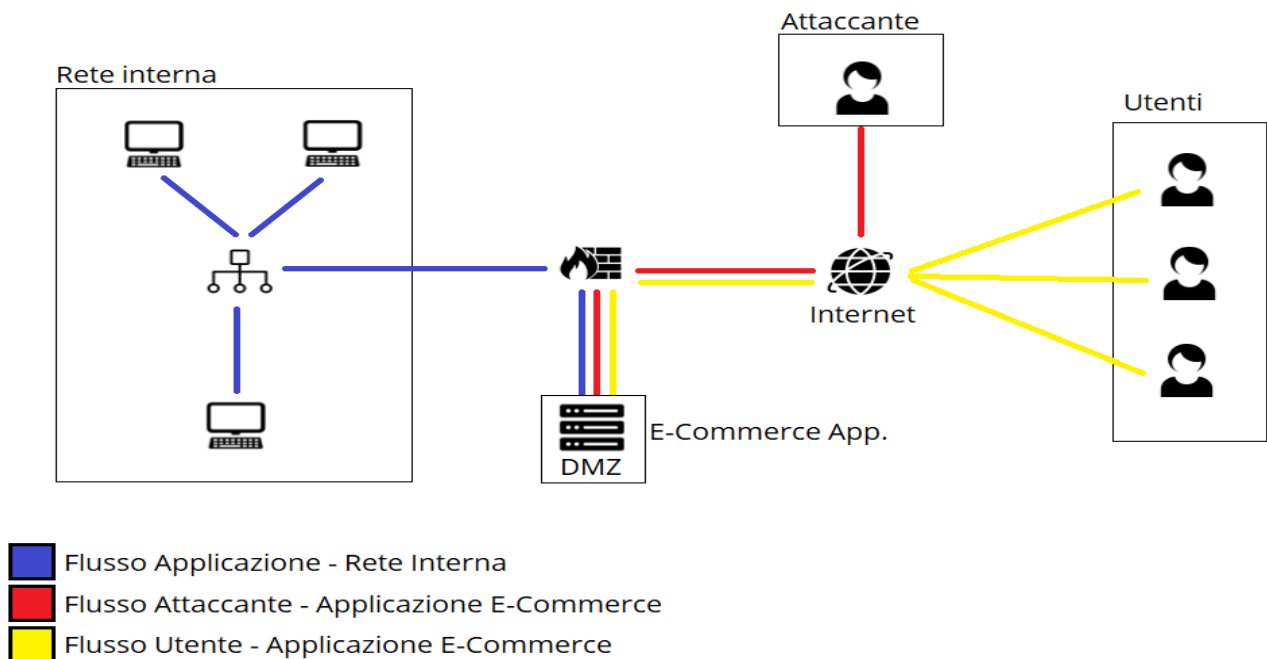
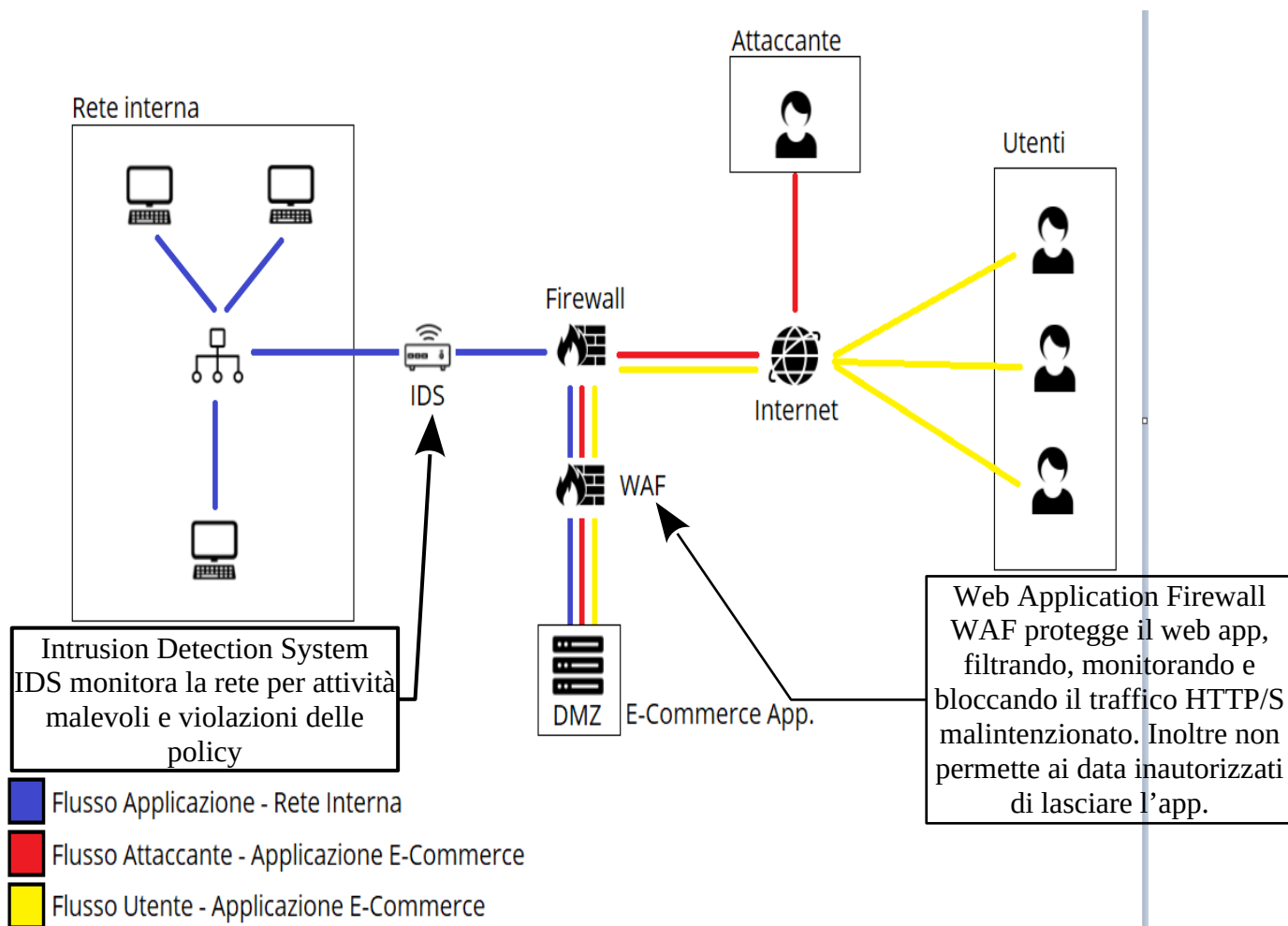


Report



Esercizio 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?



Esercizio 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.

Risposta:

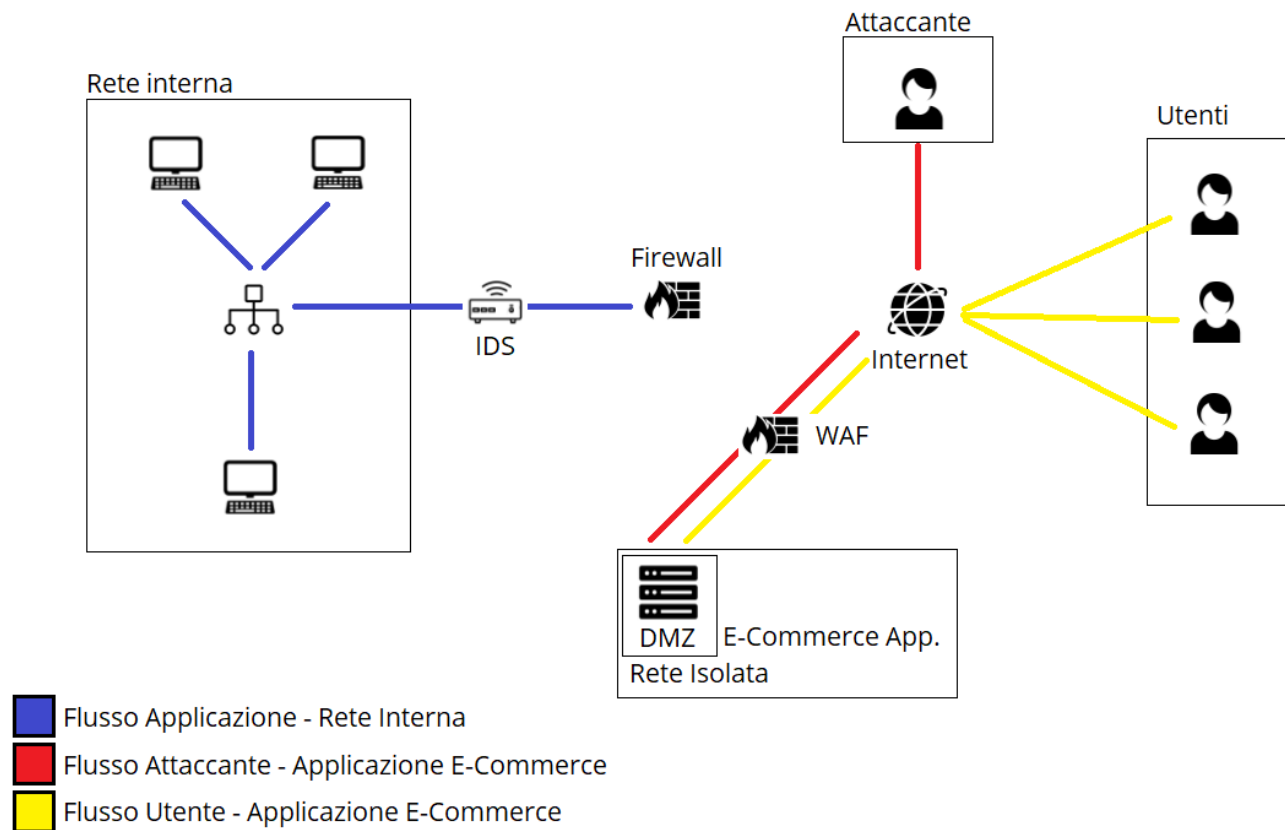
L'impatto finanziario se la piattaforma di E-commerce non può essere raggiunta dai clienti per 10 minuti sarebbe di **~15'000€ (Criticità MEDIA)**

Esercizio 3 (Response)

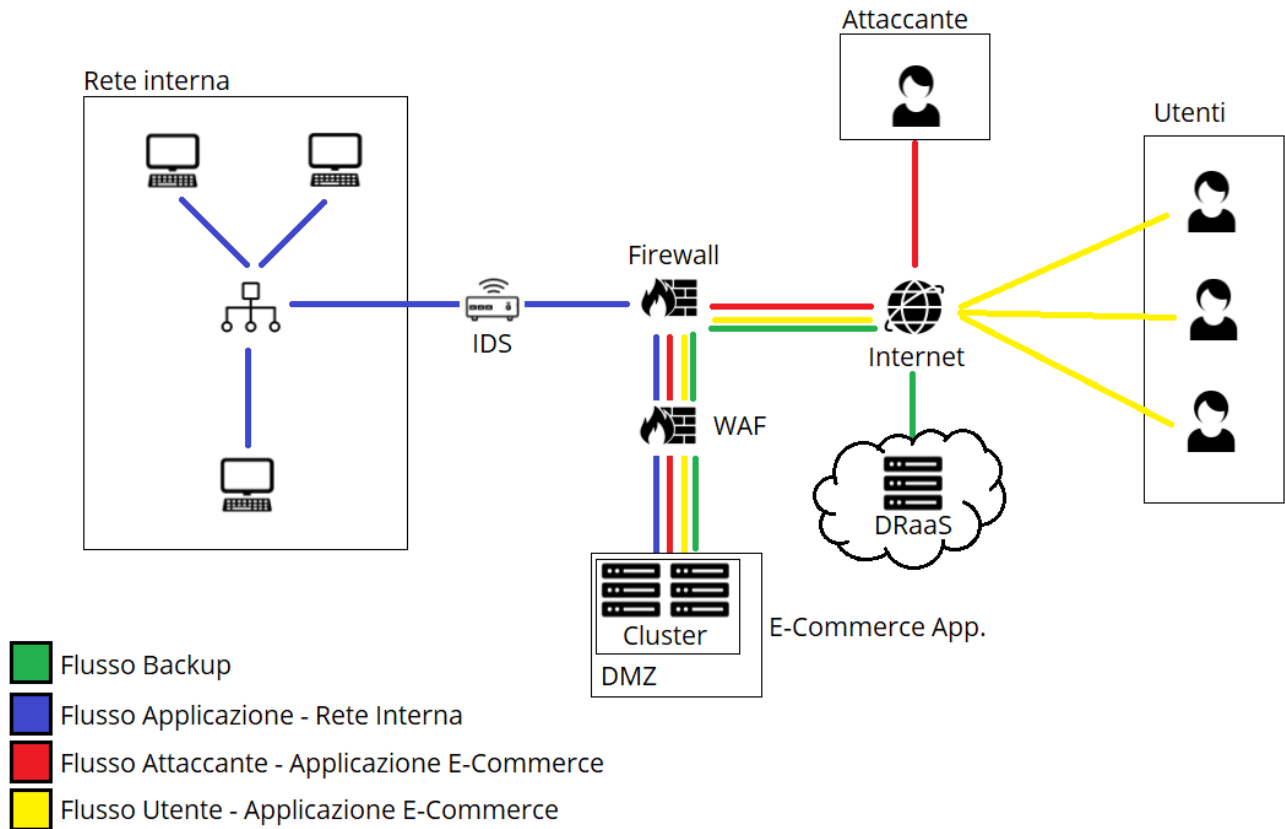
L'applicazione Web viene infettata da un malware.

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.

La rete interna scollegata dalla applicazione Web, ovvero in isolamento:



Soluzione



Cluster = due o più server che permettono la operatività del sistema anche a fronte di un errore su uno dei due server. Quando uno smette di funzionare, l'altro prende il suo posto (failover).

DRaaS = Disaster recovery as a service, i cloud provider che mettono a disposizione un'infrastruttura in cloud quale può essere immediatamente attivata in caso di un disastro.