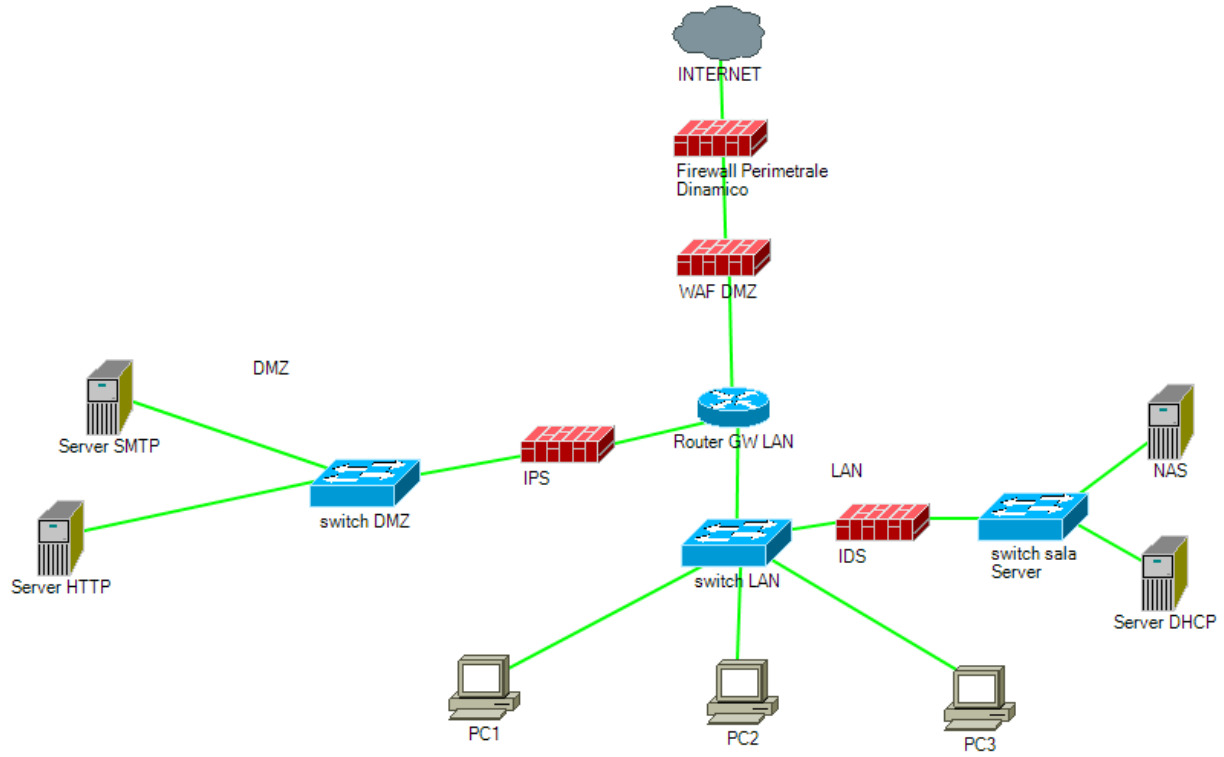
S3L4 – Disegno rete

Questo il disegno di rete secondo la consegna:



Spiegazione:

Il firewall perimetrale dinamico andrà a controllare tutto il traffico proveniente da internet, eccetto quello verso la DMZ. Essendo di tipo stateful, terrà traccia delle connessioni attive e permetterà al traffico dall'esterno di passare solo se questo è di risposta ad una comunicazione avviata dall'interno.

Il WAF, o web application firewall, (in questo disegno è separato per motivi di semplicità, ma può essere anche un modulo appartenente allo stesso firewall) andrà ad analizzare il traffico verso i server in DMZ (SMTP e HTTP), andando ad operare a livello application. Dato che la DMZ dev'essere raggiungibile in un qualunque momento dall'esterno, permetterà le connessioni in ingresso verso gli ip della DMZ.

A protezione della Sala Server interna all'azienda, ho posto un IDS, che andrà ad analizzare il traffico verso il NAS, contenente i dati più sensibili dell'azienda, ed il server DHCP. L'IDS notificherà gli addetti alla cybersecurity aziendale in caso di codice malevolo rilevato, non andando però attivamente a bloccare le connessioni. Questo in modo che, anche in caso di falsi positivi, la continuità di servizio aziendale verso i dati più critici sia garantita.

A protezione dei server in DMZ ho posto invece un IPS. L'IPS ha un livello di sicurezza maggiore rispetto all'IDS in quanto può bloccare attivamente eventuali connessioni contententi codice malevolo quando rilevate, fungendo quindi da IDS **attivo.** Ho preferito quindi collocarlo in questo punto in quanto come detto sopra la DMZ non gode della protezione del firewall perimetrale ma solo del WAF.