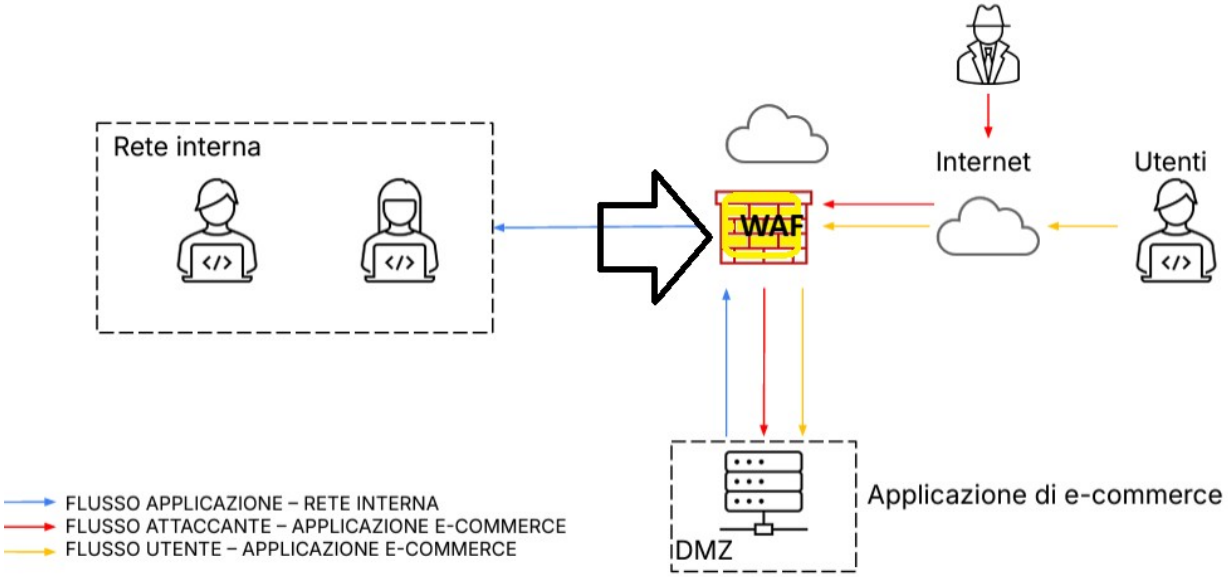
# CPTP0524 – W20D4 - Benchmark M5

*Security Operation*

## 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?
Modificate la figura in modo da evidenziare le implementazioni.

*Per proteggere il server da attacchi XSS e SQLi andrei a configurare un web app firewall che lavora a punto per questo.*



## 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.
Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

L'interruzione di 10 minuti, con una spesa media di 1.500 € al minuto, comporta una perdita di:

**1.500 € × 10 = 15.000 €**

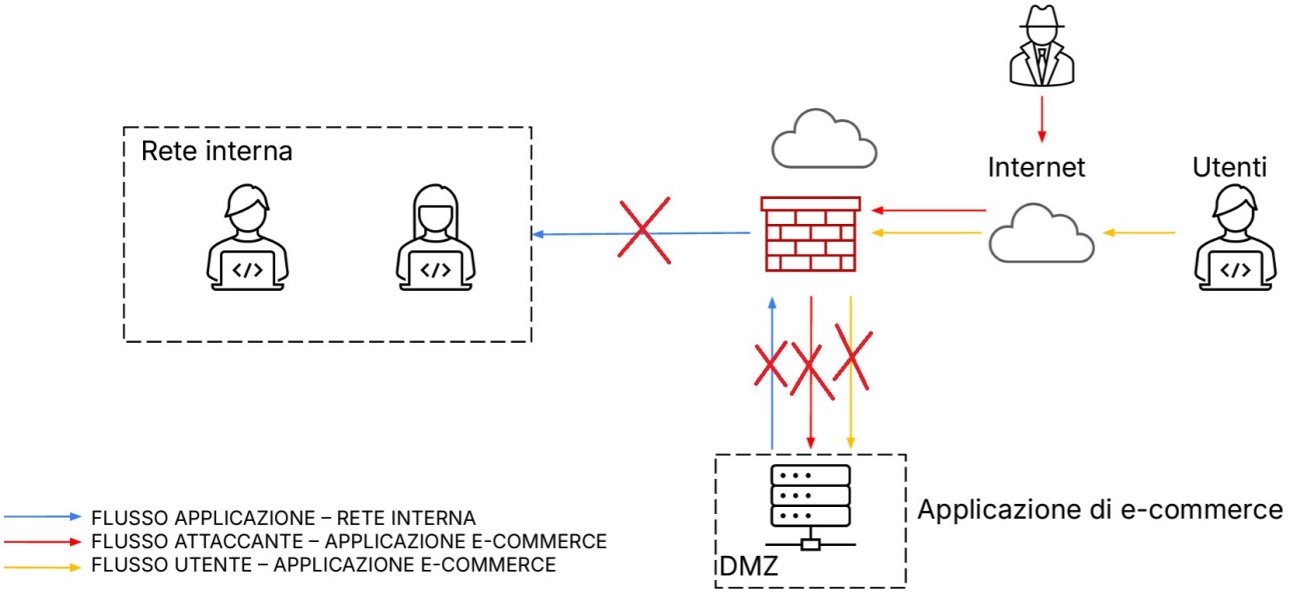
Per mitigare e prevenire future interruzioni dovute a DDoS, si possono adottare le seguenti misure:

- **Anti-DDoS:** Utilizzare soluzioni di mitigazione specializzate (come CloudFlare) che filtrano e bloccano il traffico malevolo prima che raggiunga il server.
- **Rate Limiting e Firewalling:** Implementare meccanismi di rate limiting per limitare il numero di richieste provenienti da un singolo indirizzo IP e configurare firewall per bloccare traffico sospetto.
- **Load Balancing e Autoscaling:** Distribuire il traffico su più server e utilizzare sistemi di autoscaling per gestire picchi improvvisi di traffico, assicurando così che l'infrastruttura possa assorbire l'attacco.
- **Content Delivery Network (CDN):** Usare una CDN per servire contenuti statici, riducendo il carico sui server principali e migliorando la resilienza dell'applicazione.
- **Monitoraggio e Incident Response:** Implementare sistemi di monitoraggio continuo e di logging per rilevare tempestivamente attività anomale e predisporre un piano di risposta agli incidenti.
- **Architettura Ridondante:** Progettare l'infrastruttura in modo da includere failover e ridondanza, garantendo che in caso di attacco o guasto, il servizio possa continuare a funzionare attraverso risorse alternative.

## 3. Response:

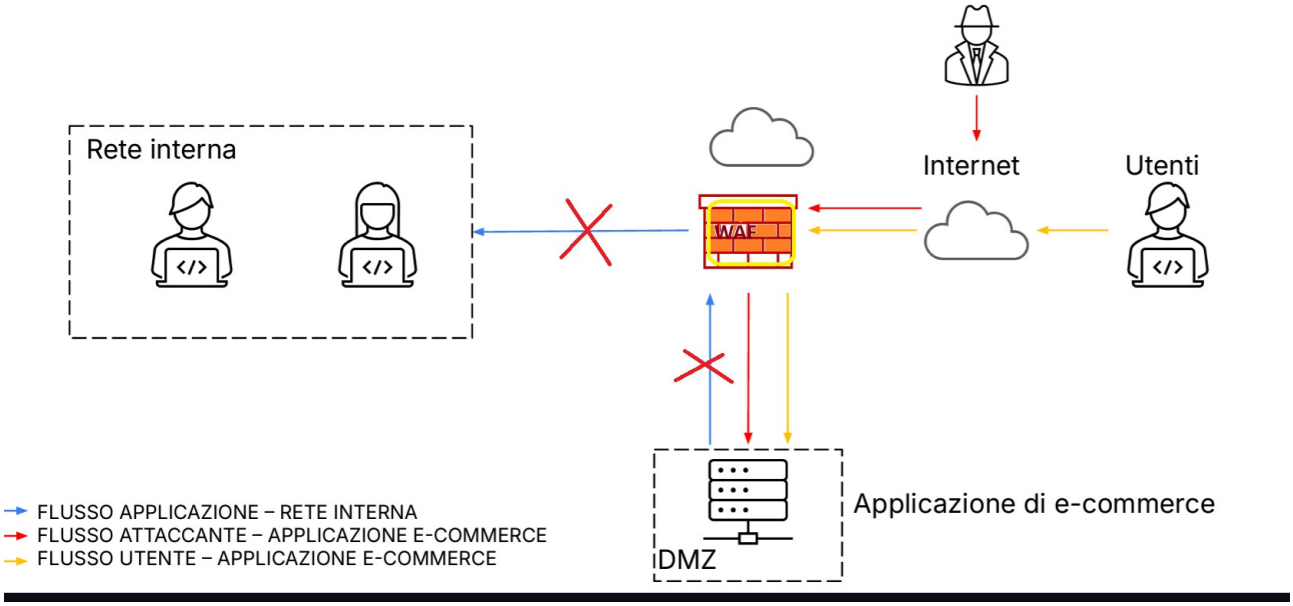
- L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

*Isolare la macchina dalla rete interna e da Internet*



## 4. Soluzione completa:

Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)




1. Ho bloccato la comunicazione dalla DMZ **alla** rete Interna, questo per evitare che in caso di compromissione del server DMZ, l'attaccante non possa raggiungere la rete interna e quindi compromettere altri host in quella rete.

2. Ho implementato un web app firewall per bloccare il traffico e le richieste malevole in caso di tentativo di attacco/intrusione. Su un firewall come pfSense implementerei Snort per bloccare e allertare traffico malevolo.

Francesco Rinaldi