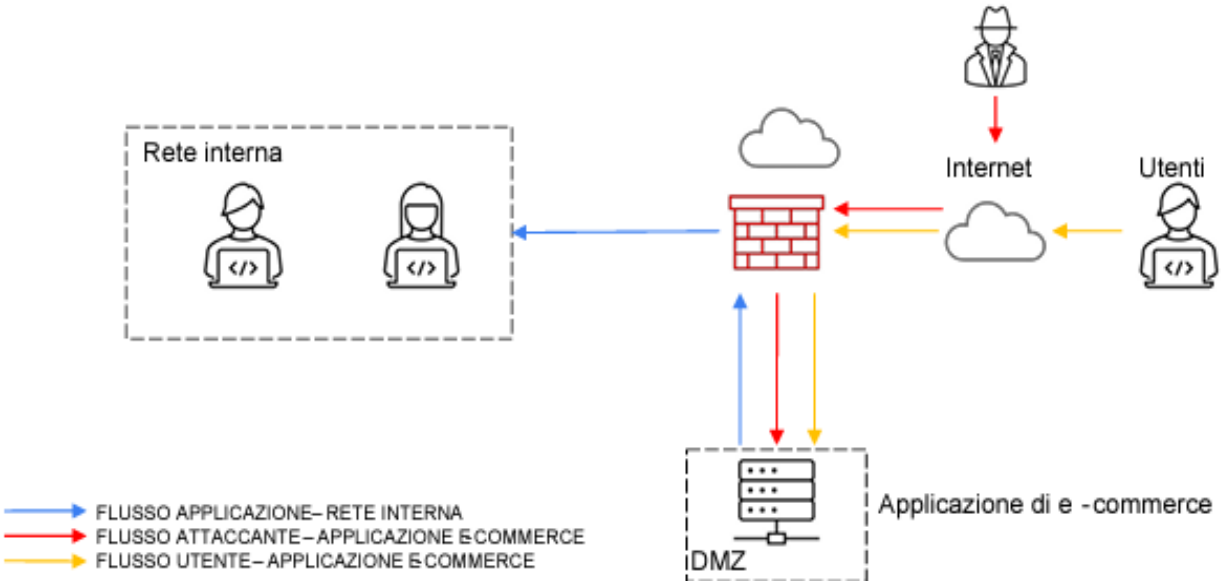
Progetto S9L5

Architettura di rete

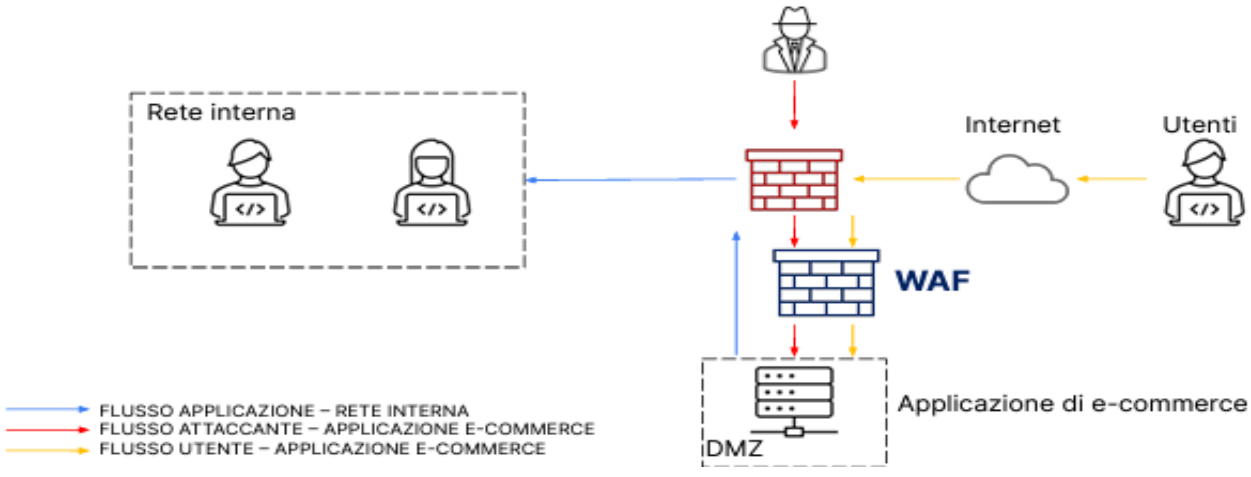


L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

Risposte ai quesiti

1. Per la protezione della Web App da minacce quali XSS e SQLi si può preventivamente adottare una soluzione basata su Web Application Firewall, che a differenza dei firewall standard, sono dedicati per proteggere le Web App da attacchi XSS e SQLi.



2. L’attacco di tipo Ddos causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10).
   Impatto sul business = 1.500 € x 10 minuti = 15.000 €

   Per quanto riguarda le azioni preventive, per evitare attacchi di questo tipo bisognerebbe avere sistemi di monitoraggio in tempo reale per rilevare anomalie nel traffico e rispondere prontamente agli attacchi DDoS in corso. Includendo l'automatizzazione delle risposte tramite script o l'intervento manuale del personale IT ad esempio utilizzando regole firewall che limitano ripetuti accessi di un ip o che regolano il numero di accessi consentiti alla volta.

3. Considerata la priorità, si può adottare una strategia basata sull’isolamento della macchina infettata. In questo caso la macchina sarà direttamente collegata ad internet, raggiungibile dall’attaccante ma non più connessa alla rete interna.