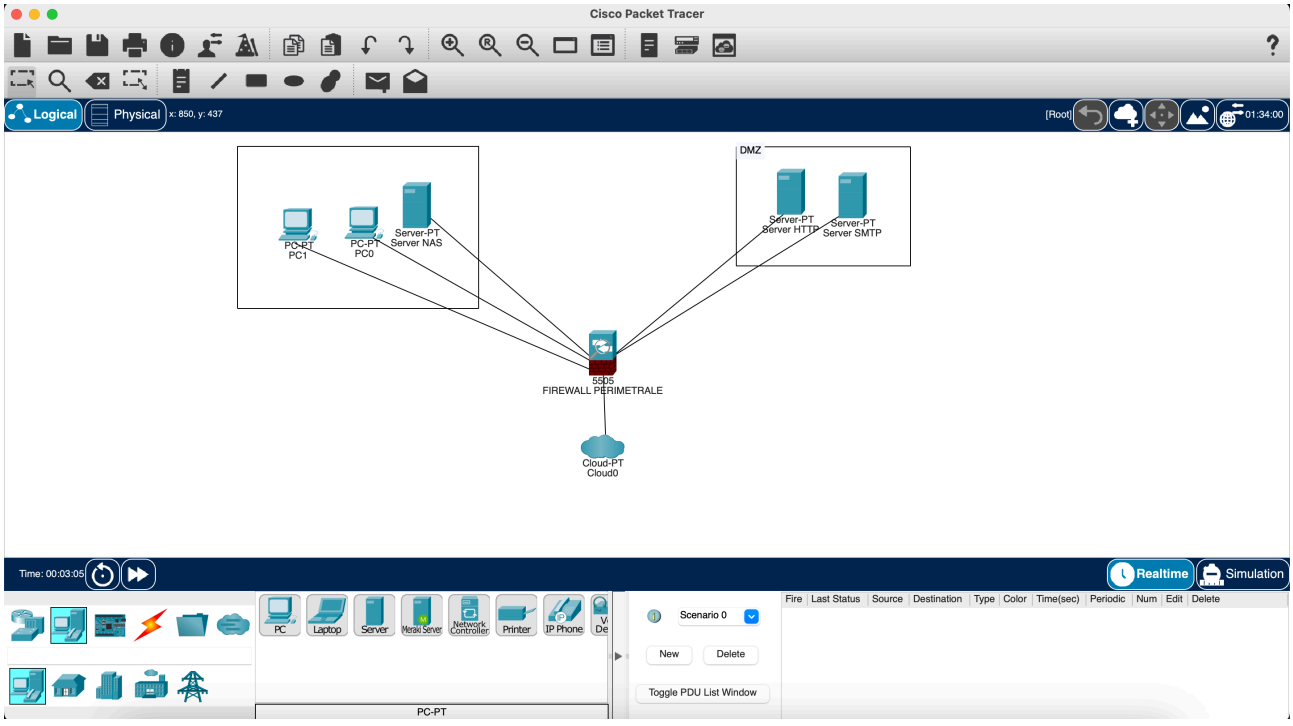
Composizione:

1. **Internet (Cloud o simbolo di Internet)**:
    - Rappresenta la connessione esterna, cioè la rete globale.
2. **DMZ (Demilitarized Zone)**:
    - **Server Web HTTP** (porta 80) per l'accesso ai servizi pubblici.
    - **Server di posta elettronica SMTP** (porta 25) per la gestione delle comunicazioni via email.
    - La DMZ è una zona separata dalla rete interna, accessibile da Internet, ma separata per motivi di sicurezza.
3. **Rete Interna**:
    - **Server o NAS** (Network Attached Storage) per la gestione e archiviazione dei dati aziendali.
    - La rete interna è protetta dal firewall perimetrale e contiene risorse che devono essere sicure e non direttamente accessibili da Internet.
4. **Firewall perimetrale**:
    - Un firewall viene posizionato tra Internet, DMZ e la rete interna. Gestisce il traffico in entrata e in uscita, applicando politiche di sicurezza.



2. Spiegazione delle Scelte

1. Internet (Cloud):

- Internet è la zona di accesso esterno. Tutti i dati che provengono dall'esterno (dal web) arriveranno tramite Internet e dovranno passare attraverso il firewall per raggiungere la DMZ e/o la rete interna.

2. DMZ (Demilitarized Zone):

- **Scopo**: La DMZ è una zona di rete isolata che ospita i servizi esposti a Internet ma separati dalla rete interna. La DMZ è un buon punto di difesa per i servizi che devono essere accessibili da Internet, ma senza compromettere la sicurezza della rete interna.
- **Server Web (HTTP)**: Serve per ospitare siti web accessibili pubblicamente. La porta standard HTTP (80) è utilizzata per il traffico web.
- **Server di Posta Elettronica (SMTP)**: È usato per la gestione delle comunicazioni e-mail in uscita (invio di e-mail). La porta standard SMTP (25) è utilizzata per il traffico di posta elettronica. La DMZ offre una protezione contro attacchi a questi servizi.

3. Firewall perimetrale:

- **Scopo**: Il firewall ha il compito di monitorare e filtrare tutto il traffico che passa tra le diverse zone (Internet, DMZ, Rete Interna).
    - Tra **Internet e DMZ**: Il firewall consente il traffico verso il server web e il server SMTP, ma blocca il traffico non autorizzato per prevenire attacchi.
    - Tra **DMZ e Rete Interna**: Solo il traffico autorizzato (ad esempio, richieste per l'accesso a database o file) è permesso. L'accesso alla rete interna è fortemente limitato per evitare che un attacco alla DMZ possa compromettere la rete interna.
    - Tra **Internet e Rete Interna**: Il firewall generalmente blocca ogni connessione in ingresso verso la rete interna, limitando l'esposizione.

4. Rete Interna:

- **Scopo**: La rete interna ospita i server e le risorse più sensibili dell'organizzazione, come un server NAS per l'archiviazione dei dati. Questi sistemi non sono direttamente accessibili da Internet e sono protetti da più livelli di sicurezza.
- Il NAS (Network Attached Storage) potrebbe essere utilizzato per archiviare file condivisi tra i dipendenti e deve essere protetto da un firewall per evitare accessi non autorizzati dall'esterno.