Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. **Impatti sul business:** l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

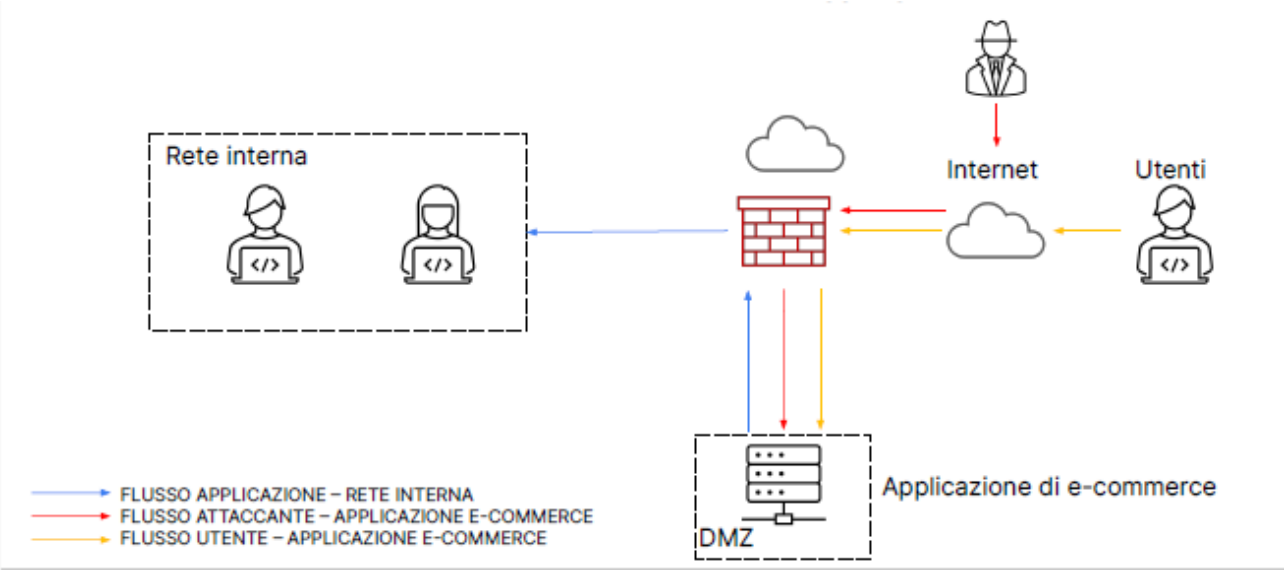
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5**. Modifica «più aggressiva»** dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

Architettura di rete iniziale:

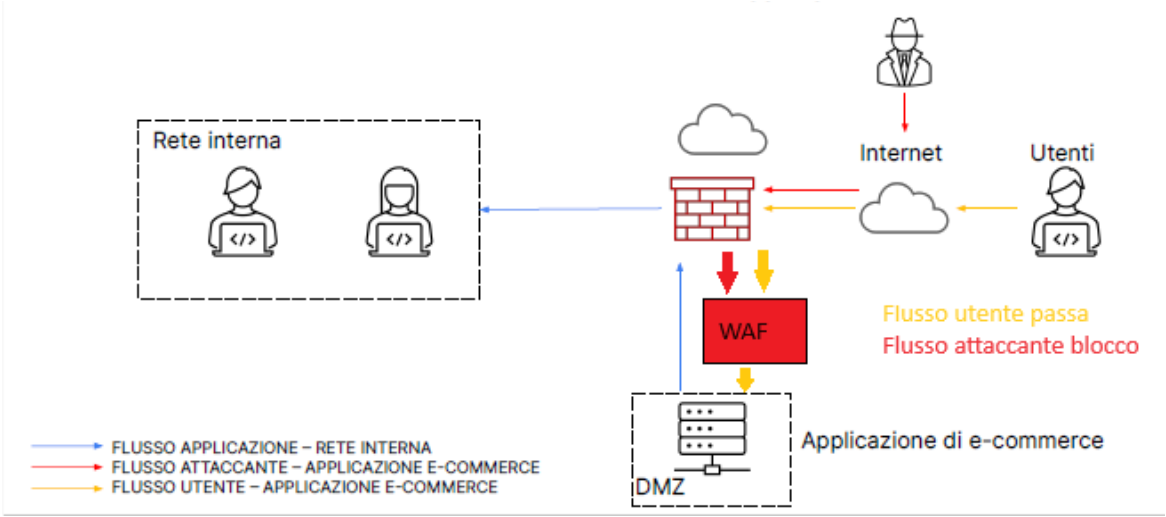
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

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.



Punto 1 Azioni Preventive: Per proteggere le Web App e difenderci dagli attacchi SQLi e XSS possiamo implementare un firewall a livello di applicazione WEB, quindi un WAF (Web Application Firewall). Un WAF funziona come una barriera tra l'applicazione Web e gli utenti Internet, analizzando il traffico in entrata e in uscita per individuare e bloccare eventuali attacchi.

Nuova architettura di Rete con WAF.

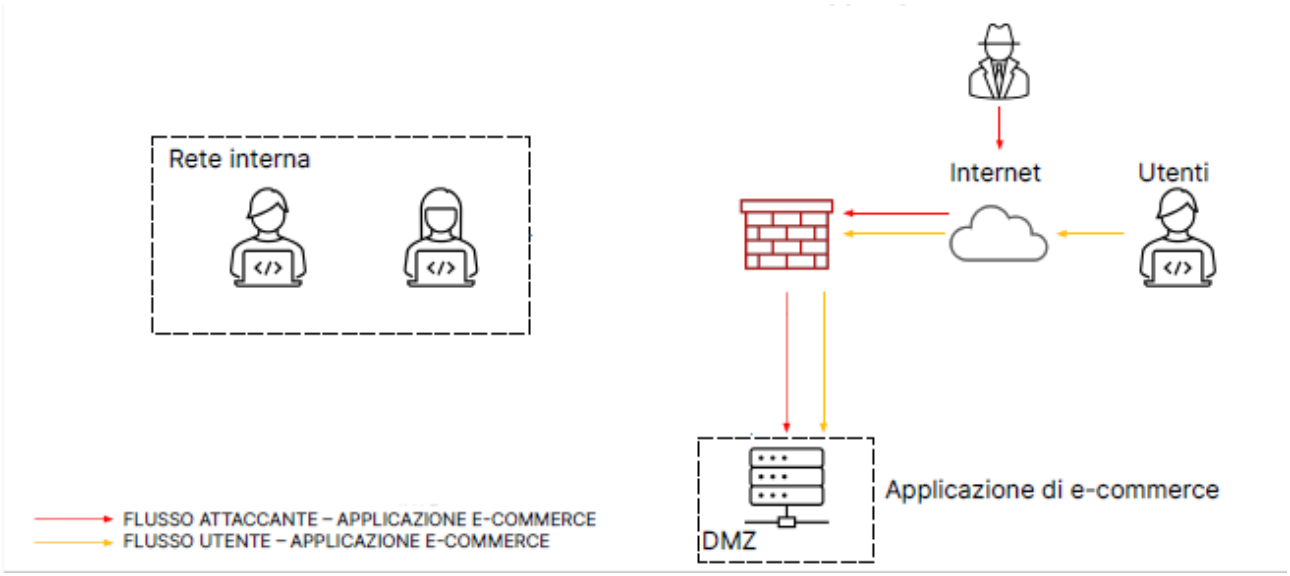


Punto 2 Impatti sul business: Il DDoS ha provocato l'inaccessibilità della piattaforma di e-commerce per 10 minuti. Se consideriamo che gli utenti spendono in media circa 1.500€ al minuto, possiamo calcolare i danni stimati moltiplicando la spesa potenziale degli utenti per il numero di minuti di interruzione del servizio

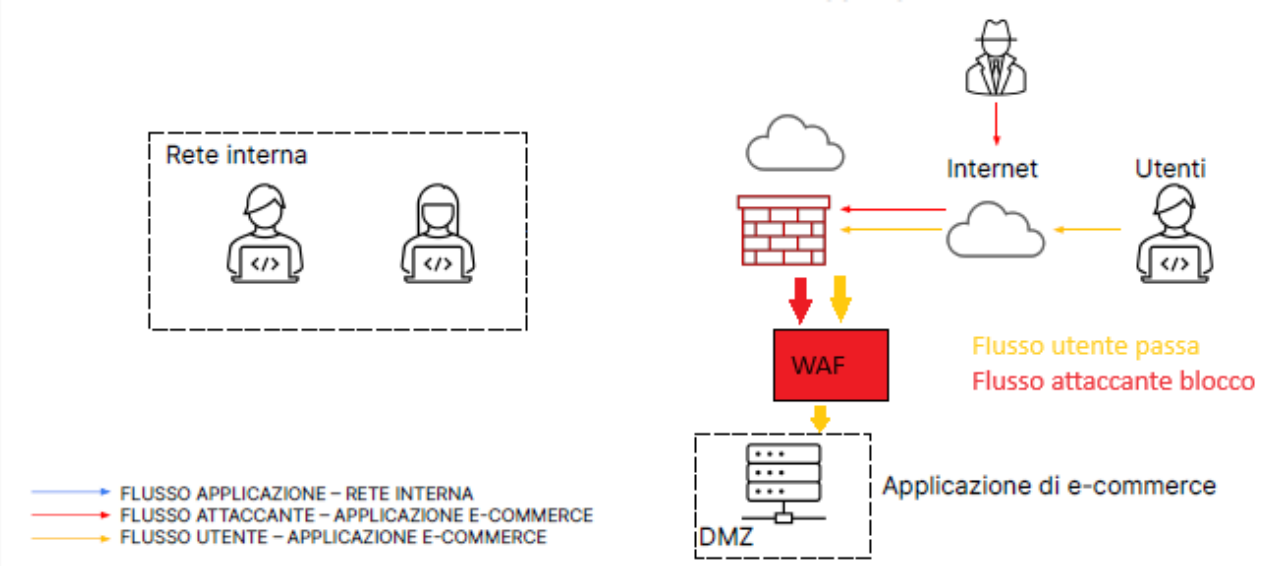
Impatto sul business = 1.500 € x 10 minuti = **15.000 €**

Per 10 minuti di indisponibilità la compagnia potrebbe perdere 15.000 € di acquisti potenziali.

Punto 3 Response: In questo caso, con la Web App infettata, si può procedere al suo isolamento dalla rete interna, impedendo all'attaccante di raggiungerla. La macchina ha comunque un firewall a protezione che però in questo caso è stato bypassato. Quindi la macchina è stata infettata ma non è più connessa alla rete interna. Web App e rete interna sono separati.



Punto 4 Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3). Rete con Firewall + WAF e DMZ isolata. Web App e rete interna sono separati.



Punto 5 Modifica «più aggressiva»: In questo caso oltre al WAF è stato anche creato un finto DMZ isolato dalla rete interna che non permette la comunicazione, mentre la vera macchina è protetta dal WAF e blocca il traffico dell'attaccante