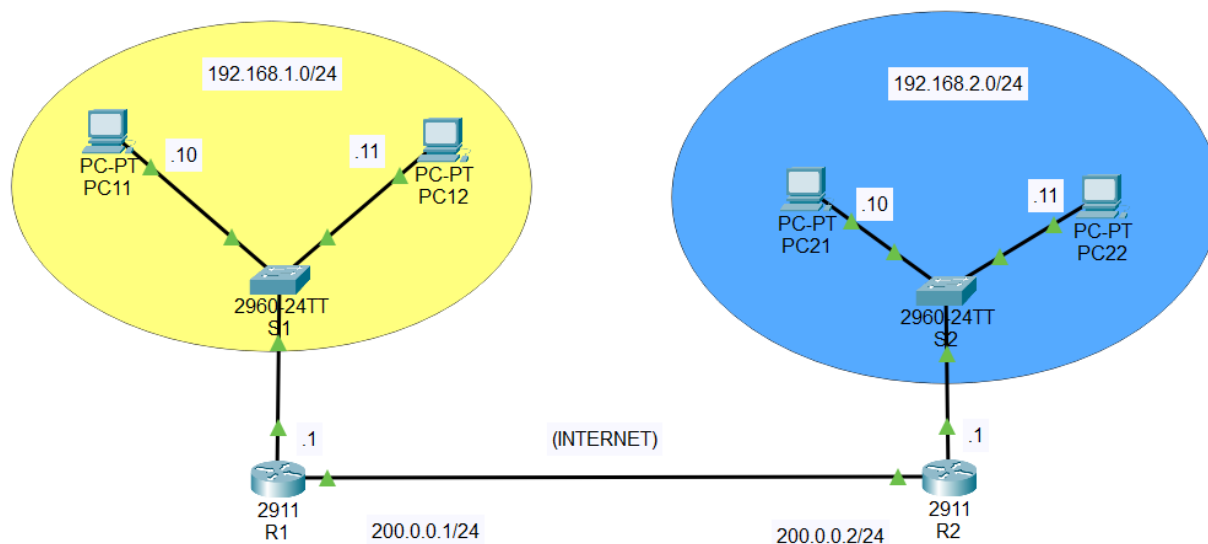


## Connessione tra due reti tramite VPN site-to-site

Configurare due router (R1 e R2) in due sedi distinte connessi a Internet, per permettere a due reti locali di comunicare attraverso una **VPN (Virtual Private Network) IPsec site-to-site**. Ogni rete contiene **due PC** che devono poter **condividere risorse** (es. ping, HTTP).



**N.B.:** La scelta dei router 2811 è resa necessaria dal fatto che è l'unico router che supporta IPsec VPN in Packet Tracer

### Concetti chiave: VPN site-to-site

Una VPN (Virtual Private Network) **site-to-site** permette a due LAN distinte di comunicare in modo **sicuro attraverso Internet**, come se fossero sulla stessa rete fisica.

- Utilizza **IPsec** per proteggere il traffico (confidenzialità, integrità, autenticazione).
- Il tunnel è stabilito tra due dispositivi (router o firewall).
- Il traffico tra le due LAN viene **incapsulato e cifrato** attraverso il tunnel.

### IPsec

Il **protocollo IPsec** (*Internet Protocol Security*) è un insieme di protocolli usato per **proteggere il traffico IP** tra due host, due gateway, o tra host e gateway. Fornisce **autenticazione, integrità, riservatezza e protezione contro il replay**. È spesso usato per **VPN** (Virtual Private Network).

#### Obiettivo di IPsec

IPsec protegge i dati a **livello di rete (livello 3 del modello OSI)**. Questo significa che tutto il traffico IP (indipendentemente dall'applicazione) può essere cifrato e autenticato.

#### Componenti principali di IPsec

## 1. Protocolli di base

IPsec è composto principalmente da **due protocolli**:

Protocollo	Funzione
<b>AH (Authentication Header)</b>	Garantisce <b>autenticità</b> e <b>integrità</b> dei pacchetti, ma <b>non li cifra</b> .
<b>ESP (Encapsulating Security Payload)</b>	Fornisce <b>confidenzialità</b> (cifratura), <b>integrità</b> e <b>autenticazione</b> . Può anche nascondere il contenuto dei pacchetti.

## 2. Modalità operative

IPsec può funzionare in due modalità:

Modalità	Descrizione	Utilizzo tipico
<b>Transport mode</b>	Protegge solo i dati nel payload, lasciando l'header IP originale intatto.	VPN tra <b>host a host</b> (es. due PC).
<b>Tunnel mode</b>	L'intero pacchetto IP originale è <b>incapsulato</b> in un nuovo pacchetto IP.	VPN tra <b>gateway</b> (es. due router o firewall).

### Protezione contro il replay

IPsec usa **numeri di sequenza** e **timestamp** per proteggere contro gli attacchi di **replay** (dove un attaccante reinvia pacchetti vecchi).

### Esempio semplice (VPN site-to-site, tunnel mode, ESP)

Due router aziendali A e B stabiliscono un tunnel IPsec:

- Router A invia a Router B un pacchetto IP.
- IPsec incapsula il pacchetto originale in un nuovo pacchetto:

```
[Header IP nuovo] [ESP Header] [Pacchetto IP originale cifrato] [ESP Trailer]
```

- Router B decifra e autentica il pacchetto, quindi lo inoltra alla rete interna.

### ESP Header

L'**ESP header** è una parte fissa all'inizio del payload cifrato. Include:

Campo	Dimensione	Descrizione
<b>SPI (Security Parameters Index)</b>	32 bit	Identifica l'associazione di sicurezza (SA)
<b>Sequence Number</b>	32 bit	Previene attacchi di replay (ogni pacchetto ha numero univoco)

Questi due campi **non sono cifrati**: servono al destinatario per capire come decriptare il resto.

### ESP Trailer

L'**ESP Trailer** ha 3 campi principali:

Campo	Dimensione	Funzione
<b>Padding</b>	variabile	Allinea i dati a un multiplo del blocco di cifratura (es. AES) Gli algoritmi di cifratura come <b>AES</b> lavorano su <b>blocchi di lunghezza fissa</b> (es. 16 byte). Se i dati da cifrare <b>non sono un multiplo esatto</b> di 16, bisogna <b>aggiungere del padding</b> per "riempire" l'ultimo blocco.

			<i>Il tutto viene cifrato insieme al payload. Il padding può contenere <b>valori qualsiasi</b> (0x00, 0x01, ...), non è rilevante: viene eliminato alla decifratura.</i>	
	<b>Padding Length</b>	8 bit	Indica quanti byte di padding ci sono	
	<b>Next Header</b>	8 bit	Specifica il tipo di protocollo del payload originale (es. TCP, UDP, IP)	

## Configurazione Router

### Su R1

```
Router (config)# hostname R1
```

#### Default Gateway R1

```
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

#### Assegnazione IP G0/1

```
R1(config)# interface fastEthernet 0/1
R1(config-if)# ip address 200.0.0.1 255.255.255.0
R1(config-if)# no shutdown
```

#### IP Route alla rete 2

```
R1(config)# ip route 192.168.2.0 255.255.255.0 200.0.0.2
```

### Su R2

```
Router (config)# hostname R2
```

#### Default Gateway R1

```
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# no shutdown
```

#### Assegnazione IP G0/1

```
R1(config)# interface fastEthernet 0/1
R1(config-if)# ip address 200.0.0.2 255.255.255.0
R1(config-if)# no shutdown
```

#### IP Route alla rete 1

```
R1(config)# ip route 192.168.1.0 255.255.255.0 200.0.0.1
```

## Configurazione VPN IPsec (manuale base)

### Configurazione ISAKMP/IKE Phase 1 (negoiazione chiave)

**R1:**

```
R1(config)# crypto isakmp policy 10
```

Creazione di una policy ISAKMP (IKE Phase 1) per avviare un tunnel VPN IPsec.

Serve per **costruire il canale sicuro iniziale** su cui poi si baserà il tunnel IPsec vero e proprio (Phase 2).

**Sintassi completa:**

`crypto isakmp policy <priority>`

`<priority>` è un numero intero (es. 10). Più basso è il numero, **più alta è la priorità** della policy

Il router può avere **più policy ISAKMP** configurate (es. 10, 20, 30...).

```
R1(config-isakmp)# encr aes
```

Scelta dell'algoritmo di cifratura (es: AES, 3DES)

```
R1(config-isakmp)# hash sha
```

Scelta dell'algoritmo di hashing (SHA, MD5)

```
R1(config-isakmp)# authentication pre-share
```

Metodo di autenticazione (pre-shared key)

```
R1(config-isakmp)# group 2
```

Gruppo DH per lo scambio di chiavi (es. 1, 2, 5, 14...). Group 2 = 1024 bit

```
R1(config-isakmp)# lifetime 86400
```

Durata della fase 1 (in secondi)

```
R1(config-isakmp)# exit
```

```
R1(config)# crypto isakmp key vpn123 address 200.0.0.2
```

Serve per definire la chiave pre-condivisa (pre-shared key) da usare con un determinato peer (cioè l'altro router) per la fase 1 della VPN IPsec (ISAKMP/IKE).

Parte del comando	Significato
<b>crypto isakmp key</b>	Comando per definire una chiave condivisa tra i peer VPN
<b>vpn123</b>	La chiave segreta pre-condivisa (PSK = pre-shared key). Deve essere uguale su entrambi i router. Se la chiave non è identica su entrambi i lati la VPN non si stabilisce

<b>address 200.0.0.2</b>	L'indirizzo IP pubblico del peer remoto con cui negoziare la VPN
--------------------------	--

**R2:**

```

R2(config)# crypto isakmp policy 10
R2(config-isakmp)# encr aes
R2(config-isakmp)# hash sha
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# lifetime 86400
R2(config-isakmp)# exit
R2(config)# crypto isakmp key vpn123 address 200.0.0.1

```

**Configurazione IPsec Phase 2 (Transform Set e ACL)****R1:**

Creazione dell'ACL

```

R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255

```

Definizione IPsec

```

R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

```

Questo comando **crea un "transform set" IPsec**, cioè un **insieme di algoritmi di sicurezza** che IPsec userà nella **fase 2** del tunnel VPN per:

- **Cifrare i dati**
- **Garantire l'integrità dei dati**
- **Proteggere contro modifiche e attacchi**

Il transform set è essenziale per costruire la parte **cifrata** del tunnel.

Parte	Significato
<b>crypto ipsec transform-set</b>	Comando per creare un set di trasformazioni IPsec
<b>VPN-SET</b>	Nome arbitrario che assegna al set. Può essere qualsiasi (es. VPN-SET, SET1, AES-SET, ecc.)
<b>esp-aes</b>	Algoritmo di <b>cifratura</b> : AES (Advanced Encryption Standard), protegge la confidenzialità dei dati
<b>esp-sha-hmac</b>	Algoritmo di <b>hashing (SHA)</b> per l'integrità dei pacchetti, con HMAC (keyed-hash message authentication code)

## Creazione o attivazione di una "crypto map"

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
```

Questo comando crea o attiva una **"crypto map"**, cioè una mappa crittografica che serve per:

- **Collegare** i vari componenti della VPN (peer, ACL, transform-set)
- **Applicare la configurazione IPsec a un'interfaccia di rete**
- Definire **quale traffico deve essere cifrato e come**

La crypto map è l'elemento che **lega tutto insieme** nella configurazione VPN IPsec.

Dopo aver creato la crypto map, di solito si completano i dettagli:

```
R1(config-crypto-map)# set peer 200.0.0.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 100
R1(config-crypto-map)# exit
```

Applicazione della crypto map all'interfaccia esterna (solitamente WAN):

```
R1(config)# interface FastEthernet 0/1
R1(config-if)# crypto map VPN-MAP
```

**R2:**

Su R2 i comandi sono speculari, con gli IP invertiti:

```
R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
```

L'ACL ora considera il traffico dalla rete B verso rete A.

```
R2(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

Deve avere lo **stesso nome** e algoritmi per essere compatibile con R1.

```
R2(config)# crypto map VPN-MAP 10 ipsec-isakmp
R2(config-crypto-map)# set peer 200.0.0.1
R2(config-crypto-map)# set transform-set VPN-SET
R2(config-crypto-map)# match address 100
R2(config-crypto-map)# exit
```

Configurazione identica, con indirizzo peer inverso (200.0.0.1 = Rete 1).

```
R2(config)# interface FastEthernet 0/1
R2(config-if)# crypto map VPN-MAP
```

L'interfaccia (WAN) di R2 è anch'essa legata alla crypto map.