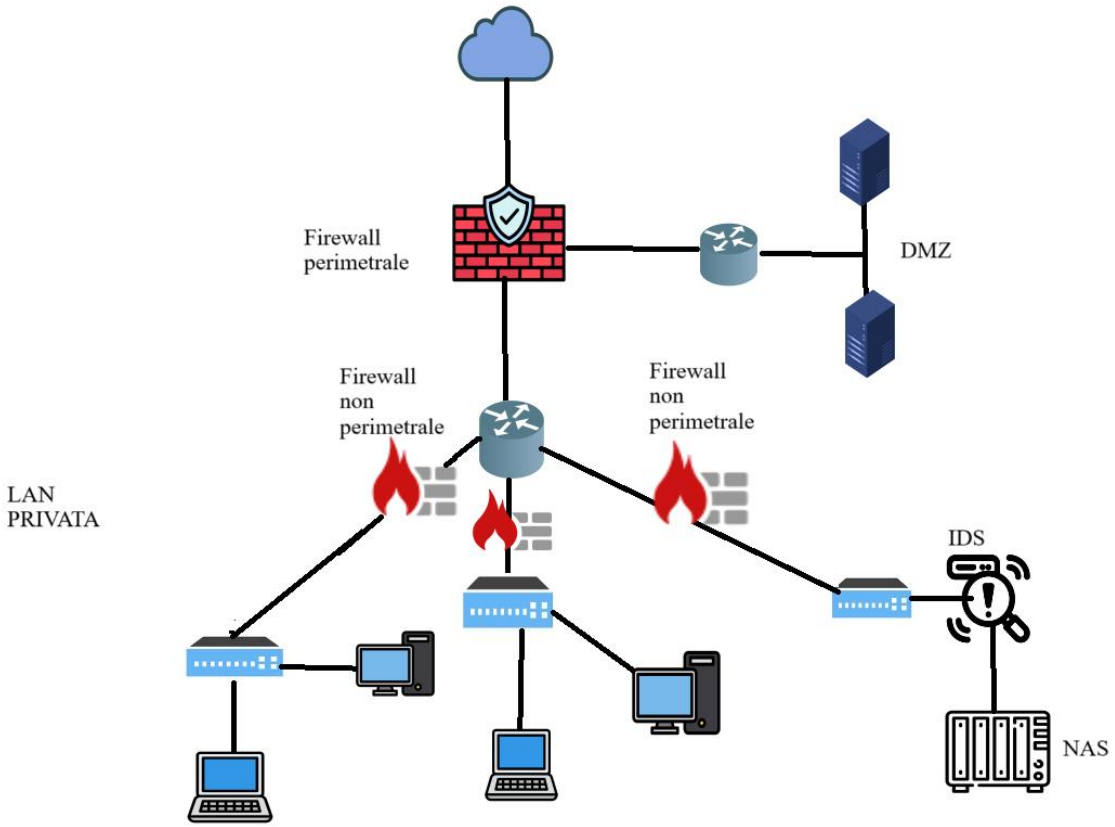

In merito al posizionamento c'è un Firewall perimetrale che si trova a cavallo tra la LAN e la WAN; viene posizionato sul perimetro per proteggere la rete aziendale dagli attacchi e dai pericoli provenienti dall'esterno. Tra lo spazio della rete interna ed internet c'è la DMZ (demilitarized zone) che viene utilizzata per servizi utilizzabili all'esterno come server web e server di posta elettronica, anch'essa protetta dal firewall perimetrale che controllerà il flusso di traffico tra internet e la DMZ.
Un altra misura presa in considerazione è l'implementazione di firewall non perimetrali per il controllo del traffico e delle minacce interne.
All'interno della LAN è presente un server NAS (Network attached storage) utilizzato per l'arcchiviazione e la condivisione sicura dei dati aziendali. Il server svolge un ruolo fondamentale nella gestione dei dati aziendali e quindi è essenziale proteggerlo, motivo per cui nella rete è presente un IDS (intrusion Detection System) (preferito ad un IPS per l'eventualità di non bloccare dispositivi legittimi) che svolge un ruolo fondamentale nel rilevare e segnalare in modo rapido le potenziali minacce. Grazie all'IDS è possibile rilevare intrusioni e comportamenti anomali consentendo una risposta rapida alle minacce.