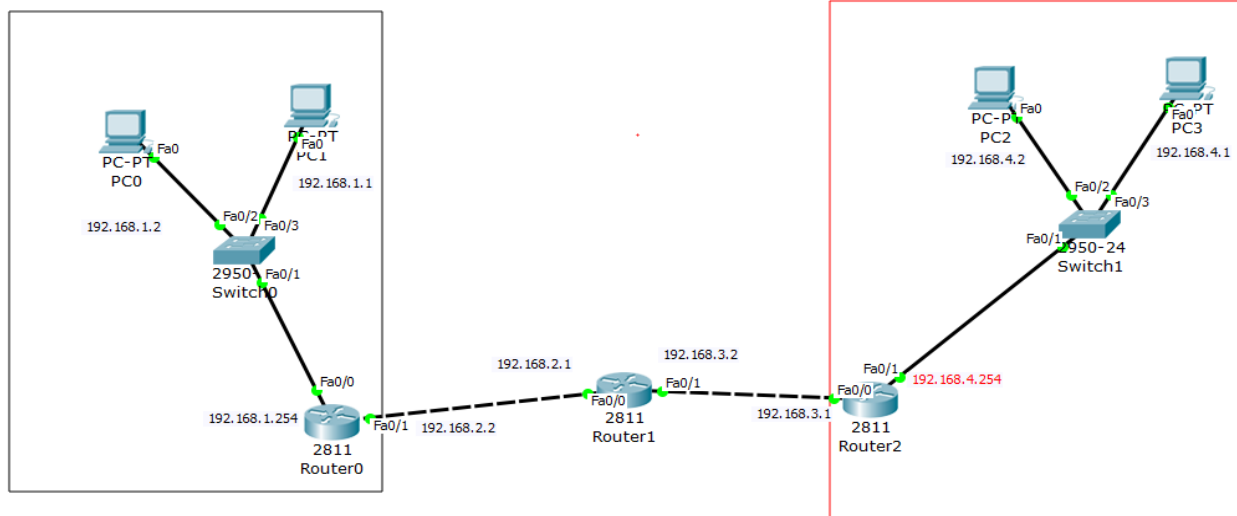


Esercitazione VPN Site-to-Site senza NAT

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-ISA_KMP_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

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets, with the selected packet (0.002) being an ICMP packet from Switch1 to Router2. The middle pane shows the 'PDU Information at Device: Router2' with tabs for 'OSI Model', 'Inbound PDU Details', and 'Outbound PDU Details'. The 'Outbound PDU Details' pane is selected and circled in green, showing the IP header and the ESP payload structure. The bottom pane shows the 'PDU Formats' section, which is also circled in green, displaying the details of the ESP payload, including the SPI, sequence number, and the encrypted data.

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	

PDU Information at Device: Router2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

PREAMBLE:		DEST MAC:	SRC MAC:
101010...1011		0001.4398.0602	0040.0B88.C201
TYPE: 0x800	DATA (VARIABLE LENGTH)		FCS: 0x0

IP

0		4		8		16		19		31	
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)											

ENCAPSULATING SECURITY PAYLOAD

0		8		16		31	
ESP SPI: 97403227							
ESP SEQUENCE: 7							
ESP DATA ENCRYPTED WITH 3DES							
ESP DATA AUTHENTICATED WITH MD5							

Simulation ☒ Constant Delay Capture 6.

Controls

Back Auto Capture / Play Capture / Forw

List Filters - Visible Events

Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, LACP, NDP, NE, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SI, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Edit Filters Show All/None

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
IHL		DSCTP: 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)						

ENCAPSULATING SECURITY PAYLOAD

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

Play Controls

Back Auto Capture / Play Capture

Event List Filters - Visible Events

Filter: ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, LACP, OSPF, OSPFv6, PAP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Edit Filters Show All/None

PDU Information at Device: Router0

OSI Model **Inbound PDU Details** Outbound PDU Details

PDU Formats

Ethernet II

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
IHL		DSCTP: 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)						

ENCAPSULATING SECURITY PAYLOAD

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

Play Controls

Back Auto Capture / Play Capture / Forward

Event List Filters - Visible Events

Filter: ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, LACP, NDP, NET, OSPF, OSPFv6, PAP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Edit Filters Show All/None