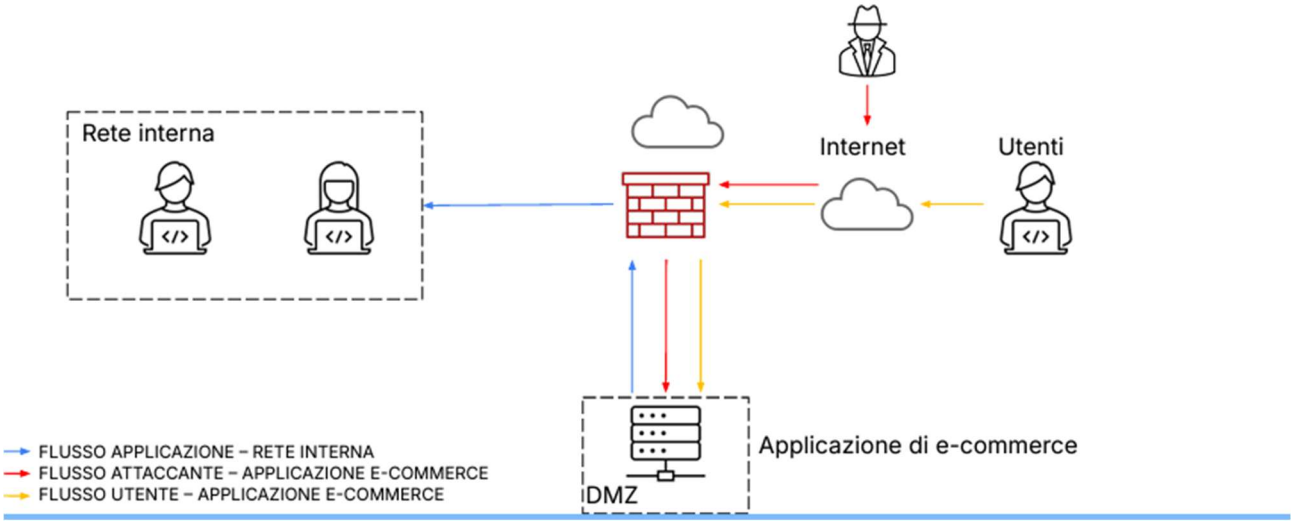
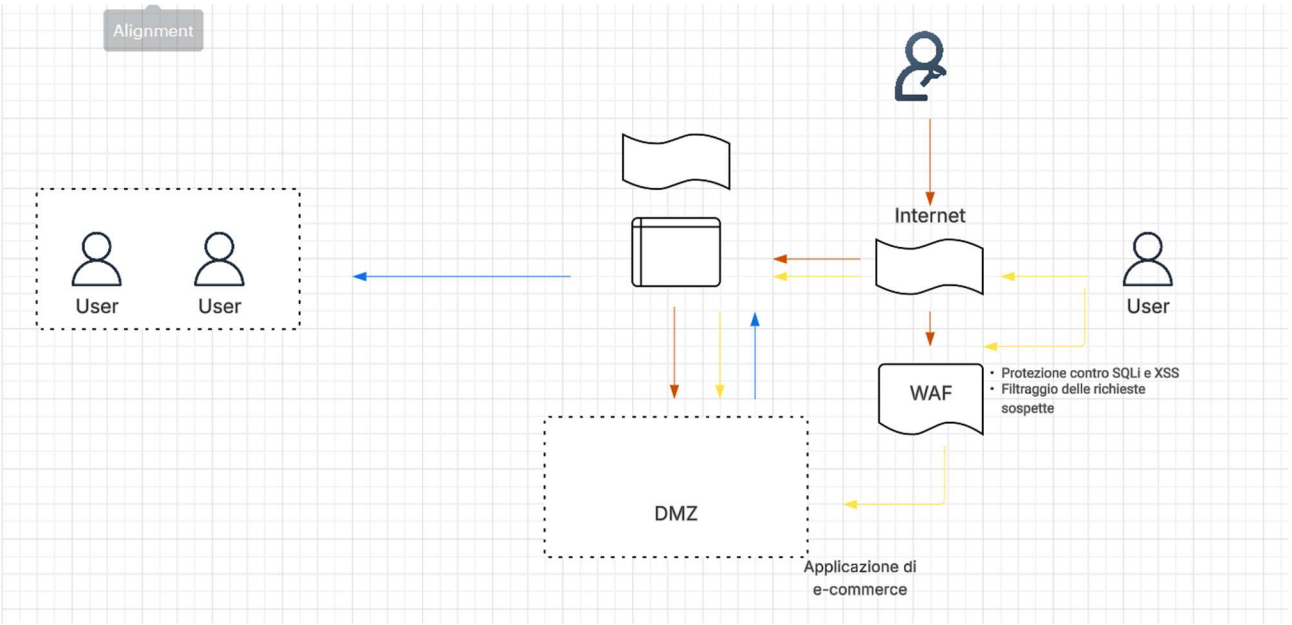


1. *Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.*

   Azioni preventive contro SQLi e XSS

   Per difendere l'applicazione Web da attacchi di tipo SQL Injection e Cross-Site Scripting, è necessario implementare le seguenti azioni preventive:

   - **Validazione degli input:** implementare una validazione rigorosa degli input utente per assicurarsi che i dati immessi siano conformi ai formati previsti, utilizzare whitelist per accettare solo caratteri specifici.
   - **Sanitizzazione degli input:** rimuovere o codificare caratteri speciali (es. <, >, ', "), utilizzare funzioni di escape per prevenire l'inserimento di codice malevolo.
   - **Prepared Statements e Query Parametrizzate: u**tilizzare query SQL parametrizzate per prevenire SQL Injection, evitare di concatenare stringhe direttamente nelle query SQL.
   - **Content Security Policy (CSP): i**mplementare una CSP per limitare le risorse che possono essere caricate dall'applicazione, riducendo il rischio di XSS.
   - **Firewall per applicazioni Web (WAF):c**onfigurare un WAF per rilevare e bloccare richieste sospette.



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*

Impatti sul business e azioni preventive contro DDoS

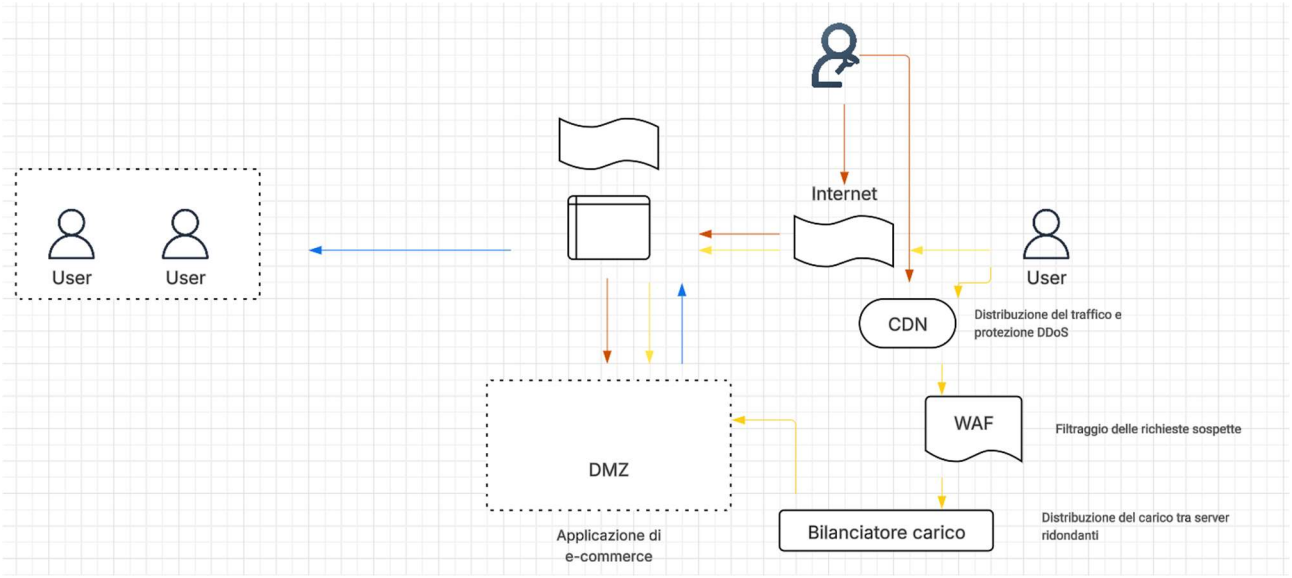
Se l'applicazione Web subisce un attacco DDoS che la rende non raggiungibile per 10 minuti, l'impatto economico viene calcolato come segue:

- **Calcolo dell'impatto**:
  Perdita al minuto: 1.500 €
  Durata dell'attacco: 10 minuti
  Impatto totale: 1.500 € × 10 = 15.000 €
- **Azioni preventive contro DDoS**:
  -Content Delivery Network (CDN): utilizzare una CDN per distribuire il traffico e ridurre il carico sul server principale.

  -Rate Limiting: implementare limiti di richiesta per utente/IP per prevenire un sovraccarico.

  -Protezione DDoS dedicata: configurare servizi di protezione DDoS.

  -Ridondanza: implementare server ridondanti e bilanciamento del carico per garantire la disponibilita.

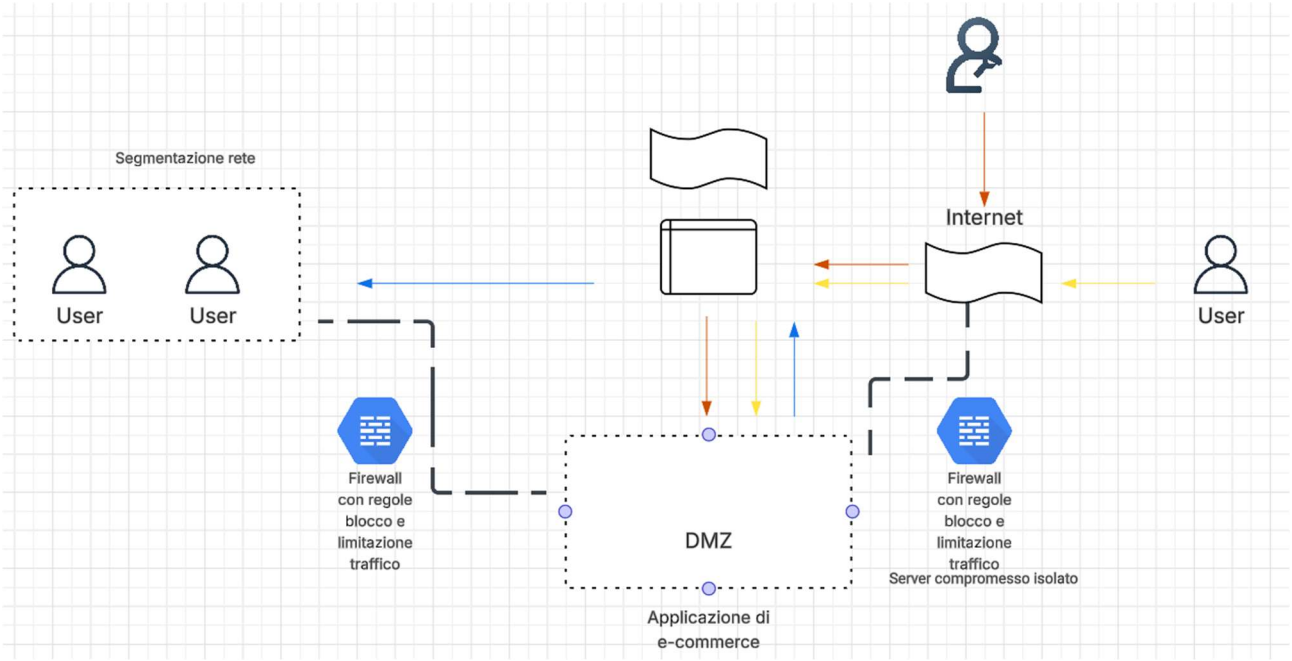


3. *Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.*

Response: Contenimento del malware

Se l'applicazione Web viene infettata da un malware, la priorità è impedire la propagazione del malware alla rete interna. Le azioni da intraprendere includono:

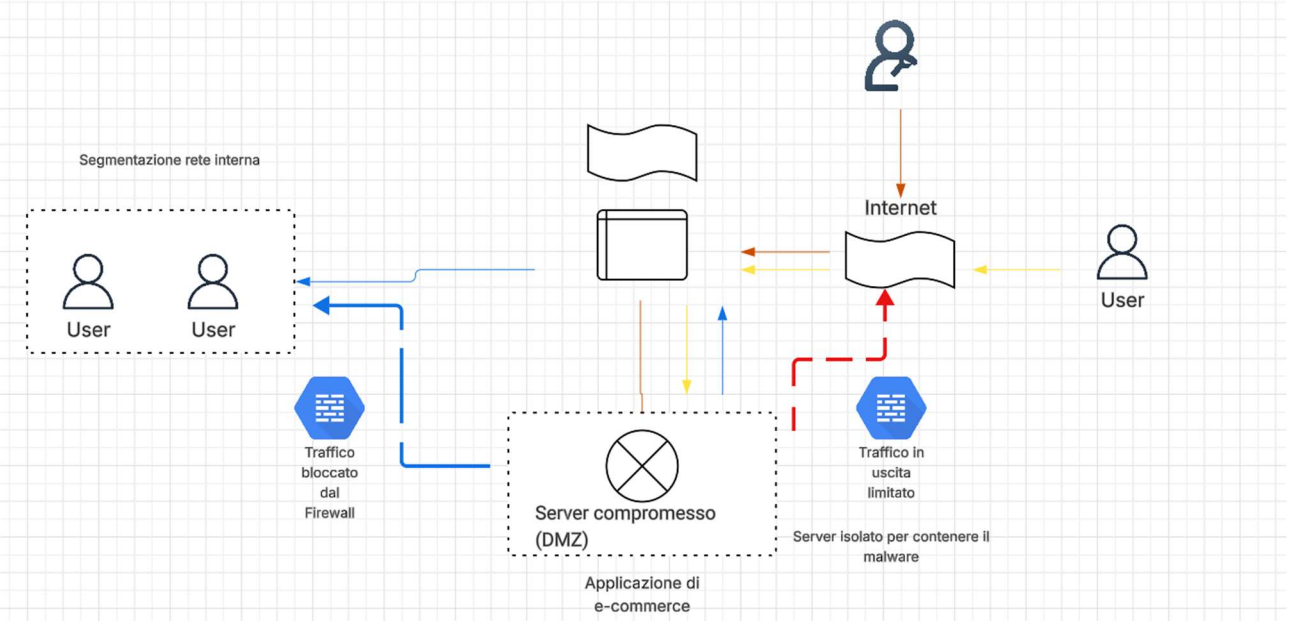
- **Isolamento del server compromesso**:configurare il firewall per bloccare immediatamente il traffico tra il server compromesso e la rete interna, limitare il traffico in uscita dal server compromesso.
- **Segmentazione della rete**: implementare una segmentazione tra la DMZ e la rete interna, utilizzare VLAN e regole di accesso per limitare la comunicazione.
- **Monitoraggio e logging**: abilitare il monitoraggio continuo per rilevare attività sospette, analizzare i log per identificare il punto di ingresso del malware.



4. *Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)*

Unendo le soluzioni preventive e di response, la figura dovrebbe includere:

- **Azioni preventive**:
  - WAF
  - Validazione e sanitizzazione degli input
  - Query parametrizzate
  - CSP
- **Azioni contro DDoS**:
  - CDN
  - Protezione DDoS
  - Bilanciamento del carico
  - Server ridondanti
- **Response al malware**:
  - Isolamento del server compromesso
  - Segmentazione della rete
  - Regole di firewall per bloccare il traffico tra DMZ e rete interna


Segmentazione rete interna
User
User
Internet
User
Traffico bloccato dal Firewall
Server compromesso (DMZ)
Traffico in uscita limitato
Server isolato per contenere il malware
Applicazione di e-commerce