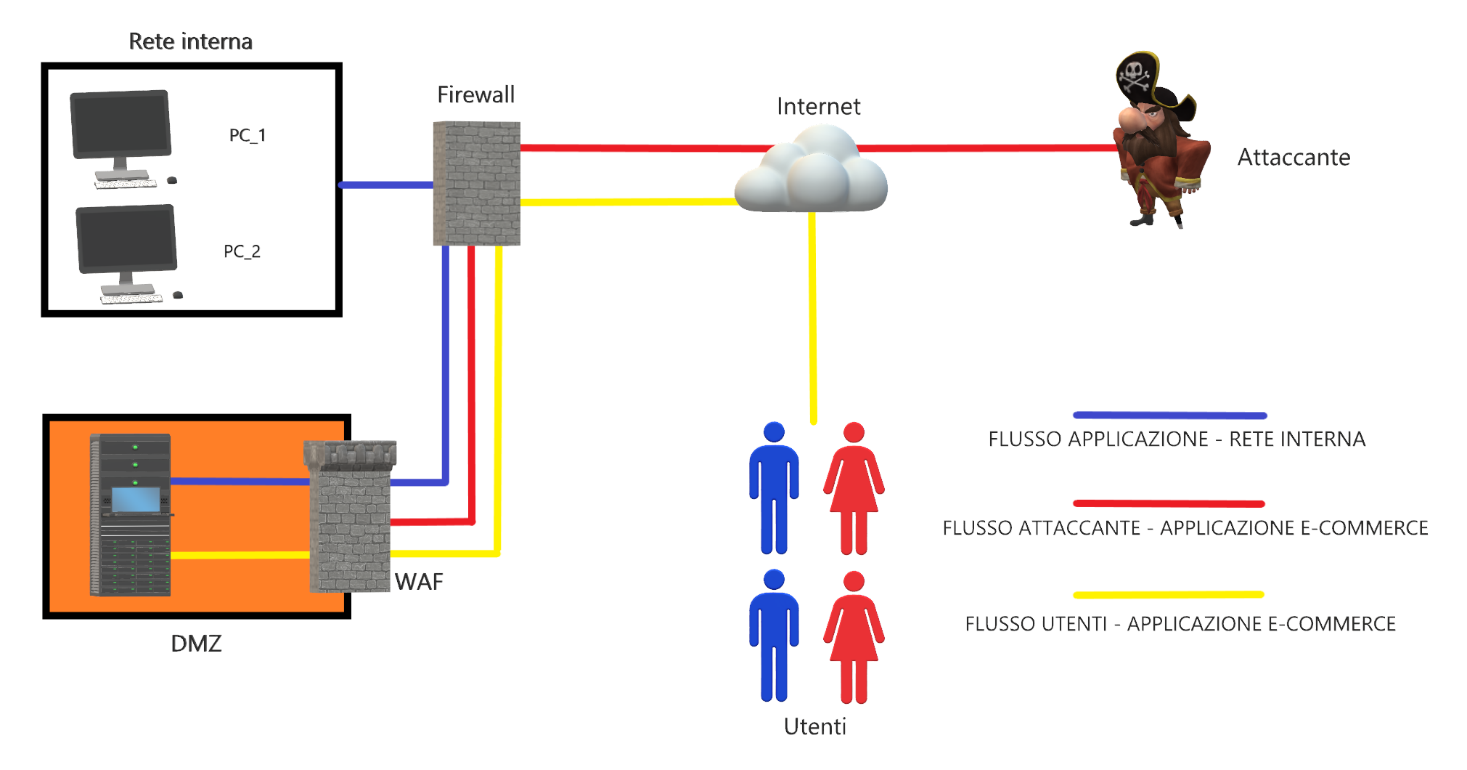
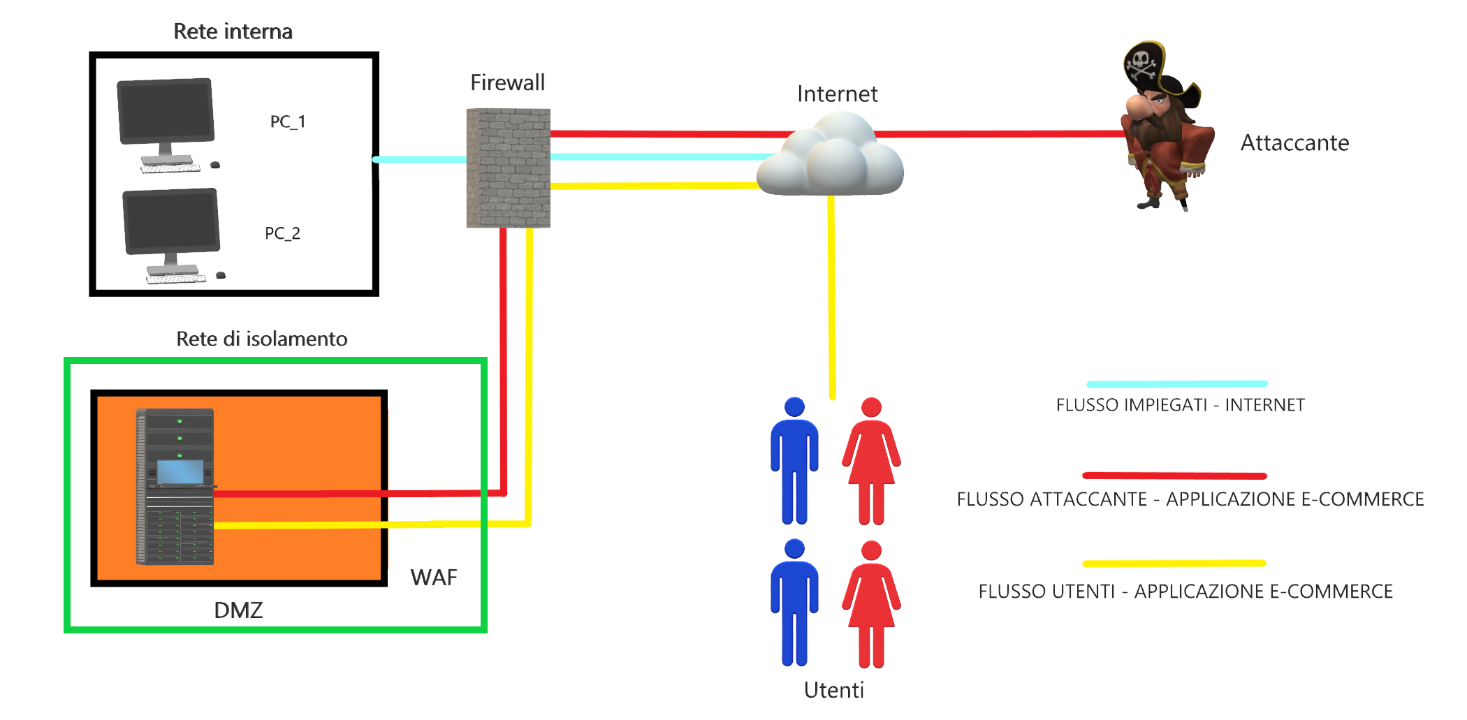
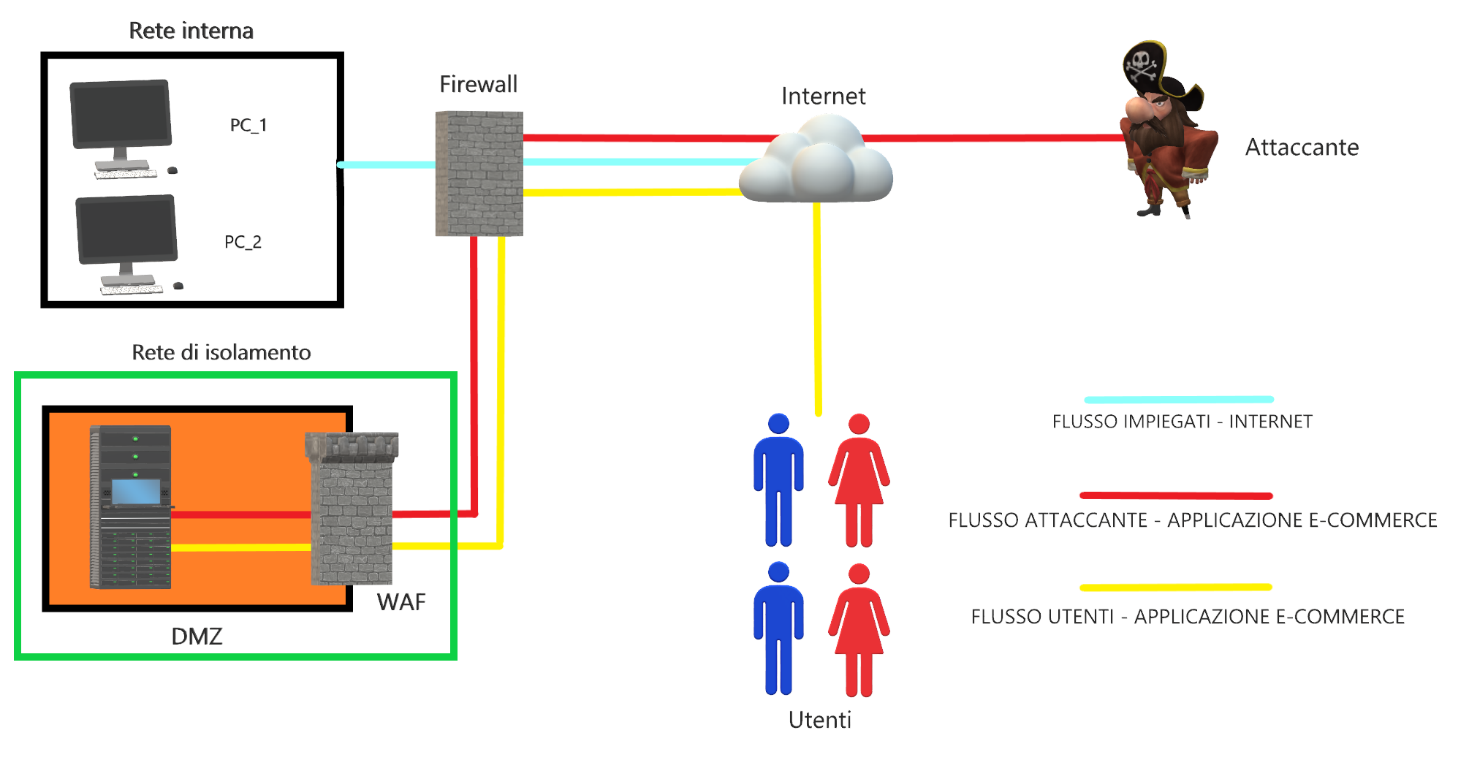
Security Operation

1. Una azione preventiva da implementare per aumentare la sicurezza dell’applicazione Web da attacchi SQLi oppure XSS è l’aggiunta di un WAF (Web Application Firewall), che è appositamente pensato per la protezione delle applicazioni Web.



1. A causa dell’attacco Ddos l’applicazione Web non è più raggiungibile per 10 minuti. Questo ha un impatto sul business poiché in media ogni minuto gli utenti spendono 1.500 euro sulla piattaforma di e-commercio e ciò comporta una perdita totale di 15.000 euro.
2. L’applicazione Web è stata infettata da un malware. Tuttavia il nostro intento, nonostante sia di evitare che si propaghi, è di non rimuovere l’accesso da parte dell’attaccante alla macchina infettata; questo perché la nostra intenzione è quella di osservare le attività e gli obiettivi dell’attaccante. Per far ciò utilizziamo la tecnica dell’isolamento, che consiste la completa disconnessione del sistema infetto dalla rete interna, con tuttavia la possibilità da parte dell’attaccante di accedere ancora con la macchina infettata su internet.





1. Una soluzione più aggressiva dell’infrastruttura tramite l’utilizzo dell’IPS/IDS e Honeypot.