# Report W20 D4

## Sommario



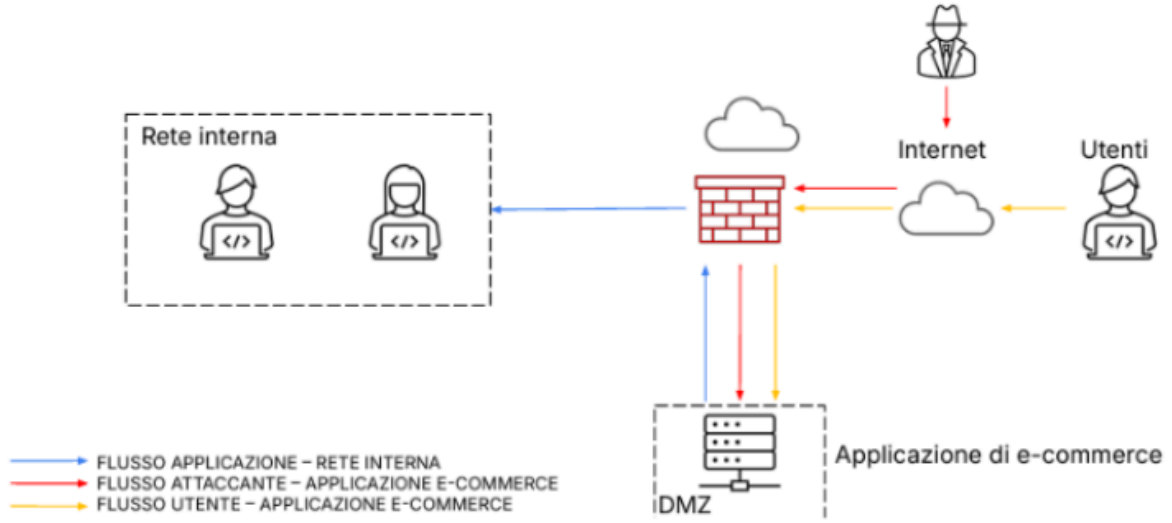
## Introduzione

In questo report analizzeremo tre scenari di sicurezza relativi a un'applicazione web, l'obiettivo è:

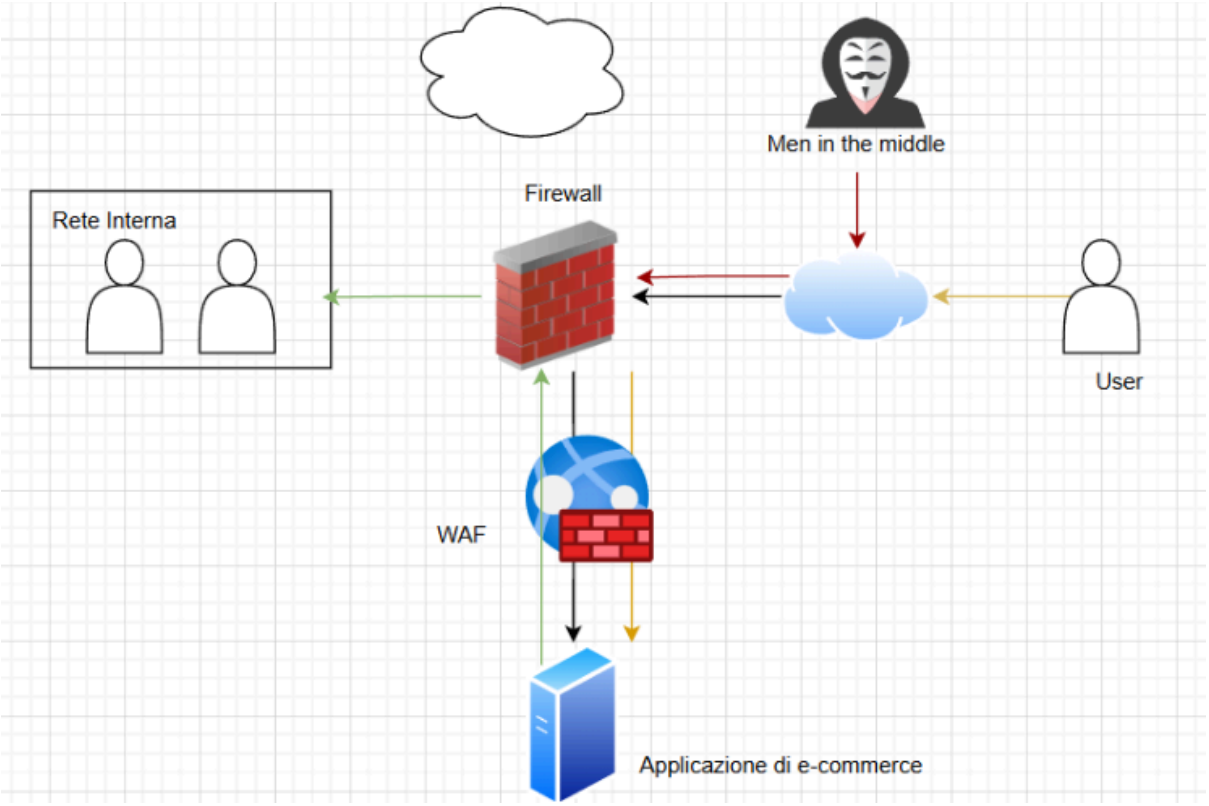
- proporre azioni preventive contro attacchi SQLi e XSS,
- stimare l'impatto economico di un attacco DDoS,
- e definire una strategia di contenimento in caso di infezione da malware.
- verranno inoltre suggerite modifiche all'architettura per migliorare la postura difensiva della rete

## Attacchi SQLi e XSS

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



Come misura preventiva useremo un web application firewall che sono dei dispositivi di sicurezza dedicati per proteggere le applicazioni da attacchi quali SQL injection e Cross Site Scripting, applicando il WAF tra il firewall e l'applicazione, l'architettura verrebbe come di seguito




## Impatti sul business

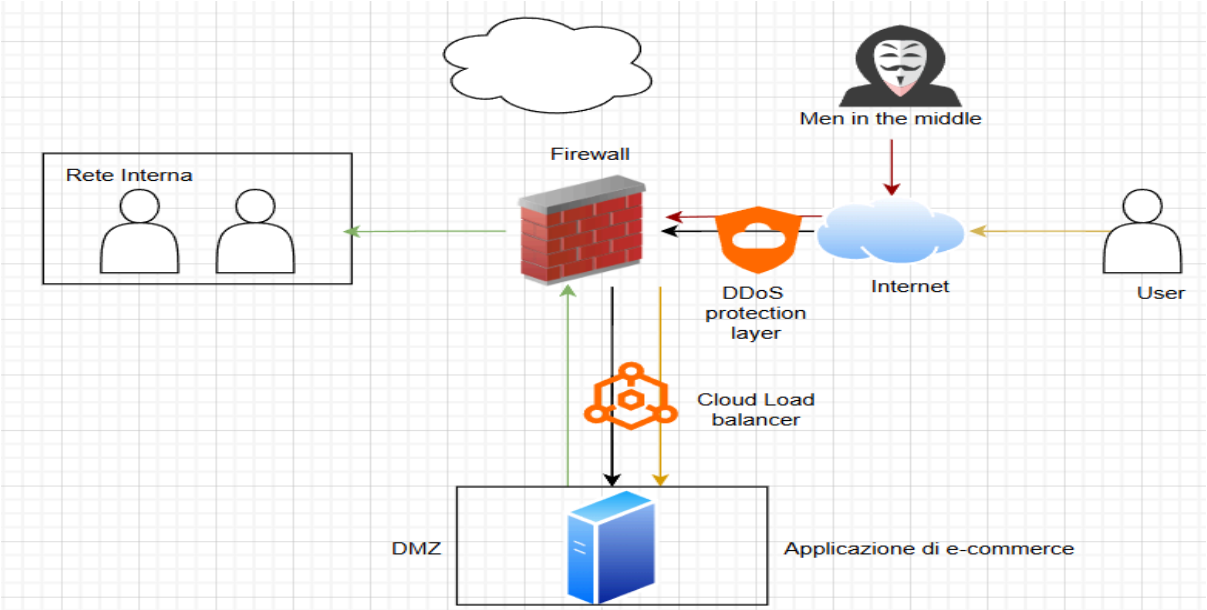
L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

Per calcolare l'impatto sul business faremo minuti dell'applicazione non raggiungibile x media spesa utente, quindi

10m x 1500€ = 15000 €

Quindi in totale abbiamo perso 15000€

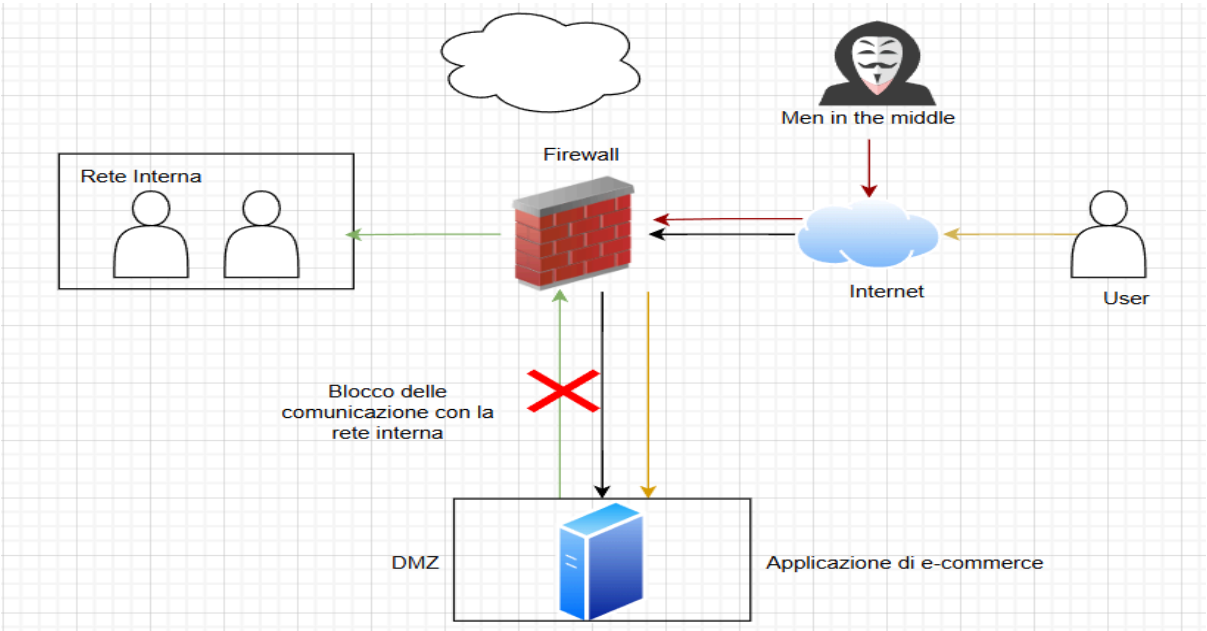
Come misura preventiva aggiungiamo un DDoS protection layer prima del firewall,ed eventualmente anche un cloud load balancer prima dell'applicazione del server, come vediamo nell'immagine sotto




## Response

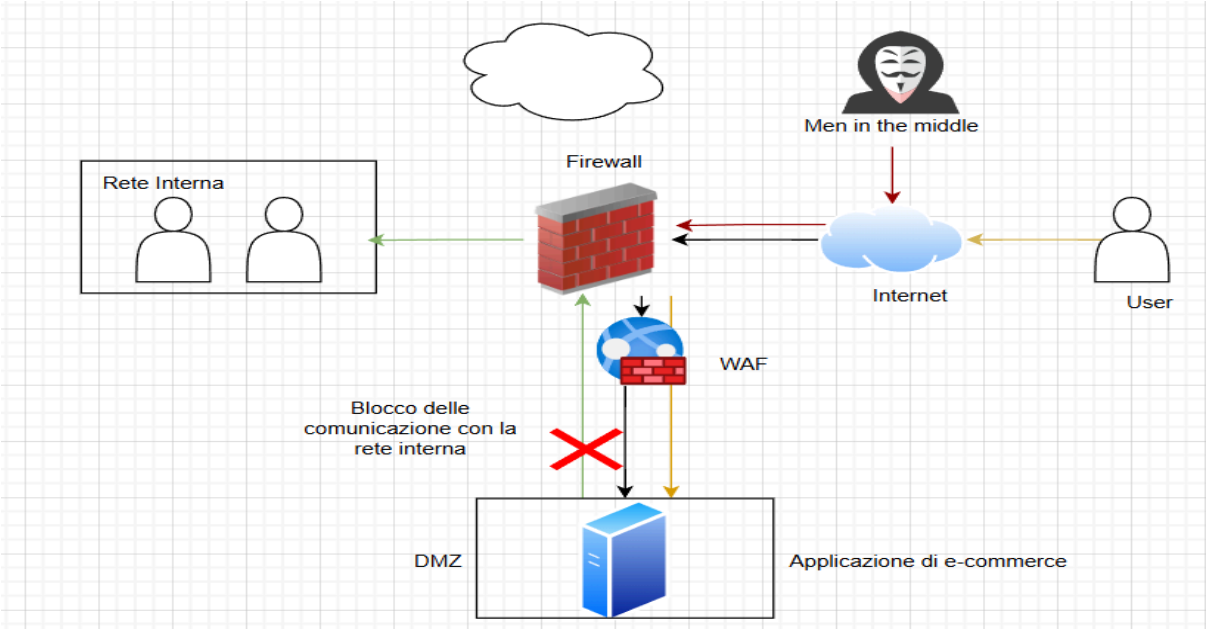
L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

La soluzione proposta è isolare la macchina infetta mediante segmentazione della rete (DMZ), bloccare le comunicazione in uscita verso la rete interna, consentire accesso solo verso Internet, così l'attaccante non si propaga.



## Soluzione completa

Mettendo insieme le azioni preventive degli attacchi sqli e XSS e l'isolamento dell'applicazione abbiamo come risultato un architettura come questa



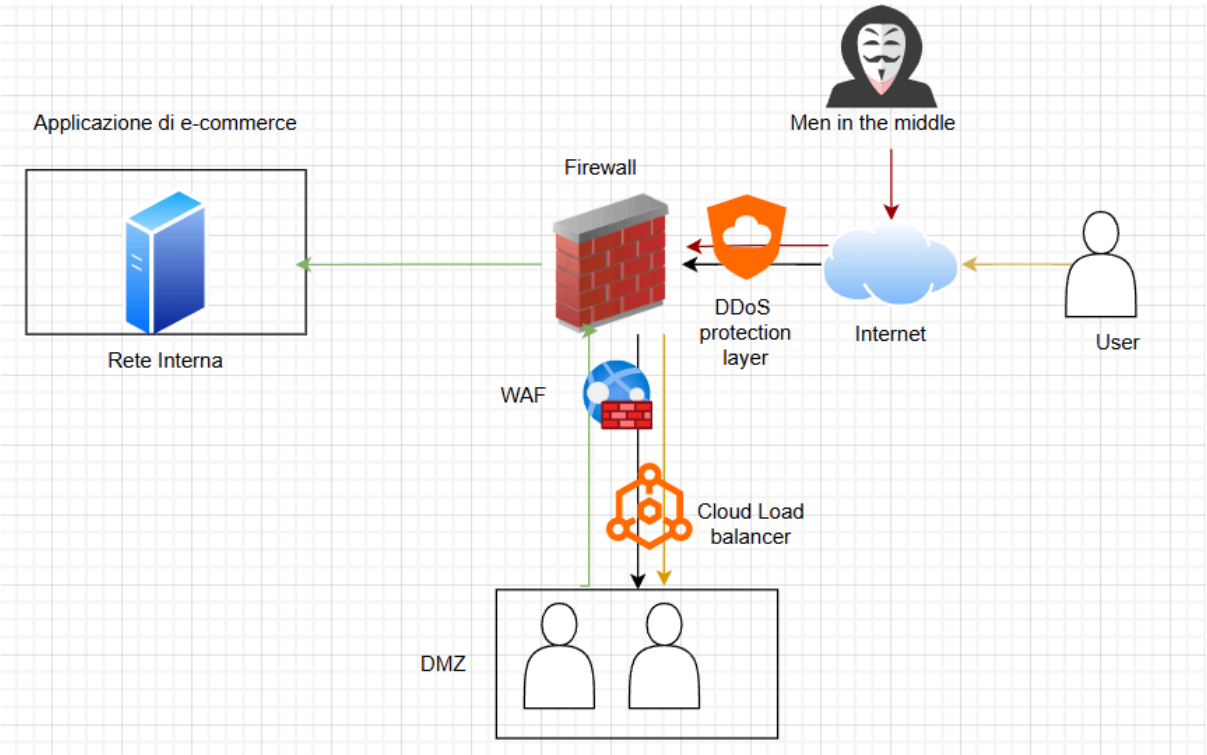

## Modifica più aggressiva dell'architettura

In questo caso uniamo tutti i casi visti finora con un budget massimo di 30 mila euro quindi gli attacchi sqli e XSS, le azione preventive del DDoS, e l'infezione del malware nell'applicazione,iniziamo subito con i costi

- Il prezzo medio di un Web Application Firewall (WAF) può variare in base al provider e alle funzionalità offerte. Ad esempio, AWS Firewall Manager ha un costo di 0,395 USD all'ora per ogni endpoint e 0,065 USD per GB elaborato, che si traduce in circa 4.469,00 USD al mese per 10 endpoint.
- Per quanto riguarda il prezzo medio per la protezione DDoS, un esempio è il servizio di Azure, che offre un prezzo di $199 al mese. Questo prezzo è basato su 730 ore al mese, il che indica un costo costante per il servizio.
- Invece Google Cloud ha tariffe per l'elaborazione dei dati che variano da 0,02 USD a 0,05 USD per 1 gibibyte, a seconda del piano. nel nostro caso useremo un piano di 100 terabyte quindi 5000 USD

Convertendo questi numeri da dollari a euro scopriamo che spendiamo un totale di 8272.62 euro, quindi nel budget ci rimangono ancora 21.727.38 euro

E il nostro grafico rimarrebbe così




# Conclusione

L'analisi condotta evidenzia l'importanza cruciale di implementare misure di sicurezza proattive in ogni fase dell'infrastruttura di rete. La prevenzione di attacchi SQLi e XSS mediante l'uso di un Web Application Firewall e l'adozione di buone pratiche di sviluppo rappresentano un primo strato di difesa fondamentale. L'impatto economico di un attacco DDoS, anche di breve durata, conferma la necessità di predisporre sistemi di mitigazione automatica e soluzioni scalabili. Infine, l'isolamento dell'applicazione compromessa in una rete segmentata consente di contenere rapidamente la propagazione di minacce come i malware, limitando i danni e preservando l'integrità della rete interna.

L'integrazione di queste contromisure rafforza la resilienza dell'intero ecosistema digitale, garantendo continuità operativa, protezione dei dati e fiducia degli utenti.