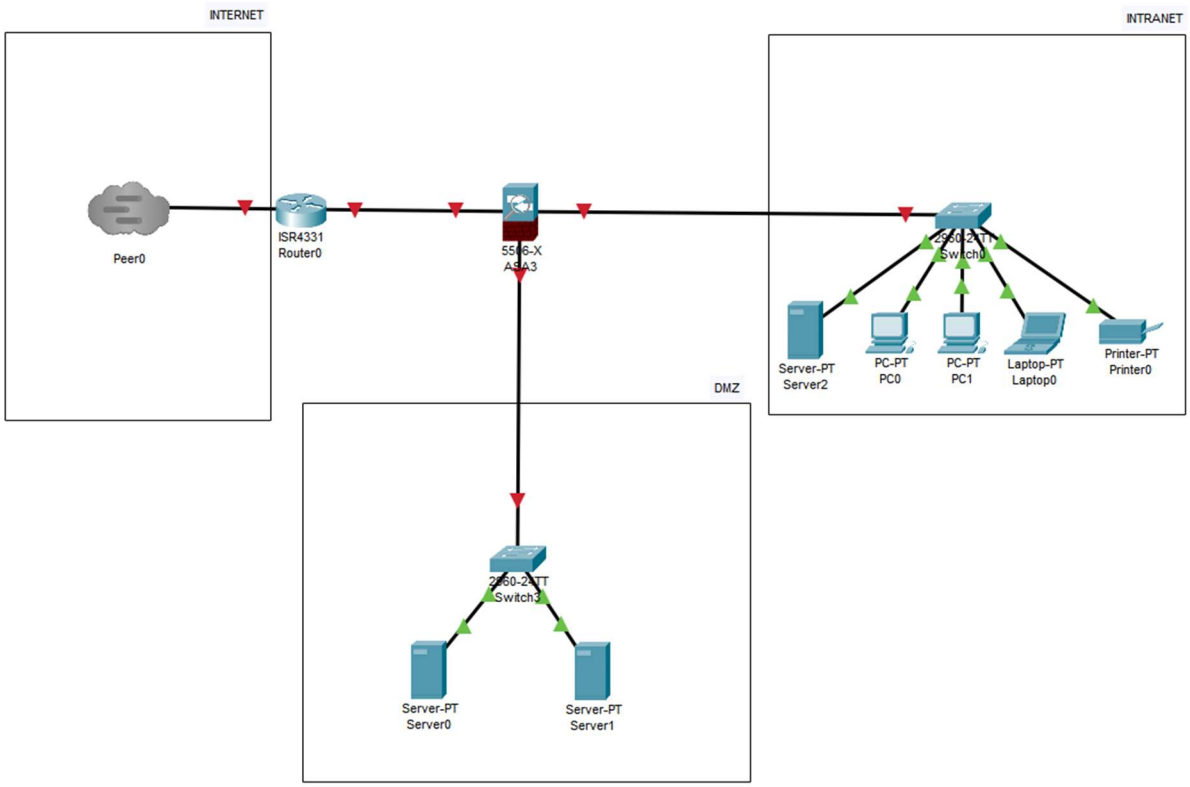

Il vantaggio principale di una DMZ è fornire a una rete interna un ulteriore livello di sicurezza, limitando l'accesso a dati e server sensibili. Una DMZ consente ai visitatori esterni di ottenere determinati servizi, fornendo al contempo una copertura tra loro e la rete privata dell'organizzazione.

La traccia richiede l'utilizzo di un solo firewall perimetrale posizionato tra le tre zone. Un approccio più sicuro consiste nell'utilizzare due firewall; un primo firewall esterno come prima linea di difesa, che deve essere configurato per consentire solo il traffico destinato alla DMZ mentre il secondo firewall è interno e consente solo il traffico dalla DMZ alla rete interna. La presenza di due firewall sarebbe una sicurezza aggiuntiva per la rete interna perché invece di un unico punto di sicurezza ne troviamo due; c'è ancora più protezione se i due firewall usati provengono da due diversi fornitori, perché questo rende meno probabile che entrambi i dispositivi soffrano delle stesse vulnerabilità di sicurezza.

La traccia richiede una rete interna con la presenza di almeno un server, non specificando esplicitamente la presenza di una sala server separata; questa si sarebbe potuta realizzare, con un ulteriore firewall a protezione considerata la natura critica degli applicativi eseguiti e dei dati contenuti in essa.

Nella DMZ in figura è presente un server web (HTTP) e un server di posta elettronica (SMTP).

La DMZ in figura con una progettazione a firewall singolo presenta tre interfacce di rete. La prima rappresenta la rete esterna, che collega la connessione Internet pubblica al firewall. La seconda forma la rete interna, mentre la terza è connessa alla DMZ. Diverse **policy firewall** (tramite azioni di Allow, Drop e Deny) monitorano e controllano il traffico autorizzato ad accedere alla DMZ, e limitano la connettività alla rete interna.