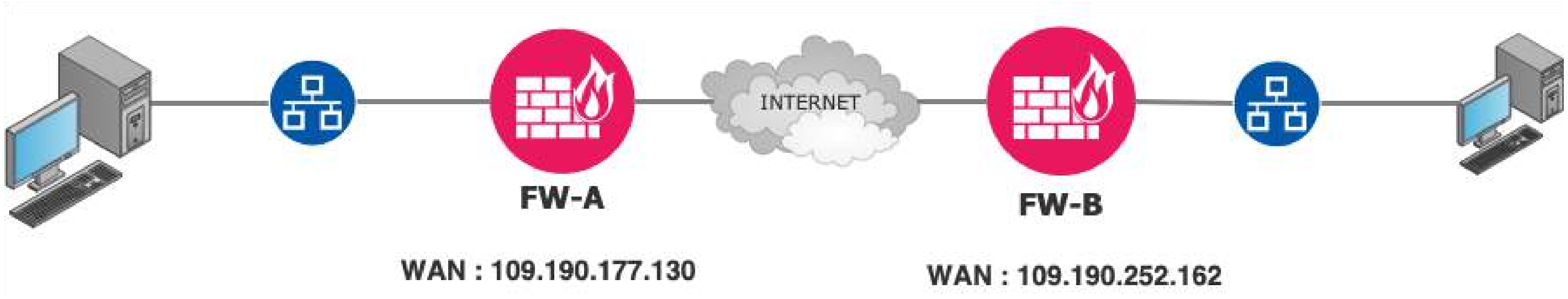
- Capture on Firewall D :
  - Both incoming and outgoing ISAKMP trafic between the two firewalls
  - Only outgoing ESP trafic from D

- => Traffic probably filtered somewhere between Firewall-C and Firewall-D

Case 2

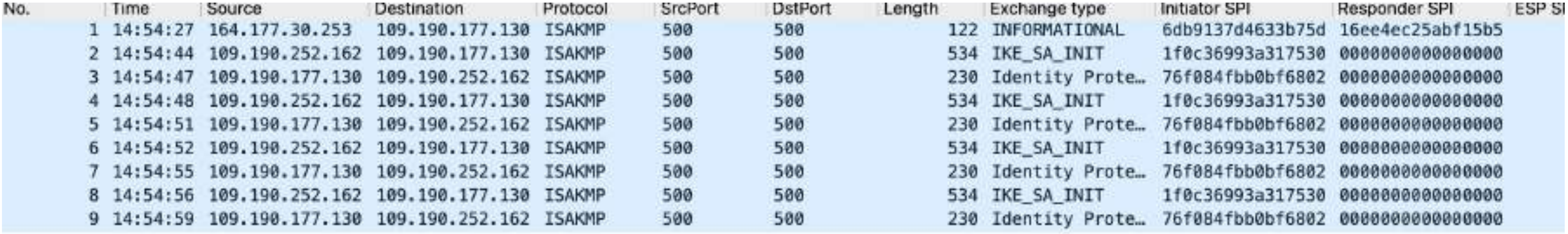
- Context
  - Site A : Firewall-A
  - Site B : Firewall-B
- Symptoms :
  - Nothing established : no IKE SA no Child or IPSEC SA

- Files :
  - Case2_FirewallA_KO.pcap
  - Case2_FirewallB_KO.pcap



Case 2 - What we see in Wireshark

- No need to decrypt anything
- Capture on site A :
  - Both sites are trying to establish IKE SA with no success



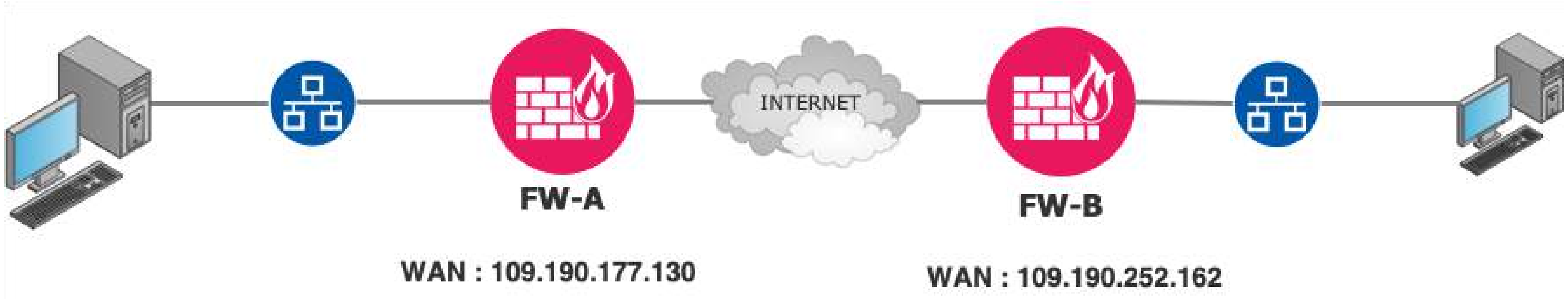
No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Length	Exchange type	Initiator SPI	Responder SPI	ESP SI
1	14:54:27	164.177.30.253	109.190.177.130	ISAKMP	500	500	122	INFORMATIONAL	6db9137d4633b75d	16ee4ec25abf15b5	
2	14:54:44	109.190.252.162	109.190.177.130	ISAKMP	500	500	534	IKE_SA_INIT	1f0c36993a317530	0000000000000000	
3	14:54:47	109.190.177.130	109.190.252.162	ISAKMP	500	500	230	Identity Prote…	76f084fbb0bf6802	0000000000000000	
4	14:54:48	109.190.252.162	109.190.177.130	ISAKMP	500	500	534	IKE_SA_INIT	1f0c36993a317530	0000000000000000	
5	14:54:51	109.190.177.130	109.190.252.162	ISAKMP	500	500	230	Identity Prote…	76f084fbb0bf6802	0000000000000000	
6	14:54:52	109.190.252.162	109.190.177.130	ISAKMP	500	500	534	IKE_SA_INIT	1f0c36993a317530	0000000000000000	
7	14:54:55	109.190.177.130	109.190.252.162	ISAKMP	500	500	230	Identity Prote…	76f084fbb0bf6802	0000000000000000	
8	14:54:56	109.190.252.162	109.190.177.130	ISAKMP	500	500	534	IKE_SA_INIT	1f0c36993a317530	0000000000000000	
9	14:54:59	109.190.177.130	109.190.252.162	ISAKMP	500	500	230	Identity Prote…	76f084fbb0bf6802	0000000000000000	

- Explanation : IKE version discrepancy , confirmed by column MjVer (Ike version)

Case 3

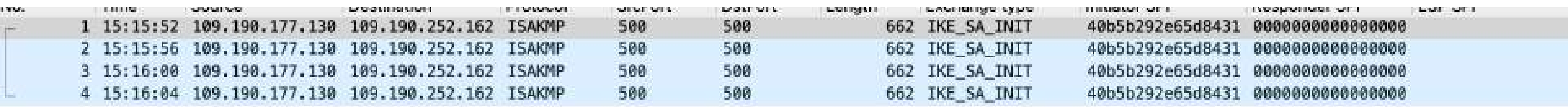
- Context
  - Site A : Firewall-A 109.190.177.230
  - Site B : Firewall-B 109.190.252.162

- Symptoms (On site B):
  - Nothing established : no IKE SA no Child or IPSEC SA
  - Only IKE SA Init
  - No response from site A



Case 3

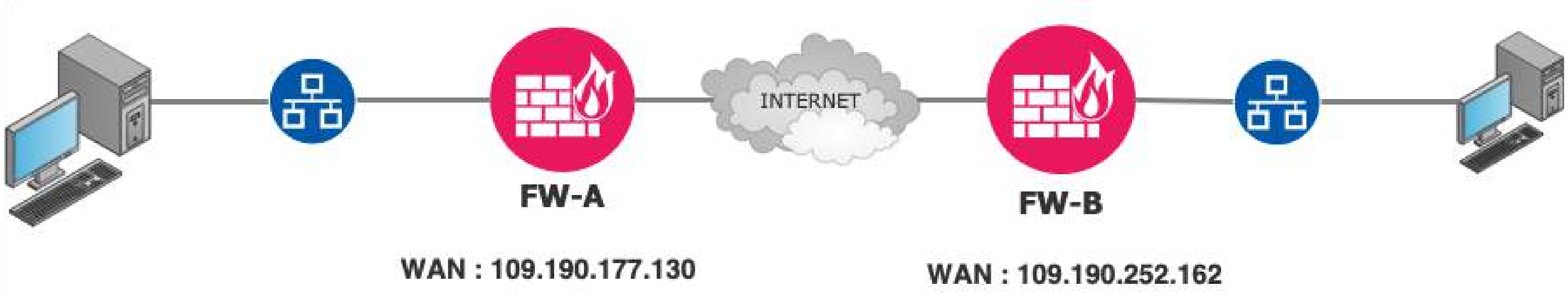
- Potential causes
  - Wrong WAN interface selected for the local gateway



```
No.  Time      Source           Destination      Protocol  SrcPort  DstPort  Length  Exchange type  Initiator SPI     Responder SPI     ESP SPI
  1  15:15:52  109.190.177.130  109.190.252.162  ISAKMP    500      500         662  IKE_SA_INIT    40b5b292e65d8431  0000000000000000
  2  15:15:56  109.190.177.130  109.190.252.162  ISAKMP    500      500         662  IKE_SA_INIT    40b5b292e65d8431  0000000000000000
  3  15:16:00  109.190.177.130  109.190.252.162  ISAKMP    500      500         662  IKE_SA_INIT    40b5b292e65d8431  0000000000000000
  4  15:16:04  109.190.177.130  109.190.252.162  ISAKMP    500      500         662  IKE_SA_INIT    40b5b292e65d8431  0000000000000000
```

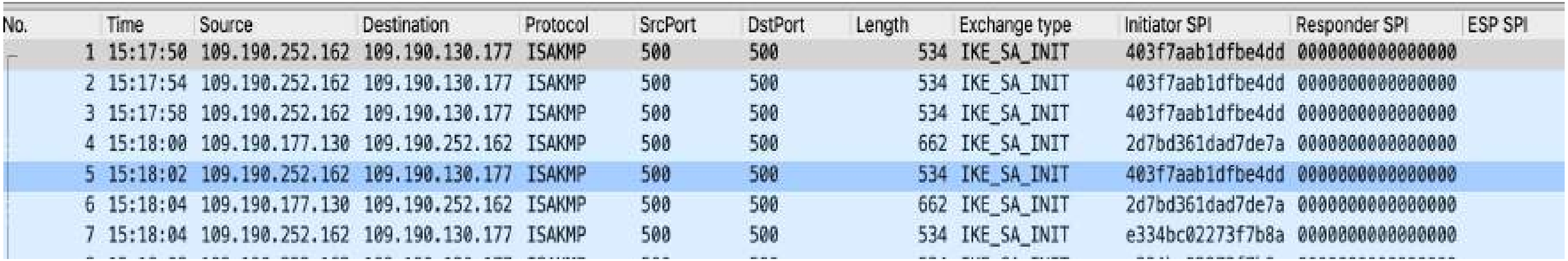
Case 4

- Context
  - Site A : Firewall-A 109.190.177.230
  - Site B : Firewall-B 109.190.252.162
- Symptoms (On site B):
  - Only IKE SA Init from both sites



Case 4

- Potential causes
  - At least one wrong IP (109.190.130.177) in the configuration of phase 1



No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Length	Exchange type	Initiator SPI	Responder SPI	ESP SPI
1	15:17:50	109.190.252.162	109.190.130.177	ISAKMP	500	500	534	IKE_SA_INIT	403f7aab1dfbe4dd	0000000000000000	
2	15:17:54	109.190.252.162	109.190.130.177	ISAKMP	500	500	534	IKE_SA_INIT	403f7aab1dfbe4dd	0000000000000000	
3	15:17:58	109.190.252.162	109.190.130.177	ISAKMP	500	500	534	IKE_SA_INIT	403f7aab1dfbe4dd	0000000000000000	
4	15:18:00	109.190.177.130	109.190.252.162	ISAKMP	500	500	662	IKE_SA_INIT	2d7bd361dad7de7a	0000000000000000	
5	15:18:02	109.190.252.162	109.190.130.177	ISAKMP	500	500	534	IKE_SA_INIT	403f7aab1dfbe4dd	0000000000000000	
6	15:18:04	109.190.177.130	109.190.252.162	ISAKMP	500	500	662	IKE_SA_INIT	2d7bd361dad7de7a	0000000000000000	
7	15:18:04	109.190.252.162	109.190.130.177	ISAKMP	500	500	534	IKE_SA_INIT	e334bc02273f7b8a	0000000000000000	

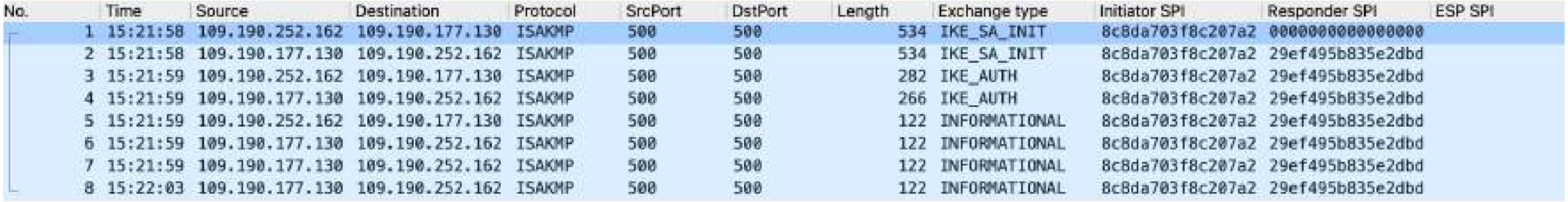
Case 5

- Context
  - Site A : Firewall-A 109.190.177.230
  - Site B : Firewall-B 109.190.252.162

- Symptoms (On site B):
  - Only IKE trafic from both sites
  - No create child attempts

Case 5

- Potential causes
  - Wrong ID ou Authentication data in phasis 1



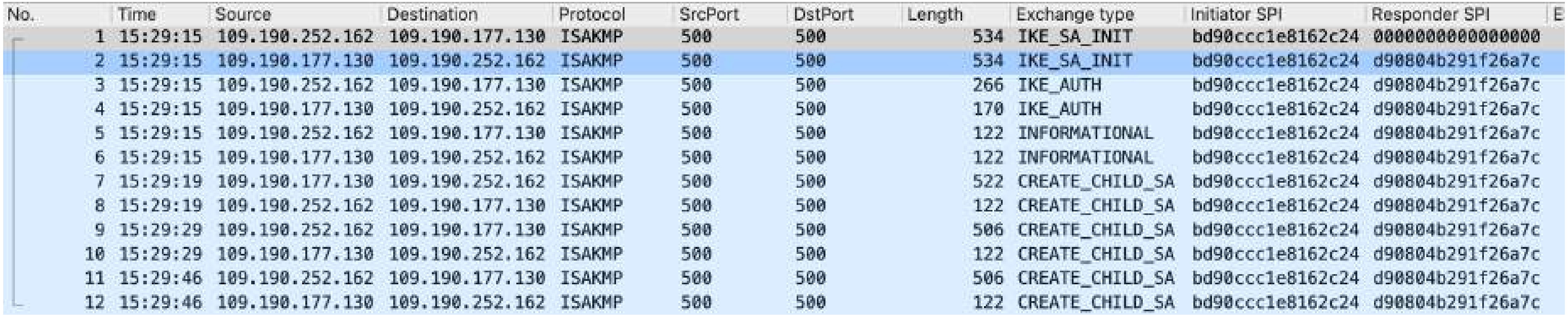
No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Length	Exchange type	Initiator SPI	Responder SPI	ESP SPI
1	15:21:58	109.190.252.162	109.190.177.130	ISAKMP	500	500	534	IKE_SA_INIT	8c8da703f8c207a2	0000000000000000	
2	15:21:58	109.190.177.130	109.190.252.162	ISAKMP	500	500	534	IKE_SA_INIT	8c8da703f8c207a2	29ef495b835e2dbd	
3	15:21:59	109.190.252.162	109.190.177.130	ISAKMP	500	500	282	IKE_AUTH	8c8da703f8c207a2	29ef495b835e2dbd	
4	15:21:59	109.190.177.130	109.190.252.162	ISAKMP	500	500	266	IKE_AUTH	8c8da703f8c207a2	29ef495b835e2dbd	
5	15:21:59	109.190.252.162	109.190.177.130	ISAKMP	500	500	122	INFORMATIONAL	8c8da703f8c207a2	29ef495b835e2dbd	
6	15:21:59	109.190.177.130	109.190.252.162	ISAKMP	500	500	122	INFORMATIONAL	8c8da703f8c207a2	29ef495b835e2dbd	
7	15:21:59	109.190.177.130	109.190.252.162	ISAKMP	500	500	122	INFORMATIONAL	8c8da703f8c207a2	29ef495b835e2dbd	
8	15:22:03	109.190.177.130	109.190.252.162	ISAKMP	500	500	122	INFORMATIONAL	8c8da703f8c207a2	29ef495b835e2dbd	

Case 6

- Context
  - Site A : Firewall-A 109.190.177.230
  - Site B : Firewall-B 109.190.252.162
- Symptoms (On site B):
  - IKE SA established but many create child attempts unsuccesful
  - Without decryption we can only see that we don't go beyond the CREATE_CHILD
- Files : Case6_FirewallB, Case6_FirewallA

Case 6

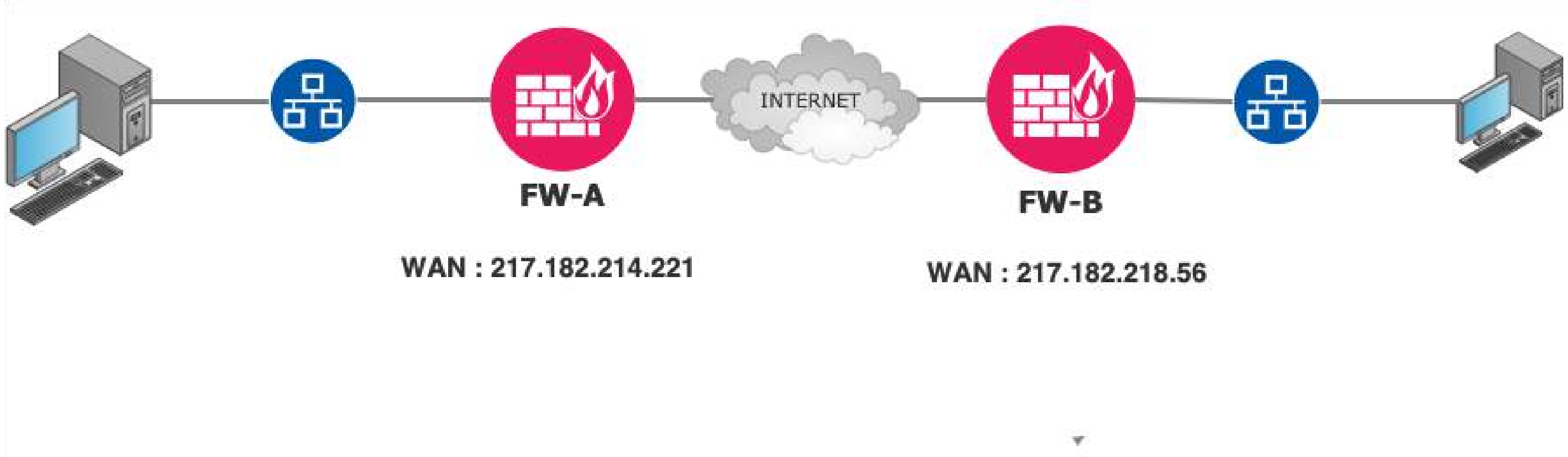
- Potential causes
  - Wrong phasis 2 parameters
  - We have to check all the phase 2 (tunnels) configuration



No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Length	Exchange type	Initiator SPI	Responder SPI	E
1	15:29:15	109.190.252.162	109.190.177.130	ISAKMP	500	500	534	IKE_SA_INIT	bd90ccc1e8162c24	0000000000000000	
2	15:29:15	109.190.177.130	109.190.252.162	ISAKMP	500	500	534	IKE_SA_INIT	bd90ccc1e8162c24	d90804b291f26a7c	
3	15:29:15	109.190.252.162	109.190.177.130	ISAKMP	500	500	266	IKE_AUTH	bd90ccc1e8162c24	d90804b291f26a7c	
4	15:29:15	109.190.177.130	109.190.252.162	ISAKMP	500	500	170	IKE_AUTH	bd90ccc1e8162c24	d90804b291f26a7c	
5	15:29:15	109.190.252.162	109.190.177.130	ISAKMP	500	500	122	INFORMATIONAL	bd90ccc1e8162c24	d90804b291f26a7c	
6	15:29:15	109.190.177.130	109.190.252.162	ISAKMP	500	500	122	INFORMATIONAL	bd90ccc1e8162c24	d90804b291f26a7c	
7	15:29:19	109.190.177.130	109.190.252.162	ISAKMP	500	500	522	CREATE_CHILD_SA	bd90ccc1e8162c24	d90804b291f26a7c	
8	15:29:19	109.190.252.162	109.190.177.130	ISAKMP	500	500	122	CREATE_CHILD_SA	bd90ccc1e8162c24	d90804b291f26a7c	
9	15:29:29	109.190.252.162	109.190.177.130	ISAKMP	500	500	506	CREATE_CHILD_SA	bd90ccc1e8162c24	d90804b291f26a7c	
10	15:29:29	109.190.177.130	109.190.252.162	ISAKMP	500	500	122	CREATE_CHILD_SA	bd90ccc1e8162c24	d90804b291f26a7c	
11	15:29:46	109.190.252.162	109.190.177.130	ISAKMP	500	500	506	CREATE_CHILD_SA	bd90ccc1e8162c24	d90804b291f26a7c	
12	15:29:46	109.190.177.130	109.190.252.162	ISAKMP	500	500	122	CREATE_CHILD_SA	bd90ccc1e8162c24	d90804b291f26a7c	

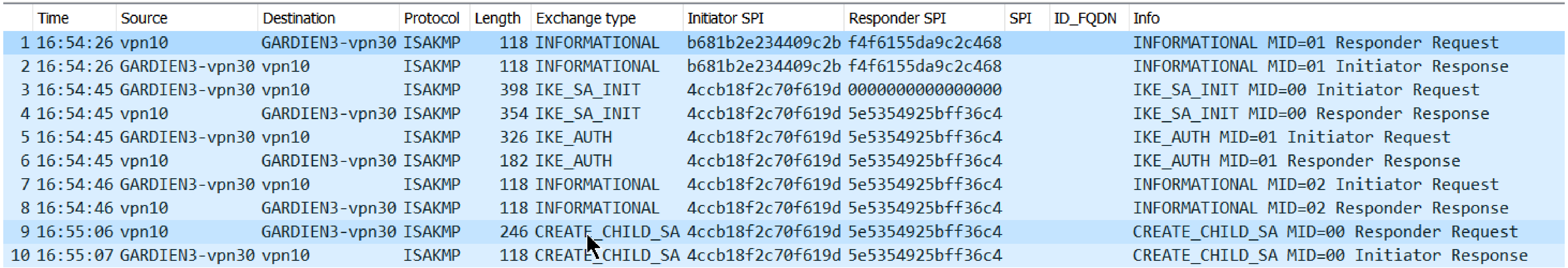
Case 6bis

- Context
  - Site A : vpn10 (217.182.214.221)
  - Site B : GARDIEN3 (217.182.218.56)
- Symptoms :
  - IKE SA established but no Child or IPSEC SA



Case 6bis - What we see in Wireshark

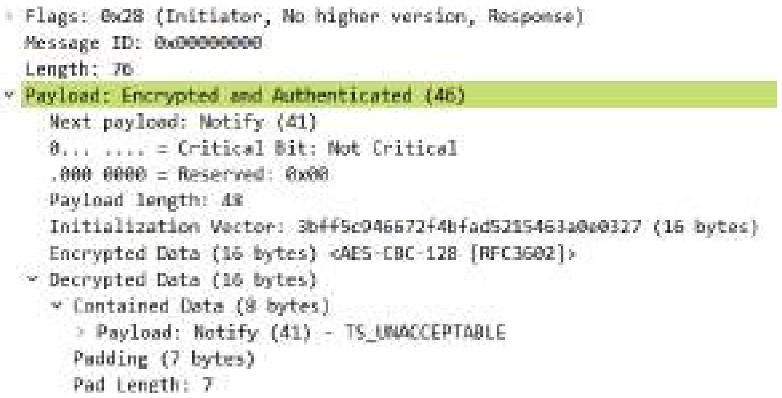
- Without decryption we can only see that we don't go beyond the CREATE_CHILD



	Time	Source	Destination	Protocol	Length	Exchange type	Initiator SPI	Responder SPI	SPI	ID_FQDN	Info
1	16:54:26	vpn10	GARDIEN3-vpn30	ISAKMP	118	INFORMATIONAL	b681b2e234409c2b	f4f6155da9c2c468			INFORMATIONAL MID=01 Responder Request
2	16:54:26	GARDIEN3-vpn30	vpn10	ISAKMP	118	INFORMATIONAL	b681b2e234409c2b	f4f6155da9c2c468			INFORMATIONAL MID=01 Initiator Response
3	16:54:45	GARDIEN3-vpn30	vpn10	ISAKMP	398	IKE_SA_INIT	4ccb18f2c70f619d	0000000000000000			IKE_SA_INIT MID=00 Initiator Request
4	16:54:45	vpn10	GARDIEN3-vpn30	ISAKMP	354	IKE_SA_INIT	4ccb18f2c70f619d	5e5354925bff36c4			IKE_SA_INIT MID=00 Responder Response
5	16:54:45	GARDIEN3-vpn30	vpn10	ISAKMP	326	IKE_AUTH	4ccb18f2c70f619d	5e5354925bff36c4			IKE_AUTH MID=01 Initiator Request
6	16:54:45	vpn10	GARDIEN3-vpn30	ISAKMP	182	IKE_AUTH	4ccb18f2c70f619d	5e5354925bff36c4			IKE_AUTH MID=01 Responder Response
7	16:54:46	GARDIEN3-vpn30	vpn10	ISAKMP	118	INFORMATIONAL	4ccb18f2c70f619d	5e5354925bff36c4			INFORMATIONAL MID=02 Initiator Request
8	16:54:46	vpn10	GARDIEN3-vpn30	ISAKMP	118	INFORMATIONAL	4ccb18f2c70f619d	5e5354925bff36c4			INFORMATIONAL MID=02 Responder Response
9	16:55:06	vpn10	GARDIEN3-vpn30	ISAKMP	246	CREATE_CHILD_SA	4ccb18f2c70f619d	5e5354925bff36c4			CREATE_CHILD_SA MID=00 Responder Request
10	16:55:07	GARDIEN3-vpn30	vpn10	ISAKMP	118	CREATE_CHILD_SA	4ccb18f2c70f619d	5e5354925bff36c4			CREATE_CHILD_SA MID=00 Initiator Response

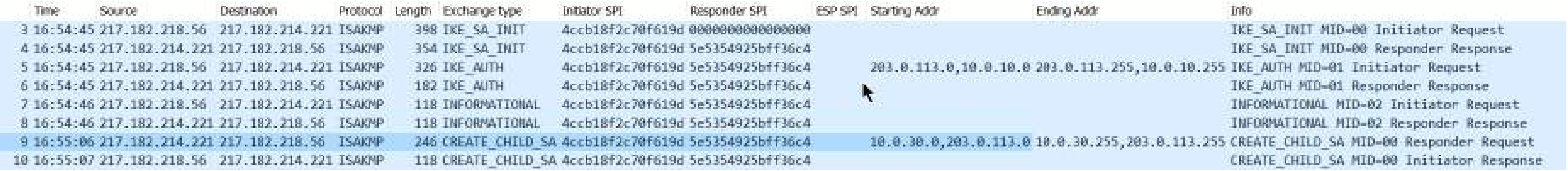
- We need unencrypted packets

Case 6bis – unencrypted IKE packets



```
› Flags: 0x28 (Initiator, No higher version, Response)
  Message ID: 0x00000000
  Length: 76
˅ Payload: Encrypted and Authenticated (46)
    Next payload: Notify (41)
    0... .... = Critical Bit: Not Critical
    .000 0000 = Reserved: 0x00
    Payload length: 48
    Initialization Vector: 3bff5c946672f4bfad5215463a0e0327 (16 bytes)
    Encrypted Data (16 bytes) <AES-CBC-128 [RFC3602]>
  ˅ Decrypted Data (16 bytes)
    ˅ Contained Data (8 bytes)
      › Payload: Notify (41) - TS_UNACCEPTABLE
      Padding (7 bytes)
      Pad Length: 7
```

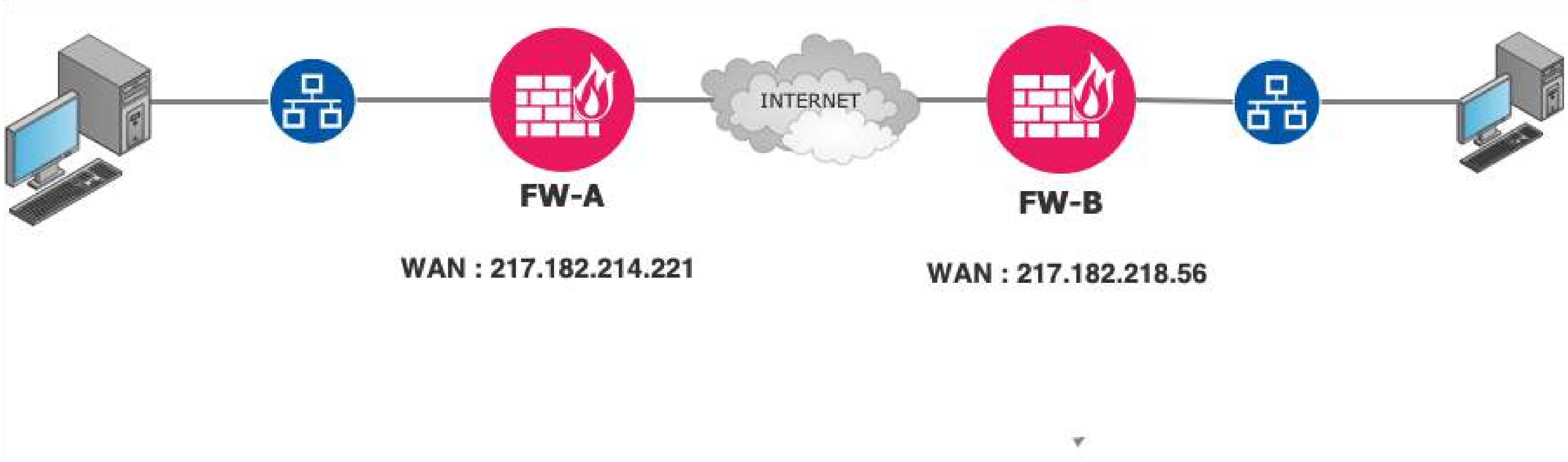
- Explanation : mismatch between the networks used for traffic selector
  - We need to check the network in the settings or in the capture



	Time	Source	Destination	Protocol	Length	Exchange type	Initator SPI	Responder SPI	ESP SPI	Starting Addr	Ending Addr	Info
3	16:54:45	217.182.218.56	217.182.214.221	ISAKMP	398	IKE_SA_INIT	4ccb18f2c70f619d	0000000000000000				IKE_SA_INIT MID=00 Initiator Request
4	16:54:45	217.182.214.221	217.182.218.56	ISAKMP	354	IKE_SA_INIT	4ccb18f2c70f619d	5e5354925bff36c4				IKE_SA_INIT MID=00 Responder Response
5	16:54:45	217.182.218.56	217.182.214.221	ISAKMP	326	IKE_AUTH	4ccb18f2c70f619d	5e5354925bff36c4		203.0.113.0,10.0.10.0	203.0.113.255,10.0.10.255	IKE_AUTH MID=01 Initiator Request
6	16:54:45	217.182.214.221	217.182.218.56	ISAKMP	182	IKE_AUTH	4ccb18f2c70f619d	5e5354925bff36c4				IKE_AUTH MID=01 Responder Response
7	16:54:46	217.182.218.56	217.182.214.221	ISAKMP	118	INFORMATIONAL	4ccb18f2c70f619d	5e5354925bff36c4				INFORMATIONAL MID=02 Initiator Request
8	16:54:46	217.182.214.221	217.182.218.56	ISAKMP	118	INFORMATIONAL	4ccb18f2c70f619d	5e5354925bff36c4				INFORMATIONAL MID=02 Responder Response
9	16:55:06	217.182.214.221	217.182.218.56	ISAKMP	246	CREATE_CHILD_SA	4ccb18f2c70f619d	5e5354925bff36c4		10.0.30.0,203.0.113.0	10.0.30.255,203.0.113.255	CREATE_CHILD_SA MID=00 Responder Request
10	16:55:07	217.182.218.56	217.182.214.221	ISAKMP	118	CREATE_CHILD_SA	4ccb18f2c70f619d	5e5354925bff36c4				CREATE_CHILD_SA MID=00 Initiator Response

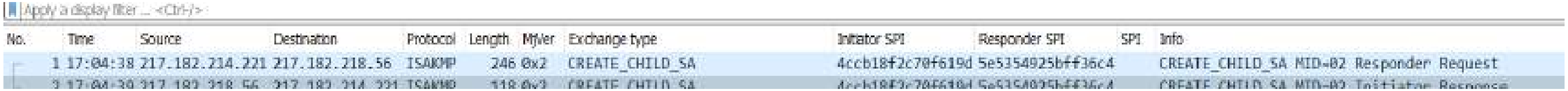
Case 6ter

- Context
  - Site A : vpn10 (217.182.214.221)
  - Site B : GARDIEN3 (217.182.218.56)
- Symptoms :
  - IKE SA established but no Child or IPSEC SA



Case 6 ter - What we see in Wireshark

- Without decryption we can only see that we don't go beyond the CREATE_CHILD

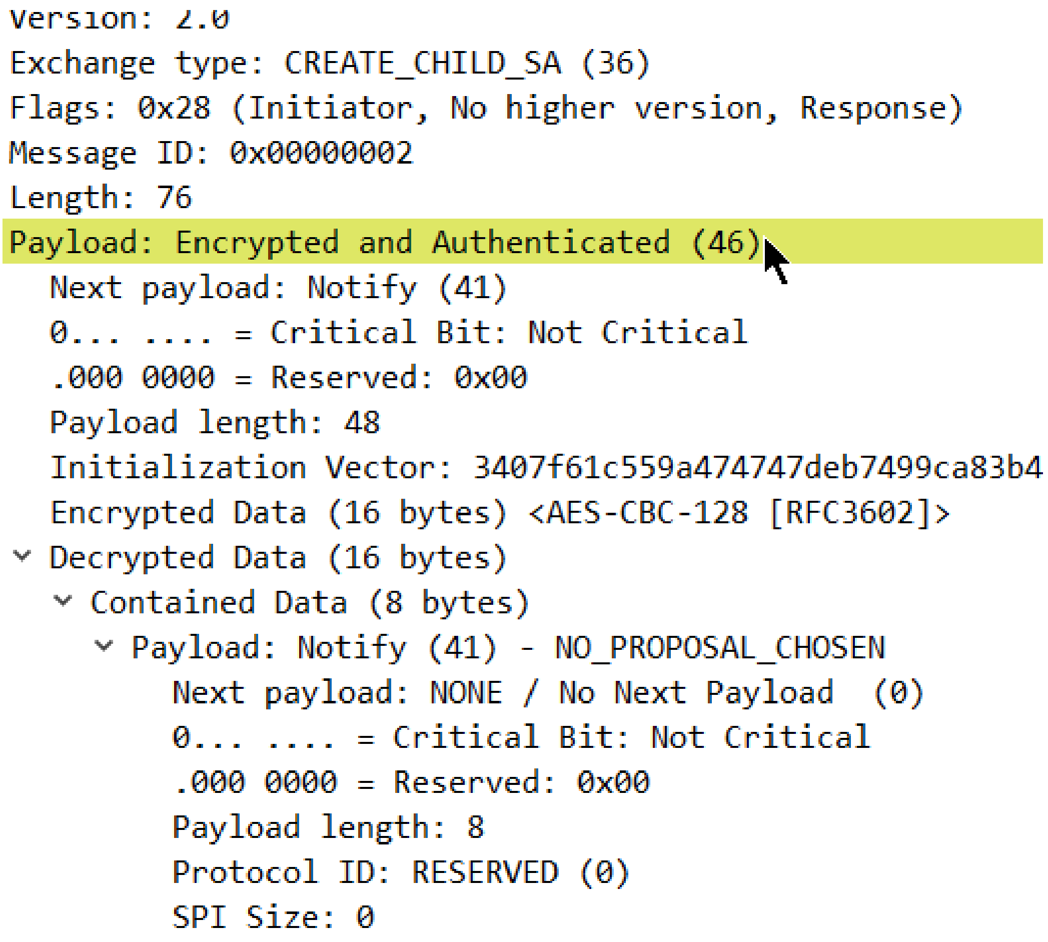


Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	MjVer	Exchange type	Initiator SPI	Responder SPI	SPI	Info
1	17:04:38	217.182.214.221	217.182.218.56	ISAKMP	246	0x2	CREATE_CHILD_SA	4ccb18f2c70f619d	5e5354925bff36c4		CREATE_CHILD_SA MID=02 Responder Request
2	17:04:39	217.182.218.56	217.182.214.221	ISAKMP	118	0x2	CREATE_CHILD_SA	4ccb18f2c70f619d	5e5354925bff36c4		CREATE_CHILD_SA MID=02 Initiator Response

- We need unencrypted packets

Case 8 – unencrypted IKE packets



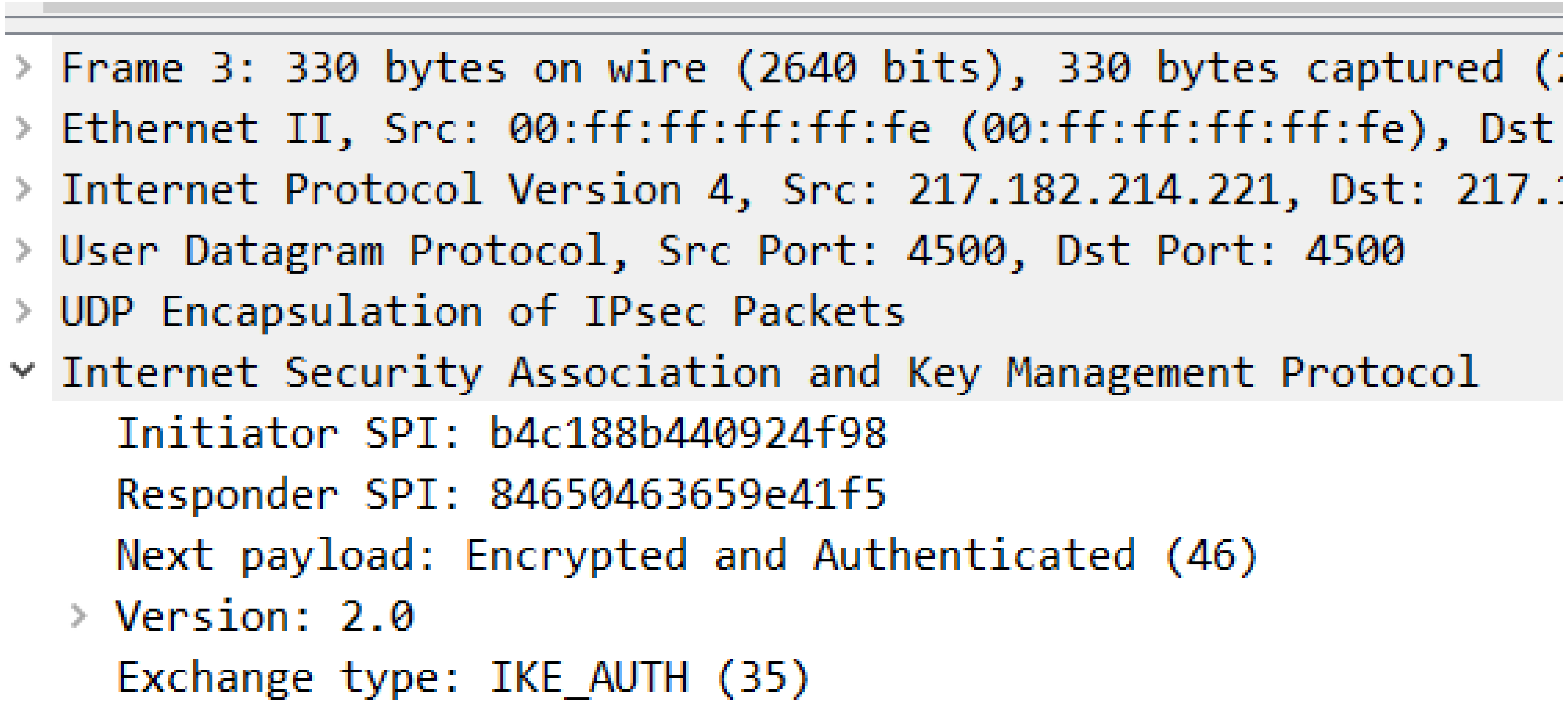
```
Version: 2.0
Exchange type: CREATE_CHILD_SA (36)
Flags: 0x28 (Initiator, No higher version, Response)
Message ID: 0x00000002
Length: 76
Payload: Encrypted and Authenticated (46)
  Next payload: Notify (41)
  0... .... = Critical Bit: Not Critical
  .000 0000 = Reserved: 0x00
  Payload length: 48
  Initialization Vector: 3407f61c559a474747deb7499ca83b4
  Encrypted Data (16 bytes) <AES-CBC-128 [RFC3602]>
⌄ Decrypted Data (16 bytes)
  ⌄ Contained Data (8 bytes)
    ⌄ Payload: Notify (41) - NO_PROPOSAL_CHOSEN
        Next payload: NONE / No Next Payload  (0)
        0... .... = Critical Bit: Not Critical
        .000 0000 = Reserved: 0x00
        Payload length: 8
        Protocol ID: RESERVED (0)
        SPI Size: 0
```

- Explanation : mismatch between the ESP settings : NO PROPOSAL CHOSEN is sent by the responder
  - We need to check the settings

How to get unencrypted IPsec packets ?

What do we need to decrypt ISAKMP ?

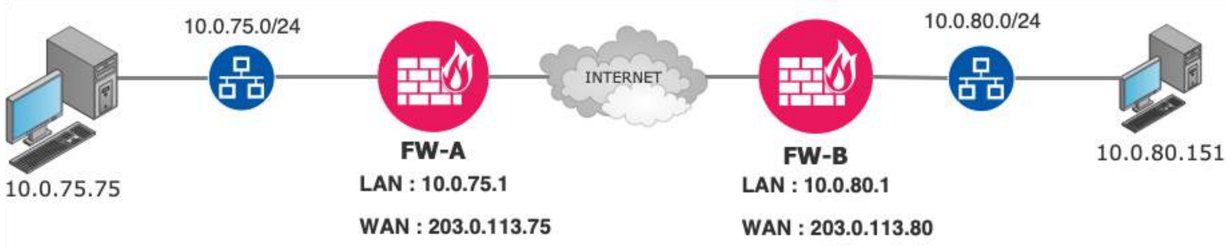
- SPI for initiator and responder
  - Very easy to get from the capture



```
> Frame 3: 330 bytes on wire (2640 bits), 330 bytes captured (
> Ethernet II, Src: 00:ff:ff:ff:ff:fe (00:ff:ff:ff:ff:fe), Dst
> Internet Protocol Version 4, Src: 217.182.214.221, Dst: 217.
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
v Internet Security Association and Key Management Protocol
    Initiator SPI: b4c188b440924f98
    Responder SPI: 84650463659e41f5
    Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
    Exchange type: IKE_AUTH (35)
```

Getting ISAKMP keys

- Seed Encryption Keys
  - Only possible if one endpoint displays them in some logs
  - Methods very variable from one device to another
  - Not always available
- Visible only when IKE SA is created



Getting ISAKMP keys with Fortinet

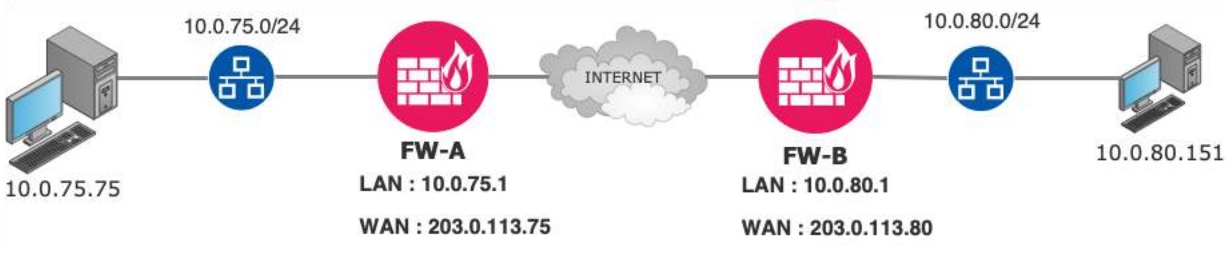
- Encryption and authentication keys
  - SK_ei : encryption key for initiator
  - SK_er : encryption key for responder
  - SK_ai : authentication key for initiator
  - SK_ar : authentication key for responder

Getting ISAKMP keys with a Firewall Fortinet?

- With a fortinet we can use a CLI command
- Command : diagnose vpn ike gateway list

File : Deciphering_Forti.pcap

```
…
  id/spi: 72 1a63972ed7410623/8f0c0c220060d9f5
  direction: initiator
  status: established 184-180s ago = 3480ms
  proposal: aes256-sha256
  child: no
  SK_ei: 2808e0d7b372a1fe01eb94a31b98e0e7268bfc4863bacf44e65e6917b25d515b
  SK_er: d3dea737acbefa7932e3fab795ba801981467e75d32a81795a0c907297aa909c
  SK_ai: 04aa8b344b66c8aef90ee17ba0203a537c17c85737a8bfa225943ee6655ba29c
  SK_ar: f937908926020d5defa9095117e22297717d1a3889b9f29bfa3d12a1110086e3
  PPK: no
  message-id sent/recv: 3/2
  lifetime/rekey: 86400/85919
  DPD sent/recv: 00000098/00000098
  peer-id: 203.0.113.80
```



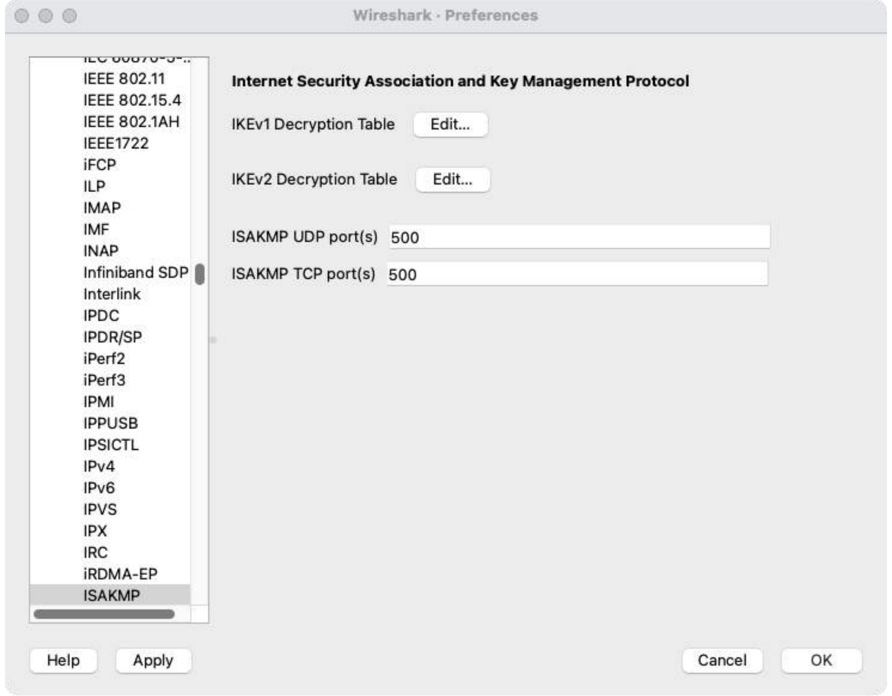
Getting ISAKMP keys with a Firewall Fortinet?

- in StrongSwan we need level 4 for logs
- Command : ipsec stroke level ike 4

```
Nov  1 14:58:50 15[IKE] Sk_ai secret => 20 bytes @ 0x7fbcec002f30
Nov  1 14:58:50 15[IKE]    0: 15 B0 04 95 A3 CF 26 95 82 AB DE E5 F9 35 0F 3E  ......&......5.>
Nov  1 14:58:50 15[IKE]   16: FF 0D BF AB                                      ....
Nov  1 14:58:50 15[IKE] Sk_ar secret => 20 bytes @ 0x7fbcec003140
Nov  1 14:58:50 15[IKE]    0: 10 F5 D6 37 15 FD 96 4F 50 8C D8 BE A2 C4 CA C0  ...7...OP.......
Nov  1 14:58:50 15[IKE]   16: AB 27 4E 67                                      .'Ng
Nov  1 14:58:50 15[IKE] Sk_ei secret => 16 bytes @ 0x7fbcec003240
Nov  1 14:58:50 15[IKE]    0: 3E B4 8A 06 96 1B 46 37 3A 5F 6F 1D 91 4B F2 3A  >.....F7:_o..K.:
Nov  1 14:58:50 15[IKE] Sk_er secret => 16 bytes @ 0x7fbcec003550
Nov  1 14:58:50 15[IKE]    0: 23 ED 30 24 CD 51 B6 65 07 32 7D 5F A7 69 59 45  #.0$.Q.e.2}_.iYEz
```

Decrypting IKE version 2 in Wireshark

- Preferences – Protocols ISAKMP
- Enter keys and IKE SPI in IKEv2 Table



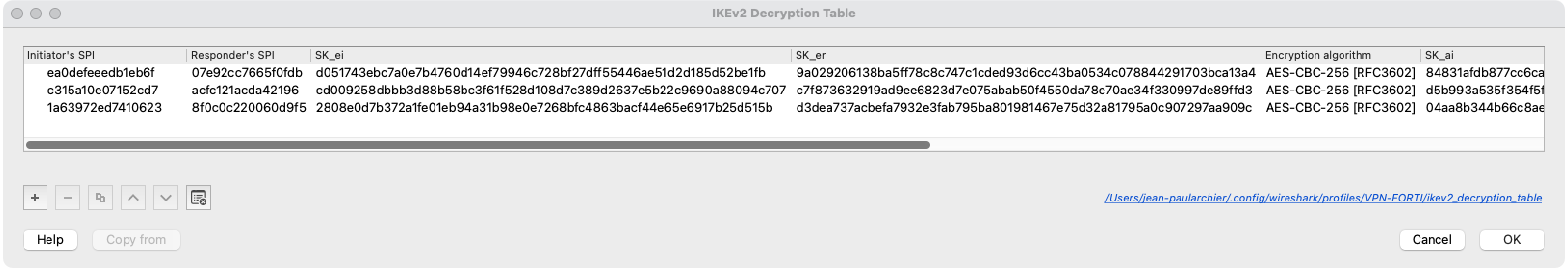
Internet Security Association and Key Management Protocol

IKEv1 Decryption Table Edit...

IKEv2 Decryption Table Edit...

ISAKMP UDP port(s) 500

ISAKMP TCP port(s) 500

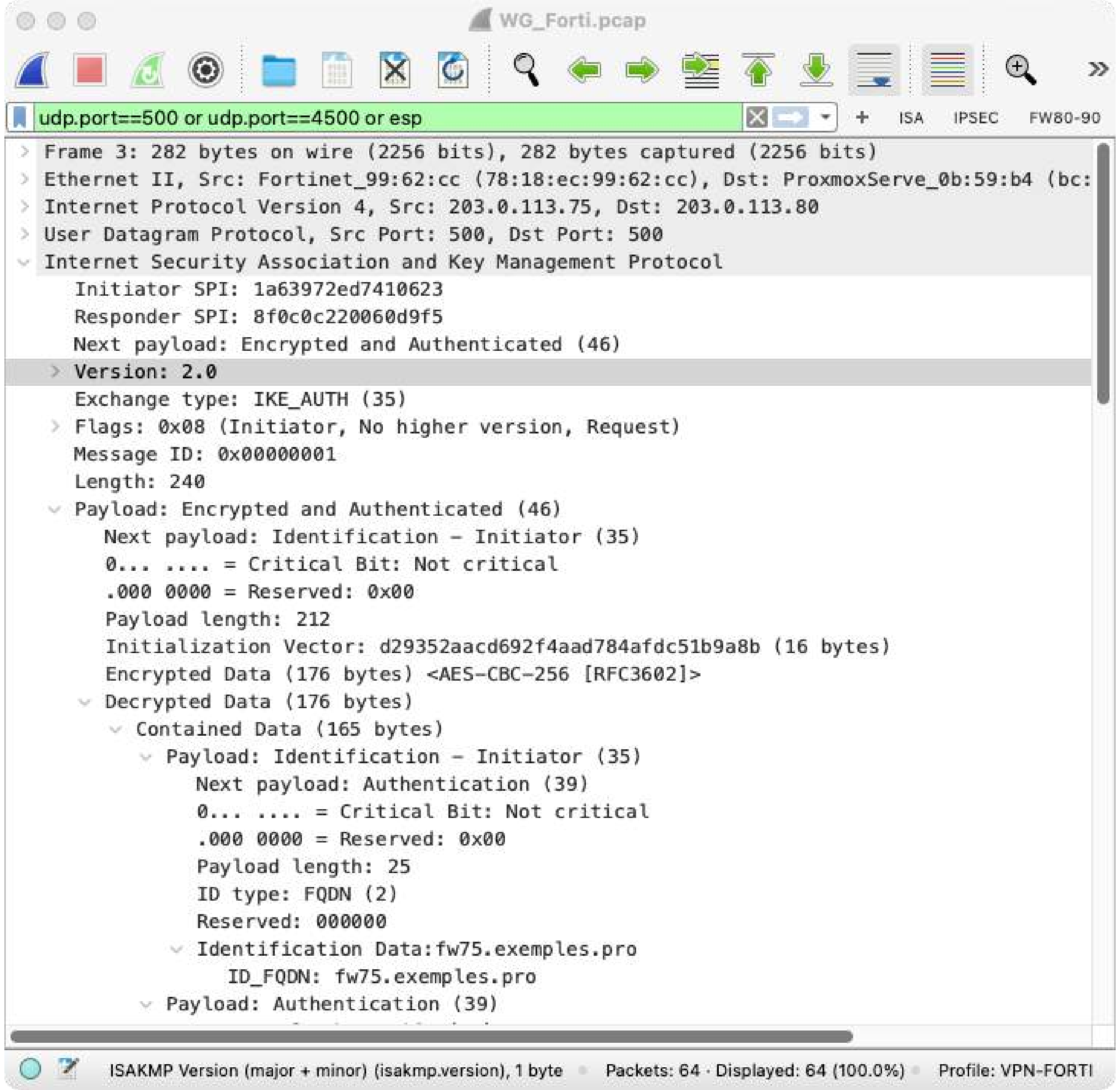


Initiator's SPI	Responder's SPI	SK_ei	SK_er	Encryption algorithm	SK_ai
ea0defeeedb1eb6f	07e92cc7665f0fdb	d051743ebc7a0e7b4760d14ef79946c728bf27dff55446ae51d2d185d52be1fb	9a029206138ba5ff78c8c747c1cded93d6cc43ba0534c078844291703bca13a4	AES-CBC-256 [RFC3602]	84831afdb877cc6ca
c315a10e07152cd7	acfc121acda42196	cd009258dbbb3d88b58bc3f61f528d108d7c389d2637e5b22c9690a88094c707	c7f873632919ad9ee6823d7e075abab50f4550da78e70ae34f330997de89ffd3	AES-CBC-256 [RFC3602]	d5b993a535f354f5f
1a63972ed7410623	8f0c0c220060d9f5	2808e0d7b372a1fe01eb94a31b98e0e7268bfc4863bacf44e65e6917b25d515b	d3dea737acbefa7932e3fab795ba801981467e75d32a81795a0c907297aa909c	AES-CBC-256 [RFC3602]	04aa8b344b66c8ae

/Users/jean-paularchier/.config/wireshark/profiles/VPN-FORTI/ikev2_decryption_table

Results of decryption for IKE

- Visible in 3rd and 4th packets of IKE exchanges
  - Algorithms
  - Traffic selector
  - Identification data



udp.port==500 or udp.port==4500 or esp

```
> Frame 3: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits)
> Ethernet II, Src: Fortinet_99:62:cc (78:18:ec:99:62:cc), Dst: ProxmoxServe_0b:59:b4 (bc:
> Internet Protocol Version 4, Src: 203.0.113.75, Dst: 203.0.113.80
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 1a63972ed7410623
    Responder SPI: 8f0c0c220060d9f5
    Next payload: Encrypted and Authenticated (46)
  > Version: 2.0
    Exchange type: IKE_AUTH (35)
  > Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000001
    Length: 240
  v Payload: Encrypted and Authenticated (46)
      Next payload: Identification - Initiator (35)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 212
      Initialization Vector: d29352aacd692f4aad784afdc51b9a8b (16 bytes)
      Encrypted Data (176 bytes) <AES-CBC-256 [RFC3602]>
    v Decrypted Data (176 bytes)
      v Contained Data (165 bytes)
        v Payload: Identification - Initiator (35)
            Next payload: Authentication (39)
            0... .... = Critical Bit: Not critical
            .000 0000 = Reserved: 0x00
            Payload length: 25
            ID type: FQDN (2)
            Reserved: 000000
          v Identification Data:fw75.exemples.pro
              ID_FQDN: fw75.exemples.pro
        v Payload: Authentication (39)
```

ISAKMP Version (major + minor) (isakmp.version), 1 byte · Packets: 64 · Displayed: 64 (100.0%) · Profile: VPN-FORTI

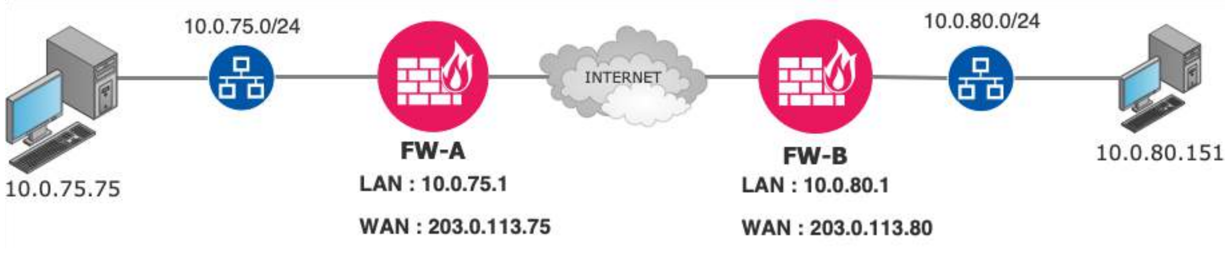
What do we need to decrypt ESP packets ?

- SPIs for both endpoint (clearly visible)
- Encryption and authentication algorithms (clearly visible)
- Encryption and authentication keys

Getting ESP keys with a Firewall Fortinet?

- With a fortinet we can use a CLI command
- Command : diagnose vpn tunnel list

```
FORTI40 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN80 ver=2 serial=1 203.0.113.75:0->203.0.113.80:0 nexthop=203.0.113.80 tun_id=203.0.113.80
…/…
  dec: spi=76551fab esp=aes key=32 1c240a3a5dfd66f0843856ab6280388da763170109989757de1a6d44e4ae0c49
       ah=sha256 key=32 9bbceb98be9d7db49a5e3713ea5dee2794f742cc982f2a883cf30e55ff3efc77
  enc: spi=d3822da0 esp=aes key=32 00688badb8c8fcf7000028821ce6c8aa687231f231d568deb4217e651031b805
       ah=sha256 key=32 47ef682717dcdfbacf0fb160410a950ede428d66bc2700e85fa9c6c3c80bab1d
…/…
```



Files :
WG_Forti.pcap

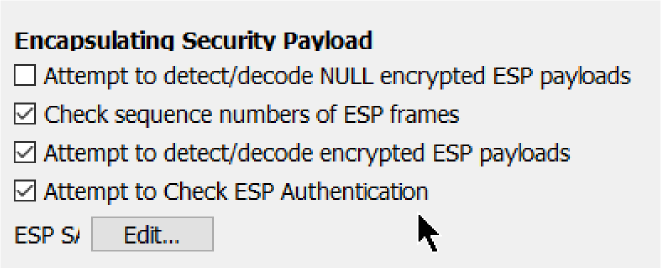
Getting keys on Strongswan?

- We must use
  - a debug loglevel of 4
  - the CLI command : ip xfrm state

```
root@vpn10:/var/log# ip xfrm state
src 217.182.214.221 dst 217.182.218.56
        proto esp spi 0x344d8192 reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha1) 0x55ae66efbd78a3eb9761e7c89771610cd6c365b9 96
        enc cbc(aes) 0x9a6fdb6af62c477cedf41bfac3e5cf43
        anti-replay context: seq 0x0, oseq 0x1e, bitmap 0x00000000
src 217.182.218.56 dst 217.182.214.221
        proto esp spi 0xc7418fbd reqid 1 mode tunnel
        replay-window 32 flag af-unspec
        auth-trunc hmac(sha1) 0x4b1be769e73d55ef2c5d851f9a7b79b3d894bf25 96
        enc cbc(aes) 0x2d95ca11f8cb25922c23a235bb3f6a85
        anti-replay context: seq 0x14, oseq 0x0, bitmap 0x000fffff
root@vpn10:/var/log#
```

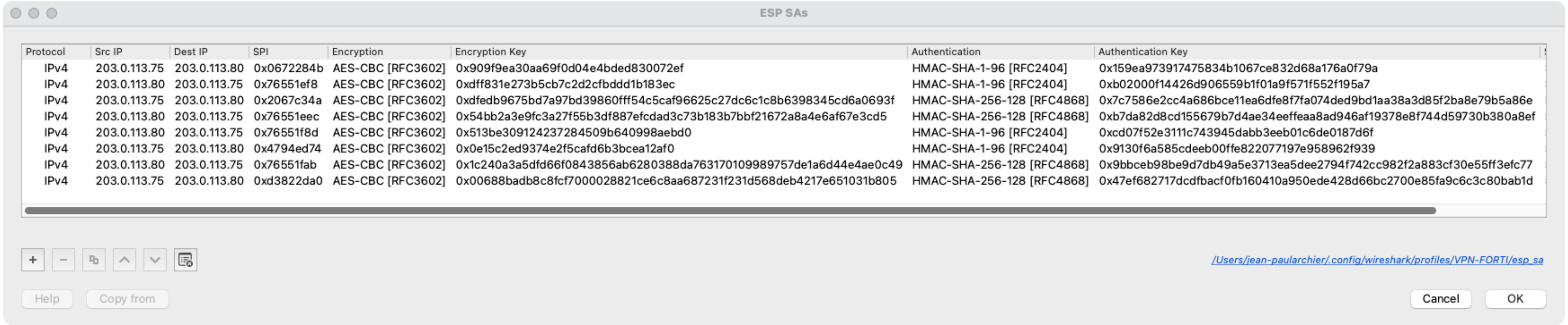
Decrypting ESP – next step ?

- Preferences – Protocols ESP – ESP SA
- Enter keys, SPI and algorithms with the Edit button



Encapsulating Security Payload

- □ Attempt to detect/decode NULL encrypted ESP payloads
- ☑ Check sequence numbers of ESP frames
- ☑ Attempt to detect/decode encrypted ESP payloads
- ☑ Attempt to Check ESP Authentication

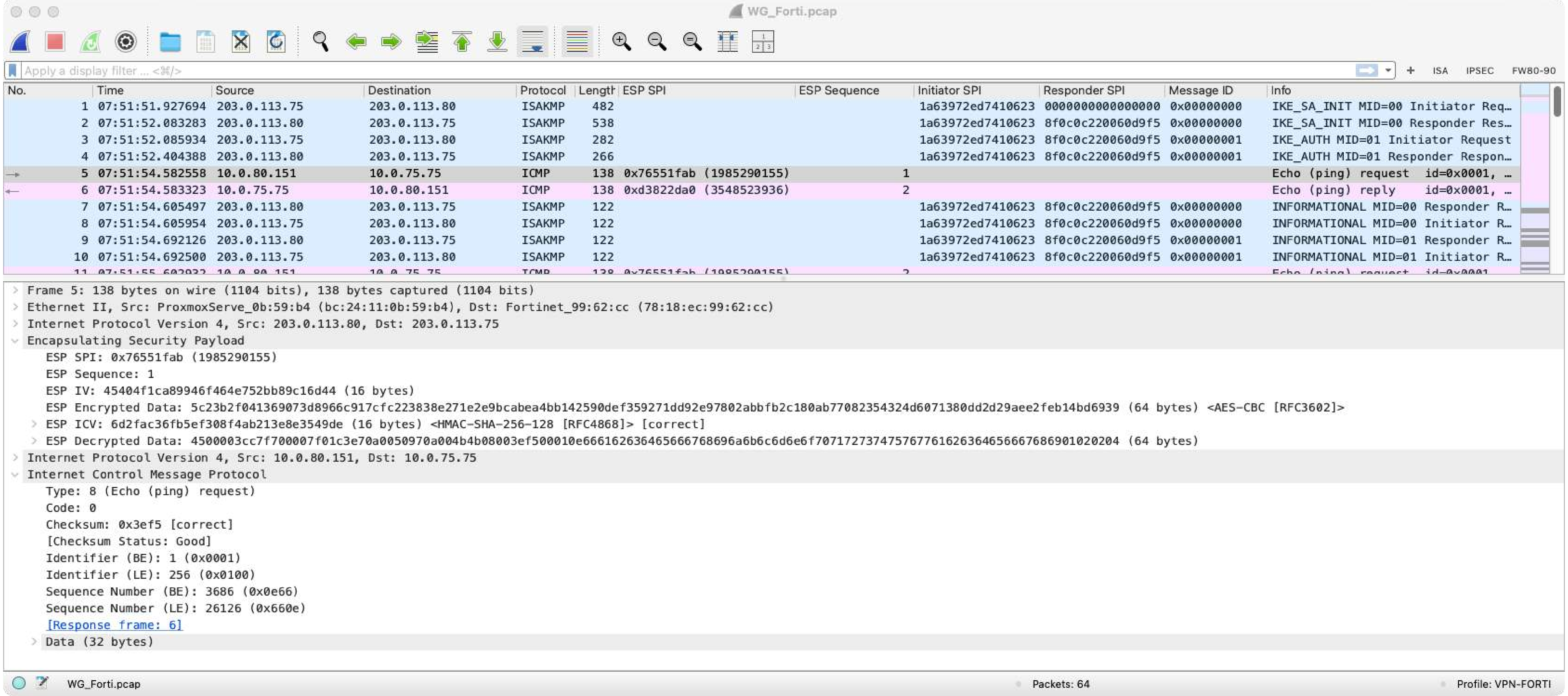


Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key	Authentication	Authentication Key
IPv4	203.0.113.75	203.0.113.80	0x0672284b	AES-CBC [RFC3602]	0x909f9ea30aa69f0d04e4bded830072ef	HMAC-SHA-1-96 [RFC2404]	0x159ea973917475834b1067ce832d68a176a0f79a
IPv4	203.0.113.80	203.0.113.75	0x76551ef8	AES-CBC [RFC3602]	0xdff831e273b5cb7c2d2cfbddd1b183ec	HMAC-SHA-1-96 [RFC2404]	0xb02000f14426d906559b1f01a9f571f552f195a7
IPv4	203.0.113.75	203.0.113.80	0x2067c34a	AES-CBC [RFC3602]	0xdfedb9675bd7a97bd39860fff54c5caf96625c27dc6c1c8b6398345cd6a0693f	HMAC-SHA-256-128 [RFC4868]	0x7c7586e2cc4a686bce11ea6dfe8f7fa074ded9bd1aa38a3d85f2ba8e79b5a86e
IPv4	203.0.113.80	203.0.113.75	0x76551eec	AES-CBC [RFC3602]	0x54bb2a3e9fc3a27f55b3df887efcdad3c73b183b7bbf21672a8a4e6af67e3cd5	HMAC-SHA-256-128 [RFC4868]	0xb7da82d8cd155679b7d4ae34eeffeaa8ad946af19378e8f744d59730b380a8ef
IPv4	203.0.113.80	203.0.113.75	0x76551f8d	AES-CBC [RFC3602]	0x513be309124237284509b640998aebd0	HMAC-SHA-1-96 [RFC2404]	0xcd07f52e3111c743945dabb3eeb01c6de0187d6f
IPv4	203.0.113.75	203.0.113.80	0x4794ed74	AES-CBC [RFC3602]	0x0e15c2ed9374e2f5cafd6b3bcea12af0	HMAC-SHA-1-96 [RFC2404]	0x9130f6a585cdeeb00ffe822077197e958962f939
IPv4	203.0.113.80	203.0.113.75	0x76551fab	AES-CBC [RFC3602]	0x1c240a3a5dfd66f0843856ab6280388da763170109989757de1a6d44e4ae0c49	HMAC-SHA-256-128 [RFC4868]	0x9bbceb98be9d7db49a5e3713ea5dee2794f742cc982f2a883cf30e55ff3efc77
IPv4	203.0.113.75	203.0.113.80	0xd3822da0	AES-CBC [RFC3602]	0x00688badb8c8fcf7000028821ce6c8aa687231f231d568deb4217e651031b805	HMAC-SHA-256-128 [RFC4868]	0x47ef682717dcdfbacf0fb160410a950ede428d66bc2700e85fa9c6c3c80bab1d

/Users/jean-paularchier/.config/wireshark/profiles/VPN-FORTI/esp_sa

ESP traffic decrypted

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



No.	Time	Source	Destination	Protocol	Length	ESP SPI	ESP Sequence	Initiator SPI	Responder SPI	Message ID	Info
1	07:51:51.927694	203.0.113.75	203.0.113.80	ISAKMP	482			1a63972ed7410623	0000000000000000	0x00000000	IKE_SA_INIT MID=00 Initiator Req…
2	07:51:52.083283	203.0.113.80	203.0.113.75	ISAKMP	538			1a63972ed7410623	8f0c0c220060d9f5	0x00000000	IKE_SA_INIT MID=00 Responder Res…
3	07:51:52.085934	203.0.113.75	203.0.113.80	ISAKMP	282			1a63972ed7410623	8f0c0c220060d9f5	0x00000001	IKE_AUTH MID=01 Initiator Request
4	07:51:52.404388	203.0.113.80	203.0.113.75	ISAKMP	266			1a63972ed7410623	8f0c0c220060d9f5	0x00000001	IKE_AUTH MID=01 Responder Respon…
→ 5	07:51:54.582558	10.0.80.151	10.0.75.75	ICMP	138	0x76551fab (1985290155)	1				Echo (ping) request id=0x0001, …
← 6	07:51:54.583323	10.0.75.75	10.0.80.151	ICMP	138	0xd3822da0 (3548523936)	2				Echo (ping) reply id=0x0001, …
7	07:51:54.605497	203.0.113.80	203.0.113.75	ISAKMP	122			1a63972ed7410623	8f0c0c220060d9f5	0x00000000	INFORMATIONAL MID=00 Responder R…
8	07:51:54.605954	203.0.113.75	203.0.113.80	ISAKMP	122			1a63972ed7410623	8f0c0c220060d9f5	0x00000000	INFORMATIONAL MID=00 Initiator R…
9	07:51:54.692126	203.0.113.80	203.0.113.75	ISAKMP	122			1a63972ed7410623	8f0c0c220060d9f5	0x00000001	INFORMATIONAL MID=01 Responder R…
10	07:51:54.692500	203.0.113.75	203.0.113.80	ISAKMP	122			1a63972ed7410623	8f0c0c220060d9f5	0x00000001	INFORMATIONAL MID=01 Initiator R…
11	07:51:55.602932	10.0.80.151	10.0.75.75	ICMP	138	0x76551fab (1985290155)	2				Echo (ping) request id=0x0001

```
> Frame 5: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
> Ethernet II, Src: ProxmoxServe_0b:59:b4 (bc:24:11:0b:59:b4), Dst: Fortinet_99:62:cc (78:18:ec:99:62:cc)
> Internet Protocol Version 4, Src: 203.0.113.80, Dst: 203.0.113.75
v Encapsulating Security Payload
    ESP SPI: 0x76551fab (1985290155)
    ESP Sequence: 1
    ESP IV: 45404f1ca89946f464e752bb89c16d44 (16 bytes)
    ESP Encrypted Data: 5c23b2f041369073d8966c917cfc223838e271e2e9bcabea4bb142590def359271dd92e97802abbfb2c180ab77082354324d6071380dd2d29aee2feb14bd6939 (64 bytes) <AES-CBC [RFC3602]>
  > ESP ICV: 6d2fac36fb5ef308f4ab213e8e3549de (16 bytes) <HMAC-SHA-256-128 [RFC4868]> [correct]
  > ESP Decrypted Data: 4500003cc7f700007f01c3e70a0050970a004b4b08003ef500010e666162636465666768696a6b6c6d6e6f707172737475767761626364656667686901020204 (64 bytes)
> Internet Protocol Version 4, Src: 10.0.80.151, Dst: 10.0.75.75
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x3ef5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 3686 (0x0e66)
    Sequence Number (LE): 26126 (0x660e)
    [Response frame: 6]
  > Data (32 bytes)
```

Conclusion

- Thank you for your attention !

- Please complete the session survey by using this Qrcode

- Contact
  - jean-paul@jpaconseil.com
  - www.jpaformation.com