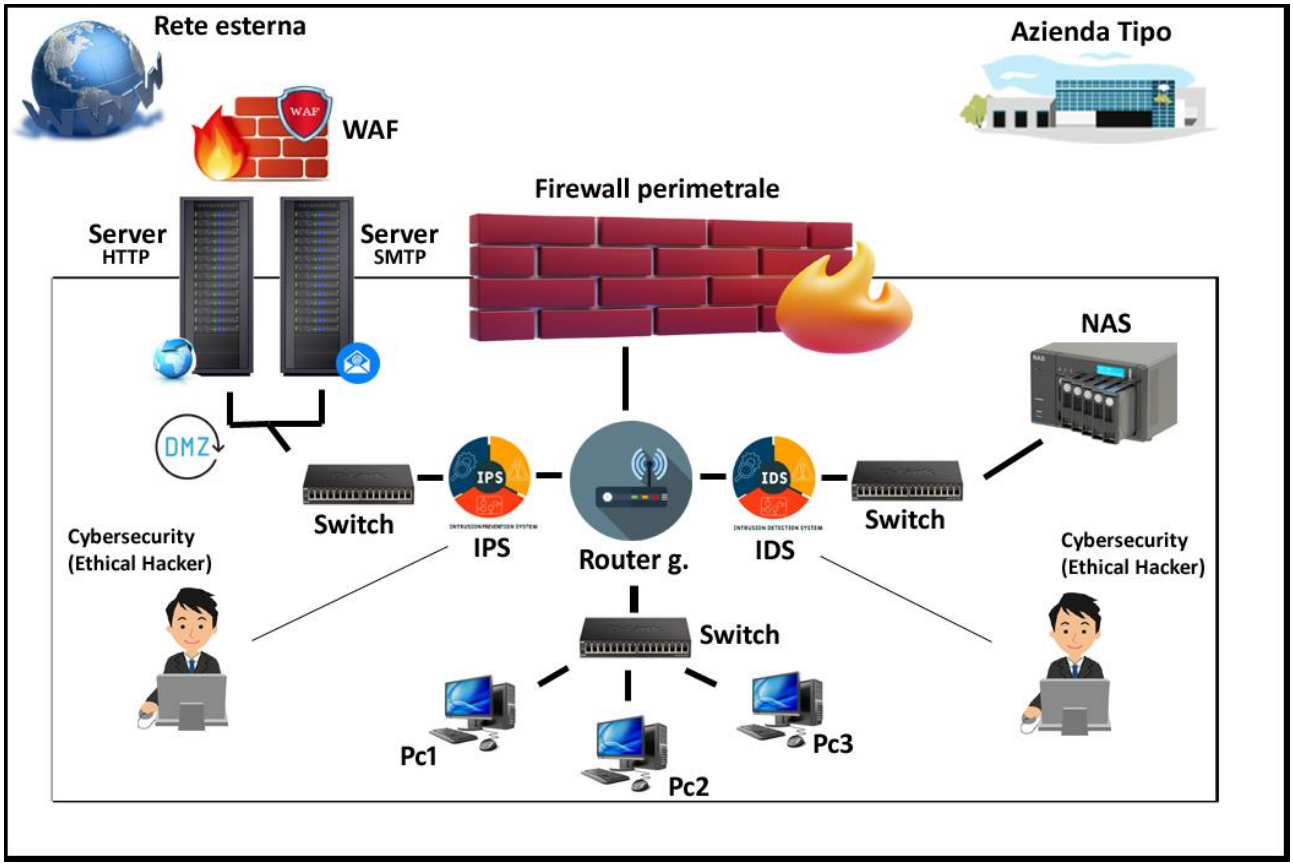
Esercizio 12/10/2023



Nell'esercizio odierno viene richiesto di disegnare una rete con i seguenti componenti:

Zona internet
Zona DMZ
Server web (http)
Server di posta elettronica (SMTP)
Rete interna con almeno un NAS o un server
Firewall perimetrale
Sistema di rilevamento IDS posizionato strategicamente
Sistema di rilevamento IPS posizionato strategicamente

Spiegazione delle scelte

Nel mio disegno ho riprodotto il funzionamento di una rete aziendale in cui ho inserito prima di tutto un **firewall perimetrale** e un **WAF** (Web Application Firewall) che va a "difendere" tutta l'area di lavoro da eventuali attacchi. Il WAF protegge tutti e 7 i livelli **ISO/OSI** che è un modello concettuale che definisce il modo in cui le reti inviano i dati dal mittente al destinatario (1Fisico – 2Collegamento – 3Rete – 4Trasporto – 5Sessione – 6Presentazione o Traduzione – 7Applicazione). Possiamo definirlo come un firewall con un filtraggio più evoluto avendo già in memoria una tabella con una sorta di "Black List" e lì dove non arriva si avvale di OWAST. Oltre a leggere l'IP mittente e IP destinatario legge anche il contenuto del file pertanto se rileva nel file un contenuto malevolo lo rifiuta. In entrata ai server, quindi, fa una prima scrematura.
Nonostante la parte più importante da proteggere sia quella del **NAS** (il sistema dove vengono immessi i dati più importanti e più sensibili) il sistema **IPS** (Intrusion Prevenction System – previene l'attacco attraverso un'azione oltre a avvisare) deve essere inserito a mio avviso tra il router e lo switch dove vengono collegati i server http e SMTP e dove troviamo la zona **DMZ**, una zona slegata da tutto, raggiungibile dall'esterno dove si vanno normalmente a mettere dei server con dei servizi poiché gli attacchi più probabili e più problematici arrivano proprio dall'esterno della rete, mente ho inserito il sistema **IDS** (Intrusion Detenction System – si limita a monitorare l'attacco e avvisare) tra il router e lo switch che si collega al NAS in modo tale che il sistema di filtraggio sia, si più deficitario, ma senza dubbio più accessibile all'interno dell'azienda stessa. Ci sarà comunque un Ethical Hacker che monitorerà la situazione evitando anche i falsi positivi (cioè il dispositivo viene riconosciuto come se fosse un Black Hat ma in realtà non lo è).