Il **Web Server** che espone diversi servizi su internet (e quindi accessibili al pubblico) si trova nella **DMZ**, che permette di fornire alla rete interna aziendale (**INTRANET**) 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.

L' **Application Server** espone sulla rete interna un applicativo di e-commerce accessibile dai soli impiegati della compagnia (quindi non accessibile da resti esterne, ovvero internet); esso si trova nella **sala server** della rete interna, separata dalla workstation.

La sicurezza delle componenti critiche viene garantita da 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 è 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**. Tale pratica di utilizzare firewall diversi da diversi fornitori è una componente della strategia di **difesa in profondità**.
Le **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.