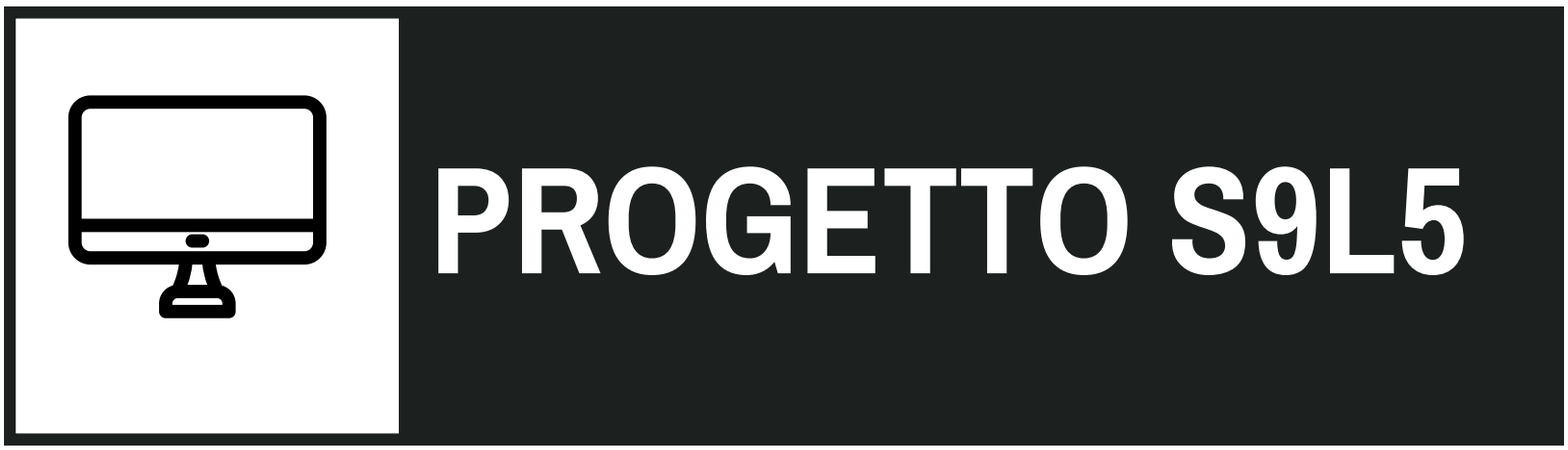
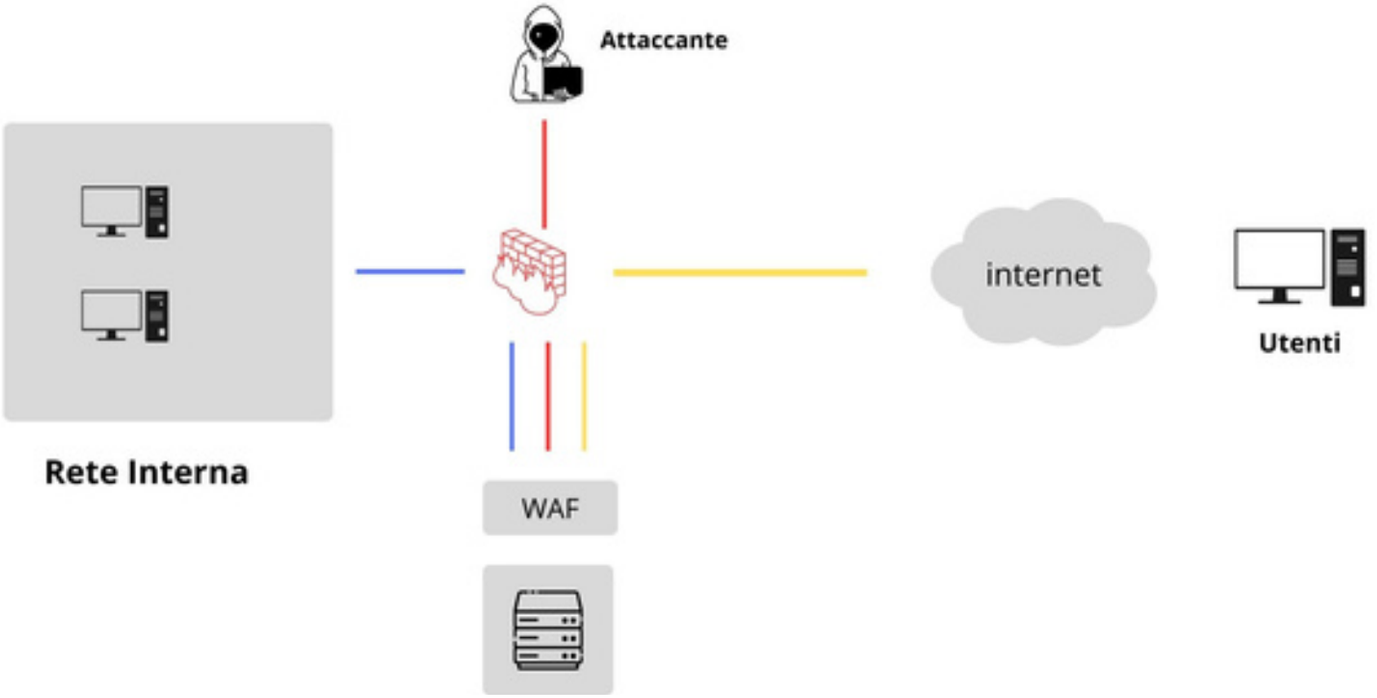

PROGETTO S9L5

Tasks:

Azione preventive:

Il progetto ci chiede d'implementare delle azioni preventive per difendere l'applicazione web da attacchi XSS e SQL Injection da parte di un utente malintenzionato.
Abbiamo modificato il progetto implementando un WAF a difesa del server e-commerce filtrando tutto il traffico che viene scambiato tra l'ambiente interno e quello esterno.



impatti sul business:

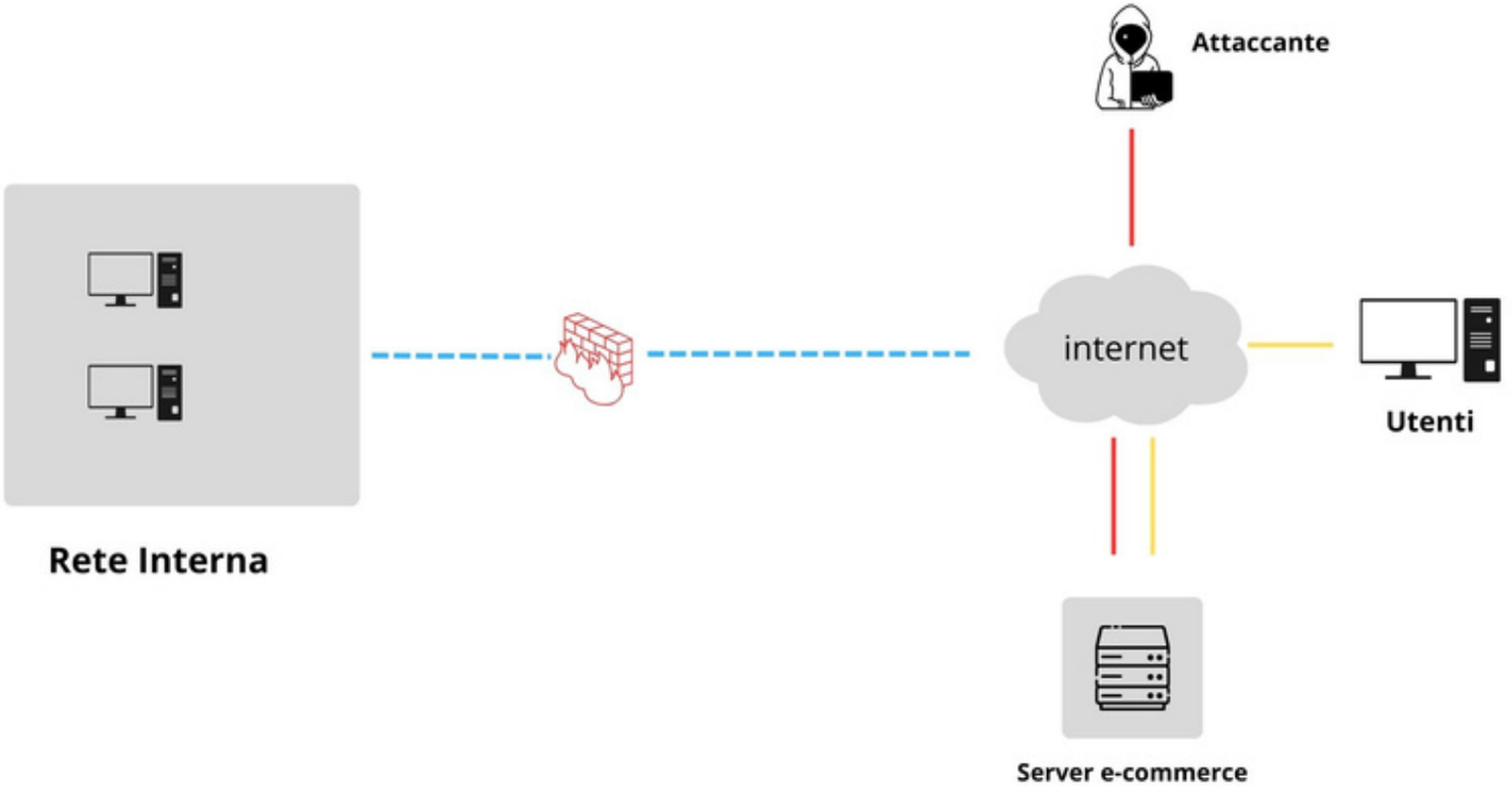
Il progetto ci chiede di calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio tenendo conto che ogni minuto gli utenti spendono 1500 euro e l'applicazione per causa di un attacco DDOS non è raggiungibile per 10 minuti.

Il danno sarà calcolato così:

1500 (euro) x 10 (Minuti) =
15.000 euro di danno

Response:

Infine l’app Web viene infettata da un Malware, il progetto ci chiede di modificare lo schema in modo che il malware non infetti il resto della rete mentre non siamo interessati a rimuovere l’accesso da parte dell’attaccante sulla macchina infetta



La soluzione apportata è quella di isolare la web app dalla rete interna in modo che l’accesso sara possibile all’attaccante e agli utenti. E’ una soluzione in cui gli utenti sono esposti momentaneamente al malware dell’attaccante, ma secondo l’azienda è un rischio accettabile che esporre la rete esterna a possibili malware.