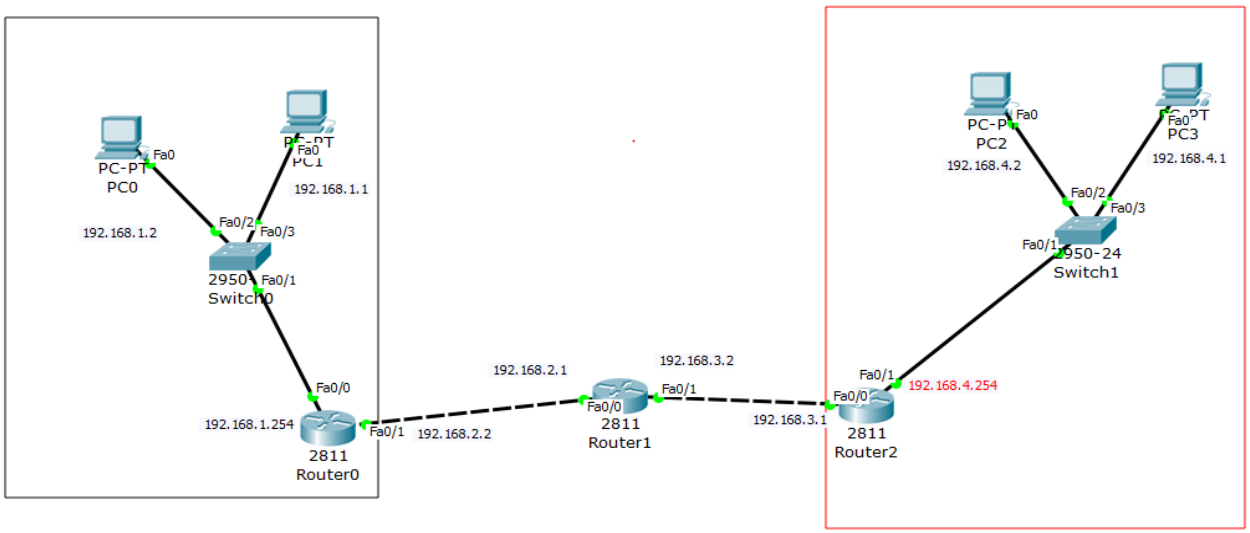
Esercitazione VPN Site-to-Site senza NAT

Obiettivo: configurare VPN su una topologia di rete molto semplificata, senza NAT.

Accorgimenti: utilizzare i router da 2811 e più.



La configurazione preliminare

Router 0

```
interface FastEthernet0/0
ip address 192.168.1.254     255.255.255.0
!
interface FastEthernet0/1
ip address 192.168.2.2     255.255.255.0

ip classless
ip route 192.168.4.0 255.255.255.0 192.168.2.1
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Router 1

```
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/1
ip address 192.168.3.2 255.255.255.0
!
ip classless
ip route 192.168.1.0 255.255.255.0 192.168.2.2
ip route 192.168.4.0 255.255.255.0 192.168.3.1
```

Router 2

```
interface FastEthernet0/0
ip address 192.168.3.1   255.255.255.0
!
interface FastEthernet0/1
ip address 192.168.4.254    255.255.255.0
!
ip classless
ip route 192.168.1.0    255.255.255.0 192.168.3.2
ip route 192.168.2.0 255.255.255.0 192.168.3.2   //questa route non serve, si può non configurarla
ip route 0.0.0.0 0.0.0.0 192.168.3.2
```

LA CONFIGURAZIONE SPECIFICA VPN

ROUTER 0

```
Router>
Router>en
Router#conf t

Router(config)#crypto isakmp policy 10   //policy, il numero è qualsiasi
Router(config-isakmp)#hash md5
Router(config-isakmp)#encr 3des
Router(config-isakmp)#authentication pre-share   //se non indichiamo il gruppo D-H, sarà n.2
Router(config-isakmp)#crypto isakmp key P5NM address 192.168.3.1  //l'IP del nostro router-peer

Router(config)#
Router(config)#crypto ipsec transform-set SEGRETO esp-3des esp-md5-hmac  //transform-set di nome
SEGRETO (scelto a caso)
Router(config)#

Router(config)#ip access-list extended VPN     //creazione ACL di nome "VPN" per VPN,
Router(config-ext-nacl)#permit ip 192.168.1.0   0.0.0.255    192.168.4.0    0.0.0.255  //traffico criptato LAN1 -> LAN4
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#crypto map CMAP 10 ipsec-isakmp   //impostazione criptomappa di nome CMAP
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.set peer 192.168.3.1
Router(config-crypto-map)#set peer 192.168.3.1
Router(config-crypto-map)#set transform-set SEGRETO
Router(config-crypto-map)#match address VPN
Router(config-crypto-map)#exit
Router(config)#
Router(config)#
Router(config)#int fa 0/1   //associare la mappa all'interfaccia esterna del router
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr mem
```

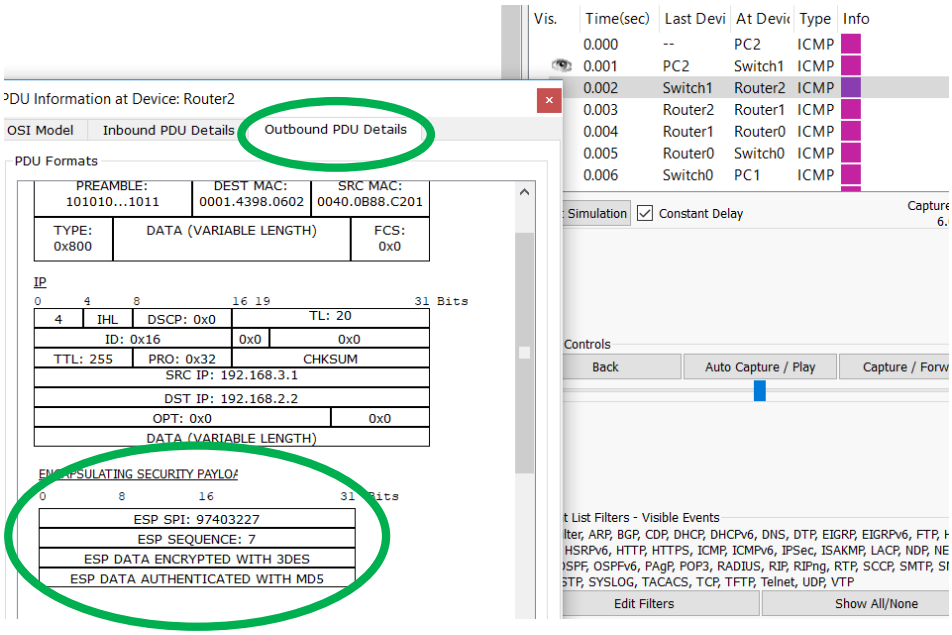
ROUTER 2

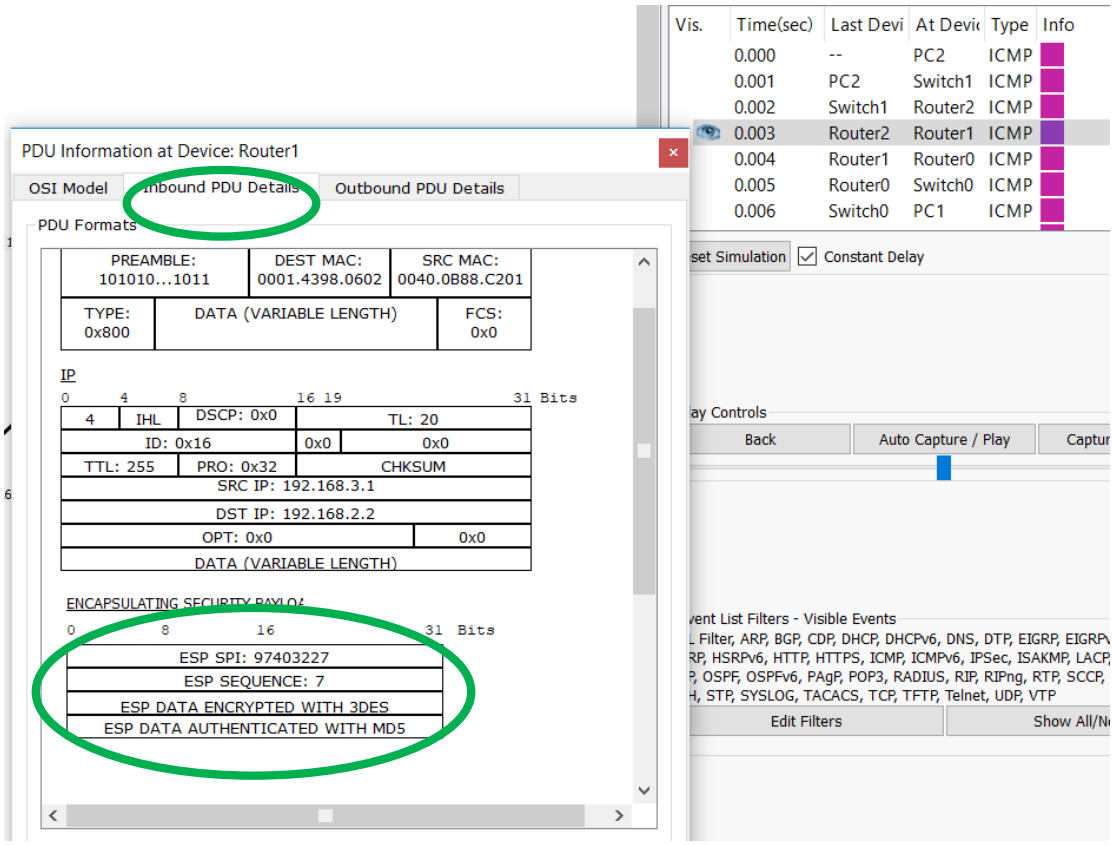
```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10   //policy, il numero è qualsiasi
Router(config-isakmp)#hash md5
Router(config-isakmp)#encr 3des
Router(config-isakmp)#authentication pre-share   //se non indichiamo il gruppo D-H, sarà n.2
Router(config-isakmp)#crypto isakmp key P5NM address 192.168.2.2
Router(config-isakmp)#exit
Router(config)#
Router(config)#
Router(config)#crypto ipsec transform-set SEGRETO esp-3des esp-md5-hmac
Router(config)#
Router(config)#ip access-list extended VPN
Router(config-ext-nacl)#permit ip 192.168.4.0    0.0.0.255    192.168.1.0    0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#
```

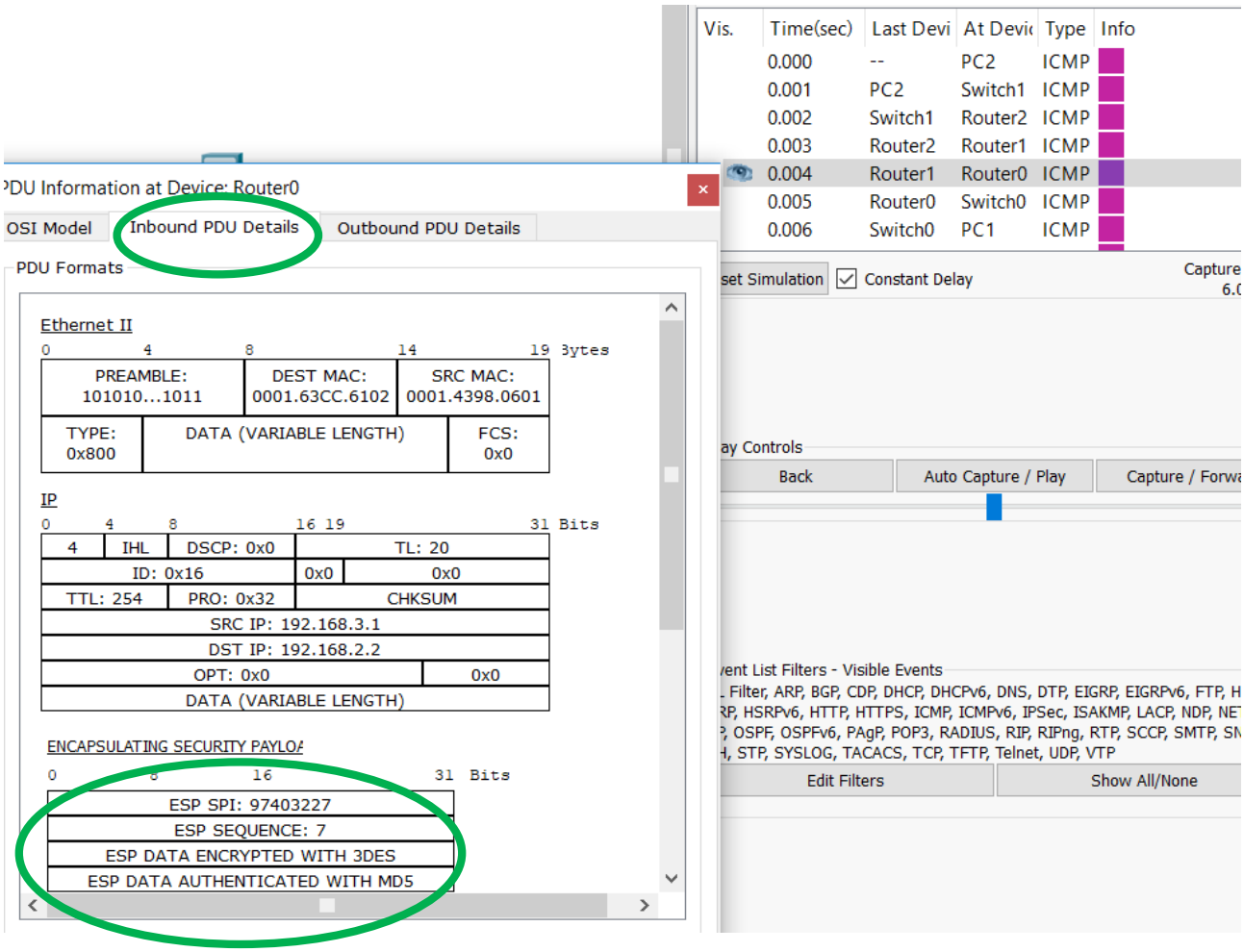
Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.168.2.2
Router(config-crypto-map)#set transform-set SEGRETO
Router(config-crypto-map)#match address VPN
Router(config-crypto-map)#exit
Router(config)#
Router(config)#int fa 0/0
Router(config-if)#crypto map CMAP
**Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON*
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#wr mem

Per mostrare agli studenti la differenza, si confrontano i pacchetti prima e dopo la configurazione VPN

Percorso dal PC2 al PC1




Vis. Time(sec) Last Devi At Devi Type Info
0.000 -- PC2 ICMP
0.001 PC2 Switch1 ICMP
0.002 Switch1 Router2 ICMP
0.003 Router2 Router1 ICMP
0.004 Router1 Router0 ICMP
0.005 Router0 Switch0 ICMP
0.006 Switch0 PC1 ICMP
set Simulation
Constant Delay
ay Controls
Back
Auto Capture / Play
Edit Filters
PDU Information at Device: Router1
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
PREAMBLE: 101010...1011
DEST MAC: 0001.4398.0602
SRC MAC: 0040.0B88.C201
TYPE: 0x800
DATA (VARIABLE LENGTH)
FCS: 0x0
IP
0 4 8 16 19 31 Bits
4 IHL DSCP: 0x0 TL: 20
ID: 0x16 0x0 0x0
TTL: 255 PRO: 0x32 CHKSUM
SRC IP: 192.168.3.1
DST IP: 192.168.2.2
OPT: 0x0 0x0
DATA (VARIABLE LENGTH)
0 8 16 31 Bits
ESP SPI: 97403227
ESP SEQUENCE: 7
ESP DATA ENCRYPTED WITH 3DES
ESP DATA AUTHENTICATED WITH MD5


Vis. Time(sec) Last Devi At Devi Type Info
0.000 -- PC2 ICMP
0.001 PC2 Switch1 ICMP
0.002 Switch1 Router2 ICMP
0.003 Router2 Router1 ICMP
0.004 Router1 Router0 ICMP
0.005 Router0 Switch0 ICMP
0.006 Switch0 PC1 ICMP
set Simulation
Constant Delay
ay Controls
Back
Auto Capture / Play
Edit Filters
Show All/None
PDU Information at Device: Router0
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
Ethernet II
0 4 8 14 19 Bytes
PREAMBLE: 101010...1011
DEST MAC: 0001.63CC.6102
SRC MAC: 0001.4398.0601
TYPE: 0x800
DATA (VARIABLE LENGTH)
FCS: 0x0
IP
0 4 8 16 19 31 Bits
4 IHL DSCP: 0x0 TL: 20
ID: 0x16 0x0 0x0
TTL: 254 PRO: 0x32 CHKSUM
SRC IP: 192.168.3.1
DST IP: 192.168.2.2
OPT: 0x0 0x0
DATA (VARIABLE LENGTH)
0 16 31 Bits
ESP SPI: 97403227
ESP SEQUENCE: 7
ESP DATA ENCRYPTED WITH 3DES
ESP DATA AUTHENTICATED WITH MD5