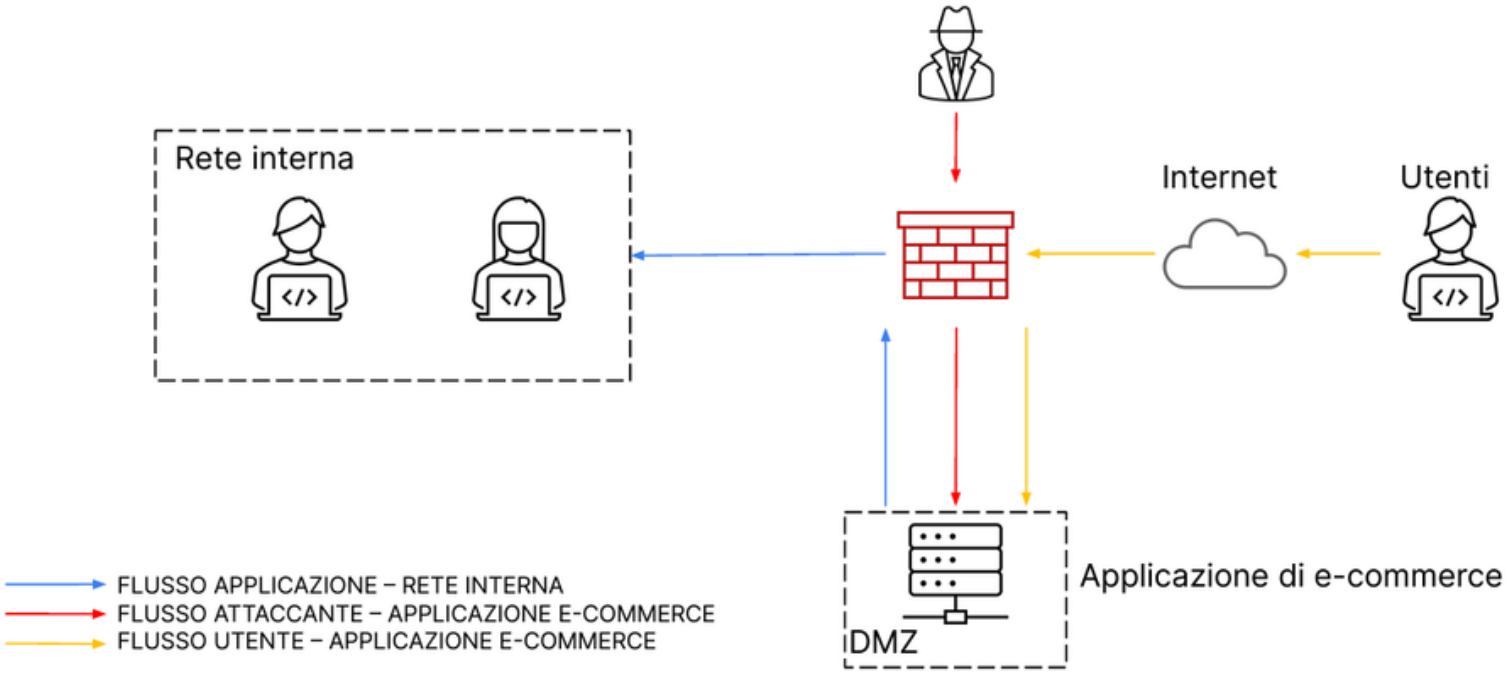
S9/L5

INCIDENT RESPONSE

Colombo Federico



A seguito della figura riportata la traccia di oggi ci chiede di eseguire:

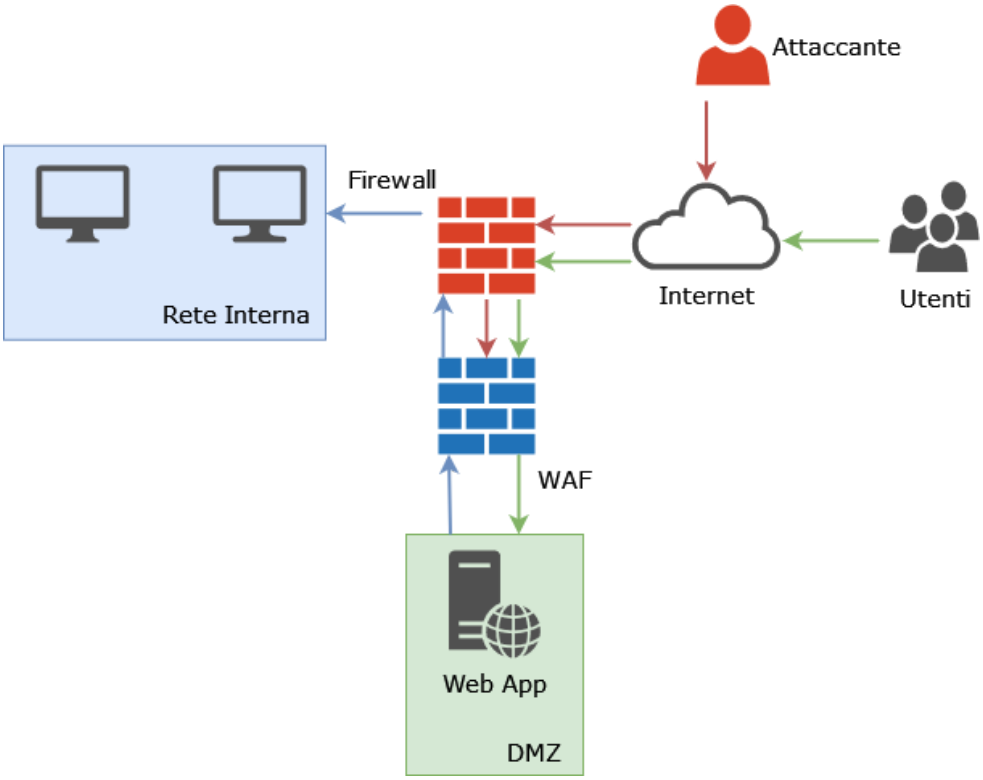
- **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

- **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.

- **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 con la soluzione proposta.

Azioni preventive

Questa in figura è la soluzione proposta per prevenire gli attacchi di tipo SQLi e XSS.



Abbiamo implementato un WAF (Web application firewall) in modo che possa analizzare il traffico in entrata per rilevare attività dannose, e in caso di rilevamento di una minaccia possa bloccare la richiesta che non viene inoltrata al server Web.
I WAF possono essere configurati per rilevare una vasta gamma di minacce tra cui SQLi, XSS, brute force e DDoS.

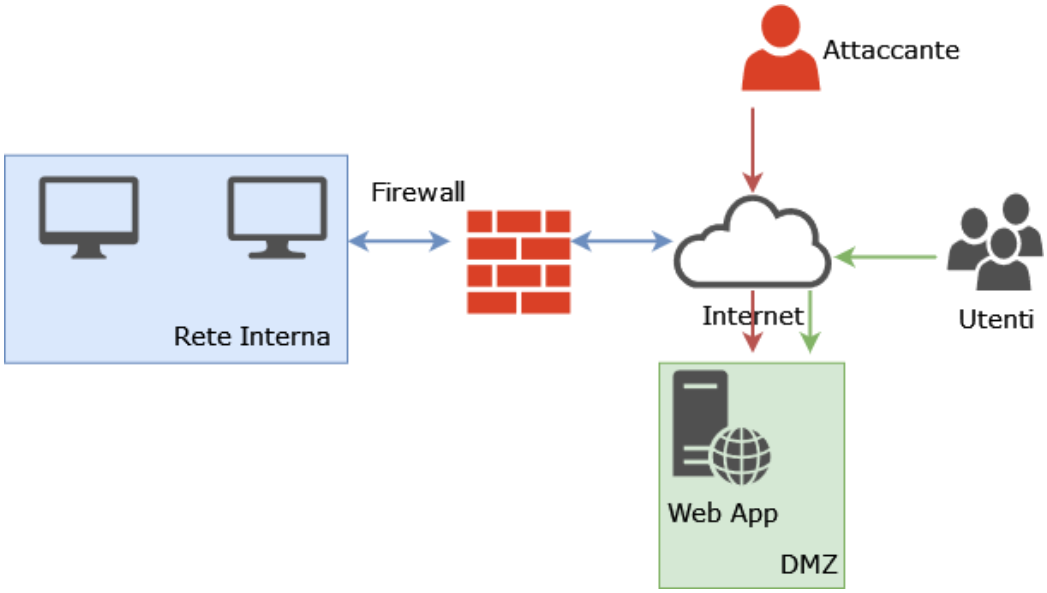
Impatti sul business

Sapendo che l'azienda ha un guadagno di media di 1.500 € al minuto e non fosse raggiungibile per 10 minuti avrebbe una perdita media di 15.000 €

Per prevenire un attacco di tipo DDoS sarebbe opportuno installare un WAF

Response

Nel caso in cui il web server venisse infettato, per fare in modo che la rete interna non venga infettata, procederemo come in figura:



In questo caso siamo andati ad isolare la nostra rete interna dalla DMZ lasciando comunque che l'attaccante abbia accesso alla Web App.
Così facendo andremo a ridurre gli impatti causati dall'incidente e potremo analizzare al meglio la minaccia per poter attuare eventuali azioni di recupero del sistema.