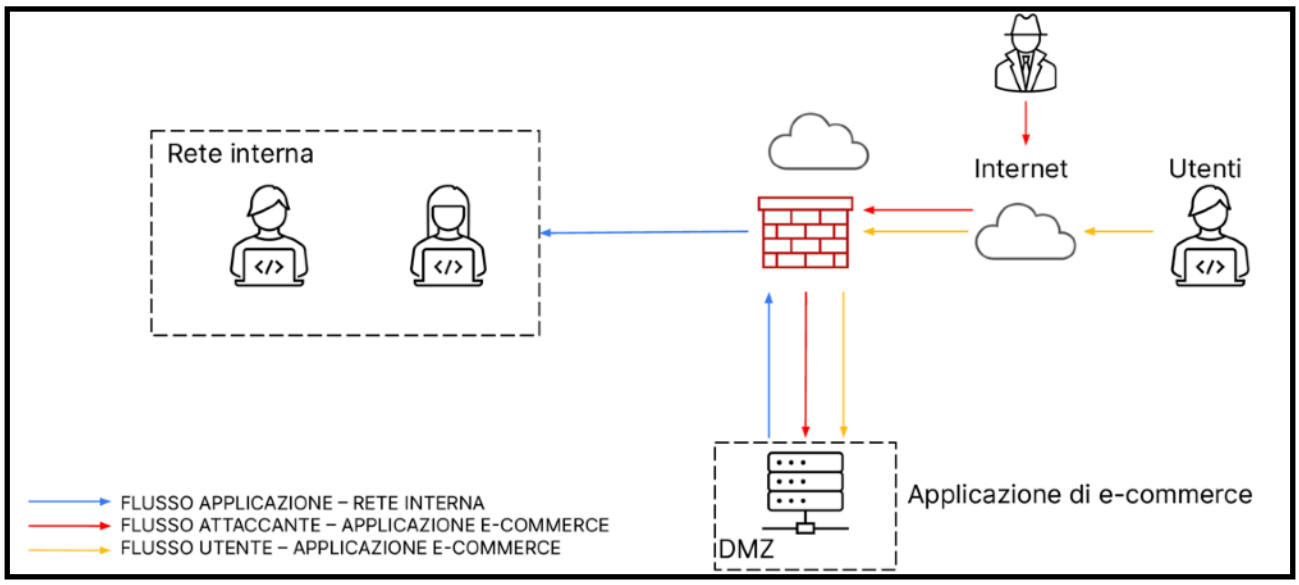
PROGETTO FINALE M5_W20D4

L'immagine sottostante mostra un'architettura di rete.
Successivamente verranno posti dei quesiti, si procederà per step nella risoluzione.



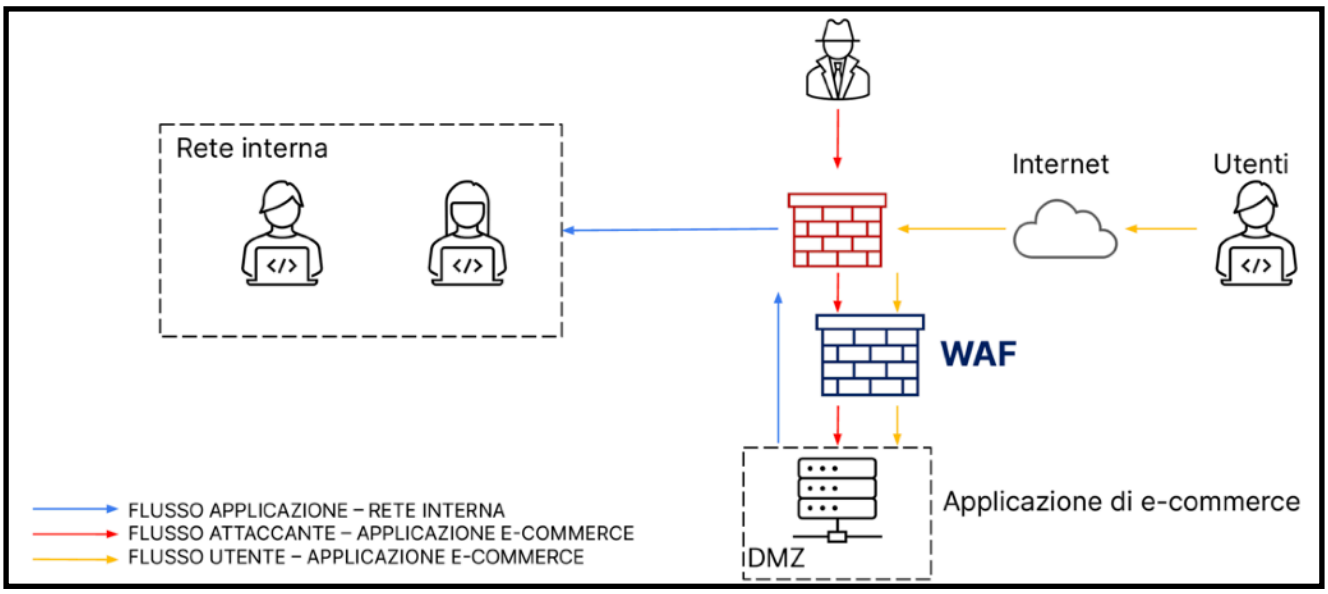
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

1. Quesito

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

Svolgimento:

Per limitare il rischio di attacchi XSS e SQLi possiamo mettere in atto delle azioni preventive:
Si utilizzerà un WAF (Web Application Firewall) per proteggere le Web App da attacchi XSS e SQLi.



2. Quesito
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.

Svolgimento:

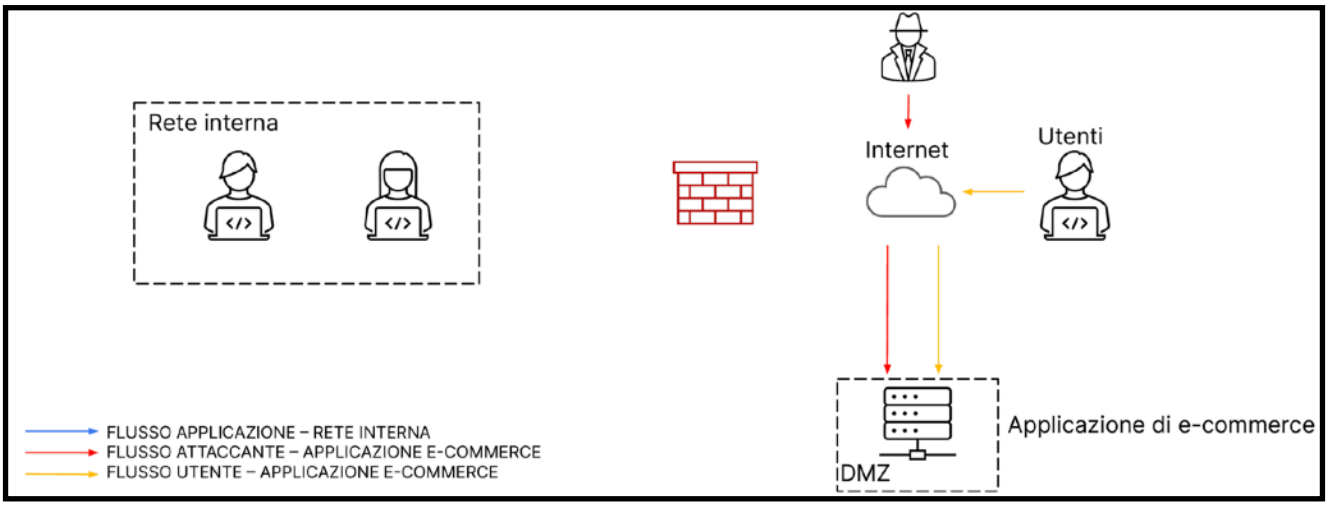
L'attacco di tipo DDoS causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti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

Di conseguenza:
Impatto sul business = 1.500 € x 10 minuti = 15.000 €
Per 10 minuti di indisponibilità la compagnia ha perso 15.000 € di potenziali acquisti.

3. Quesito
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 iniziale con la soluzione proposta.

Svolgimento:

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. La figura sottostante mostra la soluzione con la strategia dell'isolamento della macchina infetta.

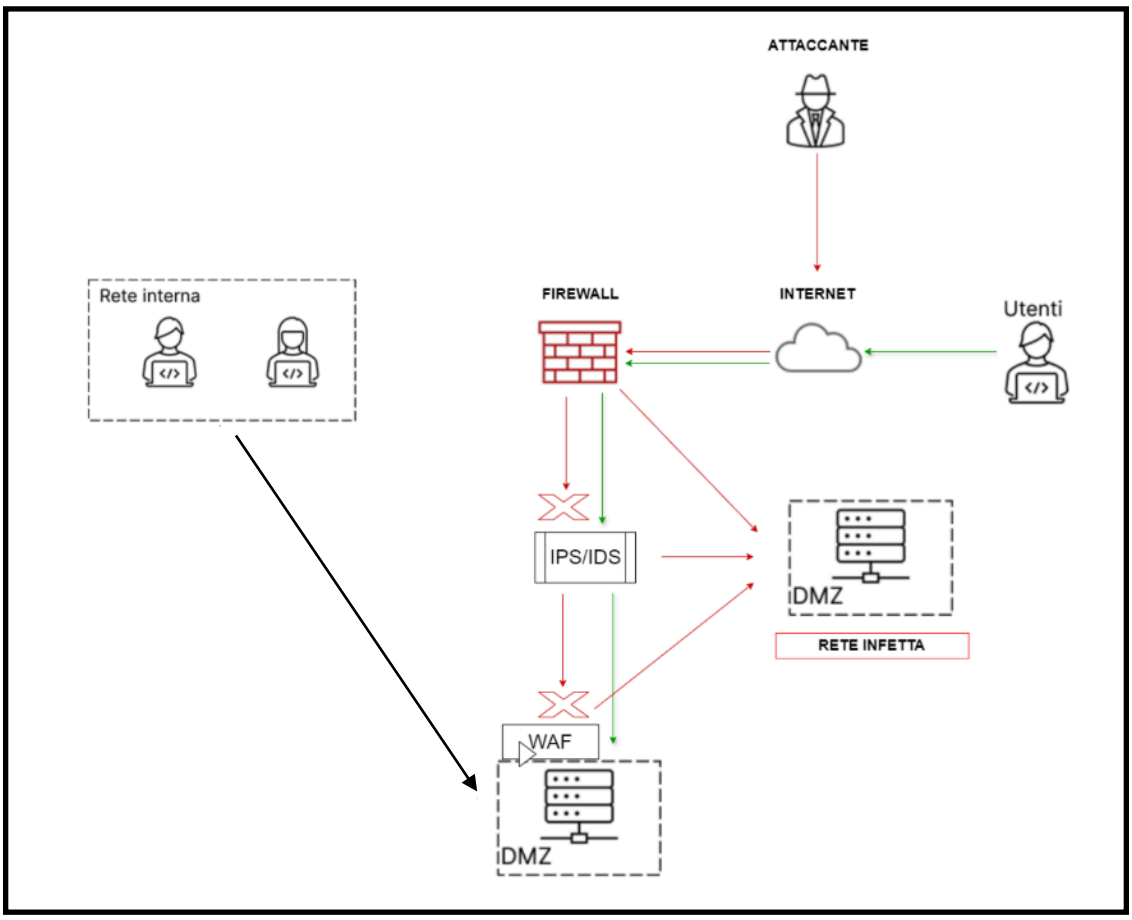


4. Quesito
Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

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

Svolgimento:

Isolare la DMZ infetta dalla rete interna interna così da poter analizzare le TTP dell'attaccante.
Creare un nuovo servizio DMZ per il normale funzionamento del business.
Implementare su quest'ultimo soluzioni IDS/IPS che impediranno all'attaccante di effettuare nuovi tentativi senza prima essere intercettato dai sistemi di rilevamento e prevenzione.


ATTACCANTE
Rete interna
FIREWALL
INTERNET
Utenti
IPS/IDS
DMZ
RETE INFETTA
WAF
DMZ