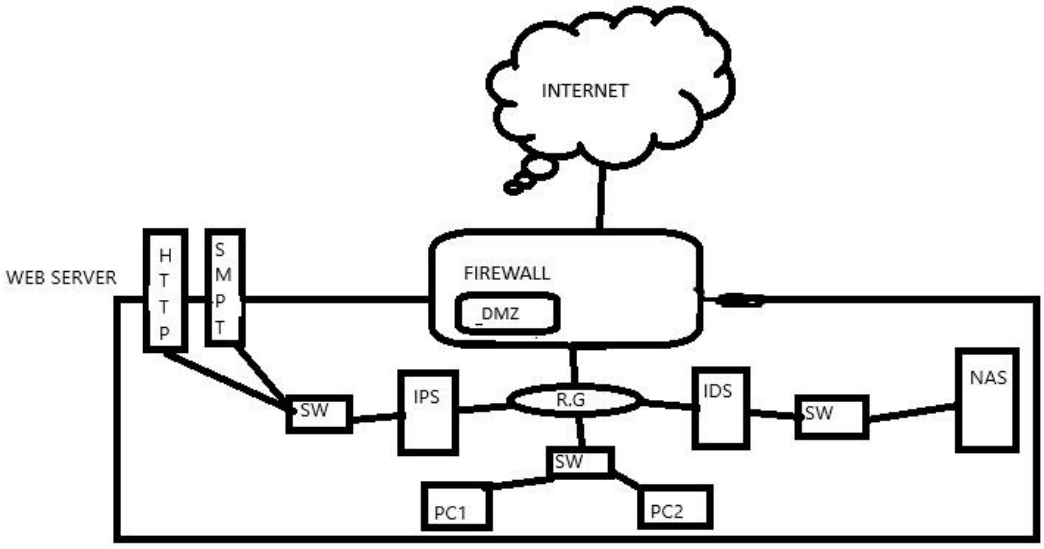
# PROGETTO DI UNA RETE SEGMENTATA:

Disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
- Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.
- Una rete interna con almeno un server o nas.
- Un firewall perimetrale posizionato tra le tre zone.
- Spiegare le scelte.




Una volta inseriti nel disegno tutte le componenti della rete andiamo a capire cosa sono e a cosa servono:

1. **FIREWALL:** abbiamo inserito un file perimetrale che faccia da protezione sia per la rete lan e la rete wan. Il firewall può avere diversi tipi di filtraggio, quelli maggiormente utilizzate dalle aziende sono i firewall a filtraggio proxy e waf. Il filtraggio proxy, fa da filtro appunto, tra due indirizzi IP che siano privati o pubblici. In base all'indirizzo IP mittente e destinatario ci sono diversi tipi di proxy, il proxy forward e il reverse proxy. Considerando che il proxy può cambiare l'indirizzo IP, nel primo caso sarà un dispositivo dell'azienda ad esempio pc1 che passa attraverso il proxy per accedere ai server web per accedere a internet, mentre nel reverse proxy è il processo inverso, chiunque voglia accedere ai miei web server dovrà passare per il proxy. Il filtraggio waf invece, legge il contenuto del pacchetto e lo analizza. Il waf ha una tabella che viene impostata in fase di configurazione secondo alcuni codici malwere, questa tabella può prendere questi codici anche da OWASP che è un'azienda no profit che trova e condivide sul web questi codici. Quindi tornando al pacchetto, una volta aperto confronterà il suo codice con quelli sulla tabella, la quale viene controllata partendo dall'alto, se il codice si trova in questa tabella in automatico questo pacchetto verrebbe bloccato, altrimenti viene fatto passare.

2. **DMZ:** dal momento in cui abbiamo questo firewall che ci difende dall'esterno e blocca tutti i pacchetti malevoli, le aziende hanno iniziato ad utilizzare una zona demilitarizzata, dentro la quale è possibile lo scambio da e verso l'interno senza essere bloccati dal firewall, in questa zona generalmente vengono inserite le web server aziendali.

3. **NAS:** abbiamo inserito anche un server nas, sarebbe un archivio virtuale che potremmo paragonare a google drive, il quale appartiene a google, mentre il nas è prorpio dell'azienda, quindi manterrà archiviati tutti i dati "sensibili" dell'azienda.

4. **IDS/IPS:** in questo progetto abbiamo aggiunto anche un ids e un ips, che di base sono lo stesso softwere, con la differenza che l'ids analizza il pacchetto e lo confronta con le regole della tabella se il pacchetto è malevolo manderà un alert, un avviso al direttore, mentre l'ips fa lo stesso procedimento ma invece di mandare l'avviso, bloccherà automaticamente il pacchetto. In un'azienda servono entrambi, poichè se il direttore volesse accedere al server nas, nonostante sarà autorizzato, potrebbe non rispettare i parametri della tabella, e se a protezione del nas ci fosse l'ips in nessun modo riuscirebbe ad accedere, verrebbe bloccato automaticamente, mentre se ci fosse l'ids, quando arriverà l'avviso lui potrà accedere ugualmente. l'ips è necessario metterlo a protezione dei web server, in quanto serve maggior sicurezza per bloccare in malwer provenienti da un possibile attacco dall'esterno.

5. **WEB SERVER:** I web server sono software o dispositivi hardware che gestiscono la distribuzione di contenuti web, ricevono le richieste dei browser (come Chrome o Firefox), elaborano queste richieste e inviano i file richiesti (come pagine HTML ). Nel nostro caso abbiamo un server http e smpt. web server HTTP è un tipo specifico di server che utilizza il protocollo HTTP per comunicare con il client. Mentre il web server SMTP è un server che gestisce l'invio e la ricezione di email attraverso il protocollo SMTP