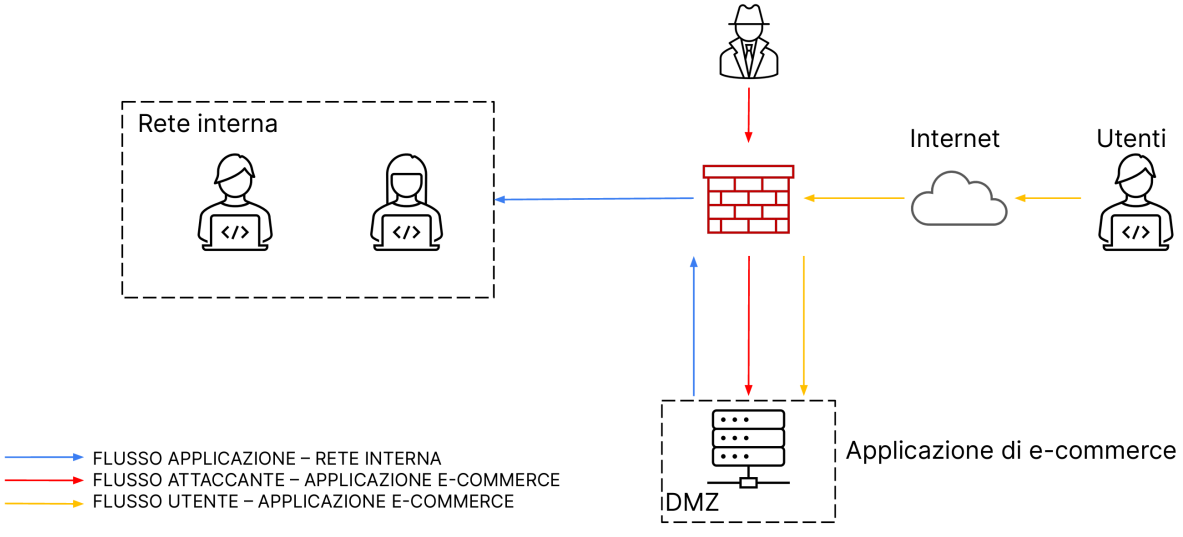
SECURITY OPERATION CENTER



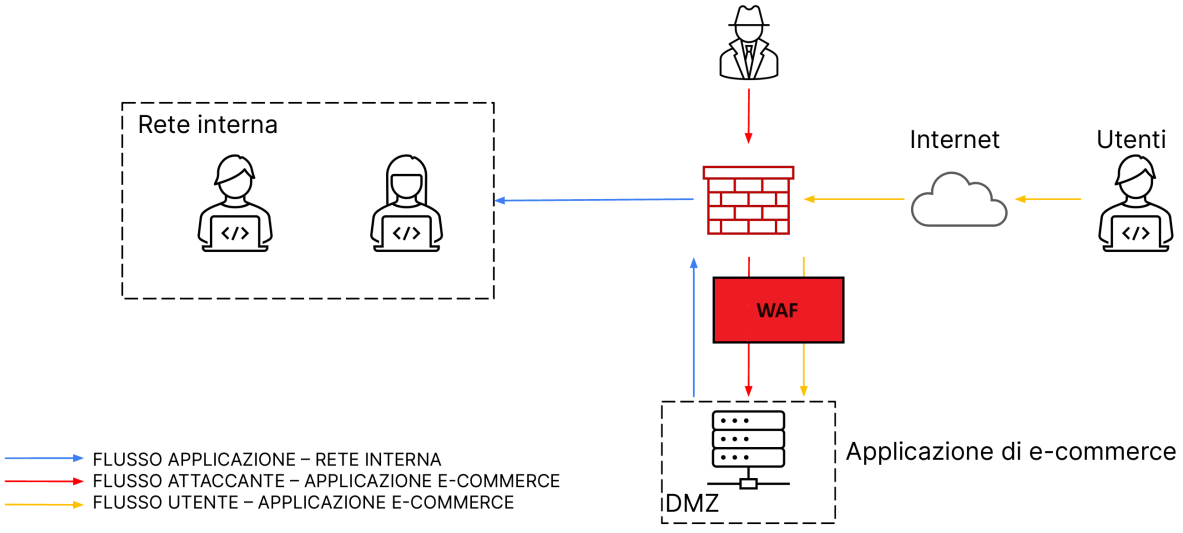
La traccia dell'esercizio chiede, relativamente alla situazione grafica in alto, di:

- **1**) Spiegare quali azioni preventive si potrebbero implementare per difendere l'applicazione Web nella DMZ da attacchi di tipo SQLi oppure XSS;
- **2**) 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, nel caso in cui l'applicazione Web subisce un attacco di tipo Ddos che rende l'applicazione non raggiungibile per 10 minuti;
- **3**) Modificare la figura per mostrare la soluzione ad un'infezione dell'applicazione web da parte di un malware, con la priorità che il malware non si propaghi sulla nostra rete, senza pensare a rimuovere l'accesso da parte dell'attaccante alla macchina infetta.

L'**architettura di rete** è impostata in modo da rendere l'**applicazione** di **e-commerce disponibile** per gli utenti **tramite internet** per effettuare acquisti, e la **rete interna raggiungibile dalla DMZ** per via delle policy sul firewall.

SOLUZIONE

1)



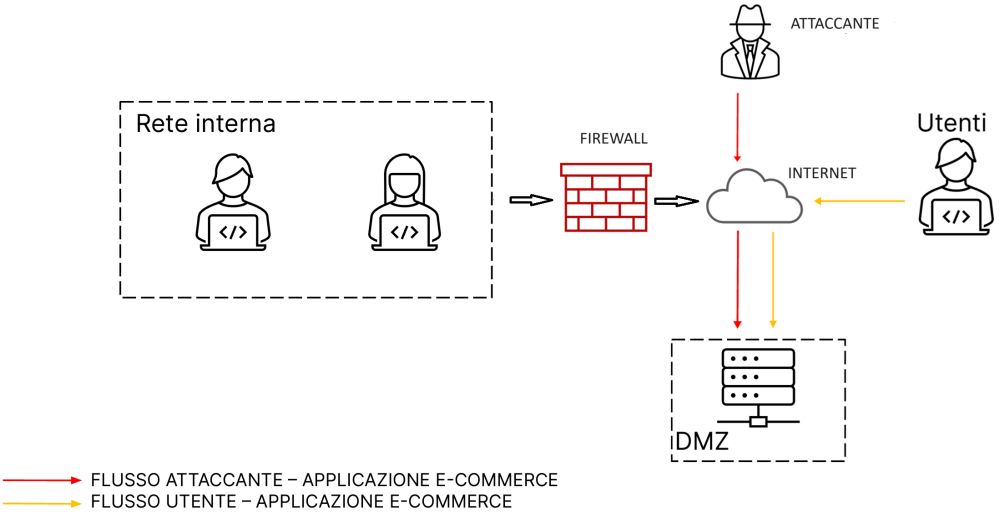
Per proteggere l'applicazione Web nella DMZ da attacchi di tipo SQLi oppure XSS, basandoci sullo schema grafico che mostra le connessioni dell'attaccante e degli utenti con le linee rosse e gialle, la soluzione migliore è quella di installare un Web Application Firewall, in modo da avere un filtraggio più approfondito di tutti i pacchetti in arrivo dall'esterno, aumentando di molto la sicurezza in quanto questa tipologia di firewall è programmata specificatamente per proteggere le applicazioni web dagli attacchi specifici.

2)

Nel caso in cui dovesse verificarsi un attacco di tipo Ddos, ovvero un invio massivo di pacchetti da moltissimi host verso il nostro server per fare in modo di saturare l'hardware e mandare il tilt il dispositivo, rendendo di fatto non raggiungibile il negozio virtuale ai clienti per 10 minuti, considerando che in media ogni minuto gli utenti spendono € 1.500, si avrebbe una perdita totale di € 15.000.

3)

Considerando che la rete interna è raggiungibile dalla DMZ (infetta) tramite firewall, considerando che la priorità è che il malware non si propaghi sulla nostra rete interna, considerando che non dobbiamo rimuovere l'accesso dell'attaccante alla macchina infetta e considerando che l'e-commerce deve rimanere collegato ed attivo in internet (nonostante ciò possa provocare danni agli utenti connessi ad esso) la soluzione migliore è quella di isolare l'applicazione web dalla nostra rete interna, come da figura seguente.


ATTACCANTE
Rete interna
FIREWALL
INTERNET
Utenti
DMZ
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE