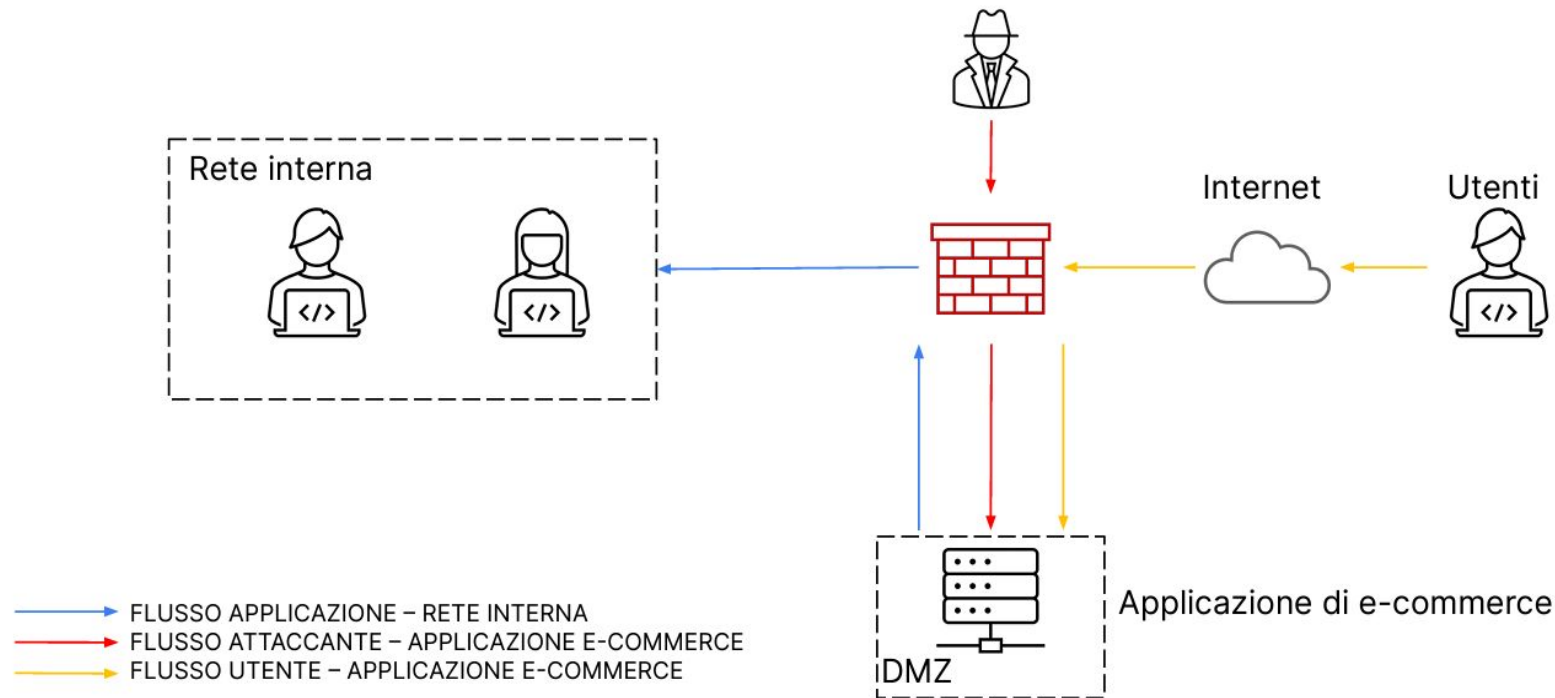


## Architettura di rete:

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.



Con riferimento alla figura, rispondere ai seguenti quesiti.

- 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.

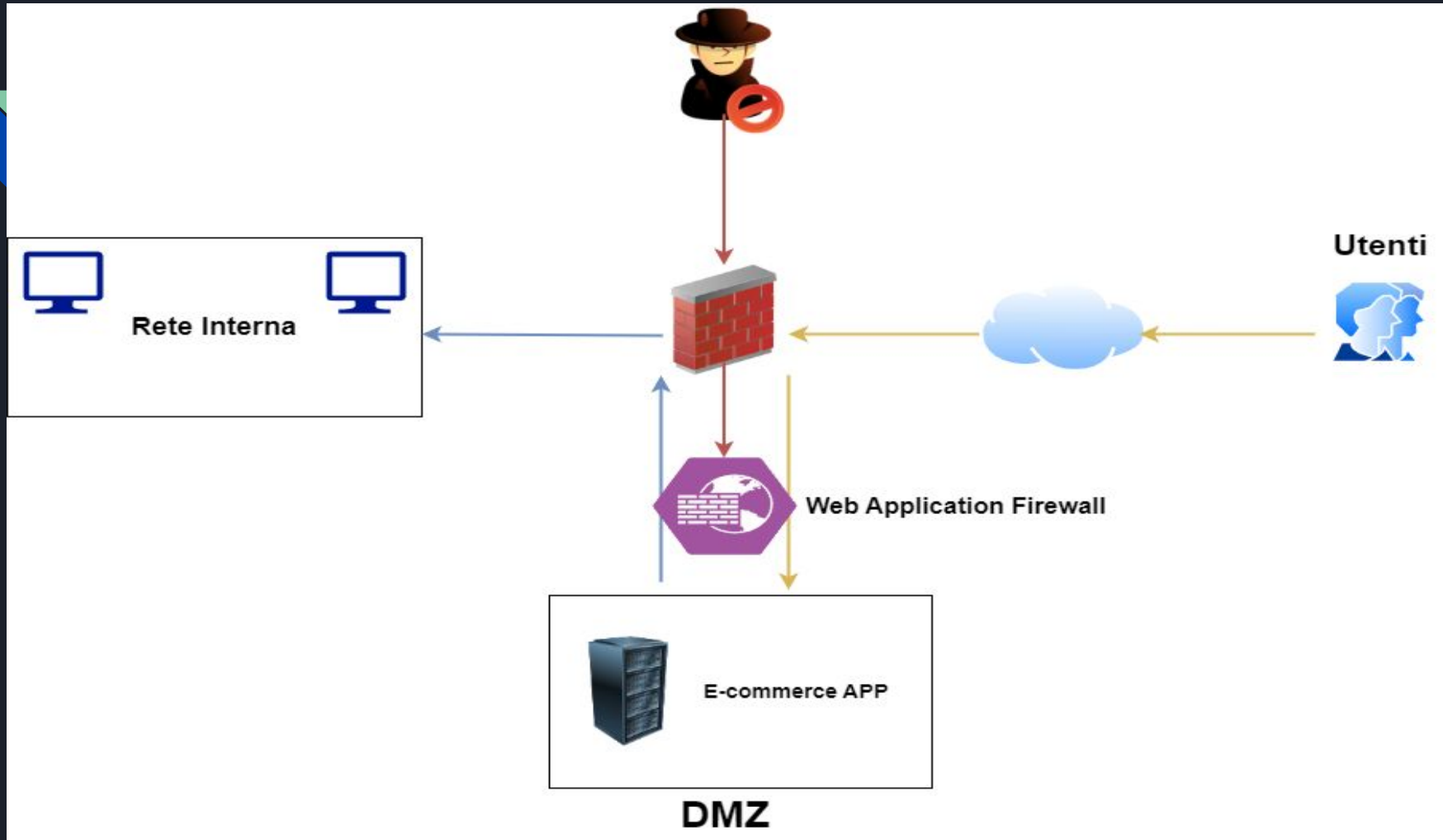
- Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

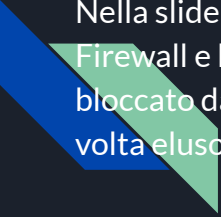
## Azioni preventive:

L'esercizio ci richiede di implementare delle azioni preventive per scongiurare eventuali attacchi XSS (Cross Site Script) e SQLi (SQL Injection) da parte di un criminale informatico che riesca ad aggirare l'iniziale protezione del Firewall.

Per fare questo possiamo utilizzare un WAF (Web Application Firewall) tra la DMZ dove abbiamo la nostra App di E-commerce e il Firewall.

Il WAF è uno specifico tipo di Firewall progettato per monitorare, filtrare ed eventualmente bloccare il traffico verso un'applicazione web, come in questo caso specifico. Costantemente aggiornato, è pensato per proteggere una Web App da attacchi comuni come XSS e SQLi. Questo perché contiene un database di firme per molti degli attacchi più comuni, e potrebbe quindi confrontare questo database con il tipo di traffico in arrivo dall'attaccante, riconoscendolo come malevolo e bloccandolo prima che acceda alla web app. Ancora, applica una validazione dell'input in entrata, accertandosi che non contenga codice potenzialmente dannoso o script malevoli, garantendo così un maggior livello di sicurezza. Quindi bloccherebbe il passaggio al traffico del Black hat, continuando però ad erogare regolarmente il servizio agli utenti comuni, purché il traffico di questi ultimi rispetti i parametri di cui sopra.





Nella slide precedente, ecco come sarebbe la situazione una volta implementato un WAF a protezione della web app tra il Firewall e la DMZ. Come vediamo, se anche il Black Hat dovesse riuscire a superare il primo controllo del Firewall verrebbe poi bloccato dal WAF che ne impedirebbe l'iniezione di codice malevolo sulla web app a differenza della prima immagine dove, una volta eluso il Firewall, il criminale informatico poteva essere libero di agire con attacchi XSS e SQLi.

## Impatti sul business:

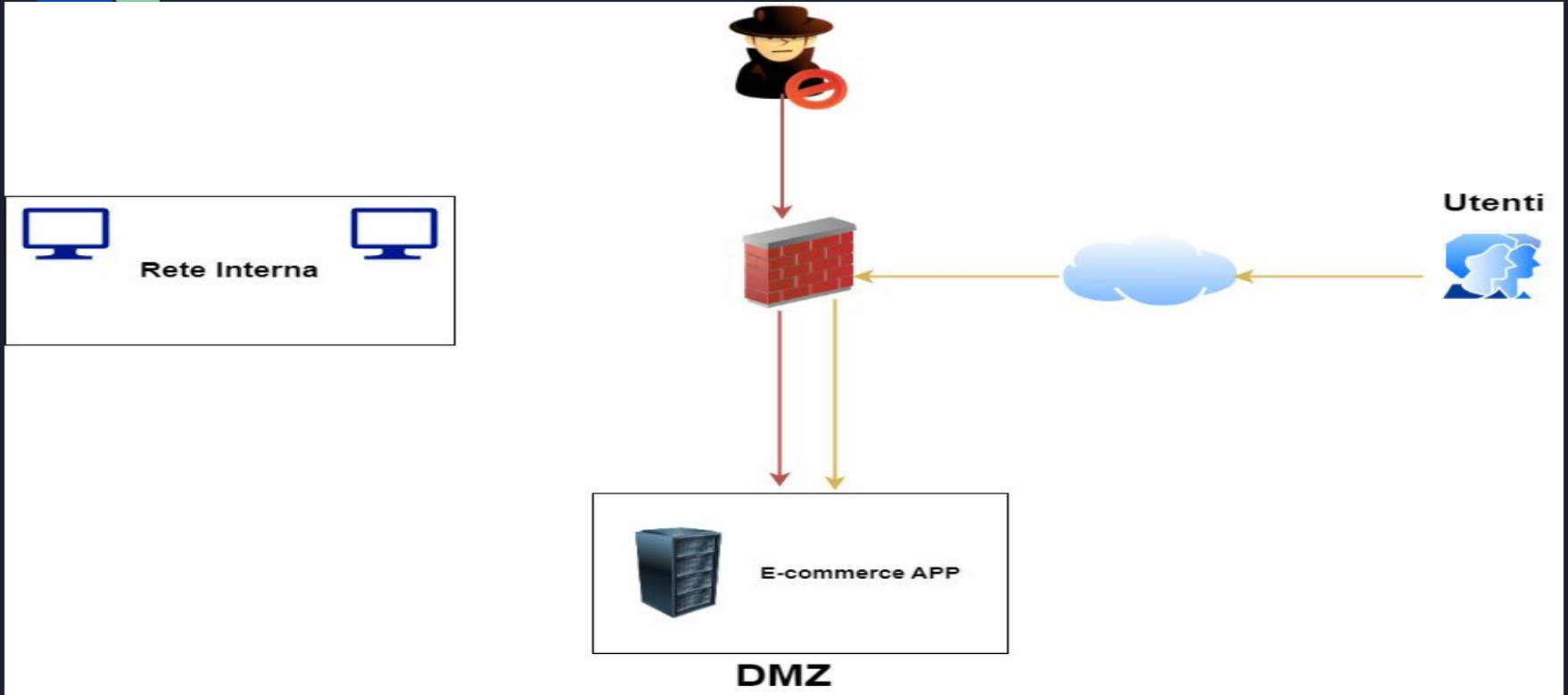
La seconda traccia del progetto chiedeva di calcolare l'impatto economico subito dall'azienda la cui web app è stata sotto attacco Ddos per dieci minuti. Questo attacco ha reso il servizio inutilizzabile. Considerando che, come da traccia, gli utenti spendono in media **1500 €** al minuto e l'app è stata fuori servizio per **10 minuti**, il calcolo è il seguente:

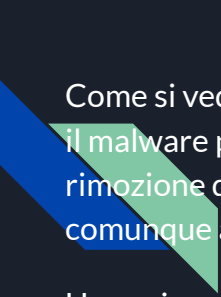
$$1500 \times 10$$

La perdita economica subita dall'azienda per dieci minuti in cui la web app è stata inutilizzabile, con una media di spesa al minuto di 1500 € è di **15000 €**.

## Response:

l'ultima traccia poneva la situazione in cui la web app sia infettata da un malware. La priorità è che il malware non si diffonda sulla rete interna, mentre non siamo interessati a rimuovere l'accesso all'attaccante sulla macchina infetta.





Come si vede dalla slide precedente, in questo caso l' applicazione web è stata **isolata** dalla rete aziendale, questo per evitare che il malware possa propagarsi rapidamente e compromettere altri dispositivi. In questo modo si potrà lavorare in sicurezza sulla rimozione del malware senza correre rischi di infettare la rete interna dell' azienda. Tuttavia questa soluzione consente comunque agli utenti di accedere alla web app con il rischio concreto di prendere loro il malware ed infettare i propri dispositivi.

Una spiegazione a questo motivo potrebbe essere che, dopo un' analisi del rischio si è visto come il costo in termini economici dell' interrompere il servizio erogato dalla web app sarebbe decisamente superiore al lasciare invece il server online, seppur con potenziali conseguenze sugli utenti che si servono del sito web.