S2/L2

Compito di oggi: disegnare una rete con i seguenti componenti:

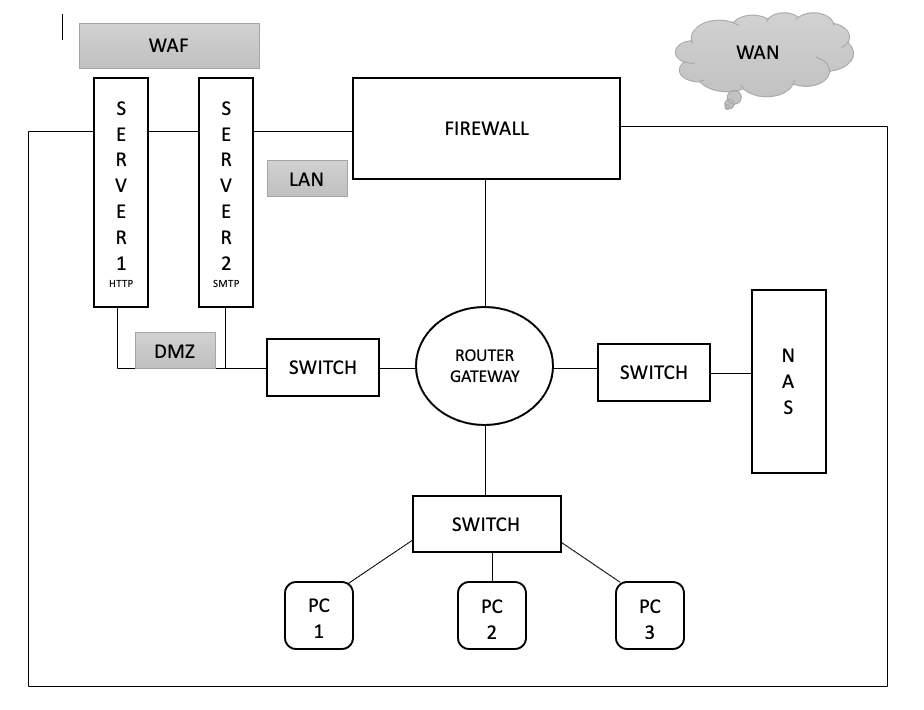
● Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).

● 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.



Il primo componente della sicurezza informatica che troviamo è il FIREWALL, ovvero un dispositivo di sicurezza della rete che permette di monitorare il traffico in entrata e in uscita.

In questo caso, abbiamo un firewall perimetrale, cioè tra la WAN (internet) e la LAN (rete locale) ed è progettato per proteggere la rete interna da minacce provenienti dall’esterno. La WAN, come possiamo vedere è posizionata esternamente rispetto al firewall ed è la zona evidenziata da un “cloud”. Ad oggi utilizziamo un firewall perimetrale a filtraggio dinamico, il quale protegge dal quarto livello ISO-OSI, e permette la connessione dall’interno verso l’esterno con la capacità di tenere traccia delle connessioni di rete in una tabella volatile chiamata ACL. Come abbiamo detto, questo tipo di filtraggio blocca tutte le connessioni dall’esterno, per surclassare questo problema e quindi avere una connessione da entrambi i lati, si inseriscono dei server web. Il primo è un server web HTTP ed il secondo è un server di posta elettronica (SMTP). Perciò nel firewall dinamico avrò delle porte in cui vado ad inserire quei server/dispositivi che erogano servizi. I server web vengono inseriti in una zona denominata DMZ o “zona demilitarizzata” ovvero un segmento di rete che espone i servizi raggiungibili da internet; tuttavia dato che questi flussi come abbiamo detto provengono da internet è difficile avere un adeguato livello di sicurezza. Per risolvere questo problema, viene inserito il WAF (web application firewall) il quale protegge da attacchi dannosi e traffico internet indesiderato (protegge dal 7° livello ISO-OSI). La sicurezza del WAF deriva da un filtraggio per contenuto, ovvero, oltre a verificare l’IP mittente, verifica anche il contenuto del pacchetto per vedere se sia o meno un malware, attraverso una tabella impostata da organizzazioni terze. A livello applicativo, vediamo dal grafico che si trova davanti o sopra il firewall, ma spesso possiamo trovarlo direttamente nella DMZ.

Il firewall e gli switch sono collegati ad un router gateway, il quale permette instradare il traffico di rete su reti diverse.

Lo switch di destra è a sua volta collegato ad un NAS (network attached storage), un server di file centralizzato che consente agli utenti di archiviare e condividere file; in sintesi è un dispositivo di back-up dove vi sono i dati più importanti dell’azienda.

Quindi, nella rete sopra descritta, possiamo identificare 3 zone contraddistinte:

* WAN
* LAN
* DMZ