NETWORK SECURITY

Université Libre de Bruxelles

Faculty of Sciences

Lab 3 - Virtual Private Networks (VPN)

Authors:

Croche Loïc
Hanquin Benjamin
Cochez Benjamin

May 9, 2021

I. Mission 1: Traffic observation

First of all, we tried the actual configuration by pinging PC2 and PC3 from PC1 (it also works with other PC's) to show if they correctly communicate with each other. We can see that, in Figure 1 and 2, the Router 3 is correctly configured. We can see that, in Figure 1 and 2, the Router3 is correctly configured. We do not display the configuration of Router 1, 2, 4 and 5 but they are also configured as it should.

```
PC1> ping 192.168.2.2

84 bytes from 192.168.2.2 icmp_seq=1 ttl=59 time=105.885 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=59 time=101.539 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=59 time=83.050 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=59 time=89.469 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=59 time=260.130 ms

PC1> ping 192.168.3.2

84 bytes from 192.168.3.2 icmp_seq=1 ttl=61 time=58.675 ms
84 bytes from 192.168.3.2 icmp_seq=2 ttl=61 time=53.140 ms
84 bytes from 192.168.3.2 icmp_seq=3 ttl=61 time=39.296 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=61 time=50.775 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=61 time=60.518 ms
```

Figure 1: Ping from PC1 to PC2 and PC3.

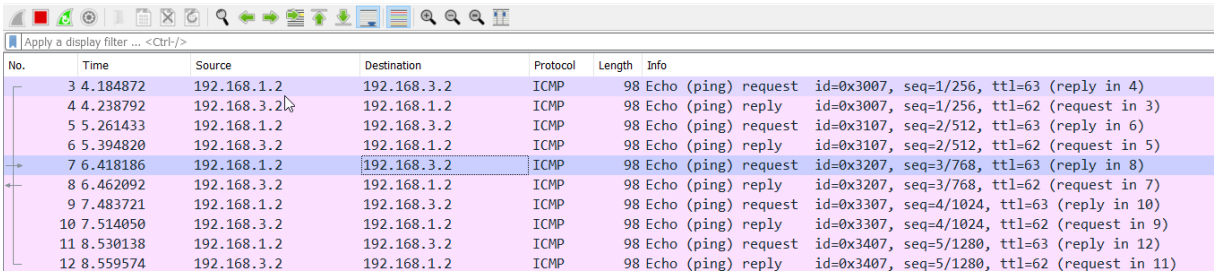
```
Router3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet0/1            10.0.2.2        YES NVRAM  up                    up
FastEthernet1/0            10.0.4.2        YES NVRAM  up                    up
Router3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 4 subnets
C       10.0.2.0 is directly connected, FastEthernet0/1
R       10.0.3.0 [120/1] via 10.0.4.1, 00:00:00, FastEthernet1/0
R       10.0.1.0 [120/2] via 10.0.4.1, 00:00:00, FastEthernet1/0
C       10.0.4.0 is directly connected, FastEthernet1/0
R    192.168.1.0/24 [120/3] via 10.0.4.1, 00:00:00, FastEthernet1/0
R    192.168.2.0/24 [120/1] via 10.0.2.1, 00:00:00, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 10.0.4.1, 00:00:00, FastEthernet1/0
```

Figure 2: Configuration of Router3.

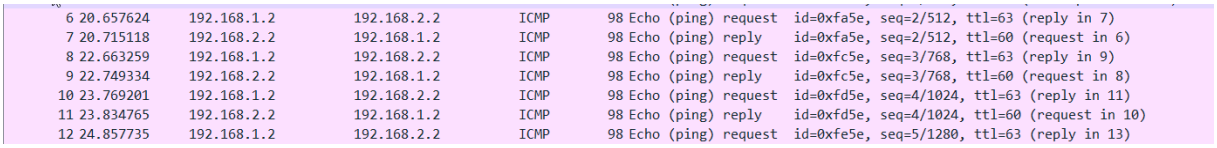
Once we looked if the configuration was correct, we analyzed the traffic between R1 and R4 with Wireshark to make sure that pings between PC1 and PC3 were in clear (same between PC1 and PC2). This is shown in figures 3 and 4.



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

No.	Time	Source	Destination	Protocol	Length	Info
3	4.184872	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x3007, seq=1/256, ttl=63 (reply in 4)
4	4.238792	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x3007, seq=1/256, ttl=62 (request in 3)
5	5.261433	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x3107, seq=2/512, ttl=63 (reply in 6)
6	5.394820	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x3107, seq=2/512, ttl=62 (request in 5)
7	6.418186	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x3207, seq=3/768, ttl=63 (reply in 8)
8	6.462092	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x3207, seq=3/768, ttl=62 (request in 7)
9	7.483721	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x3307, seq=4/1024, ttl=63 (reply in 10)
10	7.514050	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x3307, seq=4/1024, ttl=62 (request in 9)
11	8.530138	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x3407, seq=5/1280, ttl=63 (reply in 12)
12	8.559574	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x3407, seq=5/1280, ttl=62 (request in 11)

Figure 3: Analyze of ICMP packets between PC1 and PC3 with Wireshark.



6	20.657624	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0xfa5e, seq=2/512, ttl=63 (reply in 7)
7	20.715118	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0xfa5e, seq=2/512, ttl=60 (request in 6)
8	22.663259	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0xfc5e, seq=3/768, ttl=63 (reply in 9)
9	22.749334	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0xfc5e, seq=3/768, ttl=60 (request in 8)
10	23.769201	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0xfd5e, seq=4/1024, ttl=63 (reply in 11)
11	23.834765	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0xfd5e, seq=4/1024, ttl=60 (request in 10)
12	24.857735	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0xfe5e, seq=5/1280, ttl=63 (reply in 13)

Figure 4: Analyze of ICMP packets between PC1 and PC2 with Wireshark.

II. Mission 2: Site-to-site IPSec VPN

Now we will configure a Site-to-site IPSec VPN. IPSec is a L3 protocol, and it allows to create a secure communication tunnel between two remote L2 devices through internet, often two routers.

To set up an IPSec VPN, we must perform 2 phases. The first is the IKE (Internet Key Exchange) used to establish Security Associations (SA) through ISAKMP protocol. When we configure the IKE, we can choose some parameters like the type of symmetric encryption, the key exchange protocol, the integrity algorithm, the type of authentication, … The choice of these parameters is important because a bad configuration can lead to a vulnerability exploitation. For example, usage of SHA-1 is depreciated because it is a broken algorithm. In this implementation it is not really a problem but for a long-term implementation we should use as alternative SHA-256 (implicitly SHA2-256 which is second version of SHA-1) or even SHA-3 which is much more recent and should last longer than SHA-2. This choice can be done with "*hash {md5|sha|sha1-96|sha2-256-128|sha2-384-192}" as command (and choosing the hashing algorithm wanted)*. Same idea for the encryption algorithm, it is better to use AES instead of the default DES algorithm, that is also broken. The choice can be done using "*encryption {3DES|AES128|AES192|AES256|DES}*" as command.

Here we have router with IPsec feature, so ISAKMP/IKE is by default enabled. If we want to disable it: no crypto isakmp enable, and to enable it: crypto isakmp enable.

The group 2 command is pretty foggy when using it, but it is to configure the IKE Diffie Hellman group:

- 1(default): 768-bit Diffie Hellman prime modulus group.
- 2: 1024-bit Diffie Hellman prime modulus group
- 14: 2048-bit Diffie Hellman DDH prime modulus group
- 19: 256-bit random Diffie Hellman ECP modulus group
- 20: 384-bit random Diffie Hellman ECP modulus group

And finally in our implementation we did not specify any version. IKE exists in 2 versions (v1 and v2). To set the IKEv2 we would use the "*version {v1|v2}*" command. In IKEv2 a pseudo-random function (PRF) is used. By default, it is PRF-HMAC-MD5 but another version can be used using "*prf {PRF-HMAC-MD5|PRF-HMAC-SHA1|PRF-HMAC-SHA256|PRF-HMAC-SHA384}*".

```
Router1(config)#crypto isakmp policy 1
Router1(config-isakmp)#encr
Router1(config-isakmp)#encryption aes
Router1(config-isakmp)#hash sha
Router1(config-isakmp)#auth
Router1(config-isakmp)#authentication pre
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#group 2
Router1(config-isakmp)#lifetim
Router1(config-isakmp)#lifetime 86
Router1(config-isakmp)#lifetime 86400
Router1(config-isakmp)#exit
Router1(config)#copy ru
Router1(config)#copy ru
Router1(config)#copy r
Router1(config)#copy running-config startup-config
                ^
% Invalid input detected at '^' marker.

Router1(config)#exit
Router1#copy running-config startup-config
Destination filename [startup-config]?
*Mar  1 00:06:38.907: %SYS-5-CONFIG_I: Configured from console by console
```

Figure 5: ISAKMP configuration.

Final line of Figure 5 is to save the running-config. Without this command, all the configurations would be lost at restart of the router.

Because of we decided to choose the pre-share authentication, we had to choose a password, here we choose "securepassword" and assign this to the remote router which we want to communicate (here the Router2 IP). We show the configuration on figure 6. The configuration must be configured on both routers. We do not show the configuration for the Router2 but it's the same except the ip address which is 10.0.1.1.

```
Router1(config)# crypto isakmp key securepassword address 10.0.2.1
Router1(config)#
```

Figure 6: Configuration of the Router1.

We can show on the figure 7 that the configuration is correctly implemented with the cisco command called "show crypto isakmp key".

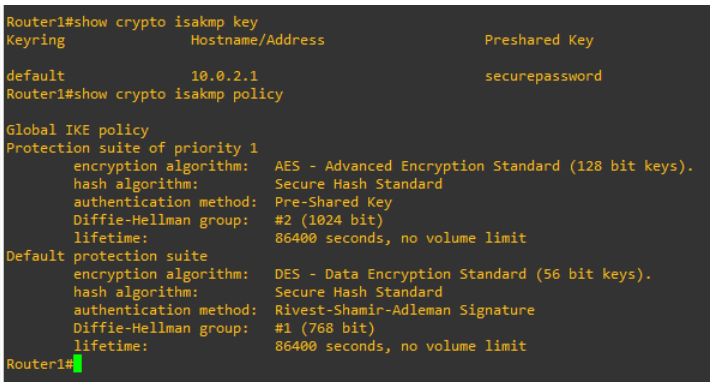


Figure 7: Display of IKE configuration on the Router1.

IPSec offers two types of security properties. The first provides authentication and integrity through the AH (Authentication Header) configuration and the other one provides authentication, integrity and confidentiality through the ESP (Encapsulating Security Payload) protocol. We chose the second option in this lab.

Now that the first phase is defined, we can configure the second phase to establish crypto transformations and access control. For this phase, we must set up different steps:

1. Creation of the extended ACL for the VPN traffic to filter input/output packets susceptible to be transformed. Here, packets to accept be linked to 192.168.1.0/24 and 192.168.2.0/24 private networks. We can show this configuration on figure 8.

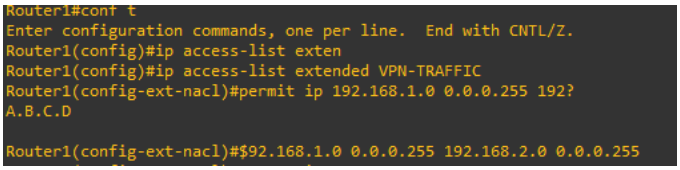


Figure 8: ACL configuration on the Router 1.

   a. Command "shows access-list" allow to see all the ACL sets on a router. An ACL has by default a "*deny any any*" rules which means that it'll drop all packets which are not in the rules set. So, all rules that allow packets must be set! The permit rule permit packet coming from and to the specified network. Comments can be added by using "*Remark <comment>*" while setting the ACL.

2. Then, we must define what's the transformation will be applied on packets. During this configuration we choose the AH or ESP configuration. Here, it's the ESP configuration. This transformation set is defined as the MYTS configuration. Because IPSec use the Encrypt-Then-MAC construction to combine the symmetric cipher and the MAC algorithm, we defined them to perform the authenticated encryption.

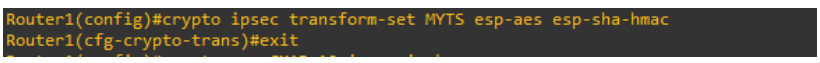


Figure 9: The IPSec packet transformation configuration.

a. MYTS is the name of the transform-set and we can specify up to 3 transform (here we only used 2) which must be from the following table. Source : Cisco Documentation.

Transform type	Transform	Description
AH Transform *(Pick up to one.)*	ah-md5-hmac	AH with the MD5 (HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (HMAC variant) authentication algorithm
ESP Encryption Transform *(Pick up to one.)*	esp-des	ESP with the 56-bit DES encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
ESP Authentication Transform (Pick up to one.)	**esp-md5-hmac**	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform *(Pick up to one.)*	**comp-lzs**	IP compression with the LZS algorithm.

Figure 10: The command "show crypto ipsec transform-set" to display all transform-sets

3. Now, we must map the configuration of IPSec with the previous ISAKMP configuration. This mapping is called CMAP. It allows to define how the packets (from 192.168.1.0/24 or .2.0/24) must be transformed using MYTS if the destination is 10.0.2.1.

```
Router1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router1(config-crypto-map)#set peer 10.0.2.1
Router1(config-crypto-map)#set transform-set MYTS
Router1(config-crypto-map)#match address VPN-TRADD
Router1(config-crypto-map)#match address VPN-TRAFF
Router1(config-crypto-map)#match address VPN-TRAFFIC
Router1(config-crypto-map)#exit
```

Figure 11: CMAP configuration.

a. *Crypto maps provide two functions: (1) filtering and classifying traffic to be protected and (2) defining the policy to be applied to that traffic. The first one affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.*

i. *IPSec crypto maps link together definitions of the following:*

- *What traffic should be protected.* Here it is matching our ACL VPN-TRAFFIC
- *Which IPSec peers the protected traffic can be forwarded to—these are the peers with which a security association can be established.* Here the peer is 10.0.2.1
- *Which transform sets are acceptable for use with the protected traffic*
- *How keys and security associations should be used or managed (or what the keys are, if IKE is not used)*

Definition comes from [Cisco Documentation](#).

4. The last step is just to define on which physical interface we apply the CMAP mapping. By this way, each packet which passes through this interface will be inspected. We can show on the figure 12 the configuration for this step.

```
Router1(config)#interface fa 0/0
Router1(config-if)#crypto map CMAP
Router1(config-if)#
*Mar  1 00:11:43.235: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router1(config-if)#
```

Figure 12: CMAP attribution on an interface.

NOTE: all these configurations (Phase 1 and Phase 2) have been applied on Router2 as well to establish the IPSec tunnel between both routers. Configurations are the same except for IP address of the router and the ACL.

III. Mission 3: Validate

Once all configurations have been implemented, we tested if the IPSec tunnel works well.

First, we try if we still can communicate with the PC3 (figure 13). It works well, all traffic is in clear.

4	6.044430	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x930f, seq=1/256, ttl=63 (reply in 5)
5	6.069079	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x930f, seq=1/256, ttl=62 (request in 4)
6	7.088570	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x940f, seq=2/512, ttl=63 (reply in 7)
7	7.130870	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x940f, seq=2/512, ttl=62 (request in 6)
8	8.188503	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x950f, seq=3/768, ttl=63 (reply in 9)
9	8.219788	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x950f, seq=3/768, ttl=62 (request in 8)
10	9.237594	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x960f, seq=4/1024, ttl=63 (reply in 11)
11	9.267758	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x960f, seq=4/1024, ttl=62 (request in 10)

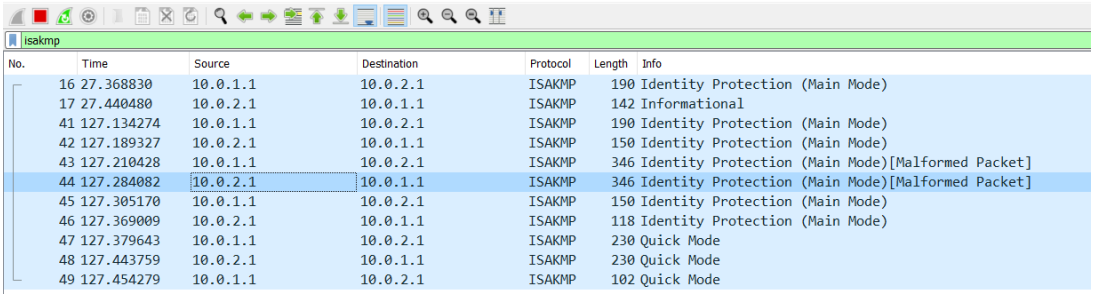
Figure 13: Ping from PC1 to PC3.

Now we try if the IPSec tunnel is correctly implemented by pinging the PC2 with PC1 (figure 14).

48	127.443759	10.0.2.1	10.0.1.1	ISAKMP	230	Quick Mode
49	127.454279	10.0.1.1	10.0.2.1	ISAKMP	102	Quick Mode
50	129.132393	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
51	129.321939	c4:04:05:61:00:01	c4:04:05:61:00:01	LOOP	60	Reply
52	131.128069	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
53	131.384981	10.0.2.1	10.0.1.1	ESP	166	ESP (SPI=0xecebccc6)
54	132.398572	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
55	132.451224	10.0.2.1	10.0.1.1	ESP	166	ESP (SPI=0xecebccc6)
56	133.469261	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
57	133.522062	10.0.2.1	10.0.1.1	ESP	166	ESP (SPI=0xecebccc6)
58	135.774252	c4:01:05:19:00:00	c4:01:05:19:00:00	LOOP	60	Reply

Figure 14: Ping from PC1 to PC2.

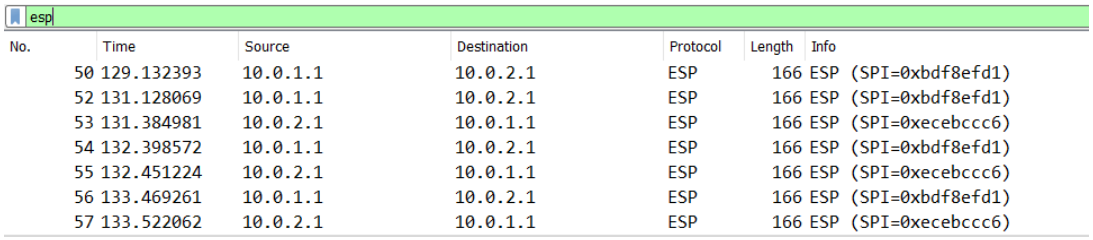
To filter ISAKMP and ESP protocols to better understand and show the configuration we can apply a filter on Wireshark with “isakmp” or “esp” (figure 14). We can show that pings are encrypted and therefore not in clear in the network traffic.



isakmp

No.	Time	Source	Destination	Protocol	Length	Info
16	27.368830	10.0.1.1	10.0.2.1	ISAKMP	190	Identity Protection (Main Mode)
17	27.440480	10.0.2.1	10.0.1.1	ISAKMP	142	Informational
41	127.134274	10.0.1.1	10.0.2.1	ISAKMP	190	Identity Protection (Main Mode)
42	127.189327	10.0.2.1	10.0.1.1	ISAKMP	150	Identity Protection (Main Mode)
43	127.210428	10.0.1.1	10.0.2.1	ISAKMP	346	Identity Protection (Main Mode)[Malformed Packet]
44	127.284082	10.0.2.1	10.0.1.1	ISAKMP	346	Identity Protection (Main Mode)[Malformed Packet]
45	127.305170	10.0.1.1	10.0.2.1	ISAKMP	150	Identity Protection (Main Mode)
46	127.369009	10.0.2.1	10.0.1.1	ISAKMP	118	Identity Protection (Main Mode)
47	127.379643	10.0.1.1	10.0.2.1	ISAKMP	230	Quick Mode
48	127.443759	10.0.2.1	10.0.1.1	ISAKMP	230	Quick Mode
49	127.454279	10.0.1.1	10.0.2.1	ISAKMP	102	Quick Mode

Figure 15: Filtered analysis of ISAKMP with Wireshark between PC1 and PC2.



esp

No.	Time	Source	Destination	Protocol	Length	Info
50	129.132393	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
52	131.128069	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
53	131.384981	10.0.2.1	10.0.1.1	ESP	166	ESP (SPI=0xecebccc6)
54	132.398572	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
55	132.451224	10.0.2.1	10.0.1.1	ESP	166	ESP (SPI=0xecebccc6)
56	133.469261	10.0.1.1	10.0.2.1	ESP	166	ESP (SPI=0xbdf8efd1)
57	133.522062	10.0.2.1	10.0.1.1	ESP	166	ESP (SPI=0xecebccc6)

Figure 16: Filtered analysis of ESP with Wireshark between PC1 and PC2.

Finally, we can show on figures 17 and 18 the correct IPSec configuration inside the Router1.

```
Router1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Router1#show crypto isakmp sa
dst             src             state          conn-id slot status
10.0.2.1        10.0.1.1        QM_IDLE              1    0 ACTIVE

Router1#
```

Figure 17: ISAKMP configuration on Router1.

```
Router1#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: CMAP, local addr 10.0.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 10.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 6, #recv errors 0

     local crypto endpt.: 10.0.1.1, remote crypto endpt.: 10.0.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xBDF8EFD1(3187208145)

     inbound esp sas:
      spi: 0xECEBCCC6(3974876358)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4388250/3153)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xBDF8EFD1(3187208145)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4388250/3148)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
Router1#
```

Figure 18: IPSec configuration on Router1.