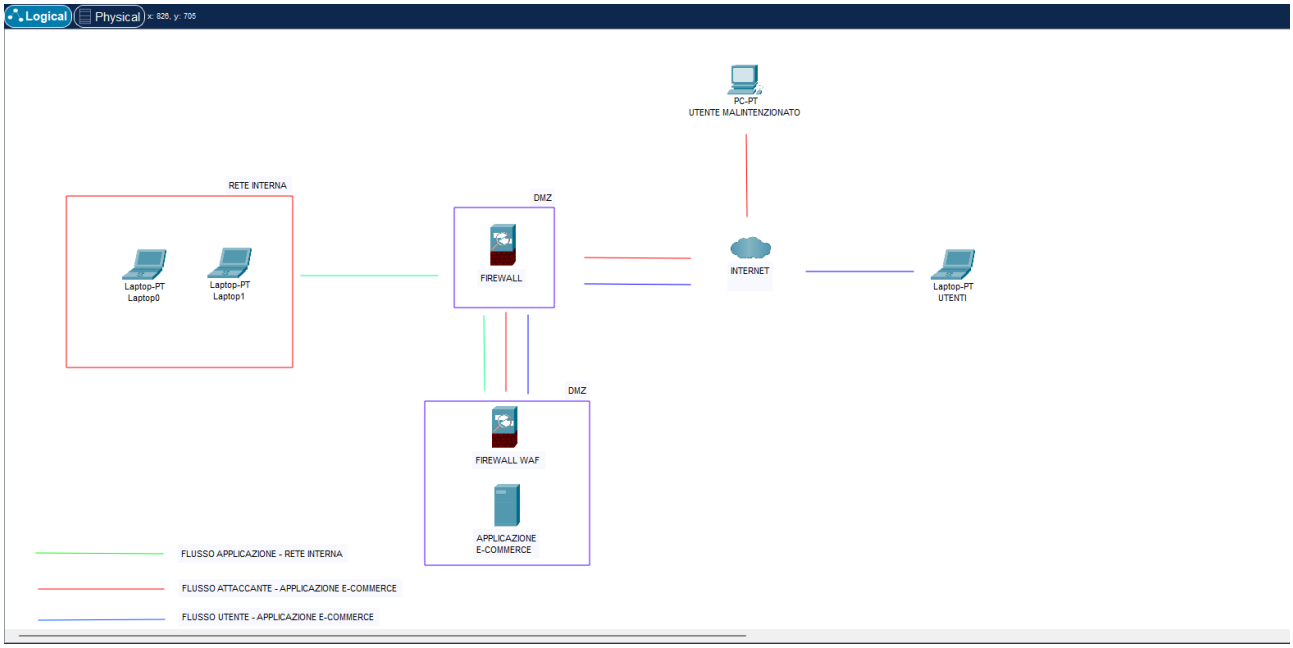
3) Impatti sul business

Per ogni minuto di inattività, gli utenti spendono in media circa 1.500 € sulla piattaforma e-commerce.

Quindi per 10 minuti di inattività, l'impatto finanziario sarebbe : 1.500 € x 10 = 15.000 €

Azioni preventive



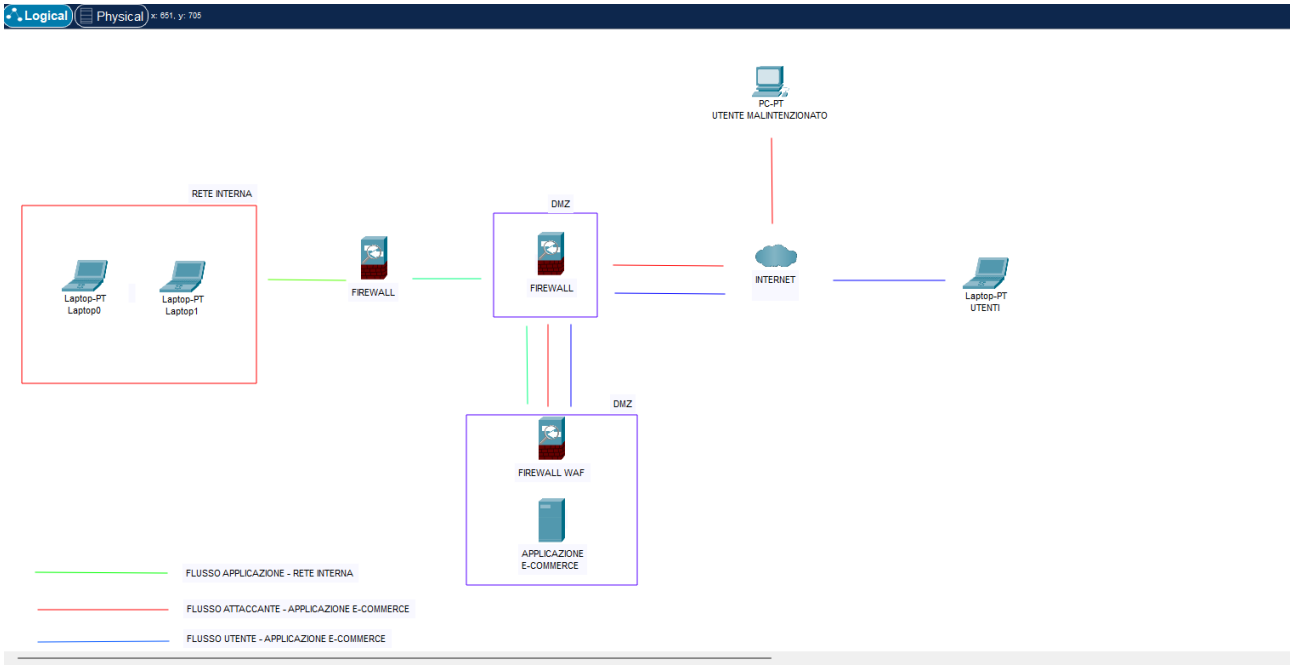
Per evitare attacchi di tipo SQLi, si possono apportare le seguenti modifiche :

Segmentazione : aggiungere una seconda DMZ, così da migliorare la sicurezza della rete interna dalle minacce esterne. Posizionare il firewall nella DMZ svolge un ruolo cruciale per garantire la sicurezza della rete e delle risorse ospitate nella DMZ stessa, permette un controllo preciso del traffico in entrata e in uscita.

Il firewall deve essere configurato solo per consentire il traffico necessario per l'applicazione web (HTTP,HTTPS) e bloccare tutto il resto. In questo caso si applica il "principio del minimo privilegio" consentendo solo ciò che è strettamente necessario.

Il firewall WAF (Web Application Firewall) nella DMZ è progettato specificamente per proteggere le applicazioni web da attacchi di tipo SQLi.

Response – Soluzione completa



In questa fase bisogna assicurarsi che la DMZ sia separata dalla rete interna da un Firewall. Limita il traffico tra la DMZ e la rete interna alle sole connessioni necessarie per il funzionamento dell'applicazione e-commerce.

Utilizza regole di Firewall rigorose per impedire qualsiasi comunicazione non autorizzata tra la DMZ e la rete interna.