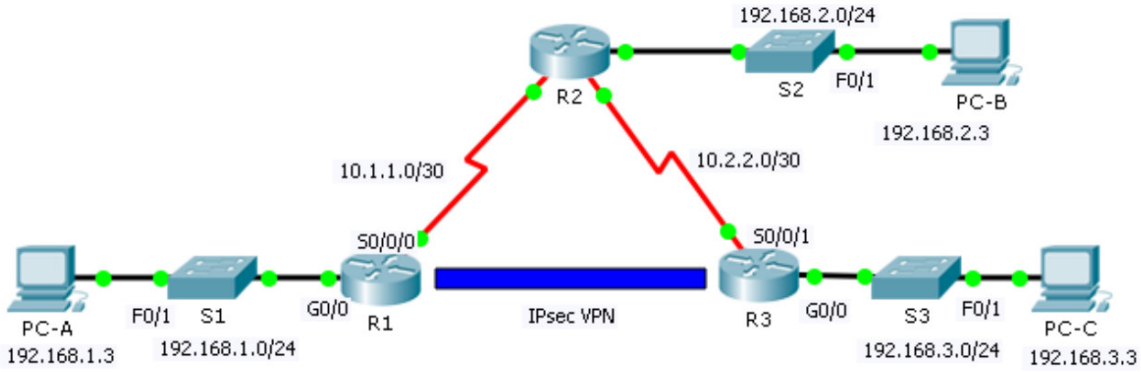
Esempio di creazione di una VPN basata sul protocollo IPSec con Packet Tracer

Creare la topologia mostrata in figura, utilizzando come router i modelli della serie 2900 cisco.



Assegnare alle interfacce gli indirizzi IP riportati nella seguente tabella:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Configurare i router con le seguenti Tabelle di Routing:

R1

Rete	Subnet mask	Next hop
192.168.2.0	255.255.255.0	10.1.1.1
192.168.3.0	255.255.255.0	10.1.1.1
10.2.2.0	255.255.255.252	10.1.1.1

R2

Rete	Subnet mask	Next hop
192.168.1.0	255.255.255.0	10.1.1.2
192.168.3.0	255.255.255.0	10.2.2.2

R3

Rete	Subnet mask	Next hop
192.168.1.0	255.255.255.0	10.2.2.1
192.168.2.0	255.255.255.0	10.2.2.1
10.1.1.0	255.255.255.252	10.2.2.1

Procedere con l'installazione del pacchetto software per la sicurezza SECURITYK9, sui due router che devono svolgere il ruolo di security gateway tra le due reti LAN dell'azienda (configurazione VPN site-to-site). Entrare in modalità Command Line Interface (CLI) sul router R1 e digitare i seguenti comandi:

```
R1> enable
R1# configure terminal
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

Dopo aver atteso il riavvio del router, digitare il comando **show version** e verificare che compare la riga evidenziata in giallo nell'immagine sotto.

```
-----------------------------------------------------------------
Technology     Technology-package          Technology-package
               Current        Type         Next reboot
-----------------------------------------------------------------
ipbase         ipbasek9       Permanent    ipbasek9
security       securityk9     Evaluation   securityk9
uc             None           None         None
data           None           None         None
```

Se la riga è presente, vuol dire che l'installazione del pacchetto software è andata a buon fine e possiamo procedere nel ripetere la stessa operazione sul router R3.

A questo punto procediamo con la configurazione della VPN sul router R1, con i seguenti comandi:

```
(Questo primo comando attiva la VPN per il traffico tra le due LAN aziendali)
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
(seguono i comandi per la configurazione della Fase-1)
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
(seguono i comandi per la configurazione della Fase-2)
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
(seguono i comandi per associare la VPN con l'interfaccia seriale s0/0/0)
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

A questo punto procediamo con la configurazione della VPN sul router R3, con i seguenti comandi:

```
(Questo primo comando attiva la VPN per il traffico tra le due LAN aziendali)
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
(seguono i comandi per la configurazione della Fase-1)
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
(seguono i comandi per la configurazione della Fase-2)
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
(seguono i comandi per associare la VPN con l'interfaccia seriale s0/0/1)
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

La configurazione dei router per la creazione della VPN è completata.

Passiamo ora alla verifica del corretto funzionamento della VPN. Lanciamo il seguente comando sul router R1 e verifichiamo quanti pacchetti dati sono stati cifrati e incapsulati e quanti decifrati e de incapsulati, voci evidenziate in giallo nella figura sotto:

```
R1# show crypto ipsec sa

  interface: Serial0/0/0
      Crypto map tag: VPN-MAP, local addr 10.1.1.2

     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): (192.168.3.0/255.255.255.0/0/0)
     current_peer 10.2.2.2 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

       local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
       path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
       current outbound spi: 0x0(0)
  <output omitted>
```

A questo punto, creiamo del traffico che riguarda la VPN, facendo il ping del PC-C dal PC-A e digitiamo nuovamente il comando **`show crypto ipsec sa`** sul router R1 per verificare il quantitativo di pacchetti che sono stati cifrati e incapsulati oltre che decifrati e deincapsulati.

L'ultima verifica da fare, consiste nel fare un ping dal PC-A verso il PC-B e verificare che il numero di pacchetti cifrati, incapsulati, decifrati e de incapsulati non è variato rispetto a prima.