

REPORT S9/L5



Presented by:

Morgan Petrelli

TRACCIA.

Con riferimento alla figura, 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

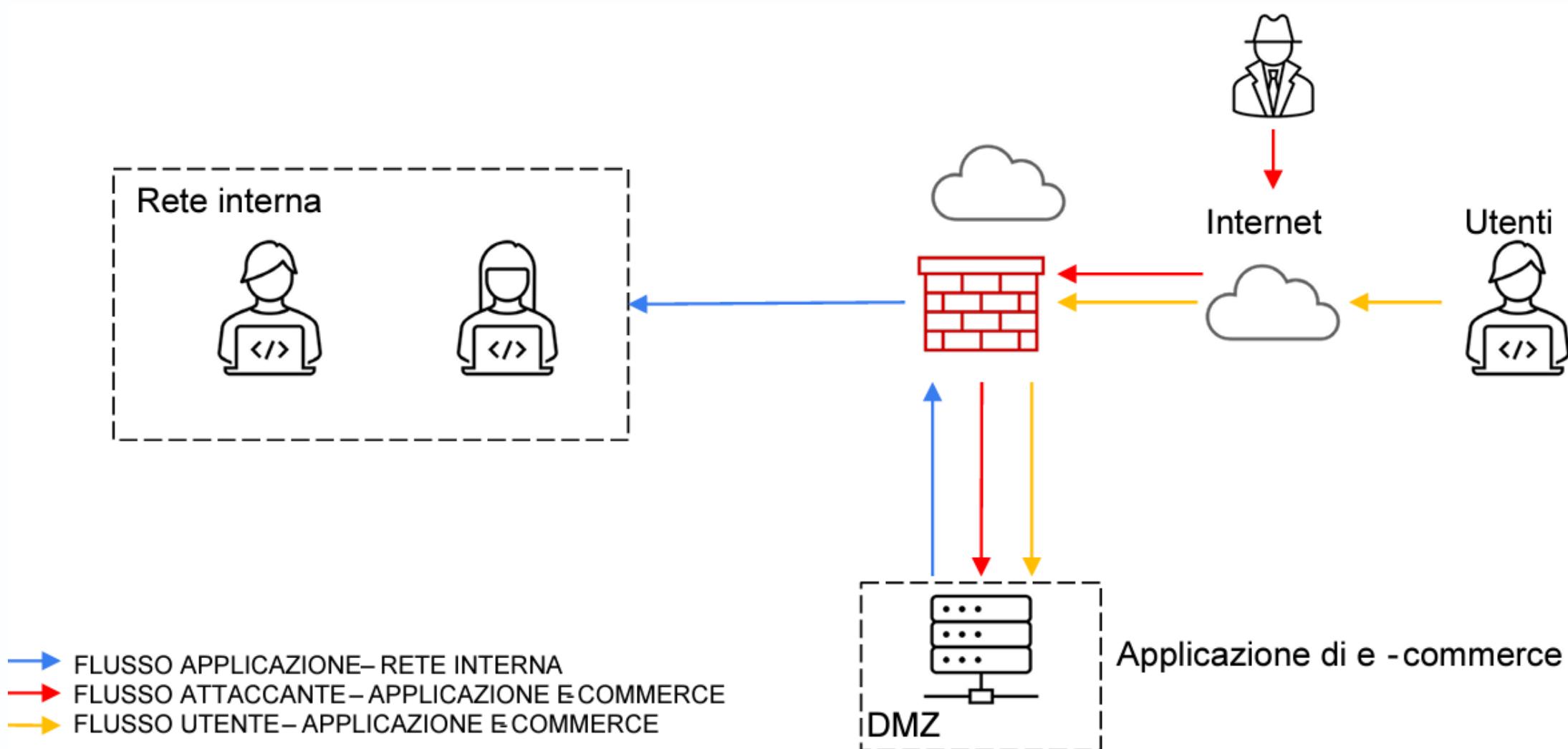
2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti .

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 vostre 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 .

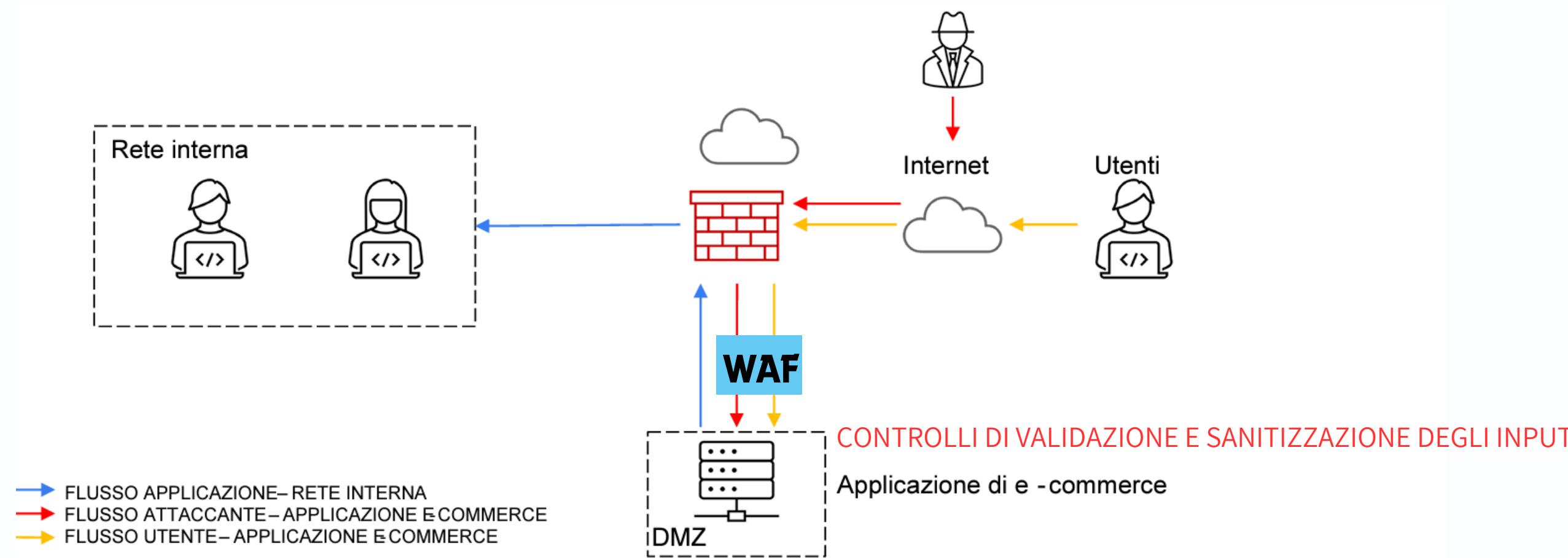
4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza necessario/facoltativo magari integrando la soluzione al punto 2)



AZIONI PREVENTIVE

Per difendere l'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), è possibile implementare una serie di azioni preventive come un Web Application Firewall (WAF) che può essere posizionato tra Internet e l'applicazione di e-commerce per filtrare e monitorare il traffico HTTP, bloccando tentativi di SQLi e XSS e implementare rigorosi controlli di validazione e sanitizzazione degli input all'interno dell'applicazione di e-commerce per prevenire l'inserimento di codice malevolo.



IMPATTI SUL BUSINESS:

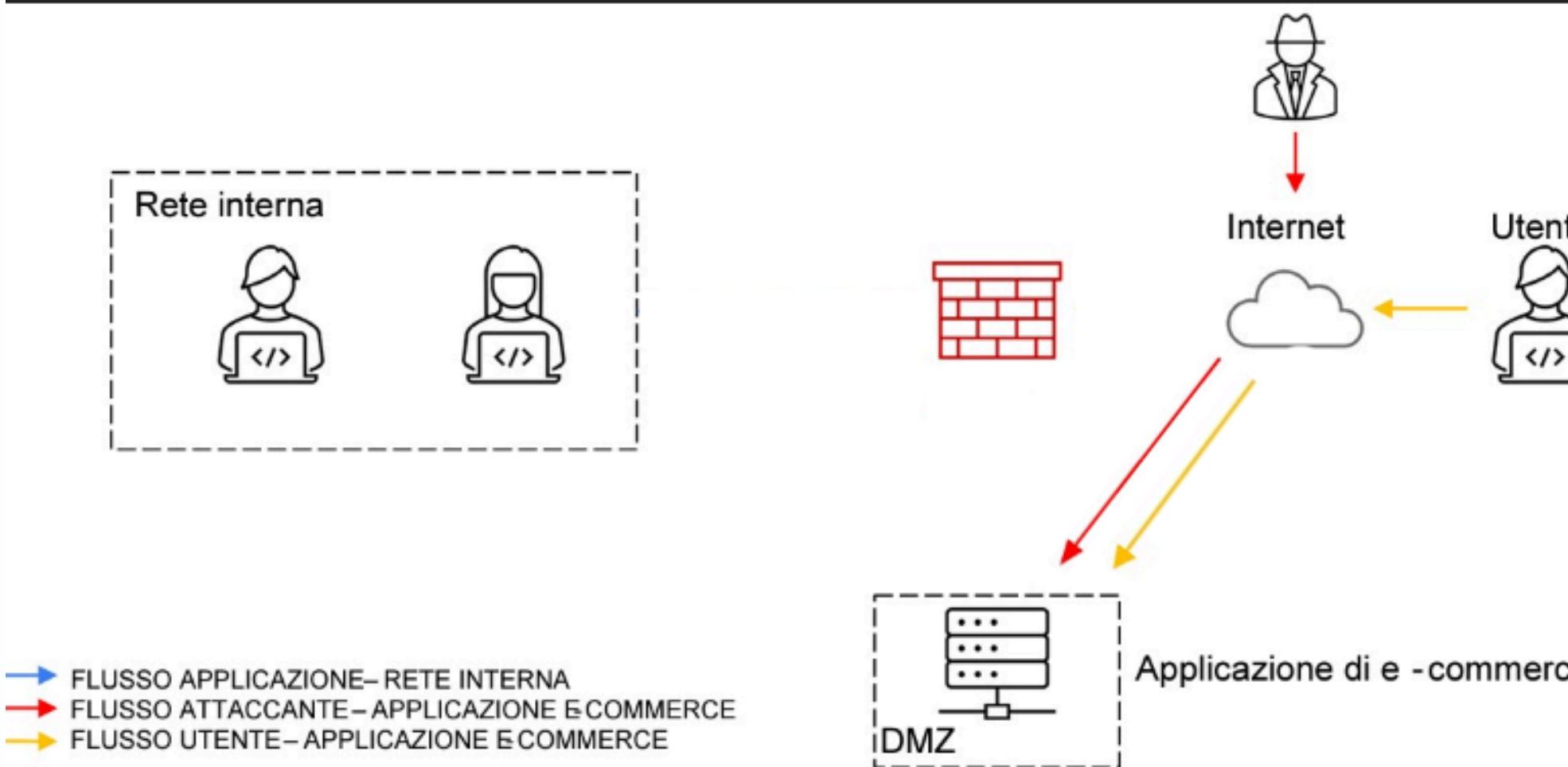
l'applicazione web subisce un attacco DDoS che la rende irraggiungibile per 10 min gli utenti in media spendono circa 1500€ al minuto. quindi per calcolare l'impatto sul business bisogna moltiplicare la spesa degli utenti al minuto per i minuti che l'applicazione web è irraggiungibile:

$$\text{IMPATTO SUL BUSINESS} = 1.500\text{€} \times 10 \text{ min} = 15.000\text{€}$$

per prevenire questo tipo di problematiche si possono implementare servizi di mitigazione DDoS, come quelli offerti da Cloudflare, che sono progettati per rilevare e bloccare il traffico malevolo diretto verso la piattaforma di e-commerce, configurare server ridondanti e utilizzare bilanciatori di carico aiuta a distribuire il traffico su più server, migliorando la resilienza dell'applicazione.

RESPONSE

per evitare che il malware si propaghi sulla rete, è essenziale implementare delle misure di contenimento che isolino la macchina infetta senza rimuovere l'accesso dell'attaccante. quindi bisogna isolare la macchina infetta all'interno della DMZ senza rimuovere il suo accesso a Internet, mantenendo comunque una barriera di protezione tra la macchina infetta e la rete interna per evitare la propagazione del malware creando una Vlan dedicata per la dmz.



SOLUZIONE COMPLETA

