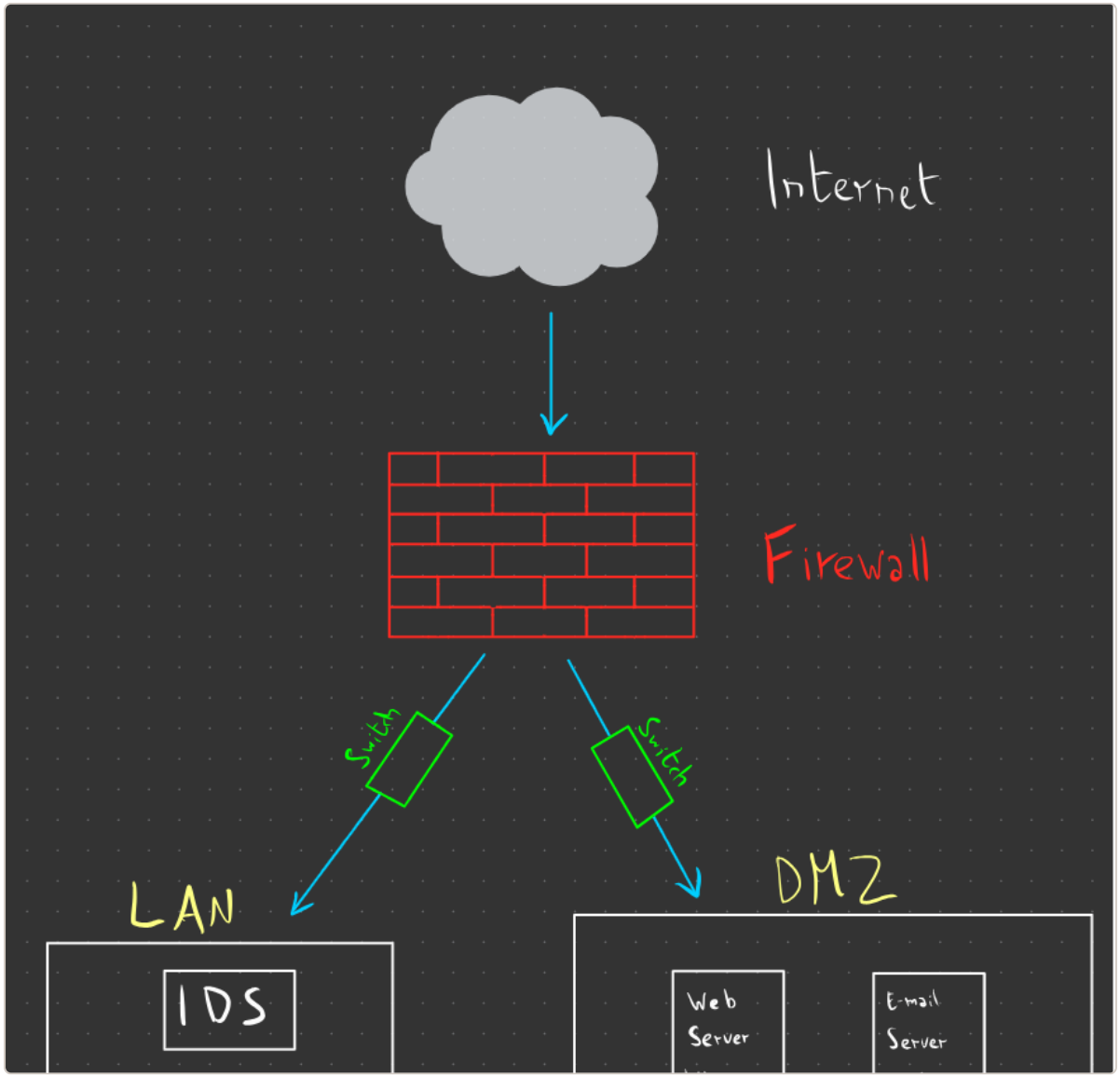

Si seguirà lo schema dall'alto verso il basso.

Il Firewall perimetrale è posizionato come prima linea di difesa nel punto più esterno della rete, come punto di collegamento con internet, questo permette di prevenire minacce e bloccarle prima che possano proseguire.

Attraverso uno switch si accede alla DMZ (Demilitarized Zone) dove sono ubicati un Server Web (HTTP) e uno di posta elettronica (SMTP), sono collocati all'esterno della rete interna per permettere una gestione più sicura del traffico, questo è un esempio della maggiore sicurezza che una segmentazione della rete porta con sé, se un malintenzionato dovesse accedere alla DMZ, comprometterebbe solo questi servizi, tenendo al sicuro i dati sensibili della rete.

Attraverso un altro switch, si accede alla LAN dove, all'interno del NAS (Network Attached Storage) si trovano i dati più importanti e che vogliamo proteggere, attraverso l'utilizzo di un IDS (Intrusion Detection System) possiamo monitorare il traffico nella rete interna, in modo da essere allarmati qualora dovessero esserci dei tentativi di accessi non autorizzati.