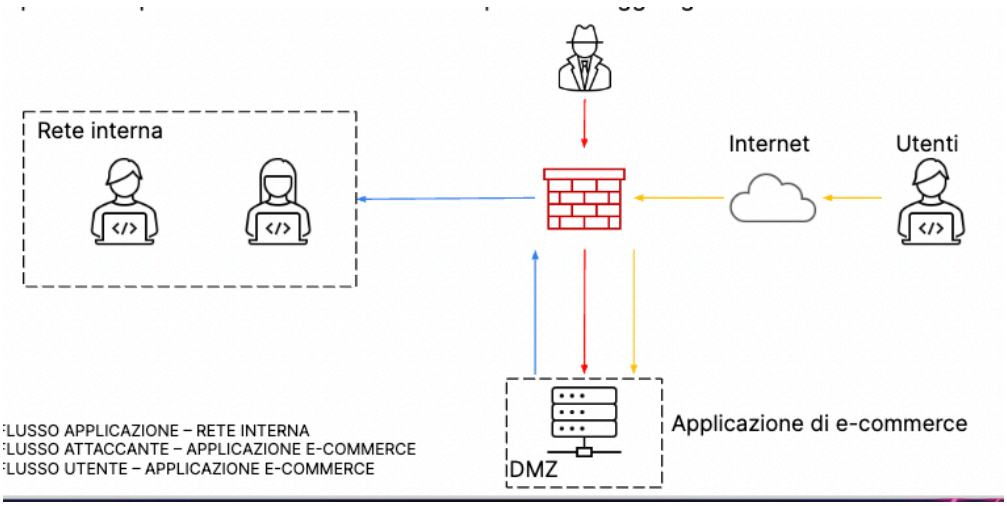
ARCHITETTURA DI RETE

L' architettura di rete della compagnia come si può vedere dalla foto sotto consiste che l'e-commerce deve essere disponibile agli utenti tramite internet per effettuare acquisti sulla piattaforma e poi la rete interna è raggiungibile dalla DMZ per via delle policy sul firewall

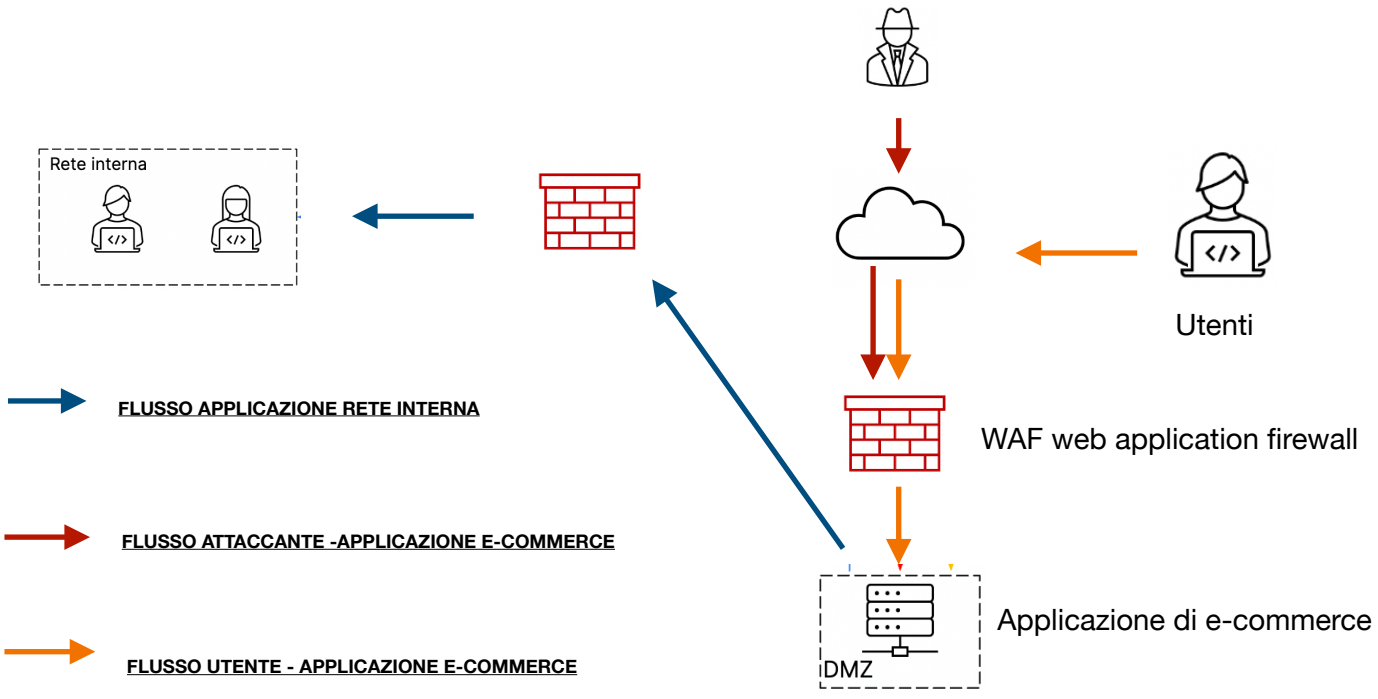


AZIONI PREVENTIVE

Le azioni preventive che si posso applicare per difendere l'applicazione dagli attacchi di tipo SQLi oppure XSS sono :

Come priva cosa possiamo mettere un web application firewall WAF, il WAF si occupa di ispezionare il traffico http assegnato un punteggio di pericolosità alla richiesta e superato il livello di attenzione previsto la bloccano

Un altra cosa che possiamo fare è la validazione dell'input:tipologia di dato, lunghezza, formato, contenuto
Un 'esempio che si può fare è se la web app si aspetta per un dato parametro un valore numerico e riceve una stringa di caratteri si capisce che c'è qualcosa che non torna



IMPATTI SUL BUSINESS

La nostra applicazione web subisce un attacco di tipo Ddos e l'applicazione non è raggiungibile per 10 minuti e gli utenti spendo in media ogni minuto 1.500 € sulla piattaforma sul e-commerce .

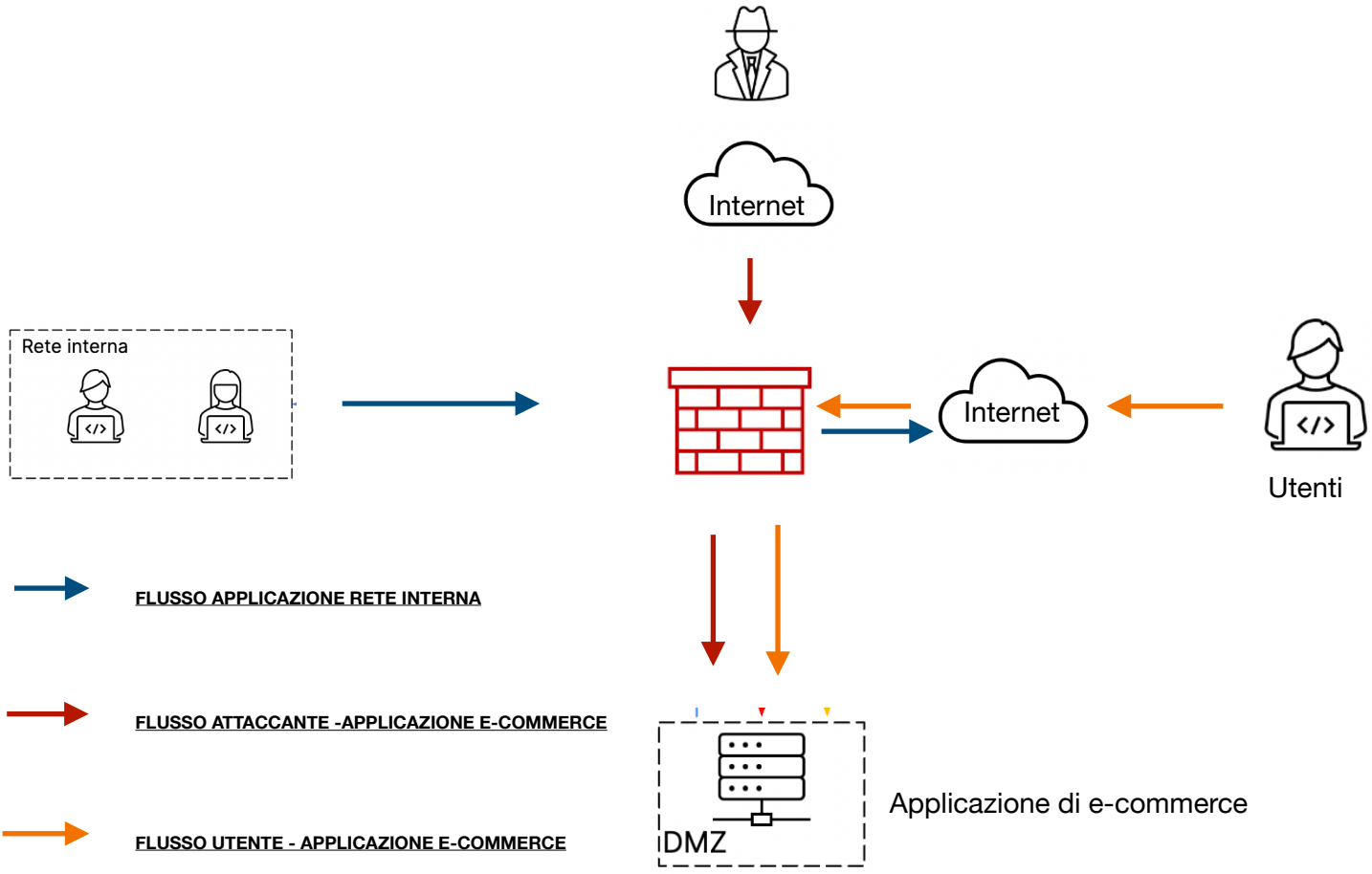
Quindi in questo caso l'impatto sul business è di media15.000€ perché se l'applicazione non è raggiungibile per 10 minuti e gli utenti spendono in media 1.500 € al minuto il calcolo è 1.500 x 10 = 15.000€

RESPONSE

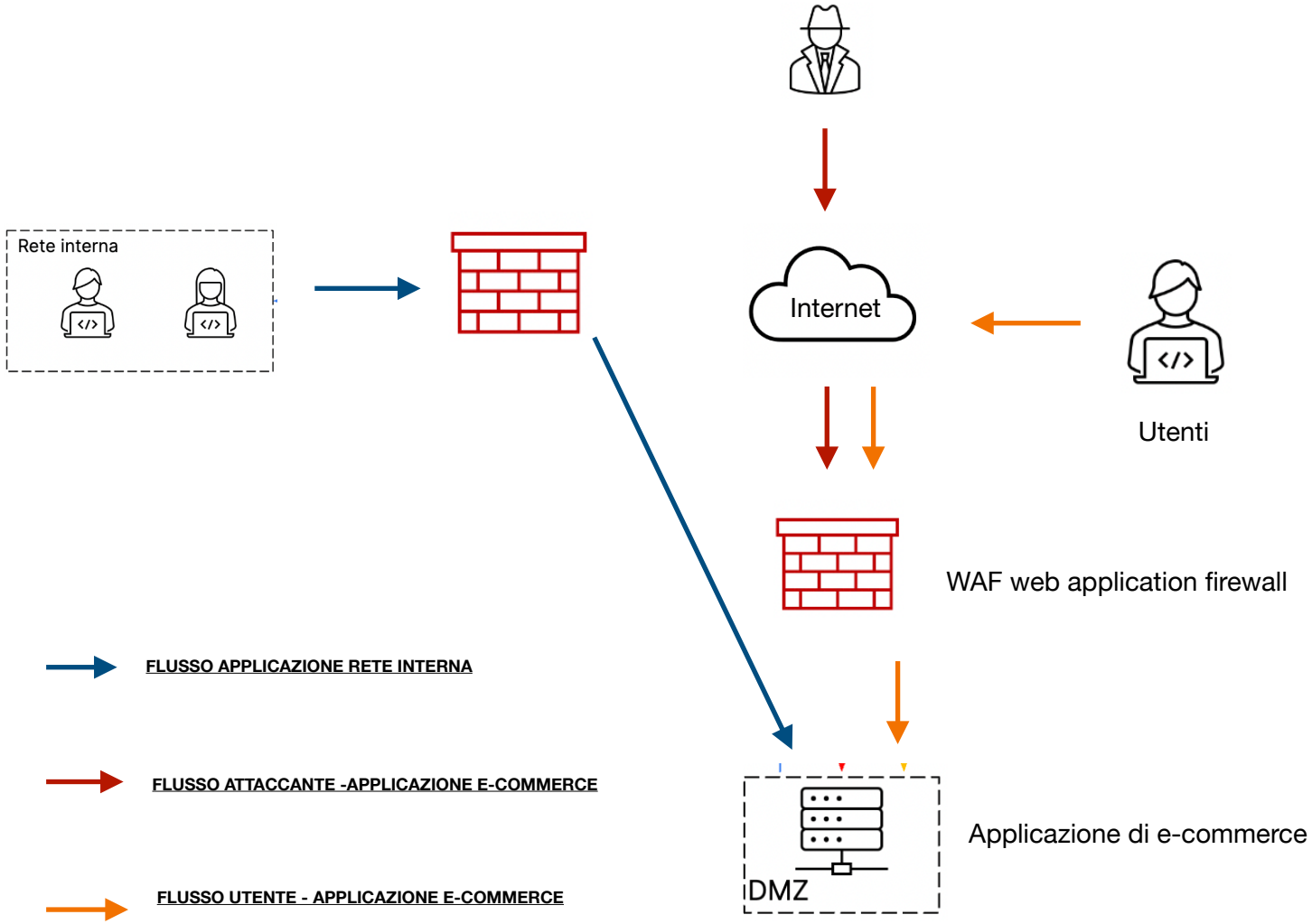
L'applicazione web viene infetta da un malware e la nostra priorità è che il malware non si propaghi alla vostra rete interna.

Lasciamo la macchina infetta connessa cosi facendo possiamo raccogliere informazioni riguardante l' attaccante questa procedura si chiama isolamento.

Questa procedura consiste nell'isolare il sistema infetto dalla nostra rete interna cosi da non permettere all' attaccate di poter infettare la nostra rete.Infatti come possiamo notare dall'architettura di rete dalla DMZ si può raggiungere la rete interna e quindi in questo caso andiamo a modificare la policy del firewall cosi da poter impedire che dalla DMZ si possa entrare alla rete interna.



SOLUZIONE COMPLETA



Come si può notare dalla soluzione completa con l'implementazione del WFA la nostra applicazione e-commerce è protetta da attacchi SQLi e XSS e non abbiamo più il problema che dalla DMZ si possa raggiungere la rete interna ma al contrario io dalla rete interna posso raggiungere la DMZ