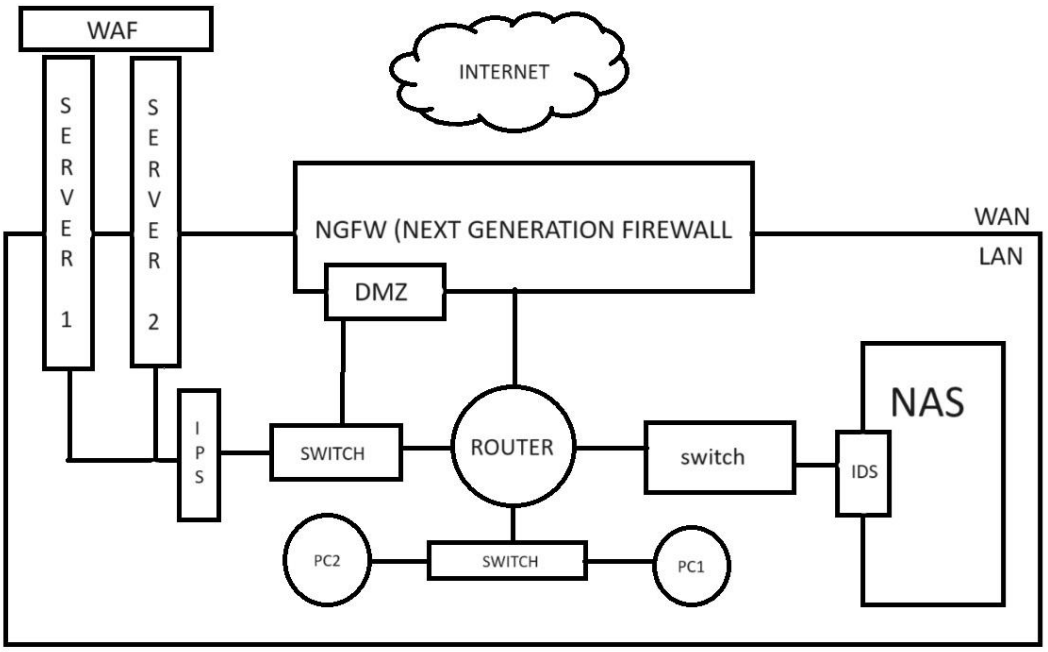
Esercizio S2-L2



Nel disegno abbiamo la rappresentazione di una rete privata LAN in cui andiamo a trovare:

- 1 NAS: è un dispositivo di archiviazione file collegato a una rete costituito da uno o più hard disk.
- 1 Firewall di nuova generazione: chiamato anche Next Generation Firewall (NGFW) è un dispositivo di sicurezza informatica moderno che opera dal livello 7 al livello 1 del modello ISO/OSI. In questo caso si tratta di un firewall perimetrale in quanto è posto a cavallo tra la LAN (rete privata) e la WAN (internet). Si tratta di una difesa che protegge da attacchi malware, DOSs, phishing, ransomware etc...
  Opera con metodologia dinamica, quindi che consente il passaggio di dati solo verso l'esterno e si necessita di inserire un sistema DMZ.
- 1 DMZ: o demilitarized zone, è un sistema informatico (sottorete fisica o logica) che consente il passaggio di informazioni sia dal client verso server che viceversa. La presenza di un firewall di tipo dinamico necessita obbligatoriamente di un DMZ per avere la possibilità di ricevere informazioni dall'esterno della rete privata.
- IPS/IDS: questi corrispondono allo stesso sistema di difesa software. Si differenziano perché l'IDS opera in modo passivo inviando un allert al client di un possibile arrivo di dati malware mentre l'IPS opera attivamente bloccandolo e inviando un allert.
  Andiamo quindi a collocare l'IDS in corrispondenza del NAS in modo che tutti riescano ad accedervi senza essere bloccati, mentre andremo a inserire l'IPS in corrispondenza dei due server, luogo in cui vi è più probabilità di ricevere un attacco.
  IDS: Sistema di Rilevamento delle Intrusioni
  IPS: Sistema di Protezione dalle Intrusioni
- 2 Server: Possediamo 2 server uno dedicato al web (HTTP) e uno dedicato alla posta elettronica (SMTP).
- WAF: Web Application Firewall. Questo firewall possiede un filtraggio di tipo dinamico e opera a livello dei contenuti andrà, quindi, a leggere indirizzo IP, porta e contenuto del pacchetto e bloccando quest'ultimo nel caso in cui il contenuto sia

malevolo o sospetto. Possiede una tabella di riferimento dove vi confronta i contenuti del pacchetto controllando che tutto figuri benevolo. Ad esempio contenuti come malware.exe vengono bloccati. Questo sistema difende al livello applicativo del sistema ISO/OSI.