Ministero dell'Istruzione dell''Università e della Ricerca

ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITTL – INFORMATICA E TELECOMUNICAZIONI

ARTICOLAZIONE TELECOMUNICAZIONI

Tema di: SISTEMI E RETI

Tipologia c

ESEMPIO PROVA

Il candidato (che potrà eventualmente avvalersi delle conoscenze e competenze maturate attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda) svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

Due edifici aziendali, distanti qualche km, ma facenti parte della stessa struttura produttiva, impiegano due reti indipendenti strutturate come di seguito definito.

Edificio 1.

Rete interna, collegata ad internet tramite un ISP (*Internet Service Provider*), costituita da due sottoreti distinte separate da un router, definite come:

- rete del settore commerciale, dedicata agli specifici operatori;
- rete contabile, dedicata agli specifici operatori, che dovrà farsi carico delle problematiche legate alla presenza di dati sensibili.

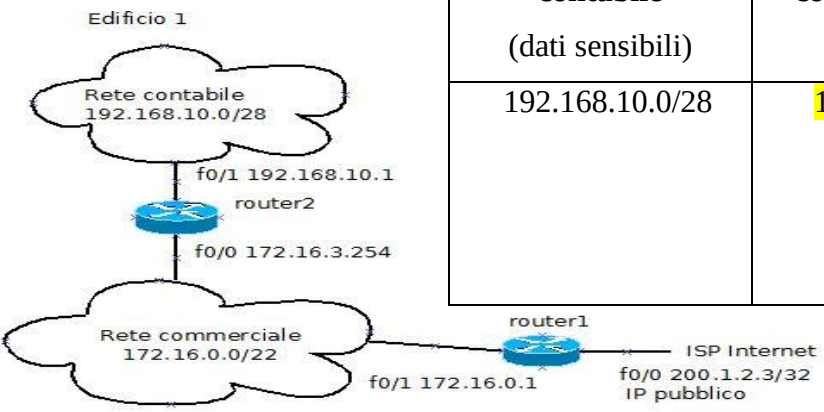
L'edificio 1 risulta già adeguatamente cablato in termini di rete e si dovrà eventualmente intervenire solo sugli aspetti relativi alla sicurezza.

Edificio 2.

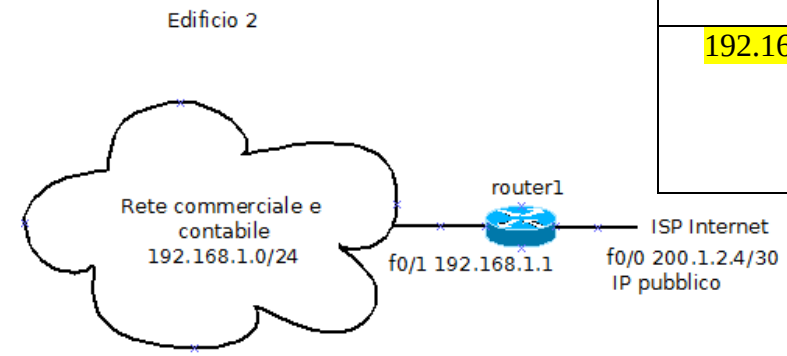
Rete unica ad uso commerciale e contabile, definita in un unico spazio di indirizzamento e collegata ad internet tramite un ISP.

I seguenti schemi ne riassumono le caratteristiche

(NB: gli indirizzi IP sono stati leggermente modificati per evitare conflitti con la rete esterna al laboratorio)



Sottorete contabile (dati sensibili)	**Sottorete commerciale**	**ISP IP pubblico**
192.168.10.0/28	172.26.0.0/22	200.1.2.3/30 ERRATO: è ind. di broadcast: subnet 200.1.2.0/30



Unica rete	**ISP IP pubblico**
192.168.110.0/24	200.1.2.4/30 ERRATO: è un indirizzo di subnet

Il candidato, formulata ogni ipotesi aggiuntiva che ritenga opportuna, predisponga quanto segue:

a. individui i punti di debolezza e le possibili soluzioni da adottare nell'edificio 1, in termini di sicurezza delle reti;

b. progetti la struttura di rete e di indirizzamento dell'edificio 2, che prevede un numero massimo di 7 host per la rete contabile e 15 host per quella commerciale;

c. descriva una soluzione tecnica per separare nell'edificio 2 la rete commerciale dalla rete contabile; gli utenti della rete commerciale non devono poter accedere alla rete contabile; entrambe le utenze devono poter accedere ad Internet aggiungendo, se necessario, anche nuovi apparati;

d. proponga una struttura di collegamento tra i settori commerciali dei due edifici, attraverso la rete Internet, che permetta agli operatori addetti alle postazioni commerciali di comunicare tra loro, con particolare attenzione alla sicurezza e riservatezza dei dati che vengono scambiati tra le due reti.

SECONDA PARTE

Il candidato scelga due fra i seguenti quesiti e per ciascun quesito scelto formuli una risposta della **lunghezza massima di 20 righe** esclusi eventuali grafici, schemi e tabelle.

QUESITO N. 1

Con riferimento al punto D) della prima parte della prova, indicare le caratteristiche principali del protocollo che si è inteso utilizzare.

QUESITO N. 2

Proporre una struttura di collegamento tra i settori contabili dei due edifici, attraverso la rete Internet, che permetta agli operatori addetti alle postazioni contabili di comunicare tra loro, con particolare attenzione alla sicurezza e riservatezza dei dati che vengono scambiati tra le due reti, anche prevedendo l'acquisizione di ulteriori indirizzi IP statici dall' ISP.

QUESITO N. 3

Descrivere le caratteristiche più importanti relative alle tecniche di crittografia a chiave simmetrica ed asimmetrica.

QUESITO N. 4

Nell'ipotesi di istituire un servizio di scambio di messaggi di testo, descrivere, eventualmente anche con un esempio utilizzando un linguaggio a scelta, un socket di comunicazione di tipo client/server adatto allo scopo e definire una possibile architettura hardware.

Durata massima della prova: 6 ore.
È consentito l'uso di manuali tecnici e di calcolatrice non programmabile.
È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.
Il candidato è tenuto a svolgere la prima parte della prova ed a rispondere a 2 tra i quesiti proposti.
Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

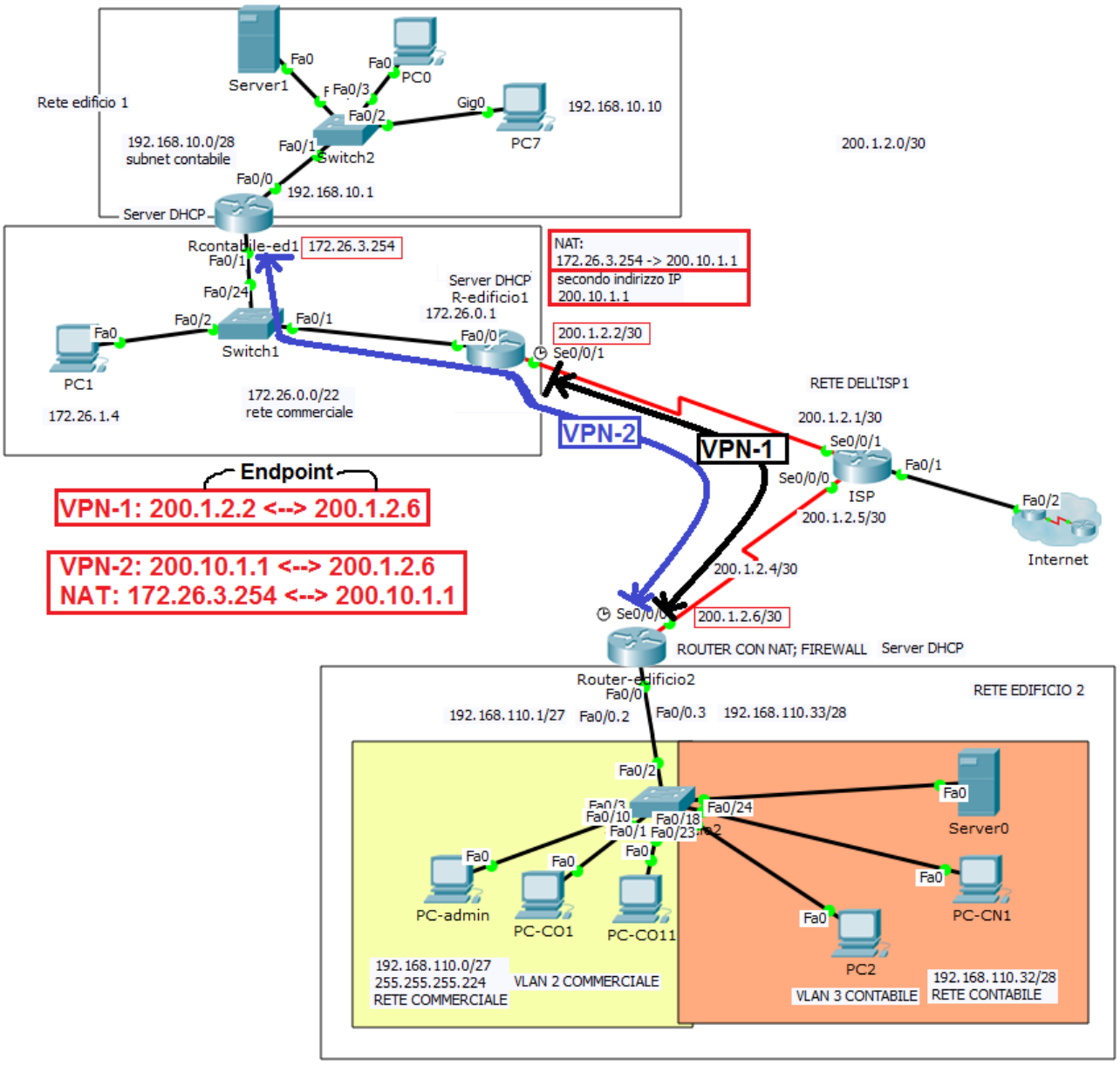
Verifica della soluzione proposta tramite la realizzazione in laboratorio dell'infrastruttura di rete
(a cura del Prof. Onelio G. Bertazioli)

Apparati impiegati: 4 router Cisco ISR 1841; 3 switch Cisco Catalyst 2950

Note:

- **per evitare conflitti tra gli indirizzi IP effettivamente in uso al di fuori del laboratorio sono stati modificati nel seguente modo i blocchi di indirizzi IP privati utilizzati:**
  - **172.26.0.0/22 invece di 172.16.0.0/22**
  - **192.168.110.0/24 invece di 192.168.1.0/24**
- **NON configurare gli indirizzi IP pubblici indicati dal tema su router direttamente collegati a Internet, ma solo nella rete del laboratorio, in quanto essi sono indirizzi IP realmente utilizzati su Internet da altre organizzazioni.**

L'infrastruttura di rete che si realizza è la seguente:



Per quanto concerne il piano di indirizzamento ricaviamo dal blocco di indirizzi IPv4 privati a disposizione (192.168.110.0/24) due sottoblocchi che abbiano un numero di indirizzi IPv4 il più possibile vicini al numero effettivo di host, ciò per motivi di sicurezza.

- **Piano di indirizzamento per la rete commerciale**
  Essendo la sottorete commerciale di 15 host sono necessari almeno 17 indirizzi IPv4 (1 per la subnet e 1 per il broadcast), per cui gli indirizzi IP devono avere una parte host di almeno 5 bit e un prefisso di rete che al massimo ha 27 bit. Scegliamo quindi la subnet mask /27 (255.255.255.224) che consente di avere nella subnet fino a 32-2=30 indirizzi per gli host.
  La sottorete commerciale può quindi essere configurata con il blocco di indirizzi IP 192.168.110.0/27
  La configurazione IP dei PC (indirizzo IP, subnet mask, gateway, server DNS) può essere fatta tramite un server DHCP oppure in modo statico (visto il numero esiguo di PC). Per motivi di sicurezza può essere conveniente dare in ogni caso indirizzi statici, in modo da individuare facilmente i PC nel caso di analisi di traffico ecc.

  Il piano di indirizzamento per la sottorete commerciale dell'edificio 2 è quindi il seguente:

SOTTORETE COMMERCIALE /27 MAX 30 HOST

Indirizzi IPv4	Subnet Mask	Note
192.168.110.0	255.255.255.224	Subnet Address
192.168.110.1	255.255.255.224	GATEWAY, Interfaccia Fa0/0.1 del router
192.168.110.2	255.255.255.224	può essere assegnato allo switch
192.168.110.3	255.255.255.224	
192.168.110.4	255.255.255.224	altri indirizzi assegnabili staticamente ad altri apparati di rete (access point, ecc.)
192.168.110.5	255.255.255.224	
192.168.110.6	255.255.255.224	
192.168.110.7	255.255.255.224	
192.168.110.8	255.255.255.224	
192.168.110.9	255.255.255.224	
192.168.110.10	255.255.255.224	----------
192.168.110.11	255.255.255.224	
192.168.110.12	255.255.255.224	
192.168.110.13	255.255.255.224	
192.168.110.14	255.255.255.224	
192.168.110.15	255.255.255.224	
192.168.110.16	255.255.255.224	indirizzi IP assegnati ai client via DHCP statico
192.168.110.17	255.255.255.224	con alcuni indirizzi di scorta
192.168.110.18	255.255.255.224	
192.168.110.19	255.255.255.224	
192.168.110.20	255.255.255.224	
192.168.110.21	255.255.255.224	
192.168.110.22	255.255.255.224	
192.168.110.23	255.255.255.224	
192.168.110.24	255.255.255.224	----------
192.168.110.25	255.255.255.224	assegnabili in modo statico a eventuali server
192.168.110.26	255.255.255.224	
192.168.110.27	255.255.255.224	
192.168.110.28	255.255.255.224	
192.168.110.29	255.255.255.224	
192.168.110.30	255.255.255.224	
192.168.110.31	255.255.255.224	Broadcast Address

- **Piano di indirizzamento per la rete contabile dell'edificio 2**
  Essendo la sottorete contabile di 7 host sono necessari almeno 9 indirizzi IPv4 (1 per la subnet e 1 per il broadcast), per cui gli indirizzi IP devono avere una parte host di almeno 4 bit e un prefisso di rete che al massimo ha 28 bit. Scegliamo quindi la subnet mask /28 (255.255.255.240) che consente di avere nella subnet fino a 16-2=14 indirizzi per gli host.
  Poiché l'indirizzo di broadcast della rete commerciale è il 192.168.110.31, a sottorete contabile può quindi essere configurata con il blocco di indirizzi IP 192.168.110.32/28.
  La configurazione IP dei PC (indirizzo IP, subnet mask, gateway, server DNS) può essere fatta tramite un server DHCP oppure in modo statico (visto il numero esiguo di PC). Per motivi di sicurezza può essere conveniente dare in ogni caso indirizzi statici, in modo da individuare facilmente i PC nel caso di analisi di traffico ecc.

RETE CONTABILE /28 (MAX 14 HOST)

Indirizzi IPv4	Subnet Mask	Note
192.168.110.32	255.255.255.240	Subnet Address
192.168.110.33	255.255.255.240	GATEWAY, interfaccia Fa0/0.2 del router
192.168.110.34	255.255.255.240	altri indirizzi statici per altri apparati di rete
192.168.110.35	255.255.255.240	
192.168.110.36	255.255.255.240	
192.168.110.37	255.255.255.240	----------
192.168.110.38	255.255.255.240	indirizzi IP assegnati ai client via DHCP statico
192.168.110.39	255.255.255.240	
192.168.110.40	255.255.255.240	
192.168.110.41	255.255.255.240	
192.168.110.42	255.255.255.240	
192.168.110.43	255.255.255.240	
192.168.110.44	255.255.255.240	----------
192.168.110.45	255.255.255.240	indirizzi assegnabili in modo statico a eventuali server
192.168.110.46	255.255.255.240	
192.168.110.47	255.255.255.240	Broadcast Address

Nel caso in cui si prevedano numerosi altri inserimenti in rete (per esempio di PC, smartphone, tablet via Wi-Fi) è possibile optare per una subnet mask **/26** (255.255.255.192) per la rete commerciale, che mette a disposizione 62 indirizzi IP per gli host, e una **/27** (255.255.255.192) per la rete commerciale, che mette a disposizione 30 indirizzi IP per gli host.
Per l'edificio 2 visto che ci sono pochi PC (7+15=22 host in totale) e si tratta di una filiale, se si desidera limitare i costi si può utilizzare un solo switch amministrabile su cui si configurano tre VLAN:

- VLAN 1, di gestione (management VLAN) a cui si collega il PC utilizzato dall'amministratore di rete collegato in modo sicuro (port security) alla Fa 0/1
- **VLAN 2 *name* Commerciale**, a cui si collegano i PC dei commerciali (supponiamo siano 13 dato consideriamo come host anche le interfacce dei router e lo switch amministrabile) sulle porte fa0/9-16
- **VLAN 3 *name* contabile**, a cui si collegano i PC dei contabili (supponiamo siano 6 dato consideriamo come host anche le interfacce dei router) sulle porte fa0/17-24; i PC siano collegati in modo sicuro alle rispettive porte (port security) che accettano solo frame con i loro indirizzi MAC; in caso di violazione la porta va in shutdown

La porta FastEthernet 0/1 dello switch, collegata alla Fa0/0 del router, viene configurata come *trunk* Le rimanenti porte dello switch possono essere spente (poste in shutdown) se si desidera evitare ulteriori inserimenti in rete (in questo caso ritenuti abusivi).

I router utilizzati hanno un sistema operativo con modulo di crittografia, sono in grado di svolgere anche la funzione di firewall e di implementare le VPN.

Condivisione dell'accesso a Internet.
Per far condividere l'accesso a Internet ad entrambe le reti sull'interfaccia fisica FastEthernet0/0 si configurano due sottointerfacce:

- Fa0/0.2, avente indirizzo IP 192.168.110.1/27, con incapsulamento 802.1q (*dot1q*) e appartenente alla VLAN 100
- Fa0/0.3, avente indirizzo IP 192.168.110.33/28, con incapsulamento 802.1q (*dot1q*) e appartenente alla VLAN 200.

Per separare le reti commerciale e contabile si configurano sul router due *Access Control List* (ACL) standard, per esempio la 2 e la 3, e le si applica alle due sottointerfacce impedendo (deny) ai pacchetti IP contenenti l'indirizzo di rete di una subnet di transitare sulla sottointerfaccia a cui è collegata l'altra subnet

Infine poiché sulle reti interne si utilizzano indirizzi IPv4 privati, è necessario implementare nel router la funzione NAT (Network Address Translation), preferibilmente richiedendo un indirizzo IPv4 pubblico statico al'ISP.

Configurazione degli switch e del/dei router

Configurazione delle VLAN su switch Cisco

- Creazione VLAN

```
Switch(config)#vlan 2
Switch(config-vlan)#name commerciale
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name contabile
Switch(config-vlan)#exit
Switch(config)# exit

Switch#show vlan brief
.......ouput omesso ......
```

- Assegnazione delle porte alle VLAN

```
Switch(config)#interface range fa0/9-16
Switch(config-if-range)#switchport access vlan 2 (commerciale)
Switch(config-if-range)#

Switch(config)#interface range fa0/17-24
Switch(config-if-range)#switchport access vlan 3  (contabile)
Switch(config-if-range)#end
```

- l'interfaccia verso il router viene configurata come trunk

```
Switch(config)#interface Fa0/2
```

```
Swirch(config-if)#switchport mode trunk
Switch(config-if)#end
```

- sul router si creano le sottointerfacce della Fa0/0 e le si associa alle rispettive VLAN

```
router-edificio2 (config)#interface Fa0/0.2                    (commerciale)
router-edificio2 (config-subif)#encapsulation dot1q  2
router-edificio2 (config-subif)#ip address 192.168.110.1 255.255.255.224
router-edificio2 (config-subif)#interface Fa0/0.3                                  (contabile)
router-edificio2 (config-subif)#encapsulation dot1q  3
router-edificio2 (config-subif)#ip address 192.168.110.33 255.255.255.240
```

- Per separare le reti commerciale e contabile si usano due Access Control List (ACL) standard, la 2 e la 3

ACL 3 che:

- nega (*deny*) l'uscita di pacchetti aventi indirizzo sorgente appartenente alla rete 192.168.110.0/27
- permette (*permit*) il resto (any):

```
router-edificio2(config)#access-list 3 deny 192.168.110.0 0.0.0.31
router-edificio2(config)#access-list 3 permit any
```

ACL 2 che

- nega (deny) l'uscita di pacchetti aventi indirizzo sorgente appartenente alla rete 192.168.110.32/28
- permette (permit) il resto (any):

```
router-edificio2(config)#access-list 2 deny 192.168.110.32 0.0.0.15
router-edificio2(config)#access-list 2 permit any
```

- applichiamo l'ACL 99 3 alla sottointerfaccia Fa0/0.2 (192.168.110.33)
- applichiamo l'ACL 1 2 alla sottointerfaccia Fa0/0.1 (192.168.110.1)

```
router-edificio2(config)#int Fa0/0.2
router-edificio2(config-subif)#ip access-group 2 out
router-edificio2(config-subif)#exit

router-edificio2(config)#int Fa0/0.3
router-edificio2(config-subif)#ip access-group 3 out
router-edificio2(config-subif)#end
```

- Configurazione del NAT overload o PAT in assenza di VPN

Poiché nelle reti interne si utilizzano indirizzi IPv4 privati, va poi configurata la funzione NAT/PAT (NAT overload) sul router, che sostituisce nei pacchetti IP in uscita gli indirizzi IPv4 privati con un indirizzo IP pubblico (qui si utilizza quello dell'interfaccia wan del router) ed effettua la sostituzione inversa per i pacchetti ricevuti da Internet.

```
router-edificio2#conf  term
Enter configuration commands, one per line. End with CNTL/Z.
router-edificio2(config)#access-list 10 permit 192.168.110.0 0.0.0.255
router-edificio2(config)#ip nat inside source list 10 interface se0/0/0 overload
router-edificio2(config)#interface se0/0/0
router-edificio2(config-if)#ip nat outside
router-edificio2(config-if)#exit
router-edificio2(config)#int Fa0/0.2
router-edificio2(config-subif)#ip nat inside
```

```
router-edificio2(config-subif)#exit
router-edificio2(config)#int Fa0/0.3
router-edificio2(config-subif)#ip nat inside
router-edificio2(config-subif)#exit
router-edificio2(config)#end
```

Verifica del NAT dopo avere fatto un ping da un PC della rete commerciale dell'edificio 2 verso l'interfaccia WAN del router dell'edificio 1

```
router-edificio2#show ip nat translations
```

....output omesso.....

NAT R-edificio1

```
router-edificio1#conf  term
Enter configuration commands, one per line. End with CNTL/Z.
router-edificio1(config)#access-list 10 permit 172.26.0.0  0.0.3.255
router-edificio1(config)#ip nat inside source list 10 interface fa0/1 overload
router-edificio1(config)#interface Fa0/1
router-edificio1(config-if)#ip nat outside
router-edificio1(config-if)#exit
router-edificio1(config)#int Fa0/0
router-edificio1(config-if)#ip nat inside
router-edificio1(config-if)#exit
```

NAT Rcontabile-ed1

```
Rcontabile-ed1#conf  term
Enter configuration commands, one per line. End with CNTL/Z.
Rcontabile-ed1 (config)#access-list 10 permit 192.168.10.0 0.0.0.15
Rcontabile-ed1 (config)#ip nat inside source list 10 interface fa0/1 overload
Rcontabile-ed1 (config)#interface Fa0/1
Rcontabile-ed1 (config-if)#ip nat outside
Rcontabile-ed1 (config-if)#exit
Rcontabile-ed1 (config)#int Fa0/0
Rcontabile-ed1 (config-subif)#ip nat inside
Rcontabile-ed1 (config-subif)#exit
```

ACL che impedisce ai PC della subnet 172.16.0.0 di accedere alla sottorete contabile

```
Rcontabile-ed1(config)#access-list 1 deny 172.16.0.0 0.0.3.255
Rcontabile-ed1(config)#access-list 1 permit any
Rcontabile-ed1(config)#interface fa0/0
Rcontabile-ed1(config-if)#ip access-group 1 out
Rcontabile-ed1(config-if)#end
```

Con le configurazioni effettuate le reti commerciale e contabile dell'edificio 2 sono separate e non comunicanti, ma possono condividere lo stesso accesso a Internet e quindi raggiungere il router dell'edificio 1.

- Verifica della connettività in assenza di VPN

Per testare il corretto funzionamento della rete, da due PC appartenenti alle due sottoreti (per esempio il 192.168.110.11 della rete commerciale e il 192.168.110.35 della rete contabile):

- facciamo un ping verso l'interfaccia WAN del router dell'edificio 1 (indirizzo IP 200.1.2.2); il ping che deve avere risposta

- facciamo un ping verso un sito Internet o vi accediamo con un browser; il ping che deve avere risposta;
- facciamo un ping da un PC (es. 192.168.110.11) verso l'altro PC (es. 192.168.110.35); il ping non deve avere risposta a dimostrazione che le due sottoreti sono effettivamente separate.

Tutto questo serve a dimostrare che:
- le due sottoreti condividono lo stesso accesso a Internet
- dalla sottorete commerciale dell'edificio 2 è possibile comunicare con il router dell'edificio 1

NB: verso Internet non è possibile utilizzare indirizzi IPv4 privati, per cui non si possono pingare direttamente gli indirizzi IP delle reti 172.26.0.0/22 e 192.168.10.0/28

QUESITO N. 2

Proporre una struttura di collegamento tra i settori contabili dei due edifici, attraverso la rete Internet, che permetta agli operatori addetti alle postazioni contabili di comunicare tra loro, con particolare attenzione alla sicurezza e riservatezza dei dati che vengono scambiati tra le due reti, anche prevedendo l'acquisizione di ulteriori indirizzi IP statici dall' ISP.

In questo caso va richiesto un ulteriore indirizzo IP pubblico, di tipo statico, da utilizzare per realizzare una seconda VPN site-to-site basata su IPsec in cui il traffico "interessante", cioè che transita attraverso il "tunnel" VPN è quello che ha come indirizzi IP quelli delle due reti contabili *opportunamente "nattate"*.

Per esempio:
- il router interno della sottorete contabile dell'edificio 1 effettua un NAT tra gli indirizzi interni (192.168.10.x/28) e l'indirizzo della sua porta tramite cui si accede alla sottorete commerciale (per esempio il 172.16.3.254/22),
- il Router-1 che dà l'accesso a Internet per l'edificio 1 effettua un NAT tra l'indirizzo interno 172.16.3.254 e il nuovo indirizzo IP pubblico statico (per esempio il 200.10.1.1);

Se le VPN vengono realizzate tramite i router (che integrano anche un firewall) si ha così che:
- la VPN1 crea un *tunnel* che collega le due sedi commerciali e quindi ha come *endpoint* i due indirizzi pubblici iniziali (200.1.2.2 lato edificio 1 e 200.1.2.6 lato edificio 2);
- la VPN2 crea un *tunnel* che collega le due sedi contabili e quindi ha come *endpoint* l'indirizzo pubblico del router dell'edificio 2 (200.1.2.6) e l'ulteriore indirizzo IP pubblico acquistato per la rete dell'edificio 1 (per esempio il 200.200.1.1), il quale viene "nattato" verso l'indirizzo IP privato dell'interfaccia del router interno (172.16.3.254).

CONFIGURAZIONE DELLE VPN CON CISCO CONFIGURATION PROFESSIONAL

Poiché in presenza di NAT la configurazione a linea di comando delle VPN è piuttosto complicata da effettuare si è preferito utilizzare il software di configurazione dei router Cisco Configuration Professional (scaricabile gratuitamente dal sito www.cisco.com).
Qui di seguito se ne esemplifica l'uso

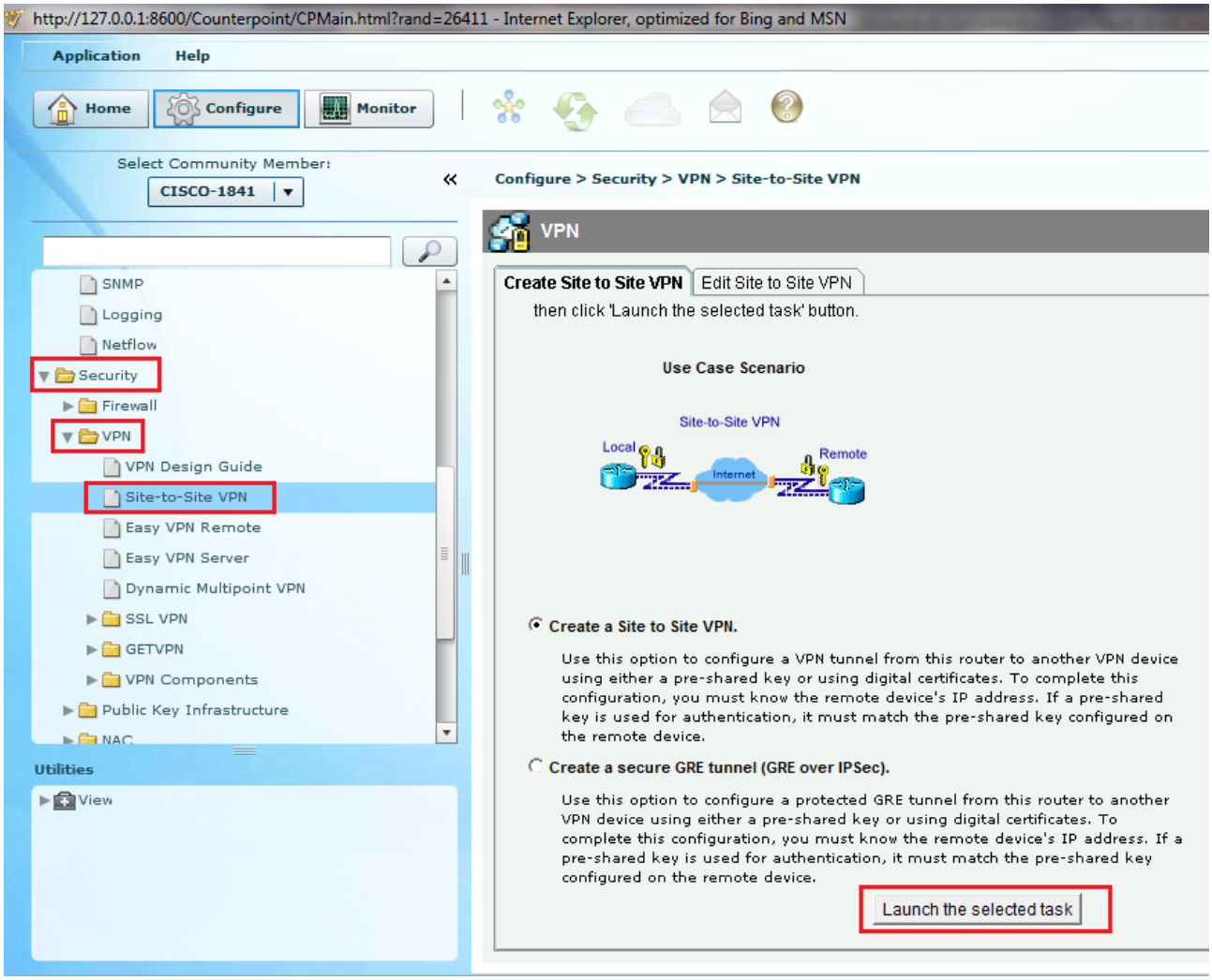
Configurazione della VPN2 sul Router-2 interno dell'edificio 1

La VPN2 crea un tunnel che collega in modo protetto le due reti contabili.

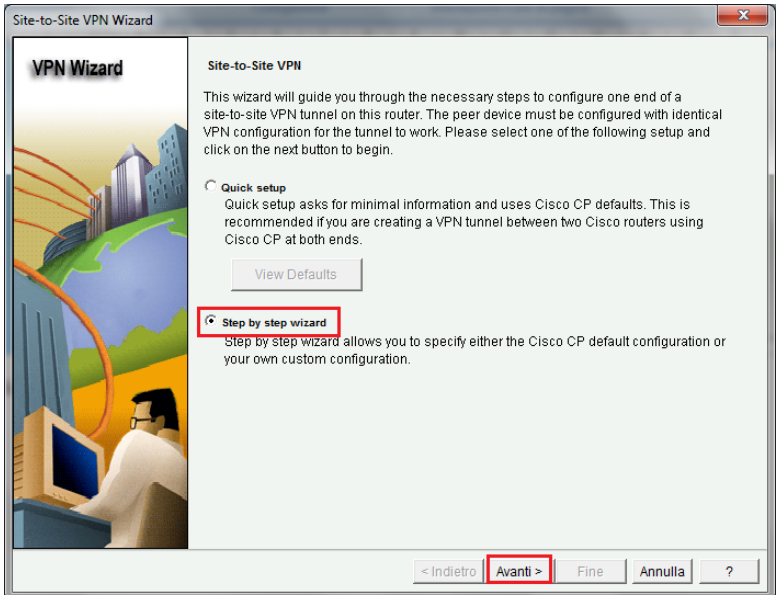
L'interfaccia esterna (Fa0/1) del Router-2 ha indirizzo IP 172.25.3.254, il quale viene "nattato" sull'indirizzo IP pubblico 200.10.1.1 ulteriore indirizzo IP acquistato) e che costituisce l'*endpoint* della VPN lato edificio 1. L'interfaccia interna del Router-2 (Fa0/0) ha indirizzo IP 192.168.10.1. L'altro *endpoint*, lato edificio 2, è l'indirizzo IP dell'interfaccia esterna (WAN) del Router 1 dell'edificio 2 (IP: 200.1.2.6).
Si procede alla configurazione della VPN operando nel seguente modo:

1. Si apre CCP ci si collega al router, si clicca su **Configure** e si seleziona:
   Security -> VPN -> Site-to-Site VPN

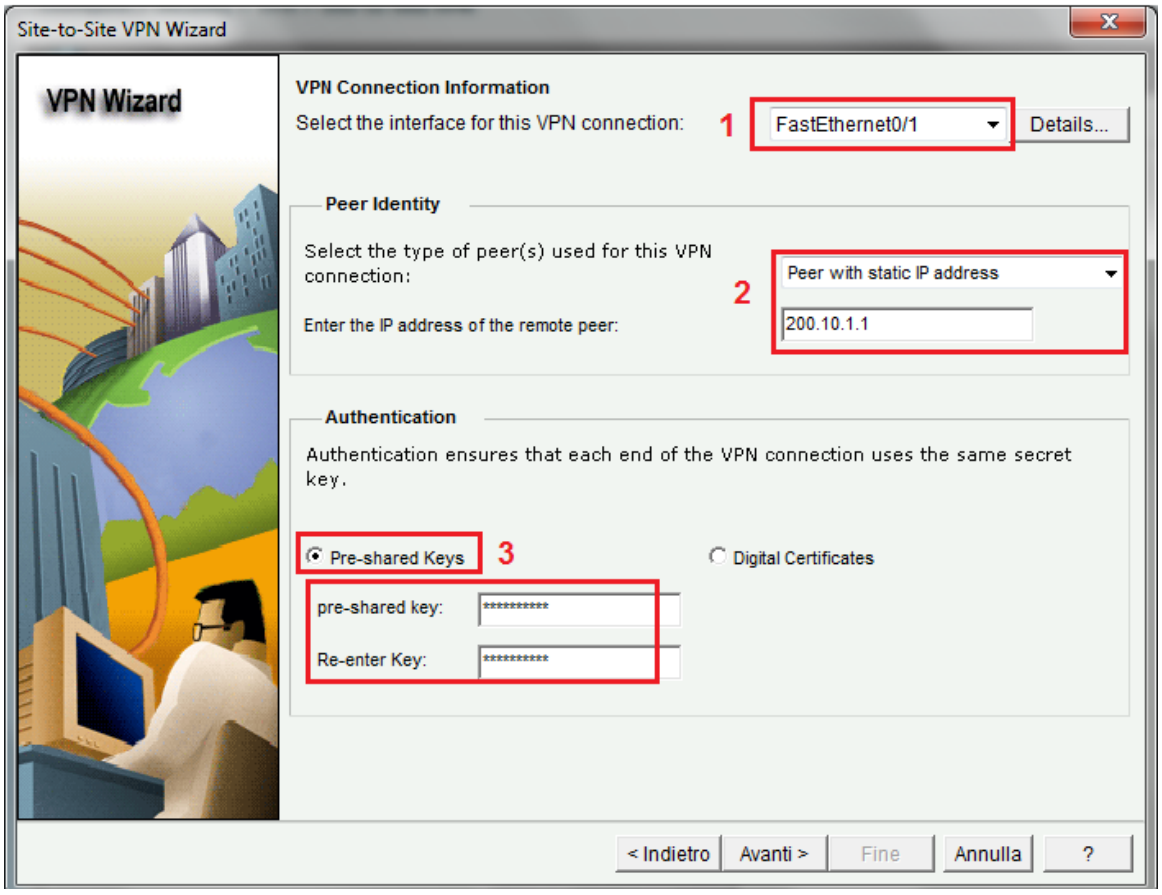
   si clicca quindi su **Launch the selected task**



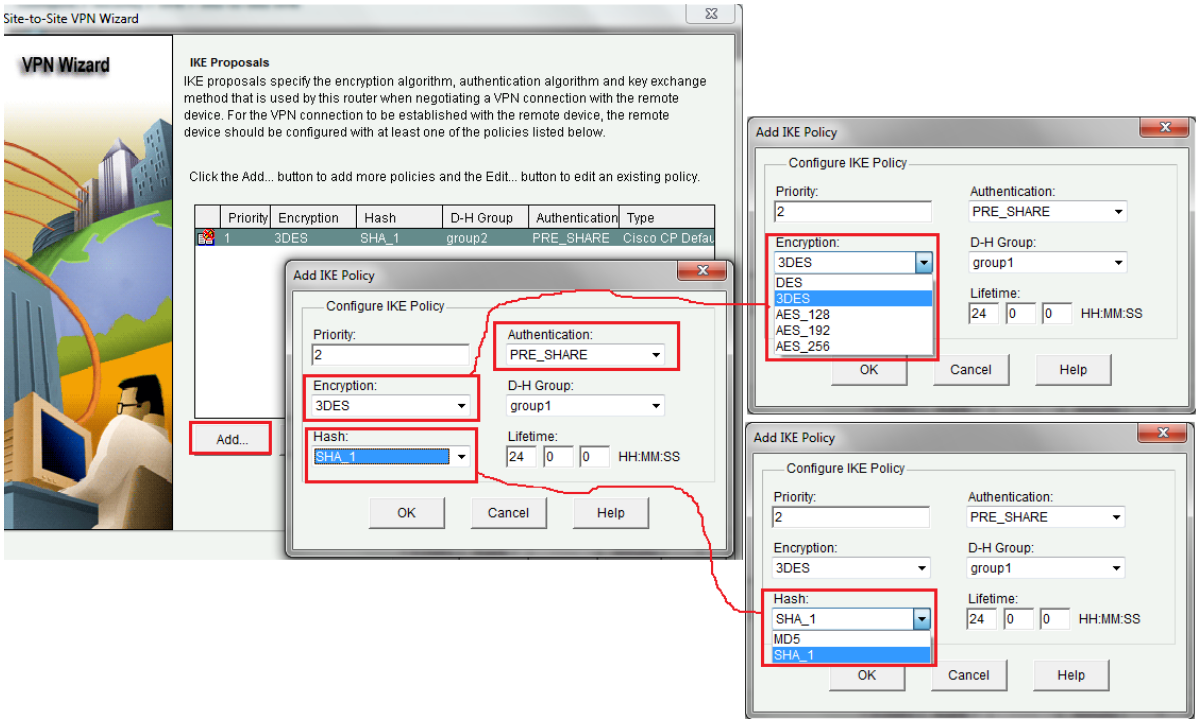
2. Si seleziona **Step by Step Wizard**



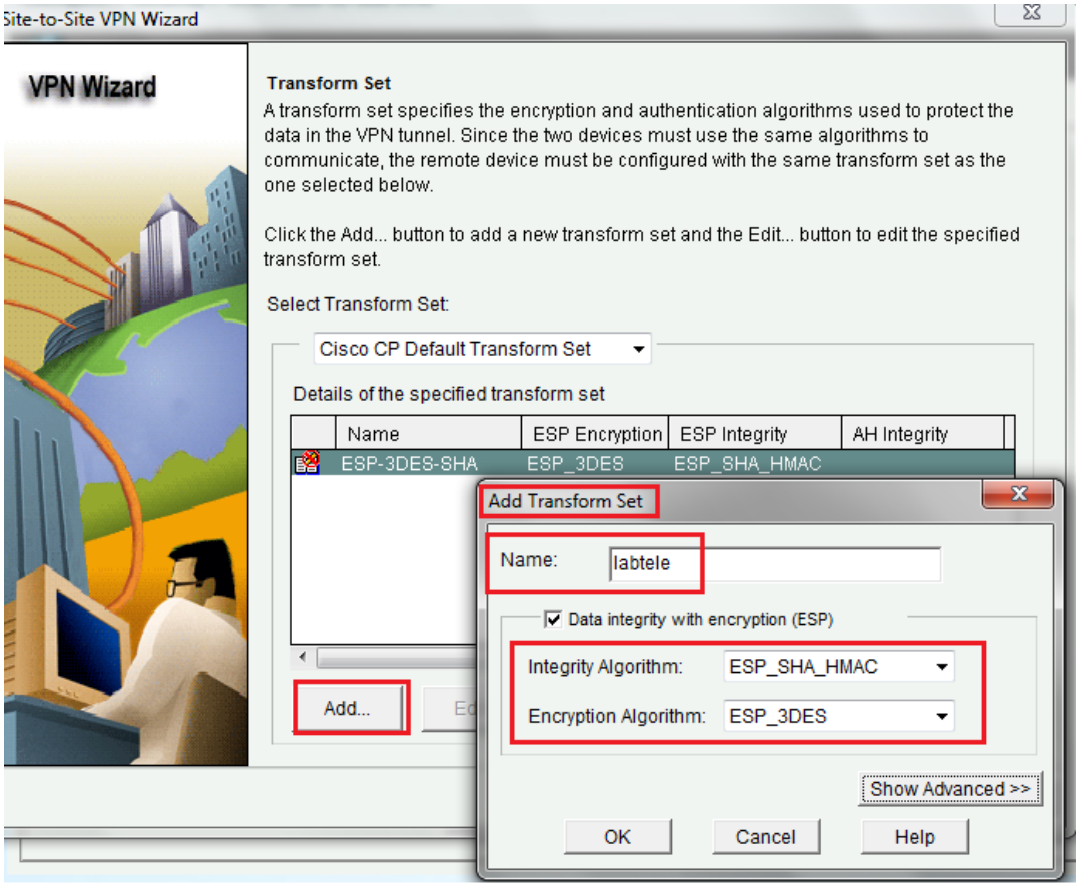
3. Si compilano i campi che appaiono nella schermata:
    1. Si sceglie l'interfaccia esterna che costituisce l'endpoint della VPN sul Router 2 (Fa0/1),
    2. Si configura l'indirizzo dell'altro endpoint (l'interfaccia esterna, WAN, del Router 1 dell'edificio 2)
    3. Si sceglie il metodo di autenticazione con chiave pre-condivisa (Pre-Shared Key) e si configura la relativa chiave (il metodo è più semplice rispetto a quello dei certificati)
    4. si clicca su Avanti



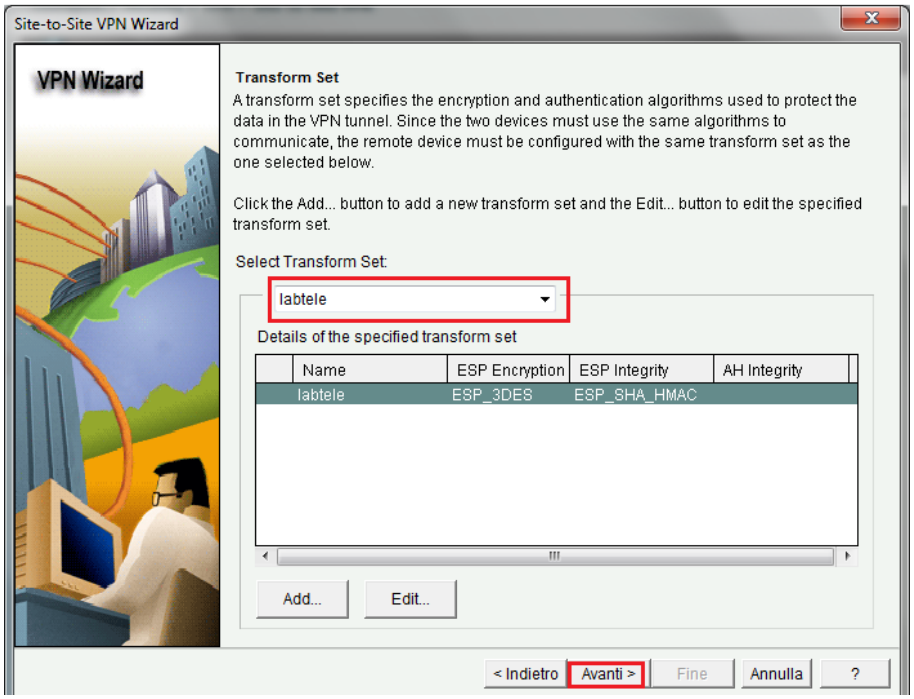
4. Cliccando su **ADD** è possibile scegliere il tipo di crittografia (DES, 3DES, AES-128 ecc.) e di autenticazione (SHA, MD5) che si vogliono impiegare.



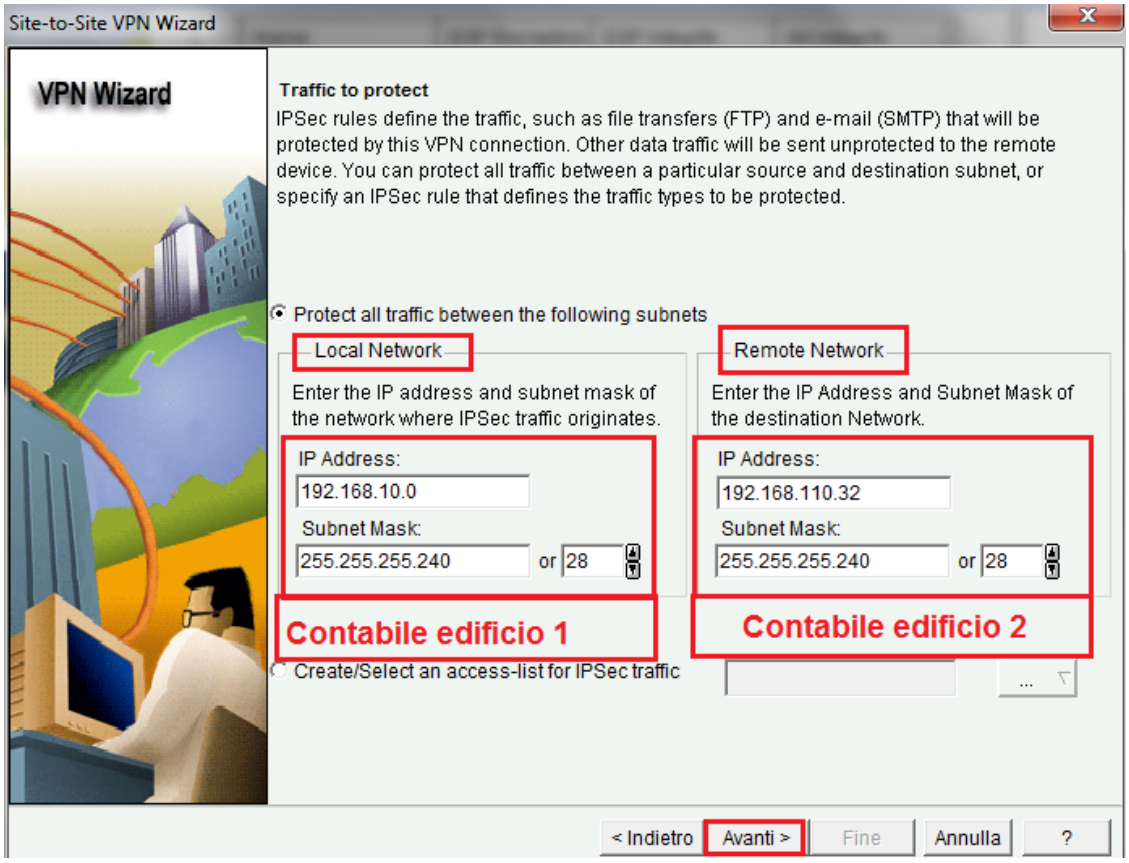
5. E' quindi possibile aggiungere un proprio **Transform Set** specificando gli algoritmi che si impiegano.



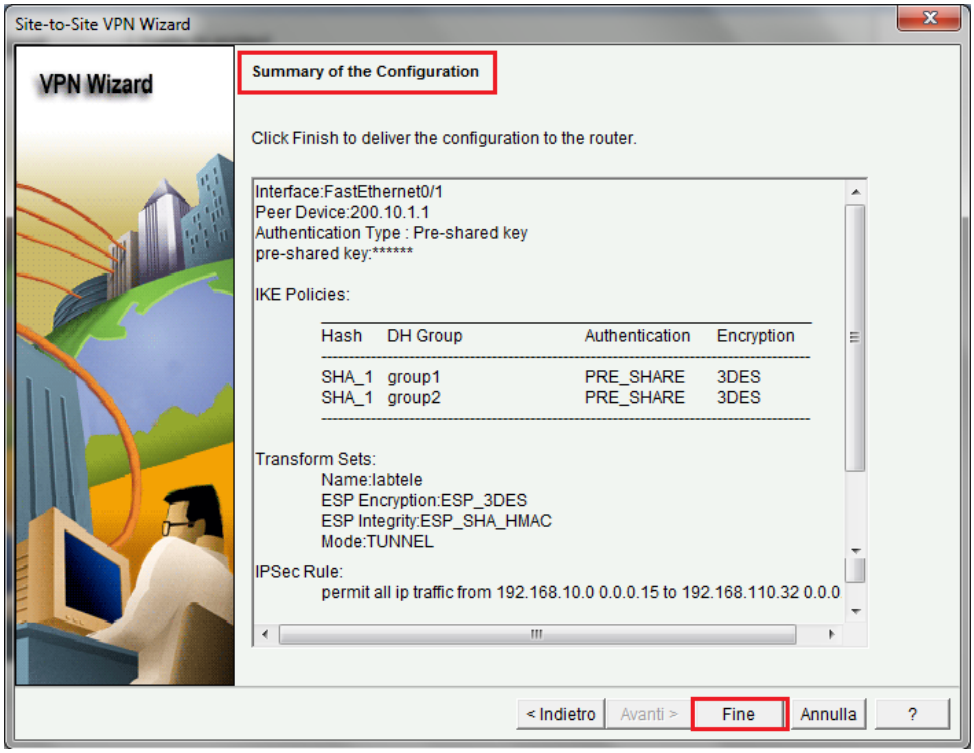
6. Si sceglie il proprio **Transform Set** (nell'esempio denominato *labtele*)



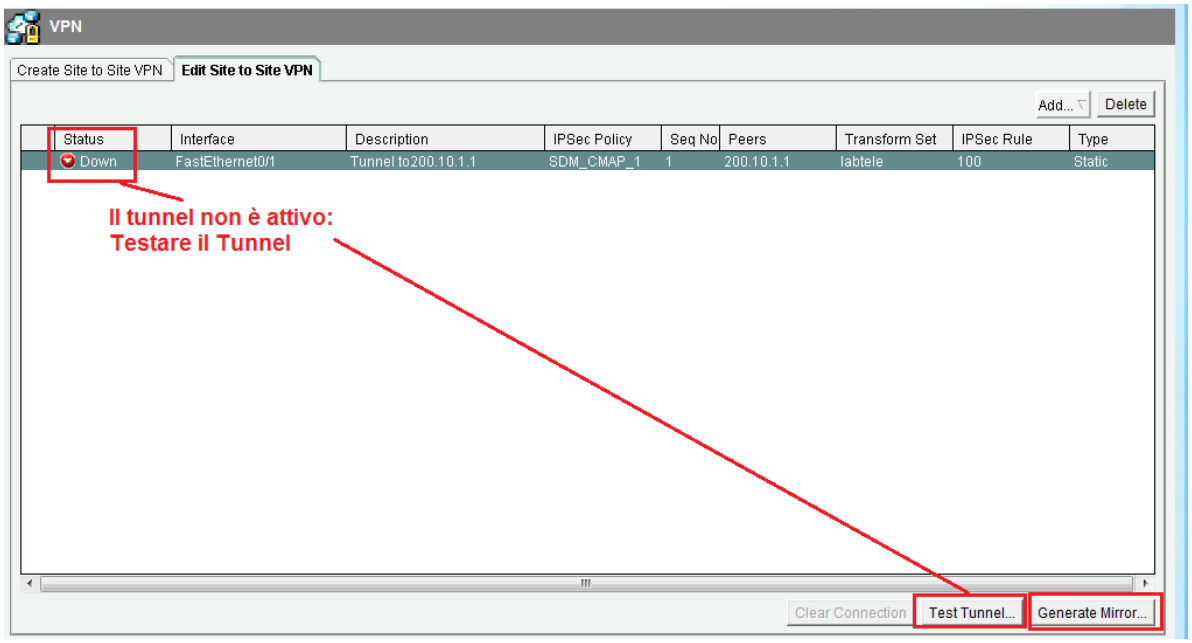
7. Si configurano gli indirizzi IP della **Local Network** (rete locale, è la sottorete contabile dell'edificio 1) e della **Remote Network** (rete remota, è la sottorete contabile dell'edificio 2), le sottoreti che devono comunicare in modo protetto



8. Si visualizza e si controlla il riassunto delle configurazioni effettuate; se tutto è corretto si clicca su **Fine**

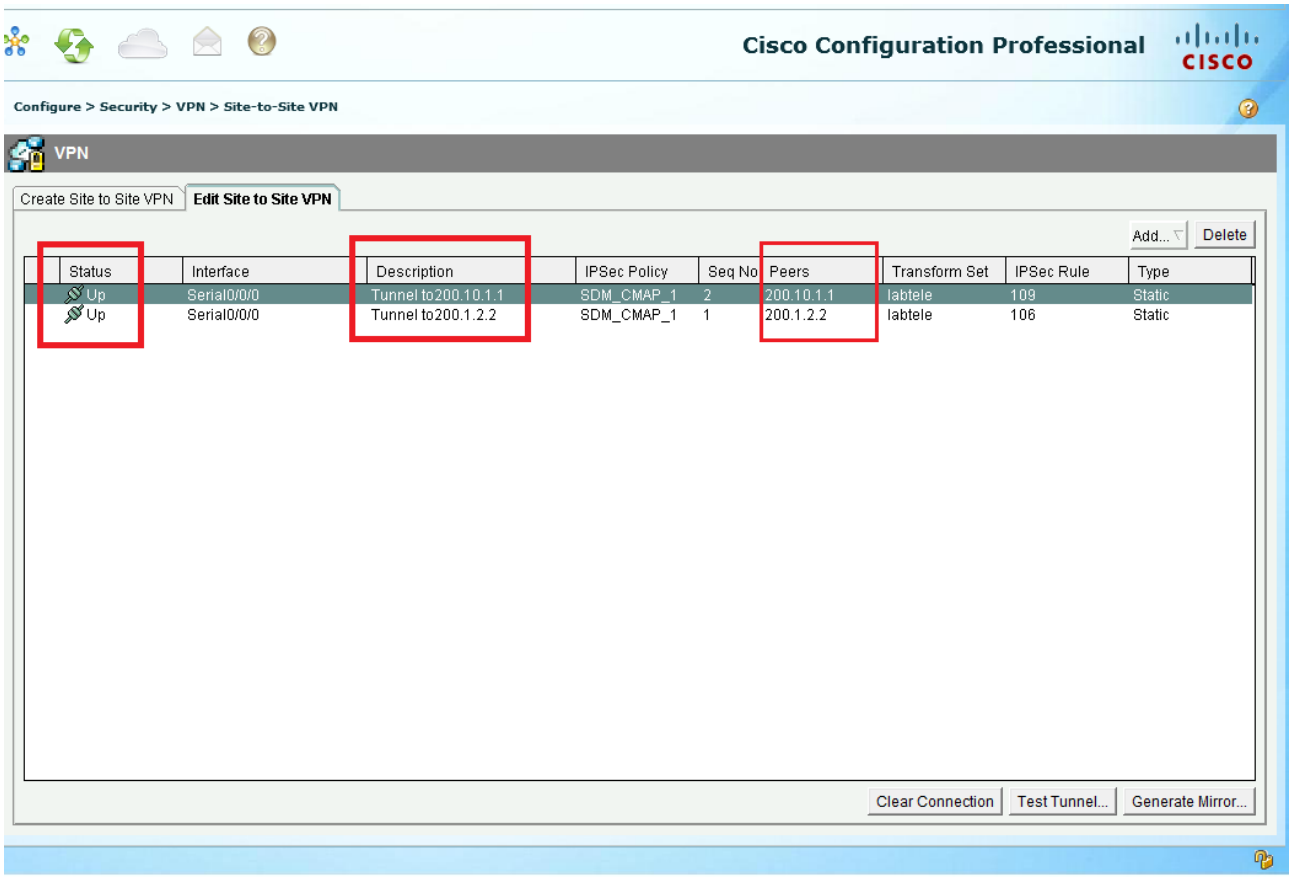


9. Se l'altro endpoint (Router 1 edificio 2) è già stato configurato si testa la funzionalità del tunnel (**Test Tunnel**); in caso di problemi CCP dà delle indicazioni per risolverli; è anche possibile generare la configurazione dell'altro endpoint (**Generate Mirror**).



Si procede in modo analogo, inserendo le configurazioni appropriate per le interfacce e gli indirizzi IP, per configurare sul Router 1 dell'edificio 1 la VPN1 che mette in comunicazione protetta da tunnel le reti commerciali degli edifici 1 e 2.

Una volta terminate le configurazioni ed effettuato il test dei tunnel, se tutto è stato configurato correttamente (compreso il NAT), le VPN diventano attive (*Status: Up*) e le reti delle due sedi vengono messe in comunicazione

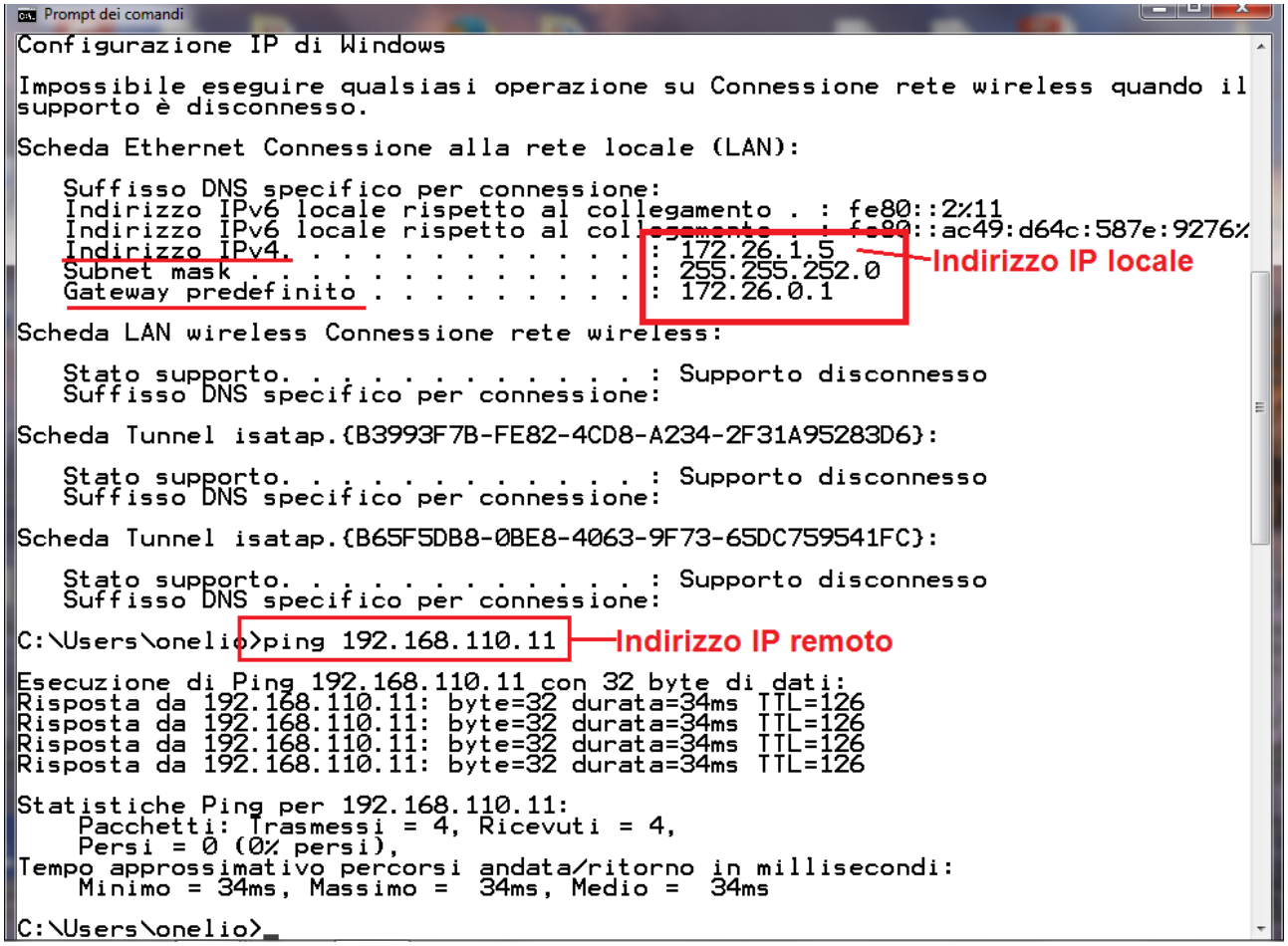


Stato attivo (Up) delle VPN instaurate sul Router 1 dell'edificio 2.

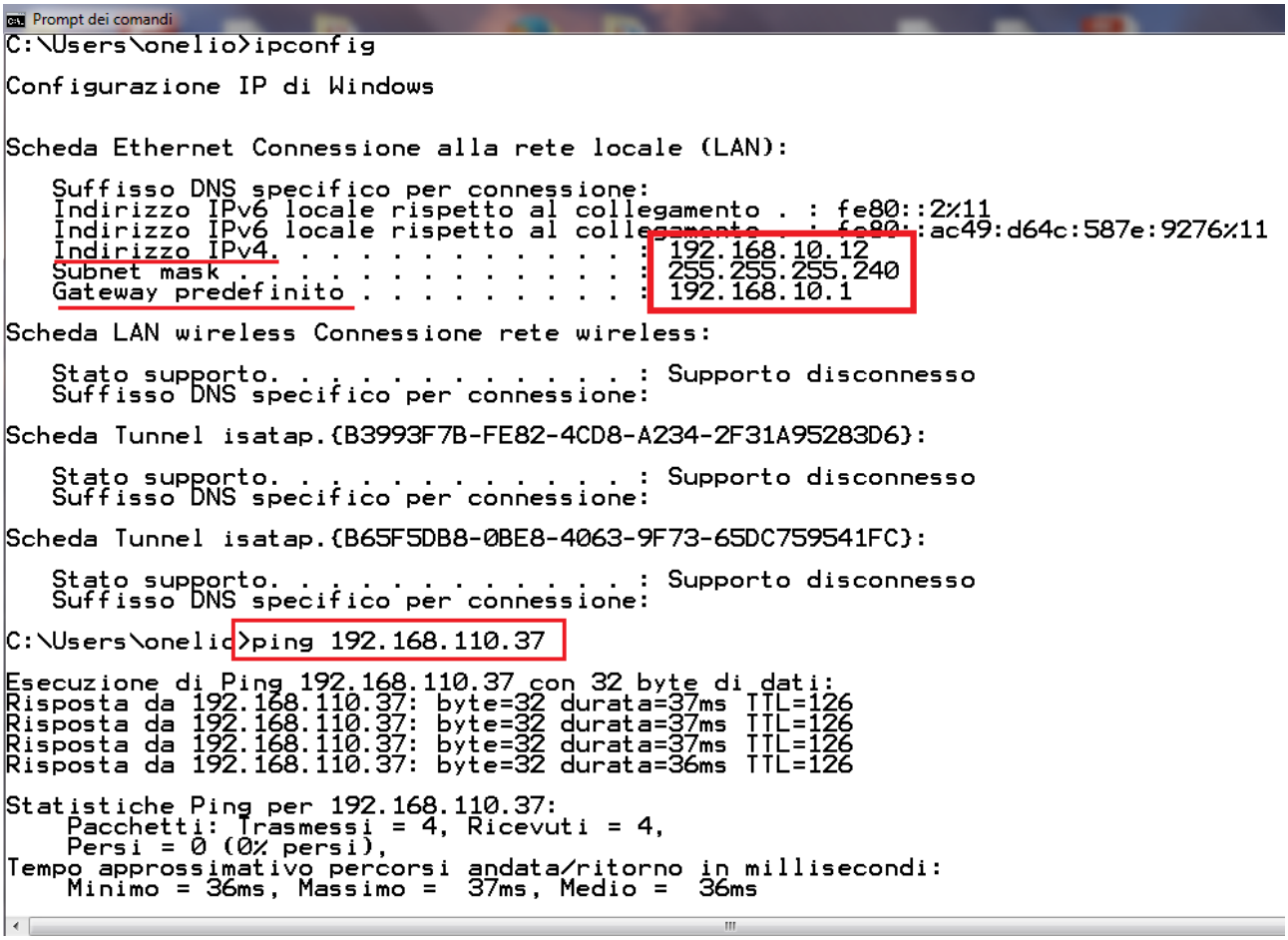
Per confermare l'avvenuta connessione tra le reti dei due edifici si effettuano dei ping (utilizzando i loro indirizzi IP privati) tra:

- un PC della sottorete commerciale dell'edificio 1 e un PC della sottorete commerciale dell'edificio 2
- un PC della sottorete contabile dell'edificio 1 e un PC della sottorete contabile dell'edificio 2

Avvertenza: prima di effettuare i ping occorre verificare se i PC hanno i Firewall personali (Windows Firewall, Zone Alarm, ecc.) attivati e in questo caso può essere necessario configurarli affinché permettano i ping stessi (o disattivarli momentaneamente prima della prova).



Ping tra un PC della rete commerciale dell'edificio 1 e un PC della rete commerciale dell'edificio 2



Ping tra un PC della rete contabile dell'edificio 1 e un PC della rete contabile dell'edificio 2

Bibliografia

Oltre ai testi scolastici di Sistemi e reti (anche per l'articolazione Informatica), consiglio l'utilizzo:

- del **Manuale Cremonese di Informatica e Telecomunicazioni** (2a edizione)
- del libro di testo:
  Onelio Bertazioli
  Corso di telecomunicazioni volume 3
  ed. Zanichelli
- del libro di testo (in particolare per la risposta al quesito 4)
  Giorgio Meini Fiorenzo Formichi
  Tecnologie e progettazione di sistemi informatici e di telecomunicazioni volume 3
  ed. Zanichelli

File di configurazione del Router-1-Edificio 1, tramite cui si accede al router dell'ISP

```
Building configuration...

Current configuration : 4676 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-edificio1
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
no aaa new-model
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 172.26.3.1 172.26.3.254
ip dhcp excluded-address 172.26.1.0 172.26.1.1
ip dhcp excluded-address 172.26.0.1 172.26.0.255
!
ip dhcp pool commerciale
   network 172.26.0.0 255.255.252.0
   default-router 172.26.0.1
   dns-server 8.8.8.8
!
!
ip name-server 85.18.200.200
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
crypto pki trustpoint TP-self-signed-2594079073
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2594079073
 revocation-check none
 rsakeypair TP-self-signed-2594079073
!
!
crypto pki certificate chain TP-self-signed-2594079073
 certificate self-signed 01
  30820243 308201AC A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32353934 30373930 3733301E 170D3730 30313031 30303031
  31385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35393430
```

```
  37393037 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100DFA2 B4C22C84 6FA4615F B482B334 EBDFDFE9 8BA6EAA6 36BE686D 4DC3BD2F
  700E51FF 6FEF91F9 D042FF42 480C1B4C 919E83F1 0FD2A336 FAD1EF8E FB55EB06
  09F26B1C 3542F790 105A5C20 9386FB25 A3E7871F C22FB576 1947F660 F551FECE
  55440622 E0620617 2BDA7ED1 F9E6D9A9 0E6C1B8A F31F71A6 83E60DAF 2D299C8A
  F0B30203 010001A3 6B306930 0F060355 1D130101 FF040530 030101FF 30160603
  551D1104 0F300D82 0B522D65 64696669 63696F31 301F0603 551D2304 18301680
  14489CE5 2A9A898D A22FAF78 71629435 390C1794 96301D06 03551D0E 04160414
  489CE52A 9A898DA2 2FAF7871 62943539 0C179496 300D0609 2A864886 F70D0101
  04050003 81810081 EB6AD918 CD0C743A EFA58DD9 50B3DFA8 4A537F97 761F4AC7
  E454BF7B 44BE4268 09B012B7 DC66A494 D959F9B1 49ED9034 8D4BC4AE C2137C01
  3AE948C7 9DB662E6 CCFD0844 34518583 64D86BF1 87D1A4B3 A52842BA E67FA8C6
  8ADDACE4 DD33FB5C FC2F6B58 A99D8472 183F39D8 C4BF778A 6B645E24 B0A01069
  7470317F 359EC4
  quit
username docente privilege 15 secret 5 $1$A/lP$PZssEE.8RkKfo8uF0jYYZ1
username studente privilege 15 secret 5 $1$3srw$3disz50i9udgF6Ugf1XL0/
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
crypto isakmp key labtelecom address 200.1.2.6
!
!
crypto ipsec transform-set labtele esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to200.1.2.6
 set peer 200.1.2.6
 set transform-set labtele
 match address 102
!
!
!
interface FastEthernet0/0
 description interf GW rete edificio1
 ip address 172.26.0.1 255.255.252.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.222 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 shutdown
 no fair-queue
!
interface Serial0/0/1
 description Interf verso ISP
 ip address 200.1.2.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 crypto map SDM_CMAP_1
!
ip default-gateway 10.0.0.1
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 200.1.2.1
!
!
ip http server
ip http authentication local
ip http secure-server
ip nat pool tele 200.10.1.1 200.10.1.1 netmask 255.255.255.255
ip nat inside source route-map SDM_RMAP_2 interface Serial0/0/1 overload
ip nat inside source static 172.26.3.254 200.10.1.1
!
access-list 10 remark CCP_ACL Category=16
access-list 10 permit 172.26.0.0 0.0.3.255
access-list 100 remark CCP_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 172.26.0.0 0.0.3.255 192.168.110.0 0.0.0.31
access-list 101 remark CCP_ACL Category=2
access-list 101 permit ip 172.26.0.0 0.0.3.255 any
access-list 102 remark CCP_ACL Category=4
access-list 102 remark IPSec Rule
access-list 102 permit ip 172.26.0.0 0.0.3.255 192.168.110.0 0.0.0.255
access-list 103 remark CCP_ACL Category=2
access-list 103 remark IPSec Rule
access-list 103 deny   ip 172.26.0.0 0.0.3.255 192.168.110.0 0.0.0.255
access-list 103 permit ip 172.26.0.0 0.0.3.255 any
!
route-map SDM_RMAP_1 permit 1
 match ip address 101
!
!
route-map SDM_RMAP_2 permit 1
 match ip address 103
!
```

```
!
!
control-plane
!
!
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input telnet ssh
line vty 5 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
end
```

File di configurazione del Router-2-Edificio 1, router interno della sottorete contabile

```
Building configuration...

Current configuration : 2685 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-contabile-ed1
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.0.0.1 192.168.10.4
ip dhcp excluded-address 192.168.10.13 192.255.255.254
ip dhcp excluded-address 192.168.10.1 192.168.10.4
ip dhcp excluded-address 192.168.10.13 192.168.10.14
!
ip dhcp pool contabile
   import all
   network 192.168.10.0 255.255.255.240
   dns-server 8.8.8.8
   default-router 192.168.10.1
!
!
!
!
!
username docente privilege 15 secret 5 $1$zMHf$hhl3OcCmtcgAULgF7X5yk.
username studente privilege 15 secret 5 $1$q7zh$pJ/gbygZBCU1tVN85PFNv0
!
!
!
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
crypto isakmp key labtelecom address 200.1.2.6
!
!
crypto ipsec transform-set labtele esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to200.1.2.6
 set peer 200.1.2.6
 set transform-set labtele
 match address 100
!
!
!
!
interface FastEthernet0/0
 description $ETH-LAN$
 ip address 192.168.10.1 255.255.255.240
 ip access-group 1 out
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description inter rete 172
 ip address 172.26.3.254 255.255.252.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface Serial0/0/0
 ip address 10.0.1.2 255.255.255.252
 shutdown
 clock rate 125000
!
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
```

```
ip route 0.0.0.0 0.0.0.0 172.26.0.1
!
!
ip http server
ip http authentication local
no ip http secure-server
ip nat inside source route-map SDM_RMAP_1 interface FastEthernet0/1 overload
!
access-list 1 remark CCP_ACL Category=2
access-list 1 permit 192.168.10.0 0.0.0.15
access-list 1 deny   172.16.0.0 0.0.3.255
access-list 1 permit any
access-list 100 remark CCP_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 192.168.10.0 0.0.0.15 192.168.110.32 0.0.0.15
access-list 101 remark CCP_ACL Category=2
access-list 101 remark IPSec Rule
access-list 101 deny   ip 192.168.10.0 0.0.0.15 192.168.110.32 0.0.0.15
access-list 101 permit ip 192.168.10.0 0.0.0.15 any
!
route-map SDM_RMAP_1 permit 1
 match ip address 101
!
!
!
!
control-plane
!
!
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input telnet ssh
line vty 5 15
 login local
 transport input telnet ssh
!
end
```

File di configurazione del Router-ISP, che rappresenta il router dell'Internet Service Provider

```
Building configuration...

Current configuration : 1619 bytes
```

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router-isp
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip cef
!
!
!
!
ip domain name lab-tele
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
username docente privilege 15 secret 5 $1$RMHK$fwRBUSg5b4.4/eFUvUVe91
username studente privilege 15 secret 5 $1$90LC$bZeyhePqNKzlEqoBkY36s0
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.252 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description interfaccia verso Internet
 ip address 192.168.4.207 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0/0
 description interf verso edificio 2
 ip address 200.1.2.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
```

```
 no fair-queue
 clock rate 125000
!
interface Serial0/0/1
 description int verso edificio 1
 ip address 200.1.2.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 clock rate 125000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.4.254
ip route 200.10.1.0 255.255.255.252 200.1.2.2
!
!
ip http server
ip http authentication local
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 remark CCP_ACL Category=2
access-list 1 permit 200.1.2.4 0.0.0.3
access-list 1 permit 200.1.2.0 0.0.0.3
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login local
 transport input telnet ssh
line vty 5 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
end
```

File di configurazione del Router-1-Edificio 2, tramite cui si accede al router dell'ISP

```
Building configuration...

Current configuration : 7441 bytes
!
```

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-edificio2
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.110.33 192.168.110.36
ip dhcp excluded-address 192.168.110.45 192.168.110.46
ip dhcp excluded-address 192.168.110.1 192.168.110.10
ip dhcp excluded-address 192.168.110.25 192.168.110.30
!
ip dhcp pool contabile
   network 192.168.110.32 255.255.255.240
   default-router 192.168.110.33
   dns-server 8.8.8.8
!
ip dhcp pool commerciale
   network 192.168.110.0 255.255.255.224
   default-router 192.168.110.1
   dns-server 8.8.8.8
!
!
!
!
crypto pki trustpoint TP-self-signed-2818932690
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2818932690
 revocation-check none
 rsakeypair TP-self-signed-2818932690
!
crypto pki trustpoint TP-self-signed-594885972
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-594885972
```

```
 revocation-check none
 rsakeypair TP-self-signed-594885972
!
!
crypto pki certificate chain TP-self-signed-2818932690
crypto pki certificate chain TP-self-signed-594885972
 certificate self-signed 01
  30820247 308201B0 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 35393438 38353937 32301E17 0D373030 31303130 30303934
  355A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3539 34383835
  39373230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  E3F7155E A430F386 8DF4F136 5B6D419C B1645EC1 215A5576 3C7E662B BE3DDC58
  0AF07B7D 4E1A703C 6C1BFF0D 779A8D6A E46CA8ED 99502F62 FC891404 6A46C78C
  4DD4D19D DFB10BDD EA6ECB25 B9FABA6E 8FCB4C2F 10BE7356 AFBE31A1 4FA9B16F
  BD4BBB5B 269E626B 6FFCD7C6 155D92CB 277D7220 5ABB8F12 A6BA65FB 01F88A29
  02030100 01A37130 6F300F06 03551D13 0101FF04 05300301 01FF301C 0603551D
  11041530 13821172 6F757465 722D6564 69666963 696F322E 301F0603 551D2304
  18301680 14110BFA BA60EDA0 8E0EB15E 4199ED3C 54801806 A7301D06 03551D0E
  04160414 110BFABA 60EDA08E 0EB15E41 99ED3C54 801806A7 300D0609 2A864886
  F70D0101 04050003 818100B0 AF19B04D 527A14F1 55D32263 4CAA4540 29D3B404
  79EBEC76 C0742AD1 2A645C02 AEFD7481 D2920046 5AF7CFF6 2031BC37 B942873F
  AC8E0512 1FBB04A3 7ED8B660 66B90A30 32788187 BF79892D 902449B4 F2CECB1D
  6C7E1015 8488BDD5 E4EC0D4A BC1D5BBF C78DE1AE 561E4AED 46429123 FDC178BC
  8CFC231C CB37544C 1C479B
  quit
username studente privilege 15 secret 5 $1$M/A8$GFmZv.rHiz3LYyEGPJB960
username docente privilege 15 secret 5 $1$TC9W$fuTiwz58E1WGcPCvswTFg1
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
crypto isakmp key labtelecom address 200.1.2.2
crypto isakmp key labtelecom address 200.10.1.1
!
!
crypto ipsec transform-set labtele esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to200.1.2.2
 set peer 200.1.2.2
 set transform-set labtele
 match address 106
```

```
crypto map SDM_CMAP_1 2 ipsec-isakmp
 description Tunnel to200.10.1.1
 set peer 200.10.1.1
 set transform-set labtele
 match address 109
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 description vlan 1 gestione
 encapsulation dot1Q 1 native
 ip address 10.0.0.239 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no snmp trap link-status
!
interface FastEthernet0/0.2
 description vlan commerciale
 encapsulation dot1Q 2
 ip address 192.168.110.1 255.255.255.224
 ip access-group 2 out
 ip nat inside
 ip virtual-reassembly
 no snmp trap link-status
!
interface FastEthernet0/0.3
 description vlan 3 contabile
 encapsulation dot1Q 3
 ip address 192.168.110.33 255.255.255.240
 ip access-group 3 out
 ip nat inside
 ip virtual-reassembly
 no snmp trap link-status
!
interface FastEthernet0/1
 no ip address
 ip virtual-reassembly
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 description int verso ISP
 ip address 200.1.2.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 no fair-queue
```

```
 crypto map SDM_CMAP_1
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
!
ip route 0.0.0.0 0.0.0.0 200.1.2.5
!
ip http server
ip http secure-server
ip nat inside source route-map SDM_RMAP_5 interface Serial0/0/0 overload
!
access-list 2 deny   192.168.110.32 0.0.0.15
access-list 2 permit any
access-list 3 deny   192.168.110.0 0.0.0.31
access-list 3 permit any
access-list 10 remark CCP_ACL Category=16
access-list 10 permit 192.168.110.0 0.0.0.31
access-list 20 remark CCP_ACL Category=16
access-list 20 permit 192.168.110.32 0.0.0.15
access-list 30 remark CCP_ACL Category=16
access-list 30 permit 192.168.110.0 0.0.0.31
access-list 40 remark CCP_ACL Category=16
access-list 40 permit 192.168.110.32 0.0.0.15
access-list 100 remark CCP_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 192.168.110.0 0.0.0.31 172.16.0.0 0.0.3.255
access-list 101 remark CCP_ACL Category=2
access-list 101 remark IPSec Rule
access-list 101 deny   ip 192.168.110.0 0.0.0.31 172.16.0.0 0.0.3.255
access-list 101 permit ip 192.168.110.0 0.0.0.31 any
access-list 102 remark CCP_ACL Category=2
access-list 102 remark IPSec Rule
access-list 102 deny   ip 192.168.110.0 0.0.0.31 172.16.0.0 0.0.3.255
access-list 102 permit ip 192.168.110.32 0.0.0.15 any
access-list 103 remark CCP_ACL Category=2
access-list 103 remark IPSec Rule
access-list 103 deny   ip 192.168.110.0 0.0.0.31 172.26.0.0 0.0.3.255
access-list 103 permit ip 192.168.110.0 0.0.0.31 any
access-list 104 remark CCP_ACL Category=2
access-list 104 remark IPSec Rule
access-list 104 deny   ip 192.168.110.0 0.0.0.31 172.26.0.0 0.0.3.255
access-list 104 permit ip 192.168.110.32 0.0.0.15 any
access-list 105 remark CCP_ACL Category=4
access-list 105 remark IPSec Rule
access-list 105 permit ip 192.168.110.0 0.0.0.31 172.26.0.0 0.0.3.255
access-list 106 remark CCP_ACL Category=4
access-list 106 remark IPSec Rule
access-list 106 permit ip 192.168.110.0 0.0.0.255 172.26.0.0 0.0.3.255
access-list 107 remark CCP_ACL Category=2
```

```
access-list 107 remark IPSec Rule
access-list 107 deny   ip 192.168.110.32 0.0.0.15 192.168.10.0 0.0.0.15
access-list 107 remark IPSec Rule
access-list 107 deny   ip 192.168.110.0 0.0.0.255 172.26.0.0 0.0.3.255
access-list 107 permit ip 192.168.110.32 0.0.0.15 any
access-list 107 permit ip 192.168.110.0 0.0.0.31 any
access-list 108 remark CCP_ACL Category=4
access-list 108 remark IPSec Rule
access-list 108 permit ip 192.168.110.0 0.0.0.15 192.168.10.0 0.0.0.15
access-list 109 remark CCP_ACL Category=4
access-list 109 remark IPSec Rule
access-list 109 permit ip 192.168.110.32 0.0.0.15 192.168.10.0 0.0.0.15
!
route-map SDM_RMAP_4 permit 1
 match ip address 104
!
route-map SDM_RMAP_5 permit 1
 match ip address 107
!
route-map SDM_RMAP_1 permit 1
 match ip address 101
!
route-map SDM_RMAP_2 permit 1
 match ip address 102
!
route-map SDM_RMAP_3 permit 1
 match ip address 103
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login local
 transport input telnet ssh
line vty 5 15
 login local
 transport input telnet ssh
!
end
```