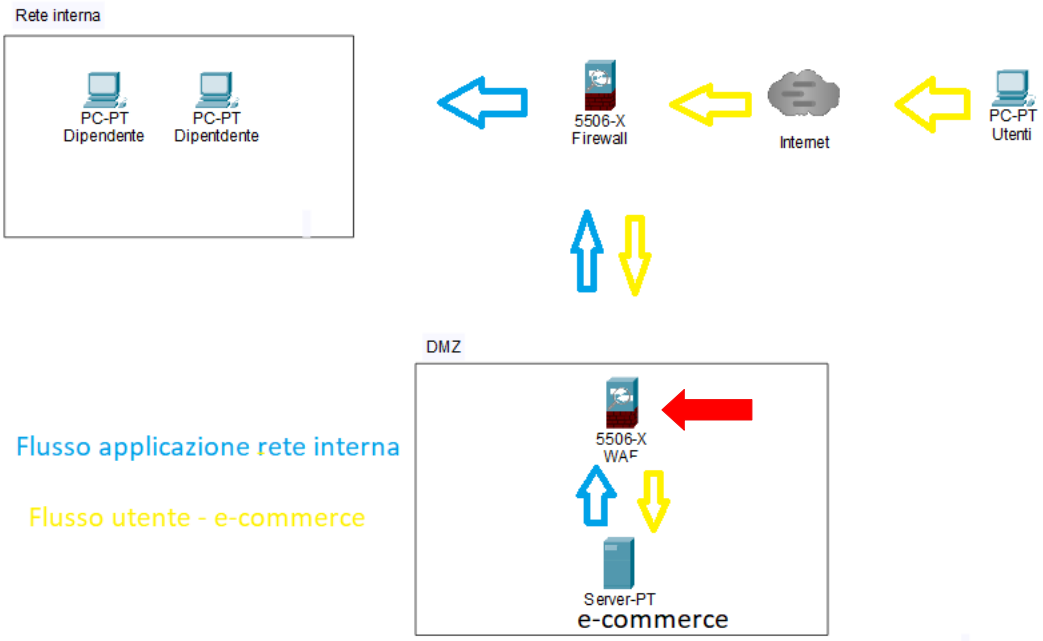
Il progetto di questa settimana ci chiedeva di occuparci di vari casi e di trovare soluzioni diverse a seconda della richiesta:

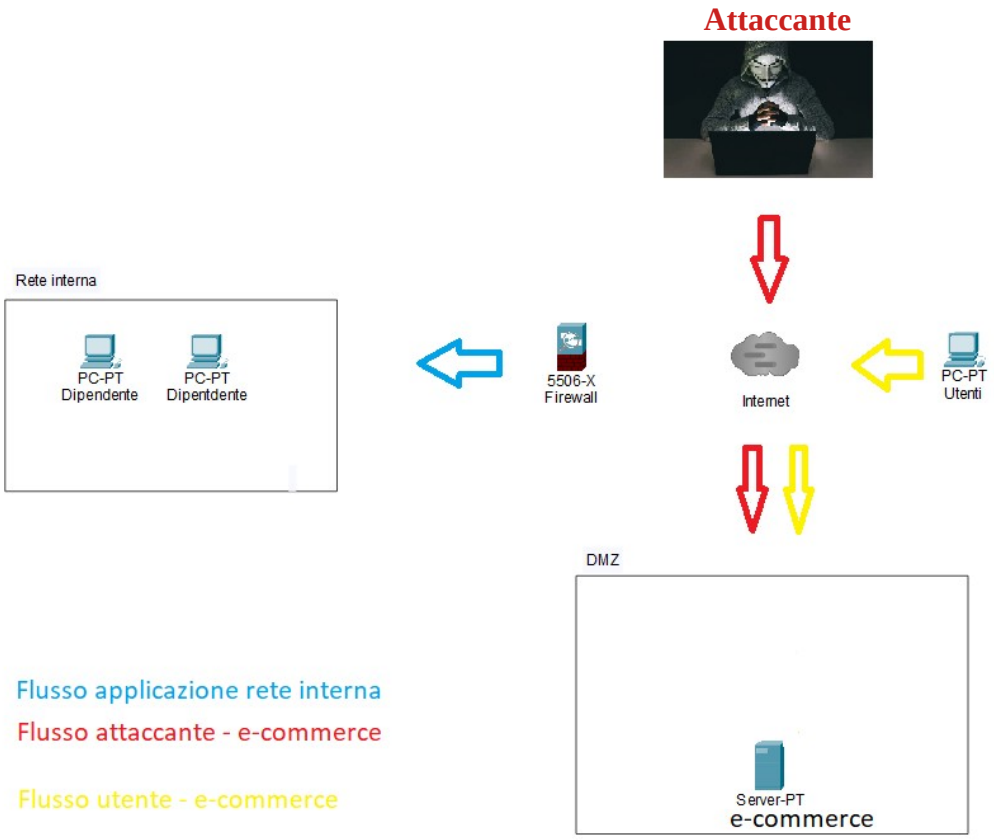
1) **Azioni preventive**: in questo caso ci veniva chiesto di implementare dei sistemi di difesa per evitare di subire attacchi di tipo **SQLinjection** o **XSS** verso l' applicazione Web. La soluzione che ho implementato è stata quella di aggiungere un **WAF** (Web Application Firewall) che offre una protezione specifica per le Web Application.



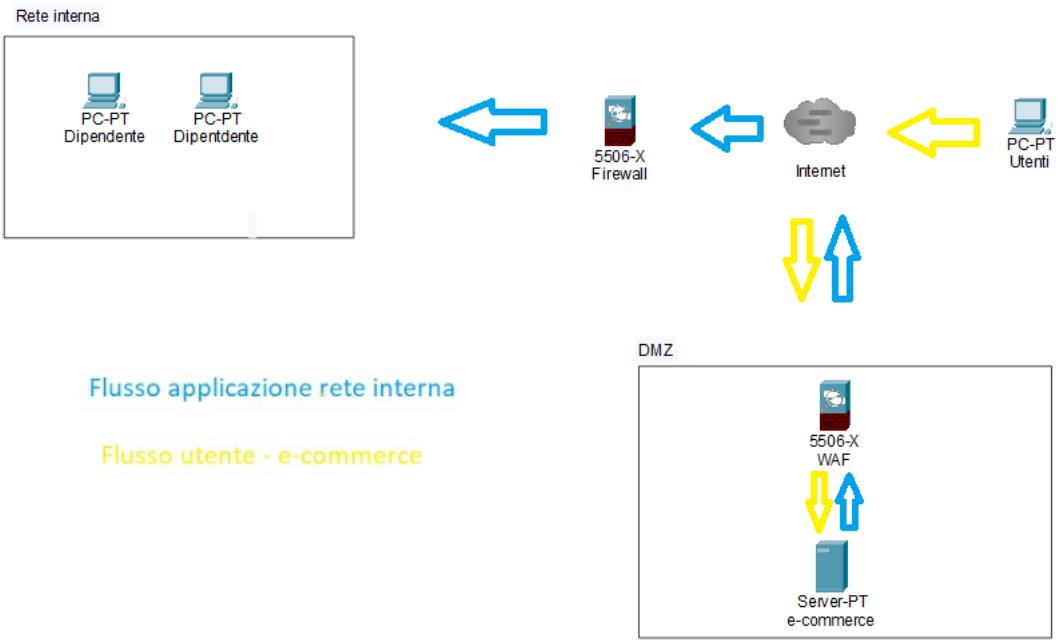
2) **Impatti sul business**: La seconda richiesta ci chiedeva di calcolare l' impatto sul business dovuto ad un attacco di tipo di **Ddos**. Questo avrebbe reso indisponibile l' e-commerce per 10 minuti, il quale generava in media 1500 euro al minuto.
Per calcolare l'impatto del attacco bisogna moltiplicare il tempo per cui il servizio è indisponibile(10 minuti), per quanto guadagno generava in media al minuto il servizio indisponibile(1500 euro al minuto):

Tempo servizio non disponibile(minuti)	Guadagno generato al minuto(euro)	Impatto sul business (euro)
10	1500	15000

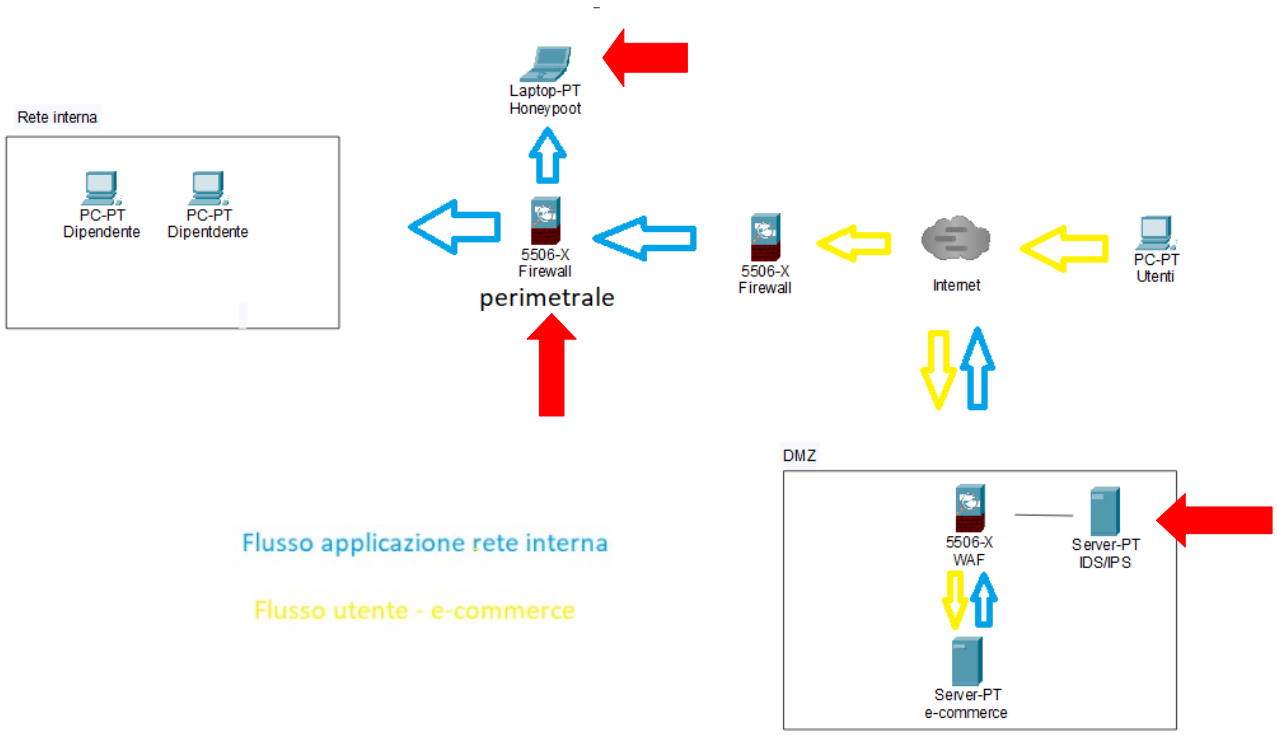
3) **Response:** La terza richiesta ci chiedeva di gestire il caso in cui la nostra web application fosse stata infetta da malware. Il nostro compito è quello di non permettere la propagazione del malware sulla nostra rete, senza essere però interessati alla rimozione del' accesso alla macchina infetta da parte del attaccante. Ho quindi proceduto ad isolare l' e-commerce facendo si che questo potesse comunicare solo verso internet, cosi facendo non abbiamo permesso la propagazione del malware verso la nostra rete, ma l' attaccante avrebbero comunque avuto l' accesso alla web application.



4) **Soluzione completa**: Ci veniva poi chiesto di unire le soluzioni della azione **preventiva** e **response:**



5) **Bonus <<modifiche aggressive>>:** Ci è stato chiesto di proporre una soluzione più aggressiva che andava a modificare se necessario anche in modo sostanziale la configurazione di rete.



Nel mio caso ho aggiunto a fianco al **WAF** un **IPS/IDS** per un ulteriore controllo del traffico nella **DMZ**. Poi si può vedere un firewall **perimetrale** per rendere ancora più protetta la rete interna, in oltre ho aggiunto un **honeypot:** un client ben protetto che pero non contiene nessuna informazione utile e funge solo come esca in caso di attacco.