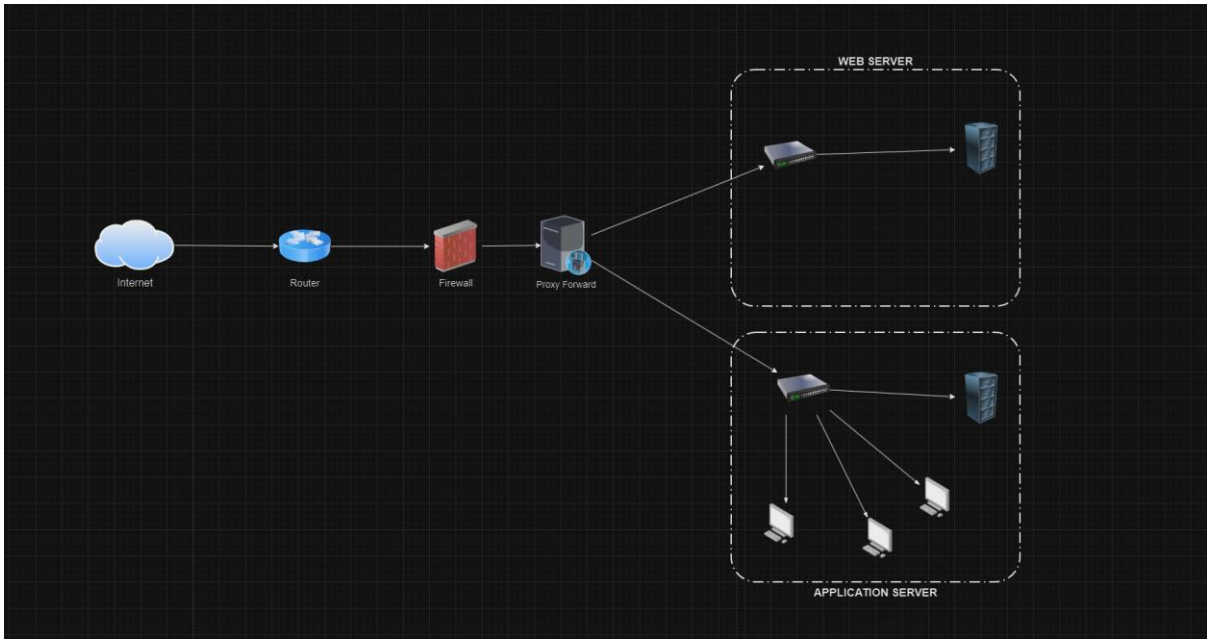

Router: usato per connettere più reti insieme e instradare il traffico dati tra di esse. Il suo ruolo principale è quello di determinare la via più efficiente e appropriata per inviare i pacchetti di dati da una rete all'altra. Usato inoltre per l'assegnazione degli indirizzi IP, gestione del traffico e sicurezza della rete.

Application server: zona DMZ dove vengono posizionati server destinati a fornire servizi accessibili dall'esterno, come server web, server di posta elettronica o server DNS. Questi server sono più esposti a potenziali minacce esterne, ma isolati dalla rete interna. La rete DMZ consente di mantenere una separazione chiara tra i server pubblici accessibili dall'esterno e i server e le risorse critici all'interno dell'organizzazione. Questo design contribuisce a ridurre la superficie di attacco e proteggere gli asset più sensibili da minacce esterne.

Firewall: il firewall è posizionato tra la rete interna, la DMZ e la rete esterna. Esso regola il traffico di rete e applica politiche di sicurezza per proteggere la rete interna da accessi non autorizzati. Ci possono essere firewall dedicati tra la rete interna e la DMZ, così come tra la DMZ e la rete esterna.

Proxy: il proxy può essere utilizzato per controllare e filtrare il traffico tra la rete interna e la DMZ. Può migliorare la sicurezza implementando funzionalità come il content filtering e la protezione dalle minacce. Abbiamo usato un proxy forward per gestire il traffico dai client agli altri server.

Servizi di sicurezza: Possono essere implementati ulteriori strumenti di sicurezza nella DMZ, come sistemi di rilevamento delle intrusioni (IDS) o sistemi di prevenzione delle intrusioni (IPS), per rilevare e mitigare eventuali attacchi.