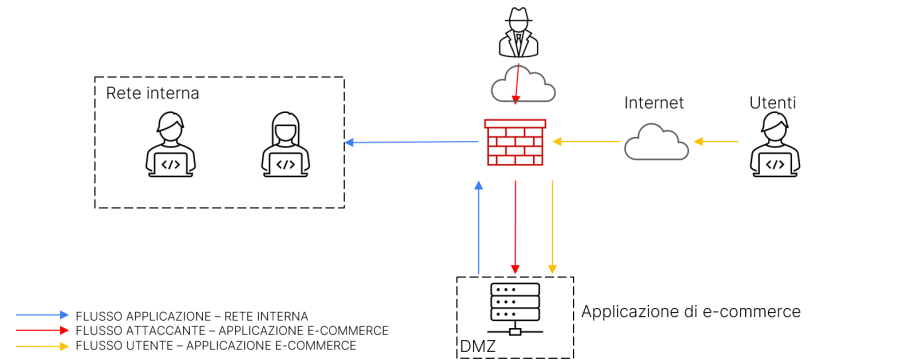
# Remiedation and Response

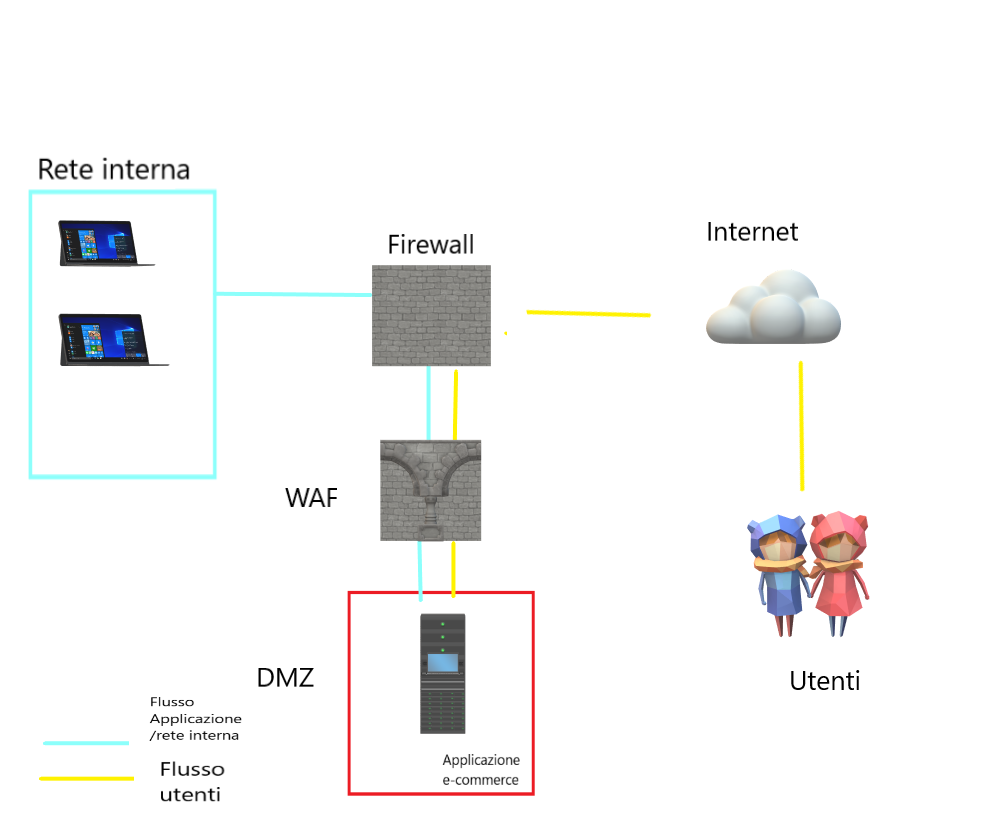
Partendo da questa base dobbiamo attuare:

* Azioni preventive contro SQLi e XSS sulla Web App.
* Attuare una risposta in caso di applicazione Web infettata da un malware.



Soluzione

Per evitare che un eventuale attaccante possa utilizzare le tecniche di SQLi e XSS, possiamo mettere prima della Web App un WAF (Web Application Firewall), un dispositivo usato per difendersi da questi tipi di attacco.

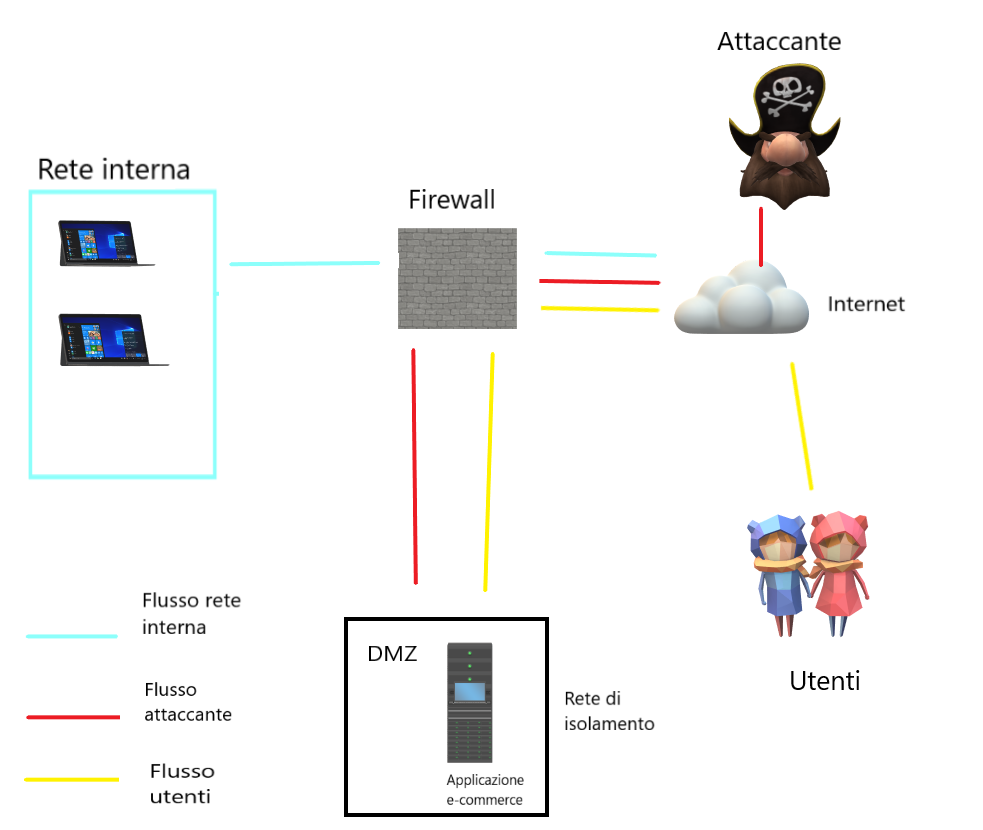


Impatto sul business

Calcolando che sulla piattaforma di e-commerce ogni minuto gli utenti spendono in media 1.500 €, se la piattaforma subisce un attacco DDOS che la rende irraggiungibile per 10 minuti, si avranno perdite per un totale di 15.000 €.

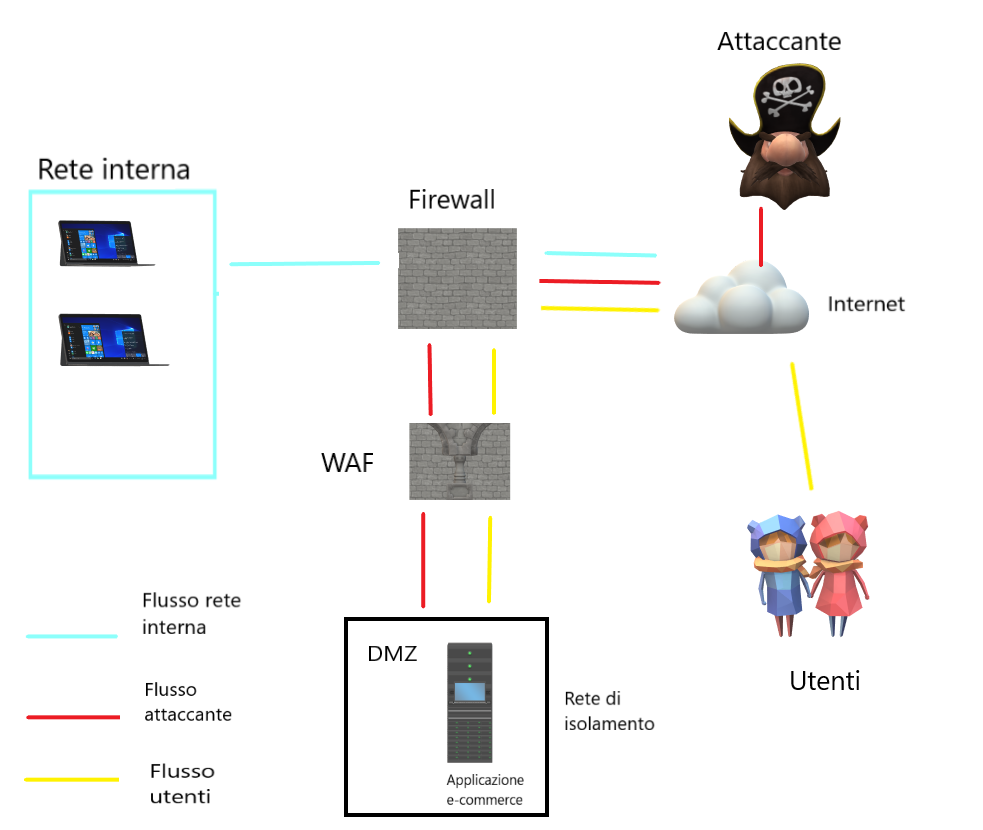
Response

Nel caso in cui l’applicazione Web sia stata compromessa da un malware, ma l’azienda non voglia rimuovere l’accesso all’applicazione Web, possiamo optare per la tecnica di isolamento. Questa tecnica consiste nel disconnettere la macchina infetta dalla rete, in modo che l’infezione non si propaghi nella nostra rete, però lasciamo ancora l’accesso dell’attaccante sul sistema tramite internet. Usiamo questa tecnica quando vogliamo studiare l’attaccante e le sue mosse, ma anche quando viene infettato un servizio critico che non possiamo eliminare.



Soluzione Finale

Possiamo unire le due soluzioni aggiungendo il WAF all’isolamento per protteggerci dalle tecniche viste.



Se si volesse avere maggiore protezione potremmo aggiungere un IPS/IDS nella DMZ per prevenire e rilevare le intrusioni.