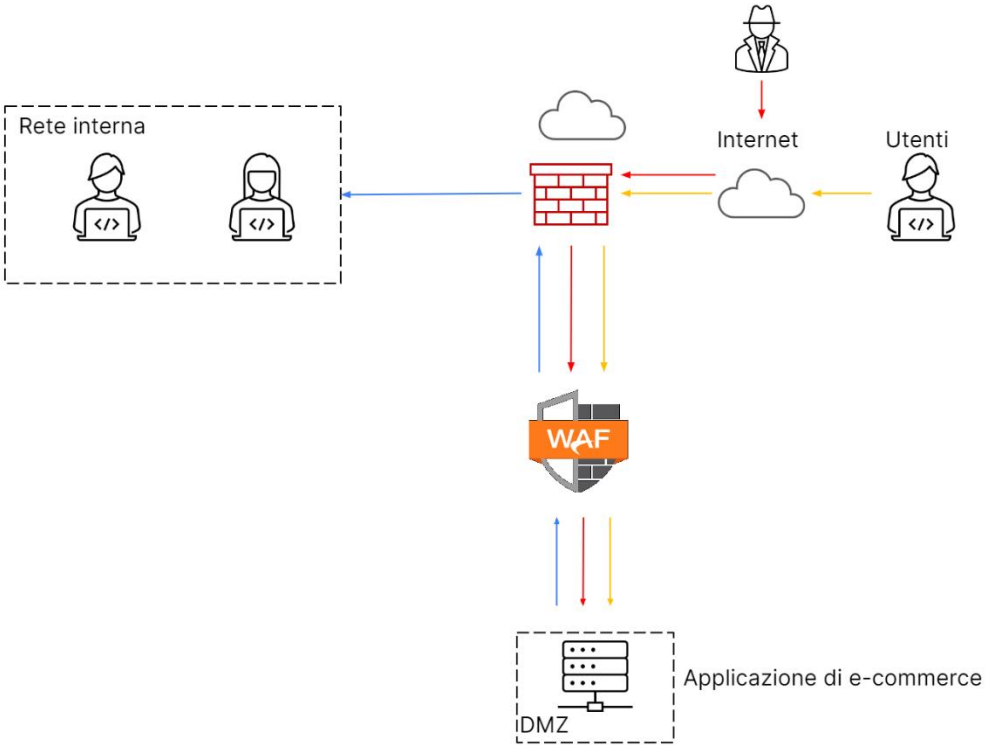
1. Azioni preventive:
    - Validazione dei dati di input.
      Assicurarsi che i dati di input siano adeguatamente validati
    - Parametrizzazione delle query
      impedisce l'esecuzione di istruzioni SQL dannose attraverso l'inserimento di input malevoli
    - Escape dei dati in output
      previene l'esecuzione indesiderata di codice JavaScript e protegge dagli attacchi XSS
    - Limitazione dei privilegi del database
    - Aggiornamento regolare del software
    - Test di sicurezza e revisione del codice
    - Inserimento WAF

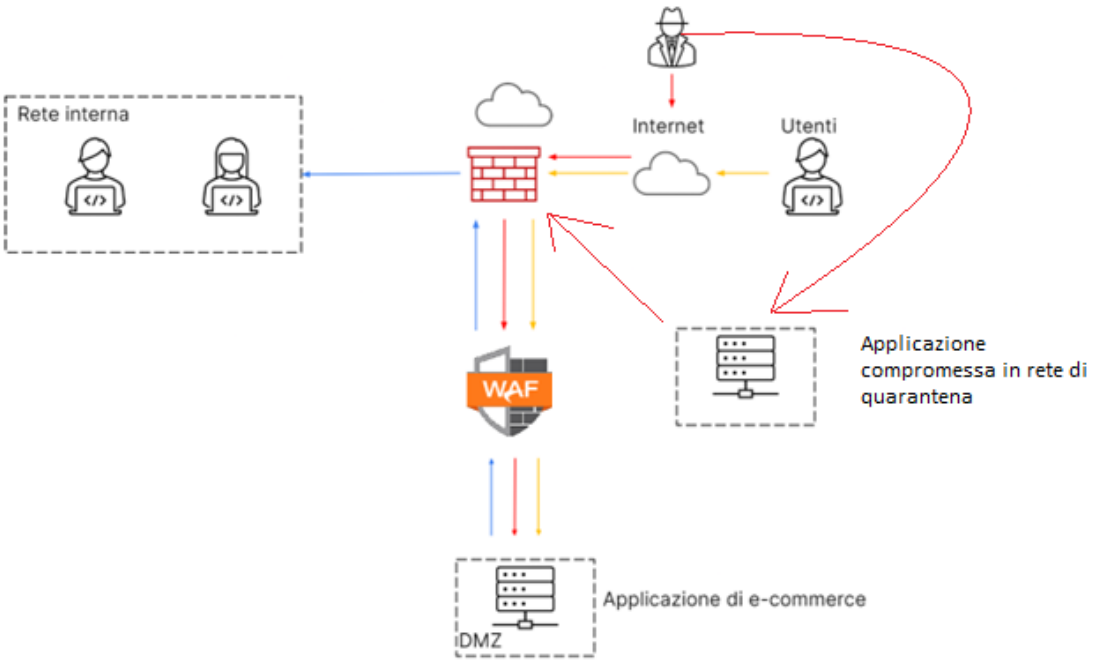


2. Impatto sul business: 15.000,00 €

   Azioni preventive:

   - configurazione regole firewall
   - migrazione infrastruttura verso cloud provider

3. Possiamo spostare l'applicazione compromessa su una rete di quarantena, reindirizzando il traffico degli utenti leciti su una nuova DMZ creata da un backup



5.Migrazione totale dell’infrastruttura in cloud