



## Configurazione tipica del router

### I fase

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
```

### Impostazione della chiave di autenticazione e dell'ip del router "peer" (partner)

```
crypto isakmp key cisco address 210.210.2.2
```

### II fase

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

### Indichiamo la provenienza del traffico che deve essere cifrato

```
ip access-list extended FOR-VPN
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

### Creazione cripto-mappa

```
crypto map CMAP 10 ipsec-isakmp
set peer 210.210.2.2
set transform-set TS
match address FOR-VPN
```

### Legare la mappa all'interfaccia

```
interface FastEthernet0/0 crypto map CMAP
```

### IPSec comprende:

- |  |
|--|
| <b>1. AH (Authentication header)</b>   |
| <b>2. ESP (Encapsulating Security Payload)</b>   |
| <b>3. IKE (Internet Key Exchange)</b><br>che a sua volta ne comprende tre:<br><b>ISAKMP</b><br><b>Oakley e Skeme</b> |

### 3) Verifica configurazione:

```
show crypto isakmp sa //controllo del tunnel "tecnologico" (SA che è Security Association)
show crypto ipsec sa // controllo del tunnel IPSec
```