

# Indice

<b>1 Introduzione</b>	<b>3</b>
1.1 Abstract-Sommario . . . . .	3
1.2 Obbiettivi del progetto . . . . .	4
<b>2 Progettazione della Rete: Topologia e Infrastruttura Fisica</b>	<b>5</b>
2.1 Struttura della Topologia . . . . .	5
2.2 Dispositivi fisici utilizzati . . . . .	5
<b>3 Progettazione Logica della Rete: Struttura e Sottoreti</b>	<b>7</b>
3.1 Struttura delle sottoreti . . . . .	7
3.2 Vantaggi della suddivisione in sottoreti . . . . .	7
3.3 Configurazione degli indirizzi IP e Gateway . . . . .	8
3.4 Struttura della Rete Aziendale: Connessioni e Dispositivi . . . . .	8
<b>4 Configurazione delle Interfacce di Rete</b>	<b>9</b>
4.1 Configurazione degli host UNIX per ogni sottorete . . . . .	9
4.2 Configurazione del Firewall Locale sugli host UNIX . . . . .	10
<b>5 Impostazione Routing</b>	<b>11</b>
<b>6 Configurazione server DNS e Posta Elettronica</b>	<b>14</b>
6.1 Server DNS interno . . . . .	14
6.2 Utilizzo del Server DNS nei PC . . . . .	14
6.3 Test di Connettività e Verifica del Funzionamento . . . . .	16
6.4 Server Posta Elettronica . . . . .	17
6.5 Configurazione del Server di Posta . . . . .	17
6.6 Configurazione dei PC degli Utenti . . . . .	17
6.7 Verifica e Test della Configurazione . . . . .	18
<b>7 Implementazione e Configurazione Firewalls</b>	<b>19</b>
7.1 Configurazione del Firewall_IN . . . . .	19
7.1.1 Configurazione delle Interfacce . . . . .	19
7.1.2 Configurazione delle Rotte . . . . .	19
7.1.3 Configurazione delle Access Control List (ACL) . . . . .	19
7.1.4 Applicazione delle ACL alle Interfacce . . . . .	20
7.1.5 Politiche di Sicurezza e Ispezione del Traffico . . . . .	20
7.1.6 Timeout per Telnet e SSH . . . . .	21
7.1.7 Conclusioni . . . . .	21
7.2 Configurazione del Firewall_OUT . . . . .	21

7.2.1	Obiettivi della configurazione . . . . .	21
7.2.2	Politiche di sicurezza implementate . . . . .	22
7.2.3	Regole di Base (Default Policies) . . . . .	22
7.2.4	Applicazione delle ACL alle Interfacce . . . . .	23
7.2.5	Implementazione del NAT . . . . .	23
7.2.6	Logging e monitoraggio . . . . .	23
7.2.7	Motivazione delle Scelte . . . . .	23
<b>8</b>	<b>Server Backup</b>	<b>25</b>
8.1	Misure di sicurezza . . . . .	25
8.1.1	Firewall Software . . . . .	25
8.1.2	Segmentazione della Rete . . . . .	25
<b>9</b>	<b>Preventivo Tanzi S.R.L</b>	<b>29</b>
9.1	Dispositivi di Rete . . . . .	29
9.2	Server . . . . .	29
9.3	Cablaggio e Accessori . . . . .	29
9.4	Licenze e Software . . . . .	30
9.5	Servizi di Installazione e Configurazione . . . . .	30
9.6	Totale Preventivo . . . . .	30

## Elenco delle figure

1	Disegno rete aziendale . . . . .	3
2	Struttura della Rete Aziendale: Connessioni e Dispositivi . . . . .	8
3	Ping da pc Giuliana (sede C) a pc Elettra (sede A) . . . . .	13
4	Configurazione del DNS Interno con Forwarding verso il DNS DMZ . . . . .	15
5	Test ping <b>tanzisrl.it</b> . . . . .	16
6	Test web <b>tanzisrl.it</b> . . . . .	16
7	Impostazioni accesso . . . . .	26
8	Firewall software backup server . . . . .	27
9	Prova accesso Backup Server da ip non permesso . . . . .	27
10	Ftp pc Mario sede B . . . . .	28

# 1 Introduzione

## 1.1 Abstract-Sommario

La ditta Tanzi S.R.L ha deciso di collegare in rete tutti i suoi reparti ed uffici e vi ha contattato per disegnare, installare e gestire l'intera rete. Quest'ultima può essere così schematizzata: All'interno dell'azienda devono essere presenti i seguenti *Server*:

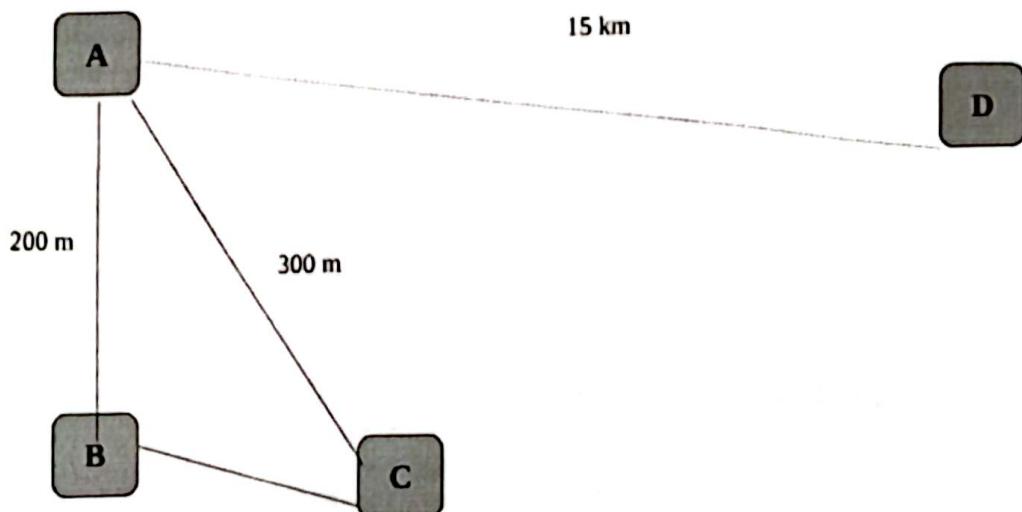


Figura 1: Disegno rete aziendale

Edificio	Uffici & Reparti	Num. Utenti	Num. Server	Copertura Wi-Fi
A	Uffici	150		NO
B	Reparti	50		NO
C	Reparti	50		NO
D	Uffici	100		SI

Tabella 1: Tabella degli edifici con numero utenti, server e copertura Wi-Fi

- Server di posta elettronica N.1
- Server Web N.1
- Server DNS  $N \geq 2$
- Server applicazioni aziendali N.0
- Server Proxy N.0
- Server di Backup N.1

## 1.2 Obbiettivi del progetto

Si richiede pertanto di :

- **Realizzare lo schema fisico della rete**, evidenziando la topologia ed indicando i dispositivi fisici (router, switch, hub, mezzi trasmissivi) da inserire;
- **Realizzare lo schema logico**, evidenziando eventuali suddivisioni della rete in sottoreti;
- **Configurare le interfacce di rete** per tutti i server ed i dispositivi di rete e per almeno un host in ambiente UNIX per ogni rete o sottorete mostrandone tutti i parametri significativi;
- **Impostare il routing** per ogni router interno e di frontiera, riportando eventuali comandi e configurazioni;
- **Configurare dettagliatamente i server DNS e di Posta elettronica**;
- **Implementare e configurare firewalls** per la protezione della rete;
- **Indicare quali tecniche si intendono adottare (e come si implementano)** per il monitoraggio della rete al fine di garantire una maggiore sicurezza;
- **Proteggere in maniera particolare il Server di BACKUP**;

## 2 Progettazione della Rete: Topologia e Infrastruttura Fisica

La rete aziendale di Tanzi Srl è stata progettata seguendo una topologia a *stella gerarchica*, che garantisce una gestione centralizzata ed efficiente del traffico di rete.

### 2.1 Struttura della Topologia

- Ogni sede dispone di uno switch centrale che connette i dispositivi locali (PC, server) e si collega al router della sede.
- I router delle sedi sono connessi a una struttura centrale che comprende la **DMZ** (Zona Demilitarizzata) e i firewall, creando una rete multilivello.
- La rete è centralizzata:
  - Tutti i router delle sedi convergono verso il firewall interno (Firewall\_IN), che regola il traffico tra le reti aziendali e la DMZ.
  - Il firewall esterno (Firewall\_OUT) gestisce l'accesso al cloud e alla rete esterna.

Questa architettura permette di ottimizzare la sicurezza e la scalabilità della rete aziendale, isolando i servizi critici nella DMZ e filtrando il traffico con firewall dedicati.

### 2.2 Dispositivi fisici utilizzati

**Router:**

- 4 router per le sedi aziendali:
  - Router\_EdificioA
  - Router\_EdificioB
  - Router\_EdificioC
  - Router\_EdificioD

**Switch:**

- 1 switch per ogni sede per la gestione della rete locale.
- 1 switch nella DMZ per connettere i server.

**Firewall:**

- 2 firewall ASA 5506-X per la protezione della rete.

- Firewall\_IN per la sicurezza interna e il controllo del traffico tra le sedi e la DMZ.
- Firewall\_OUT per l'accesso sicuro al cloud e alla rete esterna.

#### Server:

- Server DNS → collocato nella sede B
- Server di posta elettronica, Web e DNS → posizionati nella DMZ
- Server di backup → situato nella sede C per garantire la protezione dei dati aziendali.
- Server DHCP → situato nella sede D per distribuzione indirizzi ip a tutti i dispositivi wireless e wired

#### PC Client:

- Presenti in tutte le sedi per l'operatività quotidiana.

#### WiFi:

- Presente solo nella sede D, supportato da un Access Point dedicato.

### **3 Progettazione Logica della Rete: Struttura e Sottoreti**

La progettazione logica della rete prevede una suddivisione strategica in sottoreti per ottimizzare la gestione del traffico, aumentare la sicurezza e migliorare le performance complessive.

#### **3.1 Struttura delle sottoreti**

La rete è segmentata nelle seguenti sottoreti:

- Sede A: 192.168.1.0/24 → Destinata agli uffici amministrativi e ai dipendenti.
- Sede B: 192.168.2.0/24 → Ospita il server DNS e postazioni per i tecnici IT.
- Sede C: 192.168.3.0/24 → Reparto tecnico e produzione con server di Backup.
- Sede D: 192.168.4.0/24 → Unica sede con rete Wi-Fi e server DHCP.
- DMZ: 192.168.50.0/24 → Zona dedicata ai server esposti all'esterno (Web, Mail, DNS).
- Cloud/Internet: Collegato tramite il firewall esterno per accessi controllati e sicurezza perimetrale.

#### **3.2 Vantaggi della suddivisione in sottoreti**

- Isolamento del traffico: Ogni reparto ha una sottorete dedicata, evitando congestioni e migliorando la sicurezza.
- Maggiore controllo: Attraverso le regole (rotte) tra i router, è possibile gestire la comunicazione tra le sottoreti delle sedi.
- Facilità di gestione: La segmentazione permette una gestione più efficiente della rete e una più rapida identificazione dei problemi.
- Sicurezza migliorata: Gli accessi ai server critici (ad es. il server di backup e i server in DMZ) sono strettamente regolati.

### 3.3 Configurazione degli indirizzi IP e Gateway

Ogni sottorete è gestita con un proprio gateway per l'instradamento del traffico. Esempio di configurazione:

- Sede A: Gateway 192.168.1.1 (Router\_EdificioA)
- Sede B: Gateway 192.168.2.1 (Router\_EdificioB)
- Sede C: Gateway 192.168.3.1 (Router\_EdificioC)
- Sede D: Gateway 192.168.4.1 (Router\_EdificioD)
- DMZ: Gateway 192.168.50.1 (Firewall interno)

Ogni host nella rete utilizza il proprio gateway per comunicare con altre sottoreti e accedere ai servizi aziendali o esterni.

### 3.4 Struttura della Rete Aziendale: Connessioni e Dispositivi

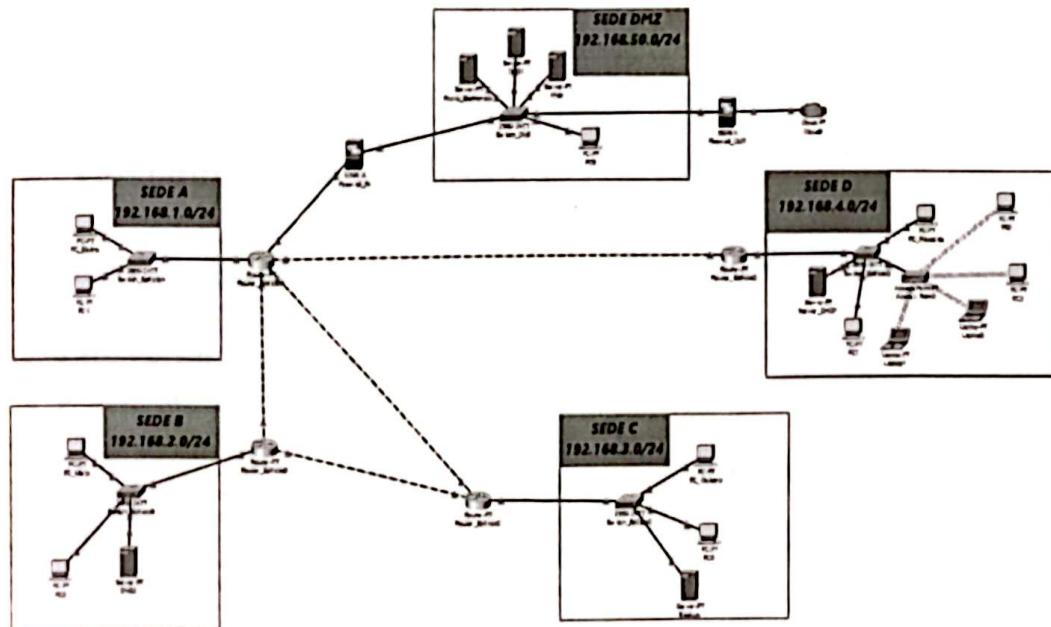


Figura 2: Struttura della Rete Aziendale: Connessioni e Dispositivi

## 4 Configurazione delle Interfacce di Rete

Ogni router è configurato con gli IP delle relative sottoreti. Esempio per Router\_EdificioA:

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

I server sono configurati con IPv4 Address, Subnet Mask, Default Gateway e DNS Server  
In via generale sia i server che i dispositivi di rete, laptop e pc, sono configurati con i seguenti parametri:

```
IPv4 Address: 192.168.x.x
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.x.1
DNS Server: 192.168.x.x
```

Nel caso specifico del server di Posta Elettronica ad esempio:

```
IPv4 Address: 192.168.50.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.50.1
DNS Server: 192.168.50.12
```

### 4.1 Configurazione degli host UNIX per ogni sottorete

Di seguito viene illustrata la configurazione di almeno un host UNIX per ogni sottorete, includendo l'assegnazione degli indirizzi IP, il gateway e il DNS.

Sede A (192.168.1.0/24)

```
ifconfig eth0 192.168.1.10 netmask 255.255.255.0 up
route add default gw 192.168.1.1
echo "nameserver 192.168.2.150" >> /etc/resolv.conf
```

Sede B (192.168.2.0/24)

```
ifconfig eth0 192.168.2.10 netmask 255.255.255.0 up
route add default gw 192.168.2.1
echo "nameserver 192.168.2.150" >> /etc/resolv.conf
```

Sede C (192.168.3.0/24)

```
ifconfig eth0 192.168.3.10 netmask 255.255.255.0 up
route add default gw 192.168.3.1
echo "nameserver 192.168.2.150" >> /etc/resolv.conf
```

Sede D (192.168.4.0/24)

```
ifconfig eth0 192.168.4.10 netmask 255.255.255.0 up  
route add default gw 192.168.4.1  
echo "nameserver 192.168.2.150" >> /etc/resolv.conf
```

Sede DMZ (192.168.50.0/24)

```
ifconfig eth0 192.168.50.10 netmask 255.255.255.0 up  
route add default gw 192.168.50.1  
echo "nameserver 192.168.50.12" >> /etc/resolv.conf
```

## 4.2 Configurazione del Firewall Locale sugli host UNIX

Configurazione con IPTABLES:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -p tcp --dport 80 -s 192.168.0.0/16 -j ACCEPT  
iptables -A INPUT -p udp --dport 53 -s 192.168.50.12 -j ACCEPT  
iptables -A INPUT -p tcp --dport 53 -s 192.168.50.12 -j ACCEPT  
iptables -A INPUT -p tcp --dport 25 -s 192.168.50.11 -j ACCEPT  
iptables -A INPUT -p tcp --dport 110 -s 192.168.50.11 -j ACCEPT  
iptables -A INPUT -j DROP  
service iptables save
```

Questa configurazione:

- Blocca tutto il traffico in ingresso, tranne connessioni stabilite.
- Permette solo accessi SSH (porta 22), traffico HTTP (porta 80), traffico verso il DNS (porta 53, UDP e TCP), traffico Posta Elettronica (porta 25 e 110) dalla rete aziendale.
- Impedisce connessioni non autorizzate, proteggendo ogni host UNIX da attacchi esterni.

## 5 Impostazione Routing

*Router\_EdificioA (di frontiera)*

```
Router>en
Router#show running-config
Building configuration ...
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet6/0
 ip address 192.168.30.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet7/0
 ip address 192.168.30.13 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet8/0
 ip address 192.168.30.10 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet9/0
 ip address 192.168.30.17 255.255.255.252
 duplex auto
 speed auto
!
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.30.2
ip route 192.168.3.0 255.255.255.0 192.168.30.9
ip route 192.168.4.0 255.255.255.0 192.168.30.14
ip route 192.168.50.0 255.255.255.0 192.168.30.18
!
```

```

Router#show ip route
C 192.168.1.0/24 is directly connected, FastEthernet0/0
S 192.168.2.0/24 [1/0] via 192.168.30.2
S 192.168.3.0/24 [1/0] via 192.168.30.9
S 192.168.4.0/24 [1/0] via 192.168.30.14
  192.168.30.0/30 is subnetted, 4 subnets
C    192.168.30.0 is directly connected, GigabitEthernet6/0
C    192.168.30.8 is directly connected, GigabitEthernet8/0
C    192.168.30.12 is directly connected, GigabitEthernet7/0
C    192.168.30.16 is directly connected, GigabitEthernet9/0
S 192.168.50.0/24 [1/0] via 192.168.30.18

```

### *Router\_EdificioB (interno)*

```

Router>en
Router#show running-config
Building configuration ...
!
interface FastEthernet0/0
  ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface GigabitEthernet6/0
  ip address 192.168.30.2 255.255.255.252
  duplex auto
  speed auto
!
interface GigabitEthernet7/0
  ip address 192.168.30.5 255.255.255.252
  duplex auto
  speed auto
!
ip classless
ip route 192.168.1.0 255.255.255.0 192.168.30.1
ip route 192.168.3.0 255.255.255.0 192.168.30.6
ip route 192.168.4.0 255.255.255.0 192.168.30.1
ip route 192.168.50.0 255.255.255.0 192.168.30.1

Router#show ip route

```

```
S 192.168.1.0/24 [1/0] via 192.168.30.1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
S 192.168.3.0/24 [1/0] via 192.168.30.6
S 192.168.4.0/24 [1/0] via 192.168.30.1
    192.168.30.0/30 is subnetted, 2 subnets
C        192.168.30.0 is directly connected, GigabitEthernet6/0
C        192.168.30.4 is directly connected, GigabitEthernet7/0
S 192.168.50.0/24 [1/0] via 192.168.30.1
```

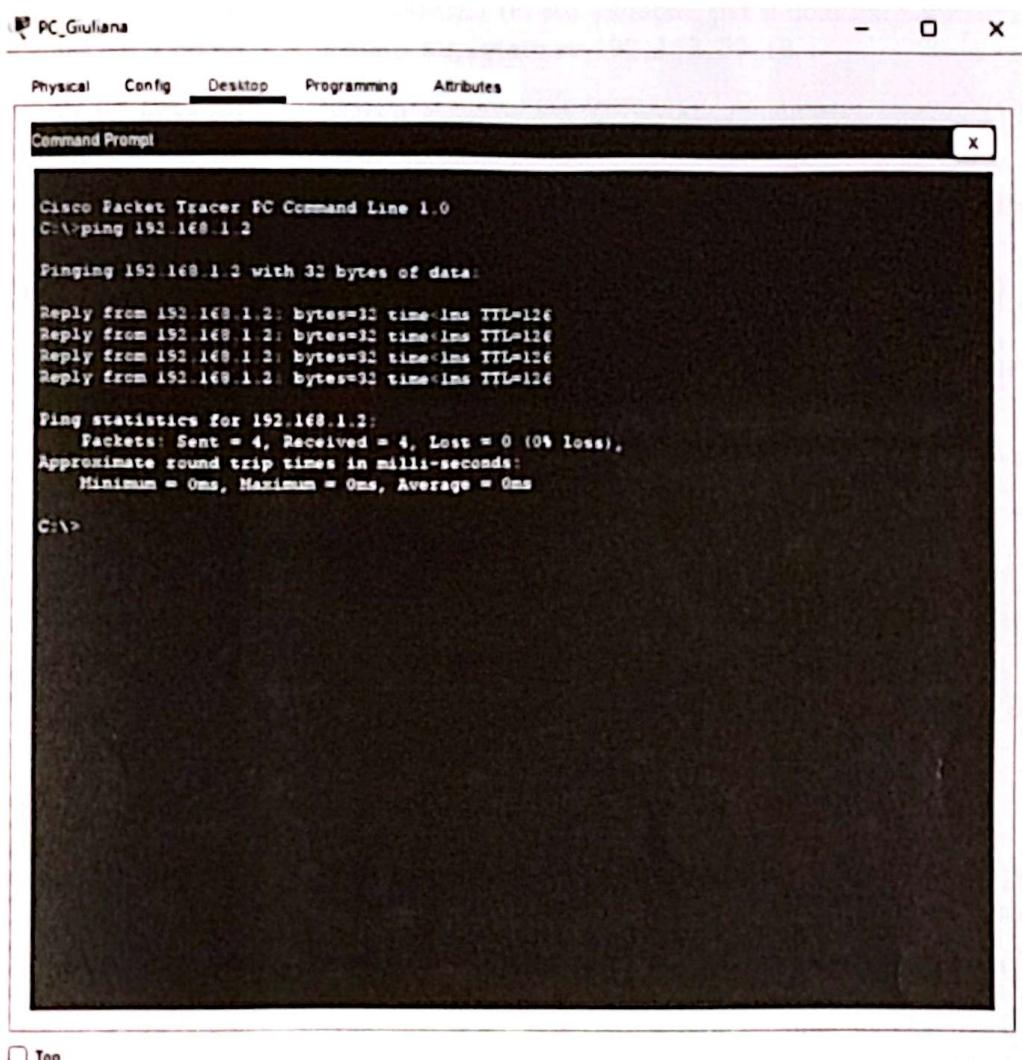


Figura 3: Ping da pc Giuliana (sede C) a pc Elettra (sede A)

## 6 Configurazione server DNS e Posta Elettronica

### 6.1 Server DNS interno

In questa sezione viene descritta la configurazione del server DNS interno (sede B) e come i PC nelle diverse sedi utilizzano il servizio DNS per risolvere i nomi di dominio e connettersi al server web, garantendo l'accesso alle risorse tramite indirizzi IP associati ai nomi di dominio.

Il servizio DNS è stato attivato e sono stati creati i record DNS necessari per l'associazione tra nomi di dominio e indirizzi IP. Ad esempio, per il dominio **tanzisrl.it**, l'indirizzo IP del server web è stato impostato su **192.168.50.13**.

### 6.2 Utilizzo del Server DNS nei PC

I PC delle varie sedi sono stati configurati per utilizzare il server DNS della rete interna aziendale, per i seguenti motivi:

#### 1 Prestazioni e latenza minore

- Il server DNS interno è più vicino ai PC aziendali e riduce i tempi di risoluzione dei nomi.
- Se ogni sede punta al DNS della Sede B, il traffico di risoluzione rimane all'interno della rete aziendale senza passare dalla DMZ.

#### 2 Sicurezza e isolamento

- Il DNS nella DMZ è esposto all'esterno e gestisce richieste pubbliche (es. record del sito web e della posta elettronica).
- I PC aziendali non dovrebbero fare query DNS direttamente verso la DMZ, per evitare di esporre informazioni interne al mondo esterno.

#### 3 Struttura tipica di una rete aziendale

- In un'azienda, di solito il DNS interno (Sede B) è il punto centrale per la risoluzione dei nomi interni e instrada solo ciò che è necessario verso l'esterno.
- Il DNS interno è stato configurato per inoltrare richieste esterne al server DNS presente nella DMZ.

Quando un PC tenta di connettersi a **tanzisrl.it**, viene inviata una richiesta al server DNS configurato, che restituisce l'indirizzo IP corretto (**192.168.50.13**). Una volta ricevuto l'indirizzo, il PC si connette automaticamente al server web.

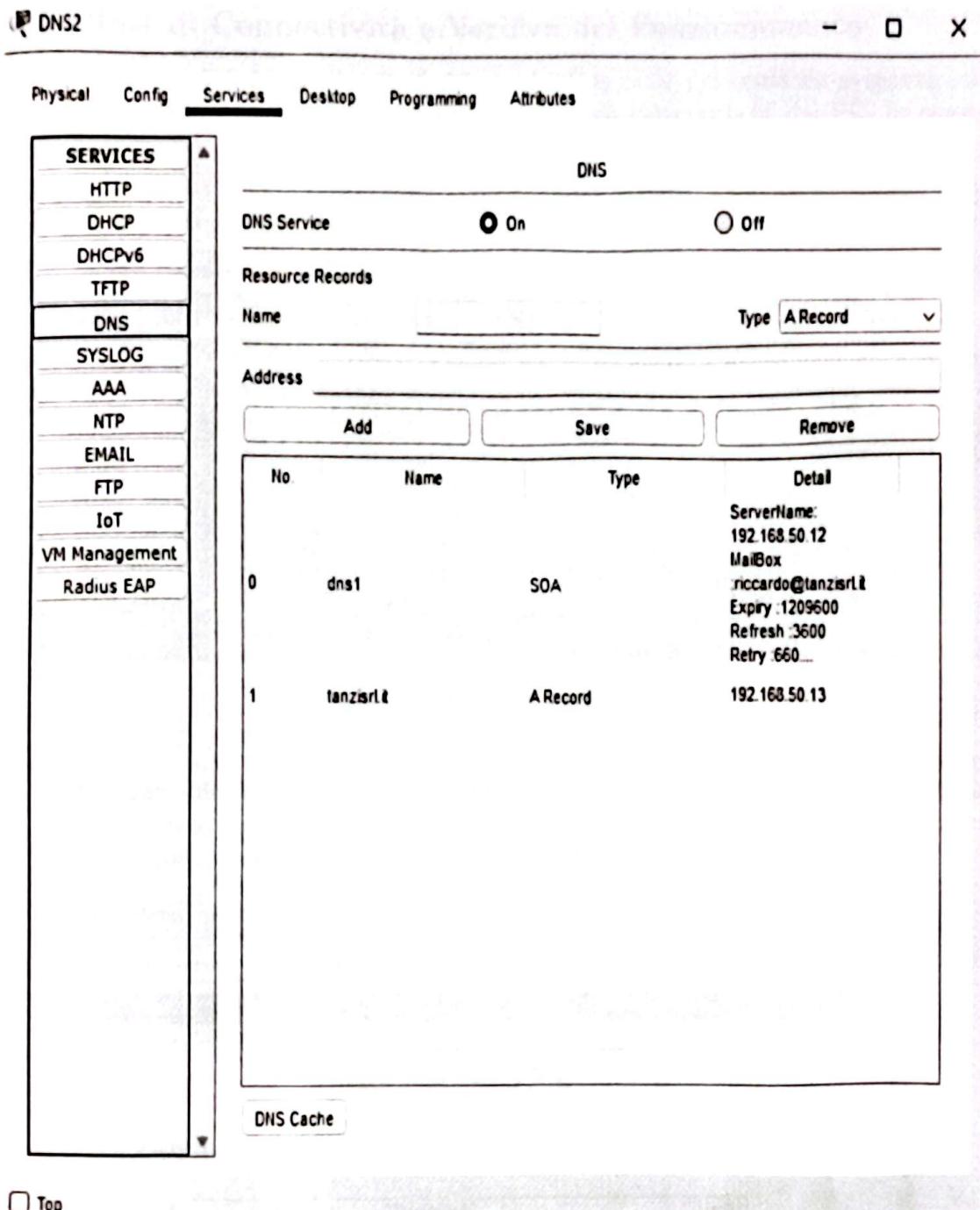
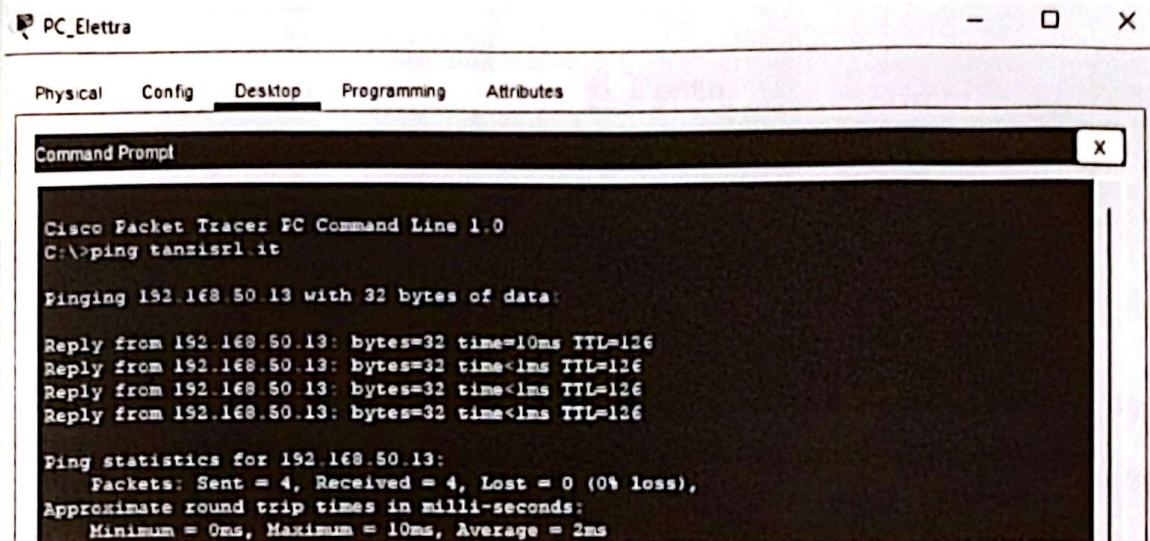


Figura 4: Configurazione del DNS Interno con Forwarding verso il DNS DMZ

### 6.3 Test di Connessione e Verifica del Funzionamento

1. **Verifica del Ping:** Per verificare che la risoluzione del nome sia avvenuta correttamente, si può eseguire un ping al dominio **tanzisrl.it** dal PC. In questo caso:



The screenshot shows a Cisco Packet Tracer Command Line interface. The command entered is "C:\>ping tanzisrl.it". The output shows four successful replies from the target IP 192.168.50.13, each with 32 bytes and an TTL of 126. It also provides ping statistics: 4 packets sent, 4 received, 0 lost (0% loss), with approximate round trip times ranging from 0ms to 10ms and an average of 2ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping tanzisrl.it

Pinging 192.168.50.13 with 32 bytes of data:

Reply from 192.168.50.13: bytes=32 time=10ms TTL=126
Reply from 192.168.50.13: bytes=32 time<1ms TTL=126
Reply from 192.168.50.13: bytes=32 time<1ms TTL=126
Reply from 192.168.50.13: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.50.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Figura 5: Test ping tanzisrl.it

- 2 Navigazione Web: Dopo aver verificato la risoluzione del nome tramite ping, si può verificare che aprendo il **Web Browser** e digitando **tanzisrl.it** nella barra degli indirizzi, vedremo la pagina di login della Tanzi S.R.L

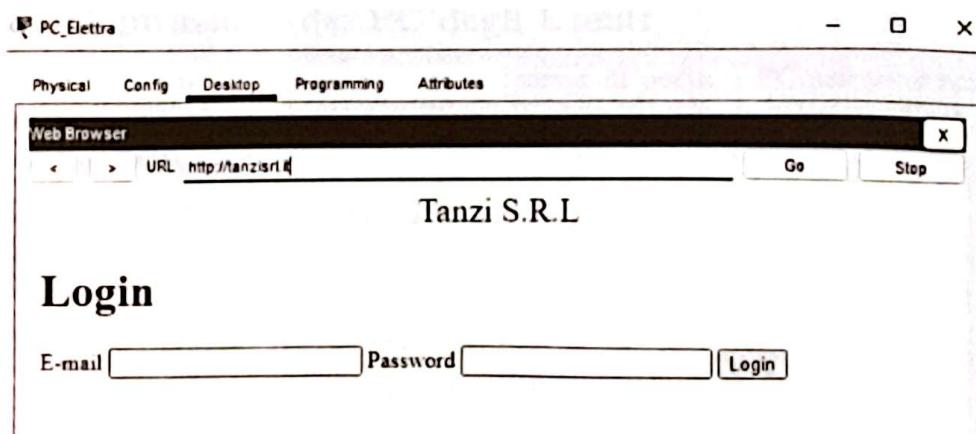


Figura 6: Test web tanzisrl.it

## 6.4 Server Posta Elettronica

Il server di posta elettronica è stato configurato e posizionato all'interno della DMZ per garantire la gestione della posta in entrata e in uscita. Il servizio SMTP è stato implementato per l'invio delle email, mentre il servizio POP3 consente agli utenti di ricevere la posta elettronica.

## 6.5 Configurazione del Server di Posta

Per garantire il corretto funzionamento del sistema di posta elettronica, sono stati attivati i seguenti servizi:

- Il protocollo **SMTP** è stato abilitato per la gestione della posta in uscita.
- Il protocollo **POP3** è stato configurato per consentire la ricezione delle email da parte degli utenti.

Il server è stato associato al dominio aziendale **tanzisrl.it**, permettendo così una gestione centralizzata degli indirizzi email.

Successivamente, sono stati creati gli account di posta elettronica per gli utenti aziendali. Ad esempio:

- **Elettra**: **elettra@tanzisrl.it**.
- **Riccardo**: **riccardo@tanzisrl.it**.

Per garantire la sicurezza, le password degli account sono state generate e assegnate direttamente agli utenti.

## 6.6 Configurazione dei PC degli Utenti

Dopo aver completato la configurazione del server di posta, i PC aziendali sono stati impostati per connettersi al sistema di email. Ogni utente ha configurato il proprio client di posta elettronica con i seguenti parametri:

- Nome utente: **Elettra** o **Riccardo**.
- Indirizzo email corrispondente:
  - **elettra@tanzisrl.it** per Elettra.
  - **riccardo@tanzisrl.it** per Riccardo
- Server di posta in entrata (POP3): **192.168.50.11**.
- Server di posta in uscita (SMTP): **192.168.50.11**.

## 6.7 Verifica e Test della Configurazione

Dopo l'installazione e la configurazione, sono stati eseguiti test per validare la corretta operatività del sistema di posta elettronica. I test hanno incluso:

- L'invio e la ricezione di email tra utenti interni alla rete aziendale.
- La verifica della connettività con il server di posta tramite comandi **ping** e **telnet**.
- Il controllo dei log del server per assicurarsi che le email venissero elaborate correttamente.

Tutti i test hanno avuto esito positivo, confermando il corretto funzionamento del server di posta elettronica e la sua integrazione con la rete aziendale.

**Link video funzionamento:** Scambio di email tra colleghi.

## 7 Implementazione e Configurazione Firewalls

### 7.1 Configurazione del Firewall\_IN

La configurazione del Firewall.IN include le seguenti componenti principali:

#### 7.1.1 Configurazione delle Interfacce

Sono state configurate due interfacce principali nel firewall ASA:

- **Inside**: l'interfaccia interna con indirizzo IP 192.168.30.18/30 e livello di sicurezza 100, utilizzata per la connessione alle reti interne.
- **DMZ**: l'interfaccia DMZ con indirizzo IP 192.168.50.1/24 e livello di sicurezza 50, utilizzata per la connessione alla zona demilitarizzata (DMZ).

#### 7.1.2 Configurazione delle Rotte

Le rotte interne sono state configurate per garantire la connettività tra le varie sottoreti interne e la DMZ. Le seguenti rotte sono state aggiunte al firewall:

- `route inside 192.168.1.0 255.255.255.0 192.168.30.17 1`
- `route inside 192.168.4.0 255.255.255.0 192.168.30.17 1`
- `route inside 192.168.2.0 255.255.255.0 192.168.30.17 1`
- `route inside 192.168.3.0 255.255.255.0 192.168.30.17 1`

#### 7.1.3 Configurazione delle Access Control List (ACL)

Sono state configurate diverse Access Control List (ACL) per gestire il traffico tra la rete interna e la DMZ:

- **INSIDE\_TO\_DMZ**: consente il traffico TCP verso i server web, HTTPS, DNS e posta elettronica nella DMZ.
  - `access-list INSIDE_TO_DMZ extended permit tcp any host 192.168.50.13 eq www`
  - `access-list INSIDE_TO_DMZ extended permit tcp any host 192.168.50.13 eq 443`
  - `access-list INSIDE_TO_DMZ extended permit udp any host 192.168.50.12 eq domain`

- access-list INSIDE\_TO\_DMZ extended permit tcp any host 192.168.50.11 eq smtp
- access-list INSIDE\_TO\_DMZ extended permit tcp any host 192.168.50.11 eq pop3
- access-list INSIDE\_TO\_DMZ extended permit tcp any host 192.168.50.11 eq 143
- **DMZ\_TO\_INSIDE**: consente il traffico ICMP e IP da e verso le reti interne. Ad esempio:
  - access-list DMZ\_TO\_INSIDE extended permit icmp any any
  - access-list DMZ\_TO\_INSIDE extended permit ip 192.168.50.0 255.255.255.0 192.168.1.0 255.255.255.0
  - access-list DMZ\_TO\_INSIDE extended permit ip 192.168.50.0 255.255.255.0 192.168.1.0 255.255.255.0
  - access-list DMZ\_TO\_INSIDE extended permit ip 192.168.50.0 255.255.255.0 192.168.30.0 255.255.255.252
  - access-list DMZ\_TO\_INSIDE extended permit tcp host 192.168.50.11 host 192.168.50.1
  - access-list DMZ\_TO\_INSIDE extended permit ip 192.168.50.0 255.255.255.0 192.168.2.0 255.255.255.0
  - access-list DMZ\_TO\_INSIDE extended permit ip 192.168.50.0 255.255.255.0 192.168.3.0 255.255.255.0
  - access-list DMZ\_TO\_INSIDE extended permit ip 192.168.50.0 255.255.255.0 192.168.4.0 255.255.255.0

#### 7.1.4 Applicazione delle ACL alle Interfacce

Le ACL sono state applicate alle interfacce utilizzando i comandi **access-group**:

- access-group INSIDE\_TO\_DMZ in interface inside
- access-group DMZ\_TO\_INSIDE in interface dmz

#### 7.1.5 Politiche di Sicurezza e Ispezione del Traffico

Sono state configurate politiche di ispezione del traffico per i protocolli DNS, FTP e TFTP. La politica **global\_policy** applica una ispezione per il traffico DNS, FTP e TFTP tramite i seguenti comandi:

- **policy-map global\_policy**
- **class inspection\_default**
- **inspect dns preset\_dns\_map**
- **inspect ftp**
- **inspect tftp**

### **7.1.6 Timeout per Telnet e SSH**

Infine, sono stati impostati i timeout per le sessioni Telnet e SSH a 5 minuti:

- **telnet timeout 5**
- **ssh timeout 5**

### **7.1.7 Conclusioni**

La configurazione implementata offre una solida protezione contro minacce esterne e gestisce in modo efficace il traffico tra la rete interna e la DMZ. Le ACL applicate alle interfacce, insieme alle politiche di ispezione del traffico, garantiscono che solo il traffico autorizzato possa attraversare il firewall.

## **7.2 Configurazione del Firewall\_OUT**

Il Firewall\_OUT è responsabile della sicurezza perimetrale della rete, regolando il traffico tra l'infrastruttura aziendale e Internet. Questo firewall protegge la rete aziendale da attacchi esterni, limitando l'accesso ai soli servizi essenziali e garantendo un controllo rigoroso sul traffico in entrata e in uscita.

### **7.2.1 Obiettivi della configurazione**

- Garantire la sicurezza della rete aziendale, impedendo accessi non autorizzati.
- Consentire solo il traffico essenziale per il funzionamento dei servizi aziendali.
- Bloccare tentativi di accesso malevoli con una politica di default deny.
- Monitorare e registrare il traffico per analisi e risoluzione dei problemi.

### **7.2.2 Politiche di sicurezza implementate**

- Bloccare tutto il traffico in ingresso, eccetto le connessioni già stabilite e servizi essenziali.
- Permettere il traffico in uscita solo per i servizi approvati.
- Limitare l'accesso remoto solo da IP autorizzati

### **7.2.3 Regole di Base (Default Policies)**

1. **Politica per negare tutto il traffico in ingresso e permettere solo traffico autorizzato in uscita:**

- `access-list OUTBOUND_TRAFFIC extended permit tcp any any eq 443`  
Permetti HTTPS
- `access-list OUTBOUND_TRAFFIC extended permit tcp any any eq 80`  
Permetti HTTP
- `access-list OUTBOUND_TRAFFIC extended permit udp any any eq 53`  
Permetti DNS
- `access-list OUTBOUND_TRAFFIC extended permit tcp any any eq 25`  
Permetti SMTP (invio mail)
- `access-list OUTBOUND_TRAFFIC extended permit tcp any any eq 110`  
Permetti POP3 (ricezione mail)
- `access-list OUTBOUND_TRAFFIC extended permit tcp any any eq 587`  
Permetti SMTP sicuro
- `access-list OUTBOUND_TRAFFIC extended permit tcp 192.168.1.10 any eq 22`  
Permetti SSH (solo per amministrazione remota)
- `access-list OUTBOUND_TRAFFIC extended deny ip any any`  
Blocca tutto il traffico non autorizzato

2. **Politica per il traffico in ingresso:** solo il traffico già stabilito è permesso, tutto il resto è bloccato.

- `access-list INBOUND_TRAFFIC extended permit tcp any any eq 80`  
Permetti HTTP
- `access-list INBOUND_TRAFFIC extended permit tcp any any eq 443`  
Permetti HTTPS
- `access-list INBOUND_TRAFFIC extended permit icmp any any echo-reply`  
Permetti risposte ai ping

- **access-list INBOUND\_TRAFFIC extended permit udp any any eq 53**  
Permetti richieste DNS (UDP)
- **access-list INBOUND\_TRAFFIC extended permit tcp any any eq 53**  
Permetti richieste DNS (TCP)
- **access-list INBOUND\_TRAFFIC extended deny ip any any**  
Blocca tutti gli altri tentativi di accesso

#### 7.2.4 Applicazione delle ACL alle Interfacce

Le ACL sono state applicate alle interfacce utilizzando i comandi **access-group**:

- **access-group INBOUND\_TRAFFIC in interface outside**
- **access-group OUTBOUND\_TRAFFIC in interface inside**

#### 7.2.5 Implementazione del NAT

Per consentire ai dispositivi interni di accedere a Internet con un solo IP pubblico:  
**nat (inside , outside) dynamic interface**

#### 7.2.6 Logging e monitoraggio

Per tenere traccia delle connessioni sospette e degli eventi critici:

```
logging enable
logging buffered 100000
logging trap informational
```

#### 7.2.7 Motivazione delle Scelte

- 1 Blocco predefinito del traffico in ingresso:
  - Riduce il rischio di attacchi esterni (DDoS, brute force, exploit).
  - Permette solo risposte a connessioni iniziata dall'interno.
- 2 Permesso solo per servizi essenziali:
  - HTTPS (443) e HTTP (80) per navigazione sicura.
  - DNS (53) per la risoluzione dei nomi.
  - SMTP/POP3 per l'invio e la ricezione delle email aziendali.
  - SSH (22) solo per amministrazione remota sicura.

**3. Implementazione di NAT:**

- Protegge gli indirizzi IP interni mascherandoli con l'IP pubblico.
- Riduce l'esposizione diretta dei dispositivi interni a Internet.

**4. Logging attivato:**

- Permette il monitoraggio delle attività sospette.
- Utile per risoluzione problemi e report di sicurezza.

## 8 Server Backup

La protezione dei dati aziendali è un elemento critico per garantire la continuità operativa e la sicurezza delle informazioni. Il server di backup, situato nella sede C con indirizzo IP 192.168.3.150, è stato configurato per garantire accessi sicuri e controllati. In particolare, è stato implementato un firewall software che permette l'accesso al servizio FTP (porta 21) solo ai PC autorizzati delle varie sedi aziendali, bloccando qualsiasi altro tentativo di connessione.

### 8.1 Misure di sicurezza

#### 8.1.1 Firewall Software

Il firewall software è configurato per filtrare il traffico in entrata, permettendo connessioni FTP esclusivamente ai PC autorizzati, con specifiche Access Control Rules (ACL) che definiscono gli indirizzi IP consentiti.

- **Whitelist IP:** Sono stati specificati gli indirizzi IP dei PC nelle sedi aziendali, impedendo qualsiasi altra connessione esterna o non autorizzata.
- **Deny All Policy:** Qualsiasi traffico FTP proveniente da indirizzi non presenti nella whitelist viene automaticamente rifiutato.
- **Protezione dagli attacchi di brute force:** Riducendo il numero di dispositivi autorizzati, si limita la superficie di attacco per tentativi di accesso non autorizzati.

#### 8.1.2 Segmentazione della Rete

Per migliorare ulteriormente la sicurezza del server, sono state adottate le seguenti misure:

- **Isolamento del Server:** Il server di backup è stato mantenuto nella rete della sede C (192.168.3.0/24) invece della DMZ, riducendo l'esposizione agli attacchi esterni.
- **Restrizioni di Accesso:** Solo le reti autorizzate possono comunicare con il server, limitando il rischio di accessi non autorizzati.

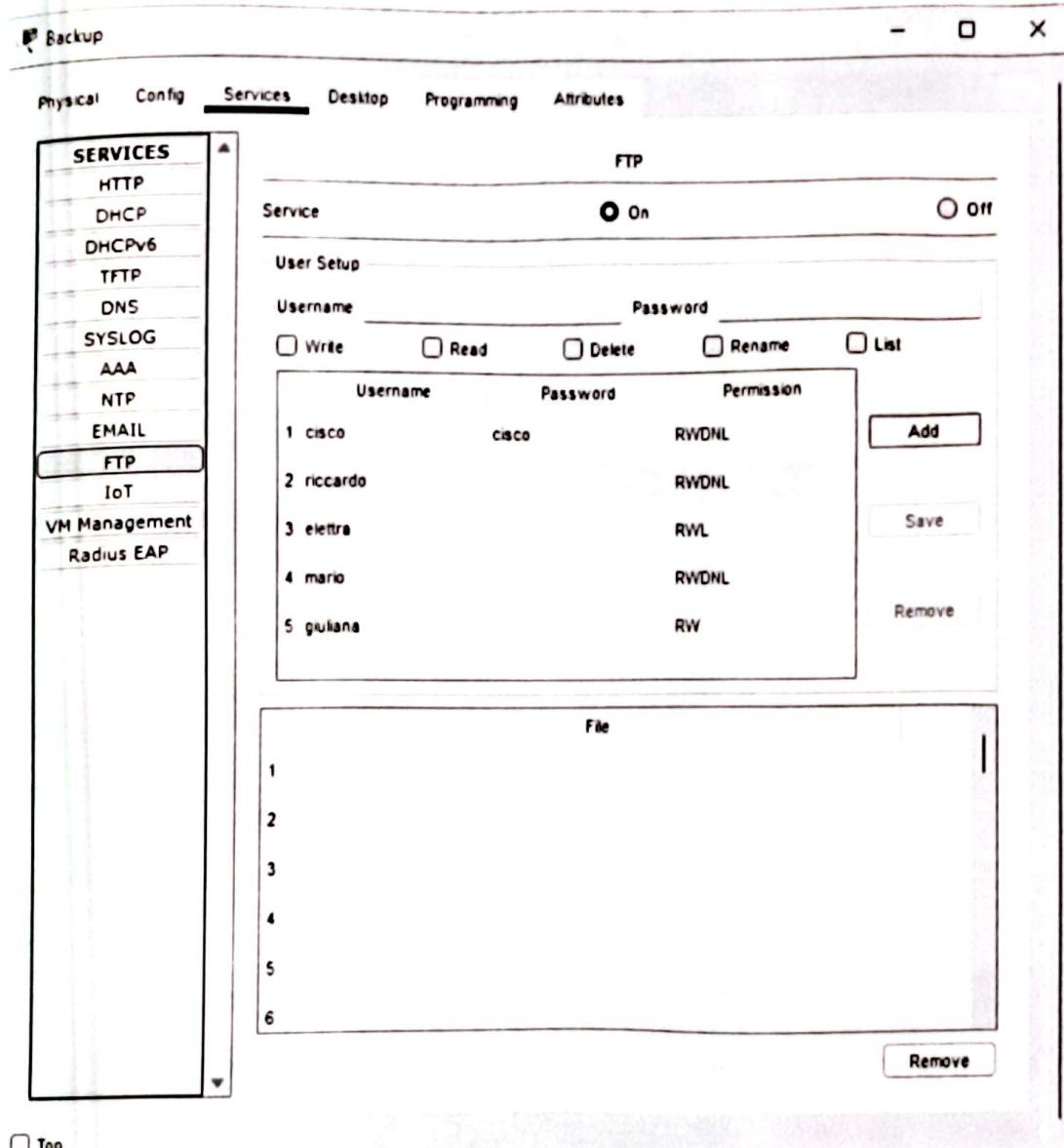


Figura 7: Impostazioni accesso

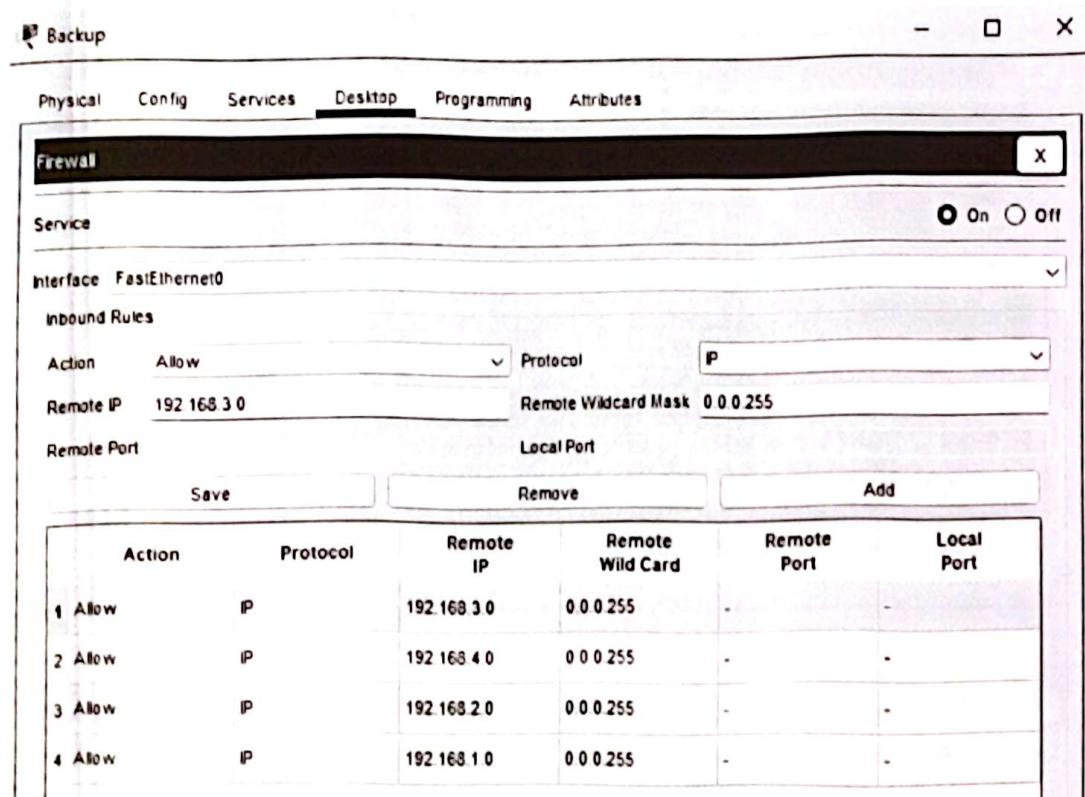


Figura 8: Firewall software backup server

```
C:\>ftp 192.168.3.150
Trying to connect...192.168.3.150
*Error opening ftp://192.168.3.150/ (Timed out)

(Disconnecting from ftp server)
```

Figura 9: Prova accesso Backup Server da ip non permesso

PC\_Mario

Physical Config Desktop Programming Attributes

**Command Prompt**

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.3.150
Trying to connect...192.168.3.150
Connected to 192.168.3.150
220- Welcome to PT Ftp server
Username:mario
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put ciaodapcmariofotoprogetto.txt

Writing file ciaodapcmariofotoprogetto.txt to 192.168.3.150:
File transfer in progress...

(Transfer complete - 5 bytes)

5 bytes copied in 0.044 secs (113 bytes/sec)
```

PC\_Mario

Physical Config Desktop Programming Attributes

**Command Prompt**

```
S bytes copied in 0.044 secs (113 bytes/sec)
ftp>dir

Listing /ftp directory from 192.168.3.150:
0 : asa842-k8.bin
1 : asa923-k8.bin
2 : cl841-advp�servicesk9-ms.124-15.T1.bin
3 : cl841-ipbase-ms.123-14.T7.bin
4 : cl841-ipbasek9-ms.124-12.bin
5 : cl900-universalk9-ms.SPA.155-3.M4a.bin
6 : c3600-advp�servicesk9-ms.124-15.T1.bin
7 : c3600-i-ms.122-28.bin
8 : c3600-ipbasek9-ms.124-8.bin
9 : c3800nm-advp�servicesk9-ms.124-15.T1.bin
10 : c3800nm-advp�servicesk9-ms.151-4.M4.bin
11 : c3800nm-ipbase-ms.123-14.T7.bin
12 : c3800nm-ipbasek9-ms.124-8.bin
13 : c2900-universalk9-ms.SPA.155-3.M4a.bin
14 : c3950-ifq412-ms.121-22.EA4.bin
15 : c3950-ifq412-ms.121-22.EA8.bin
16 : c2950-lanbase-ms.122-25.FX.bin
17 : c2950-lanbase-ms.122-25.SE1.bin
18 : c2950-lanbasek9-ms.150-2.SE4.bin
19 : c3550-advp�servicesk9-ms.122-37.SE1.bin
20 : c3550-advp�servicesk9-ms.122-46.SE1.bin
21 : c800-universalk9-ms.SPA.152-4.M4.bin
22 : c800-universalk9-ms.SPA.154-3.M4a.bin
23 : cat3k_caa-universalk9.16.03.02.SPA.bin
24 : cgr1000-universalk9-ms.SPA.154-2.CG
25 : cgr1000-universalk9-ms.SPA.156-3.CG
26 : ciao.txt
27 : ciaodapcmariofotoprogetto.txt
```

28  
Figura 10: Ftp pc Mario sede B

## 9 Preventivo Tanzi S.R.L

Il presente documento riporta il preventivo di spesa per la realizzazione della rete aziendale, comprendente dispositivi di rete, server, cablaggio, software e servizi di installazione.

### 9.1 Dispositivi di Rete

Componente	Modello/Descrizione	Quantità	Costo Unitario (€)	Totale (€)
Router	Cisco ISR 4321	4	1.200	4.800
Switch	Cisco Catalyst 2960-24TT	5	800	4.000
Firewall	Cisco ASA 5506-X	2	1.500	3.000
Access Point	Cisco Aironet 1832i	1	400	400

Tabella 2: Dispositivi di rete

### 9.2 Server

Componente	Modello/Descrizione	Quantità	Costo Unitario (€)	Totale (€)
Server DNS	Dell PowerEdge R350	1	2.500	2.500
Server Web e Mail	HP ProLiant DL380	1	3.000	3.000
Server di Backup	Synology RackStation RS1221+	1	2.000	2.000

Tabella 3: Server aziendali

### 9.3 Cablaggio e Accessori

Componente	Modello/Descrizione	Quantità	Costo Unitario (€)	Totale (€)
Cavi Ethernet Cat6	10m per connessione	50	10	500
Armadio Rack 42U	APC NetShelter SX	1	1.500	1.500
Patch Panel 24 porte	Panduit DP245E88TGY	2	200	400
UPS	APC Smart-UPS 1500VA	2	900	1.800

Tabella 4: Cablaggio e accessori

## 9.4 Licenze e Software

Componente	Descrizione	Costo (€)
Licenza Firewall ASA	Cisco Smart License per ASA 5506-X	500
Licenza Windows Server	Per gestione Active Directory	1.200
Software di backup	Veeam Backup Essentials	1.500
Software di monitoraggio	PRTG Network Monitor (500 sensori)	1.800

Tabella 5: Licenze e software

## 9.5 Servizi di Installazione e Configurazione

Servizio	Costo (€)
Installazione, cablaggio e Configurazione router, switch, firewall e server	3.000
Test, collaudo, Verifica connettività e sicurezza	1.500
Formazione IT interno e Training per gestione rete	1.000

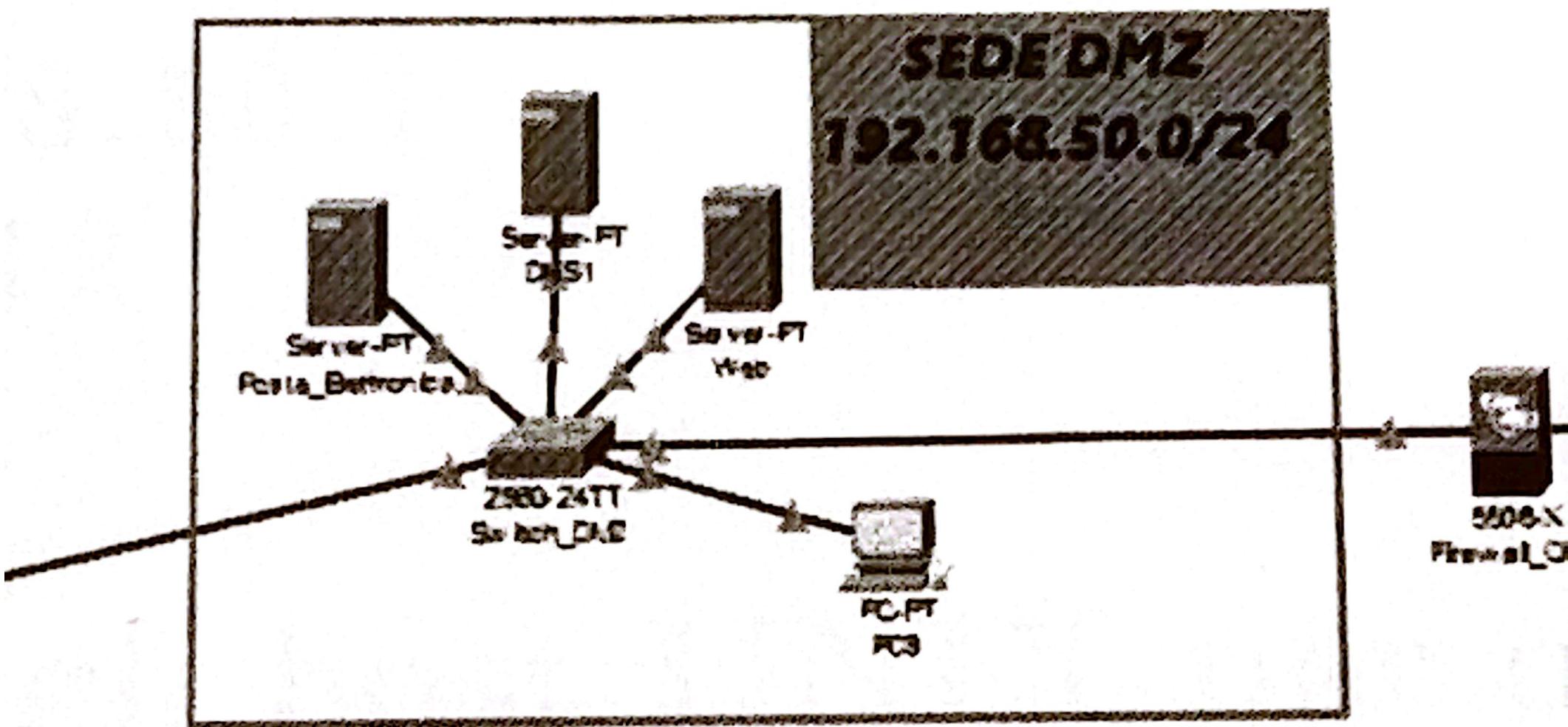
Tabella 6: Servizi di installazione e configurazione

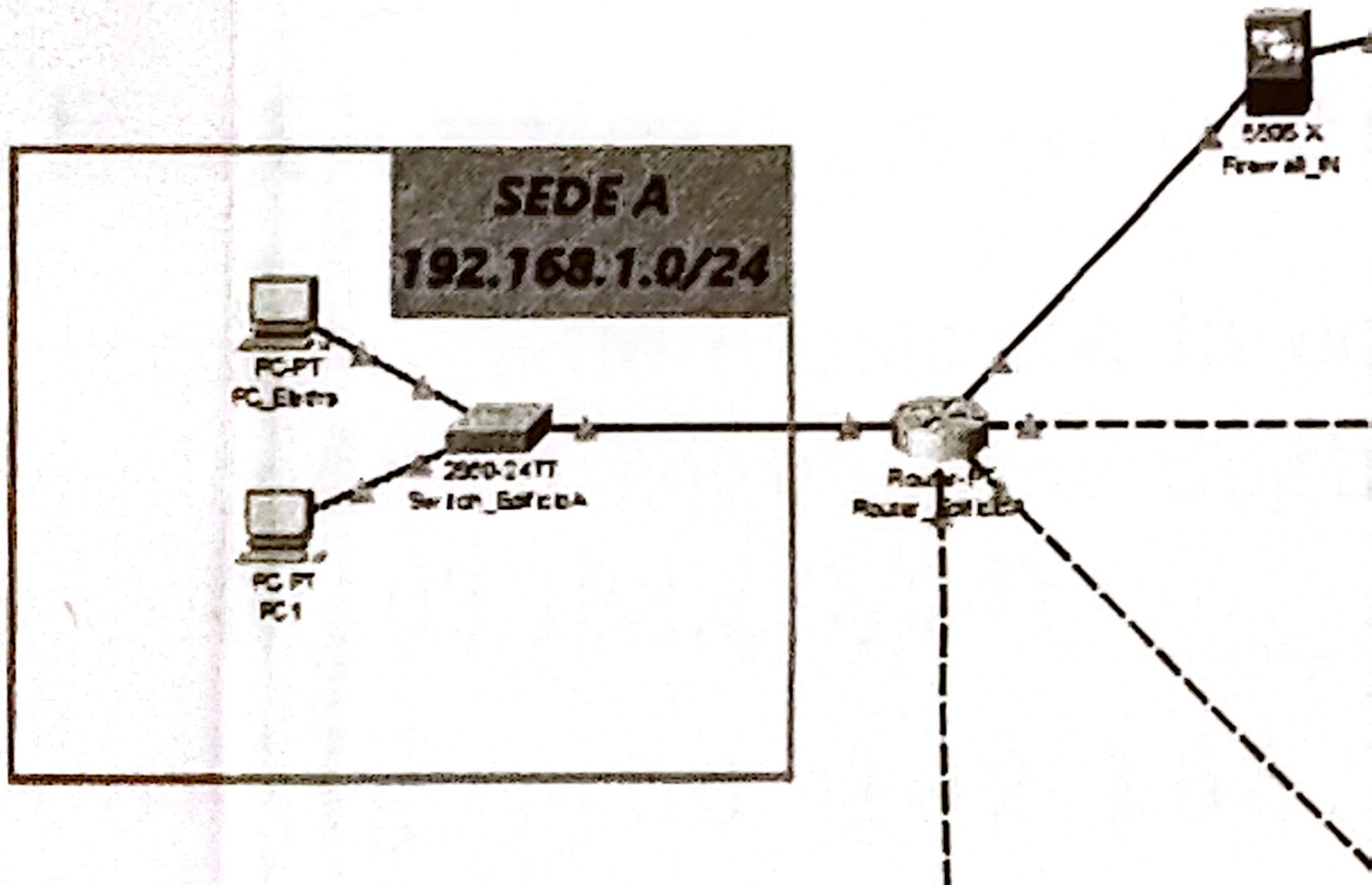
## 9.6 Totale Preventivo

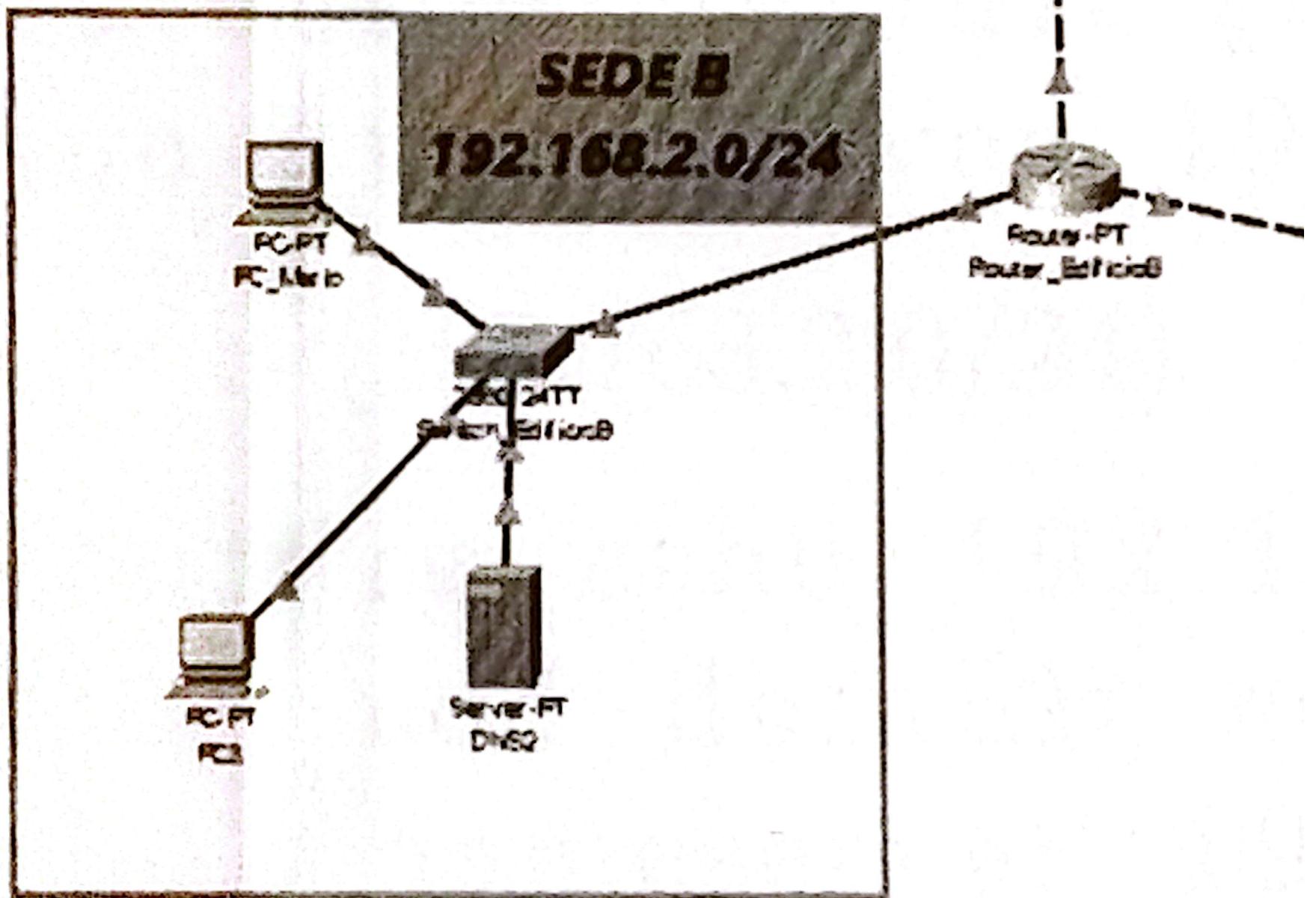
Costo totale stimato: € 34.900

### Note:

- I prezzi sono indicativi e possono variare a seconda del fornitore.
- Include hardware, software, installazione e formazione.
- Il sistema di backup garantisce la protezione dei dati aziendali.







Server\_PDC

