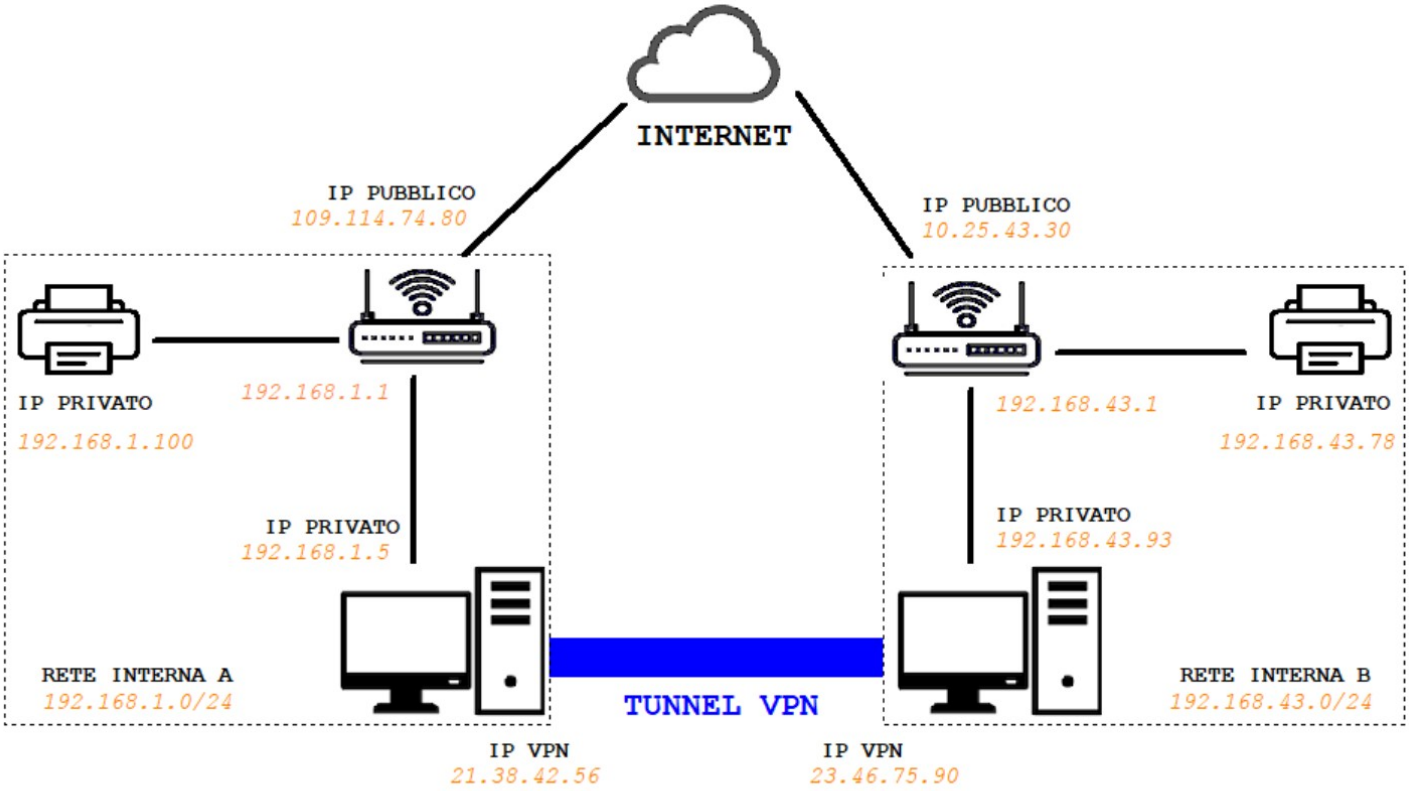
VPN (Virtual Private Network)

La VPN è una rete privata virtuale cioè un servizio che permette di instaurare una connessione sicura e criptata tra due dispositivi.



IN ARANCIONE UN ESEMPIO DI INDIRIZZI IP

Con una VPN, i due computer in figura, risulteranno connessi tra di loro mediante i due indirizzi IP forniti dal servizio VPN, come fossero in una rete privata, con la differenza che al posto del collegamento fisico (cavo o wifi) ci sarà o un percorso predefinito e riservato, o un **tunnel VPN** dove i dati transitano in maniera cifrata (**tunneling**).

Nel secondo caso, il pacchetto dati originale prima di uscire sulla rete viene criptato ed incapsulato in un ulteriore pacchetto dal software VPN per poi essere decriptato e decodificato dal software VPN dal lato destinatario.

La VPN nasce per sopperire all'esigenza di collegarsi da remoto ad i server aziendali, o per consentire il collegamento tra reti private di sedi differenti. Pensiamo ad esempio all'esigenza di collegare due reti della stessa azienda con sedi in differenti città o paesi, o all'esigenza del lavoratore che deve accedere ad i server aziendali.

Inoltre questa tecnologia non richiede risorse aggiuntive, per instaurare una rete sicura è infatti sufficiente una connessione ad internet da entrami i lati ed la piattaforma software che gestisce la connessione VPN.

Negli ultimi anni la VPN ha subito un ulteriore evoluzione in quanto viene utilizzata anche per avere l'anonimato nella navigazione e per accedere alla rete internet mediante dei server messi a disposizione dalle varie compagnie che offrono il servizio, nei vari paesi del mondo.

Considerando le caratteristiche tecniche del servizio possiamo suddividere le VPN in 3 tipologie:

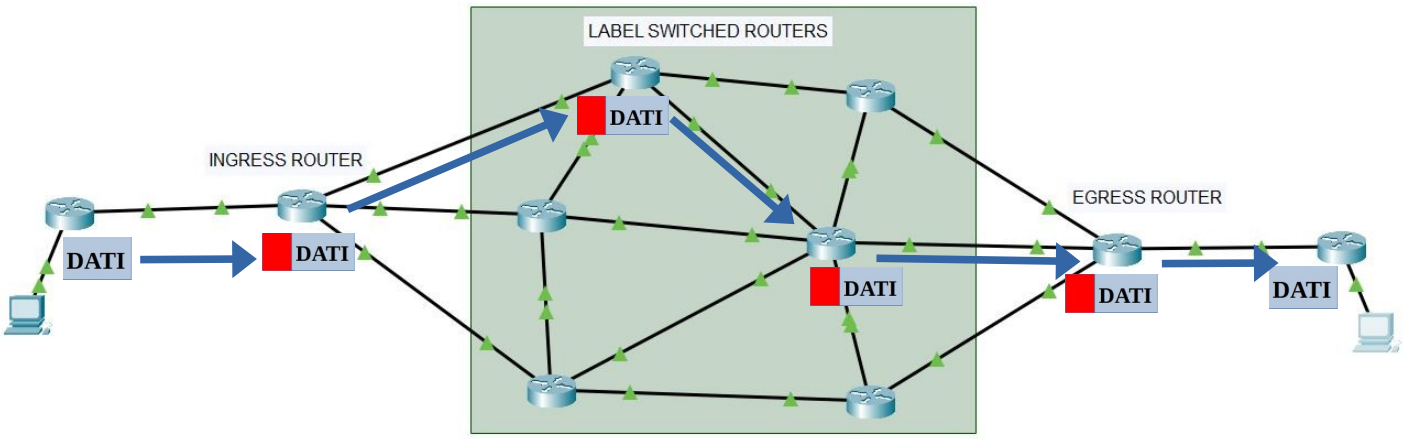
- **Trusted VPN**

  In questo caso la rete privata viene creata dall'ISP (Internet Service Provider) il quale crea un percorso definito e non accessibile da altri per far viaggiare i pacchetti. Nella Trusted VPN non viene creato il tunnel virtuale, e pertanto non c'è crittografia. Il traffico viene istradato in percorsi definiti e dedicati, gestiti dall'ISP, e per questo c'è un buon QoS (**Q**uality **O**f **S**ervice).

  In questo tipo di VPN viene utilizzato il protocollo MPLS (**M**ulti**P**rotocol **L**abel **S**witching) aggiungendo tra il livello 2 ed il livello 3 (DataLink e IP) una Label al pacchetto dati, che lo identifica e lo instrada in maniera definita tra i vari Router,

  Un piccolo approfondimento.

  Il protocollo MPLS viene definito dalle RFC 3031 e 3032 pubblicate dall'Internet Engineering Task Force (IETF). Prevede l'instradamento del traffico tra sorgente e destinazione, tramite delle Label identificative aggiunte al pacchetto dati e riconosciute dai router MPLS che implementano questo protocollo. I router di ingresso nel protocollo MPLS vengono chiamati **ingress router,** quelli intermediari **label switched router**, e quelli in uscita **egress router**.



I pacchetto dati parte dal router del mittente e nell'ingress router, gli viene aggiunta la label, uccessivamente il pacchetto verrà instradato nel percorso definito fino ad uscire nell'egress router senza label.

- **Secure VPN**

  In questo caso la rete privata sfrutta il tunneling, cioè la creazione di un tunnel virtuale protetto dalla crittografia dei dati con i protocolli IPsec, SSL/TLS o SSH.

  In questo caso gli utenti possono utilizzare la VPN da qualsiasi postazione internet anche utilizzando wifi pubbliche, in quanto un'eventuale cattura dei pacchetti trasmessi non consentirebbe la lettura del loro contenuto perché criptato.

- **Hybrid VPN**

  In questo caso vengono messe insieme le due precedenti tecnologie, ottenendo così una sicurezza nel percorso e nella cifratura del pacchetto.

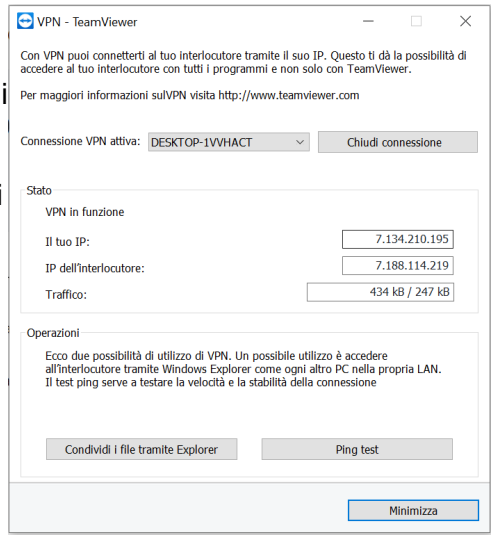
Un’altra suddivisione può essere fatta considerando l’utilizzo che si fa della VPN, in questo caso possiamo considerari i seguenti tipi di VPN:

- **Remote Access VPN**
  Utilizzata ad esempio per collegarsi da una singola postazione remota alle risorse interne di un’azienda, come ad esempio ad un server NAS (**N**etwork **A**ttached **S**torage) in pratica un Hard Disk condiviso in rete.
- **Site to Site VPN**
  Utilizzata ad esempio per stabilire una connessione sicura tra due sedi differenti di un’azienda, utilizzando la rete internet.

Come detto inizialmente, un’ulteriore applicazione della VPN che ha di recente preso piede, è quella legata alla protezione dell’anonimato per la navigazione in rete.
Ci sono in rete diversi servizi che offrono una VPN per la navigazione anonima, in questo caso, il client si collega ad uno tra i server messi a disposizione da chi offre il servizio tramite un tunnel virtuale e criptato, consentendo perciò l’accesso ad internet con un indirizzo IP non riconducibile al proprio PC.
Uno di questi servizi ad esempio è NordVPN, di seguito l’indirizzo IP con cui viene visto il PC senza una VPN e con un servizio come NordVPN, connesso ad un server australiano.

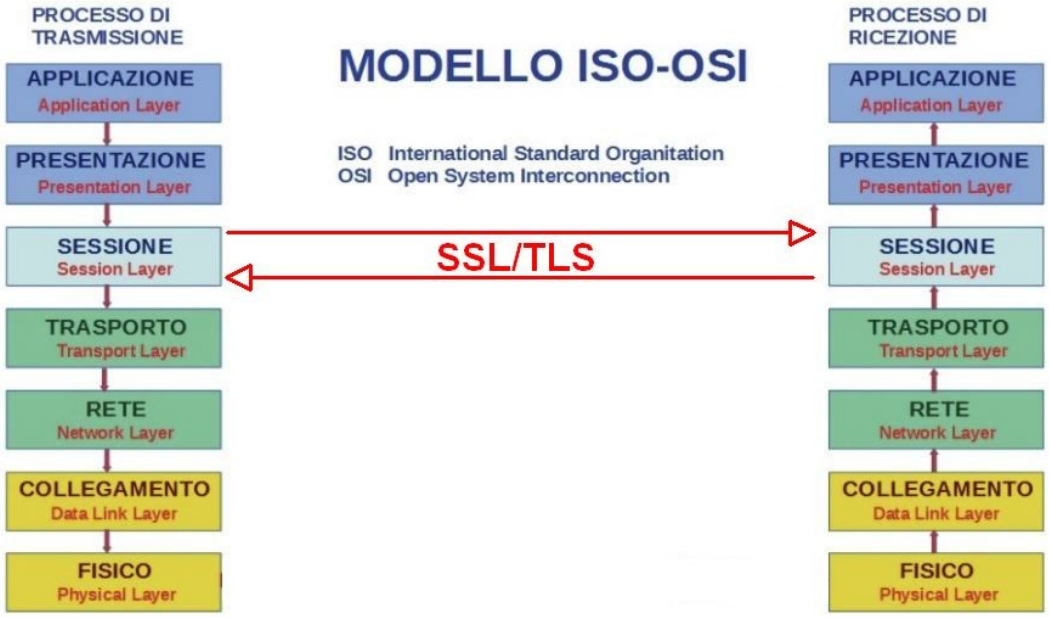
Nel secondo caso il pacchetto dati esce dal PC e viene incapsulato e criptato fino al server di uscita, in questo caso in Australia, dove si ricostruisce il pacchetto iniziale per accedere alla risorsa web richiesta.

Esistono inoltre diversi software che consentono l’instaurazione di una connessione VPN tra due PC, come ad esempio Teamviewer, Hamachi o Radmin. L’immagine a fianco, è relativa ad una connessione VPN attivata con Teamviewer, si possono notare nella schermata gli indirizzi IP dei due computer connessi ai lati del tunnel virtuale, come fossero connessi in una LAN interna.



Protocollo SSL/TLS (Secure Socket Layer, Transport Layer Security)

Questi protocolli operano nel livello SESSIONE del modello ISO/OSI.



Il protocollo nasce nel 1994 con le seguenti funzionalità:

- **segretezza delle comunicazioni**, garantita da algoritmi di crittografia a chiave simmetrica (DES, RC4) in questo tipo di crittografia, le due parti sono in possesso della stessa chiave necessaria per criptare e decriptare il messaggio.
- **Autenticazione**, grazie ad una crittografia a chiave pubblica (RSA, DSS). Lo scambio delle chiavi precedentemente citate, avviene con una crittografia asimmetrica o a chiave pubblica.
- **Affidabilità**, garantita da un codice MAC che utilizza delle funzioni SHA e MD5, cioè degli algoritmi in grado di generare una stringa di caratteri di lunghezza fissa univoca e completamente differente per piccole variazioni dei dati di input. In questo modo è possibile validare con certezza il dato ricevuto.

Questo protocollo sfrutta una struttura di tipo client-server, il client si connette al server richiedendo l'autenticazione indicando l'elenco degli algoritmi di cifratura supportati. Il server risponde a questa richiesta inviando il proprio certificato di autenticazione contenente la chiave pubblica e il tipo di cifratura.
Il client una volta verificata la validità del certificato ricevuto, crea una chiave segreta che codifica con la chiave pubblica del server, ottenendo così la **chiave di sessione** che invia al server.
Il server decripta la **chiave di sessione** ricevuta con la sua chiave privata.
A questo punto sia client che server nelle comunicazioni successive utilizzeranno la **chiave di sessione** per il criptaggio/decriptaggio.
Il successore del protocollo SSL è il TLS, composto da due sottoprotocolli; il TLS Handshake Protocol, utilizzato per stabilire la connessione client-server, ed il sottoprotocollo TLS Record Protocol, che si interfaccia con il livello trasporto TCP, per gestire il trasferimento dei dati. Le specifiche del protocollo **TLS** sono definite nella **RFC8446**.

Protocollo IPsec

Questo protocollo definito dalle RFC2401 e RFC2411, opera a **livello di rete** ed in realtà esso rappresenta un insieme di protocolli che consentono di implementare lo scambio delle chiavi, di autenticare il mittente e di cifrare il flusso di dati. Il protocollo IPsec, è opzionale nell'IPV4, ma già integrato nell'IPV6.

Il protocollo IPsec utilizza il protocollo AH (Authentication Header) per garantire l'identità e l'integrità dell'indirizzo IP del mittente, ed il protocollo ESP (Encapsulation Security Payload) che aggiunge al primo la cifratura del pacchetto IP.

Il protocollo apre due canali virtuali tra mittente e destinatario, per il transito dei dati nelle due direzioni. I canali vengono definiti SA (Security Association).

IPsec può funzionare in due modalità differenti:

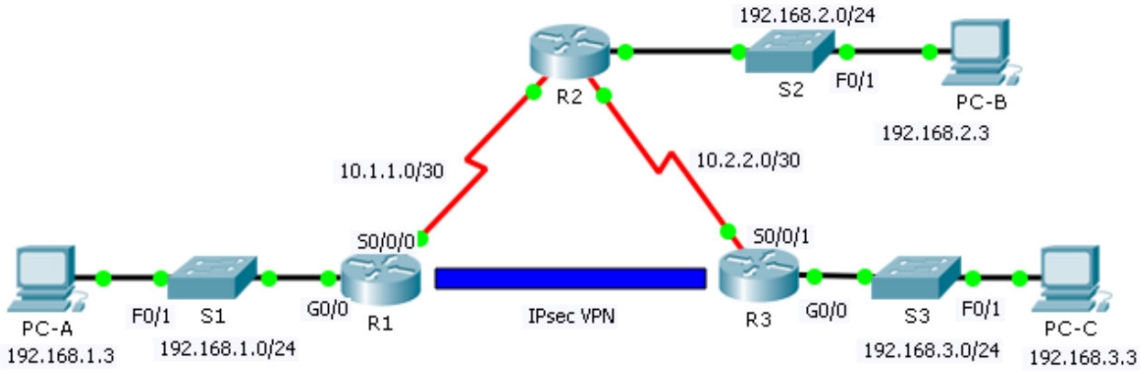
Transport mode, in questo caso il protocollo è eseguito direttamente sui terminali ai lati della connessione (connessione end to end) in ogni Host necessariamente ci deve essere tutto il software necessario per implementare il protocollo IPsec.

Tunnel mode, in questo caso il protocollo è eseguito sui router, dove ovviamente dev'essere presente il software necessario per implementare il protocollo IPsec. Gli host collegati alla rete invece, non necessitano del software necessario a questo protocollo di sicurezza.

Senza scendere molto nel dettaglio del funzionamento dei protocolli di sicurezza, vediamo ora un'esperienza da realizzare con il software Cisco Packet Tracer.

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.