# PROGETTO S9-L5

**SCOPO: Rispondere a seguenti quesiti con riferimento alla figura sotto; tra l'altro dobbiamo:**

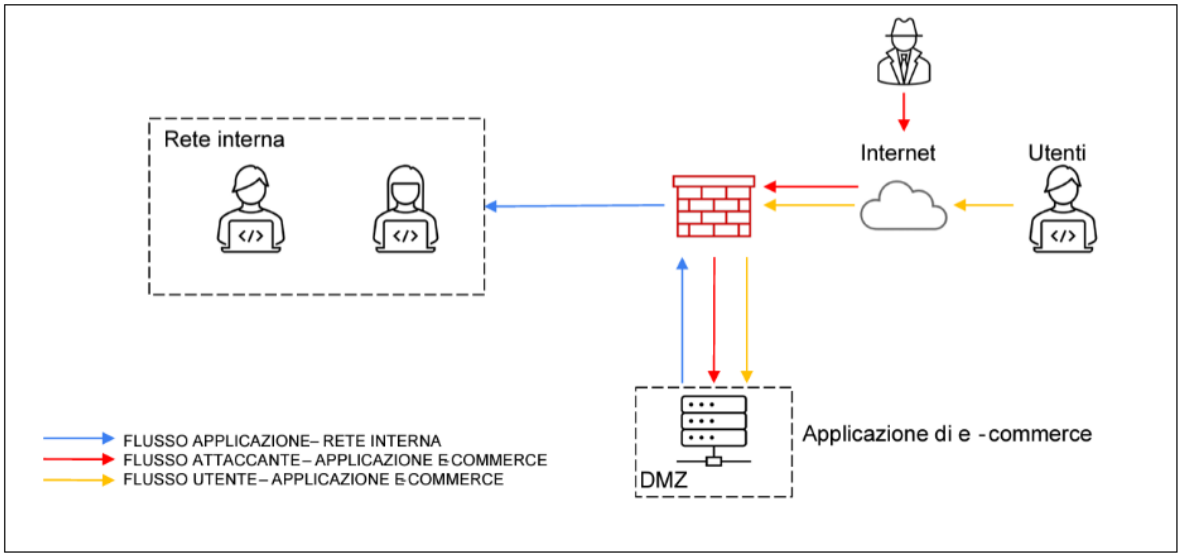
**1-Spiegare gli azioni preventive che si potrebbe implementare per difendere l'Applicazione web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato;e modificare la figura in modo da evidenziare le implementazione.**

**2-Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio;considerando che in media ogni munito gli utenti spendono 1500€.**

**3-Modificare la figura sotto in modo da impedire l'acesso da parte dell'attaccante alla rete interna.**

**4-Unire i designi dell'azione preventiva e della response(1-3)**

**5-Modificare l'infrastruttura integrando altri elementi di sicurezza.**




## 1-Azioni Preventive

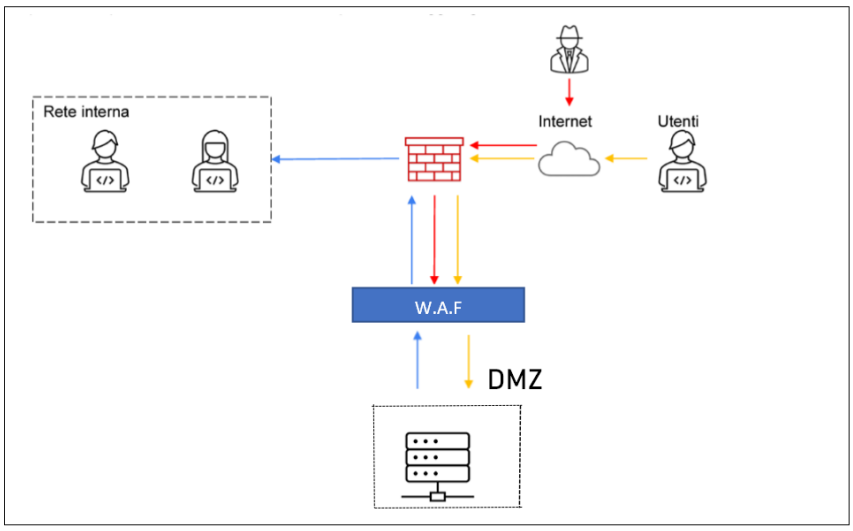
Prima di dare azioni preventive,proviamo di capire che cos'è **SQLi** e **XSS? .**
**SQLi e XSS** sono due tipi di attacchi informatici che mirano a sfruttare vulnerabilità nei siti web o nelle applicazioni web.

# PROGETTO S9-L5

**SQL Injection** è un tipo di attacco che sfrutta le vulnerabilità nei sistemi di gestione dei database.avendo come obiettivo principale la manipolazione dei query SQL eseguite sul database sottostante.

**XSS(**Cross-Site Scripting) è un tipo di attacco che si verifica quando un'applicazione web consente a un utente malintenzionato di inserire script malevoli all'interno del browser degli utenti che visitano la pagina vulnerabile.

-come azione preventive  da implementare abbiamo  aggiunto  un W.A.F(Fire Wall delle Applicazioni Web).questo pemetterebe di blocare il flusso in ingresso.come possiamo vedere sull'imagine qua sotto:




**2-)Calcolo dell'impatto sul Business(IP)**

**IP =** 1500€ × 10 = 15000€

Possiamo come azione preventivo in questa problematica fare:

- il monitoraggio del traffico.

- Aggiornare regolarmente il software

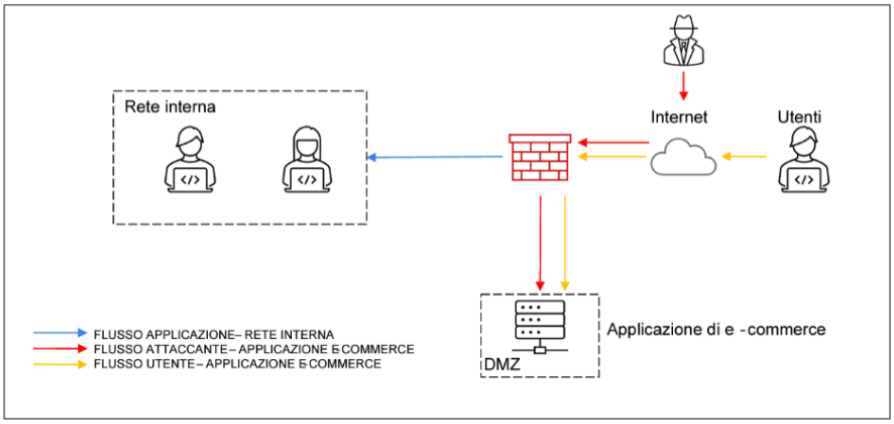
- prevedere un piano di risposta agli incidenti

- fare Backup regolari dei dati

# PROGETTO S9-L5

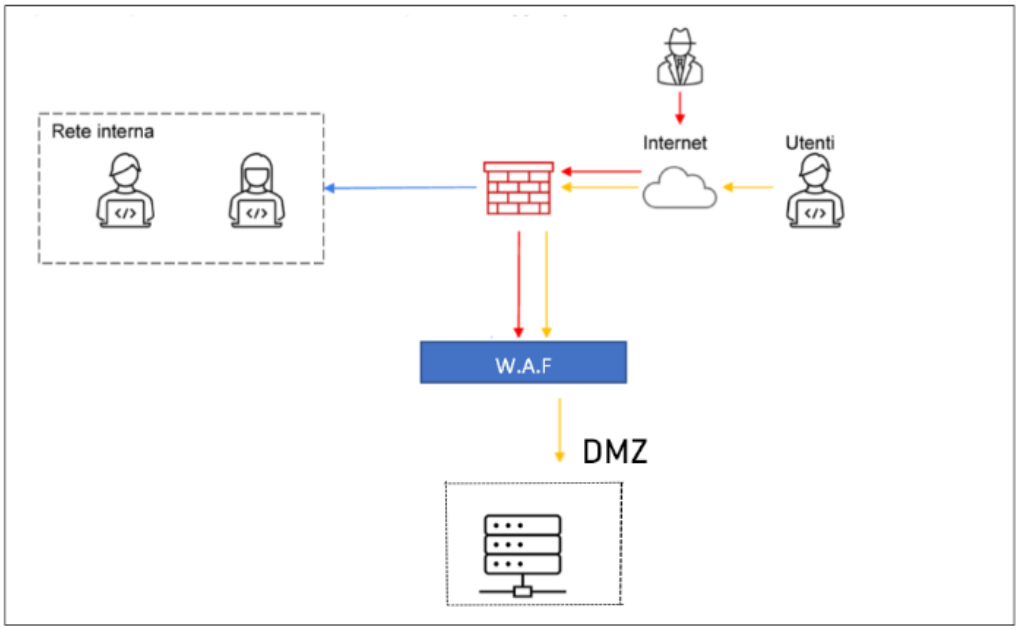
- Valutare l'acquisto di servizi di mitigazione DdoS da fornitori specializzati.

**3-) Modificazzione della figura  in modo da impedire  l'acesso da parte dell'attaccante alla rete interna.**




Per impedire all'attaccante di accedere alla rete interna abbiamo fatto un isolamente senza rimozione visto che non vogliamo rimuovere l'accesso all'attaccante al database. Per fare questo abbiamo tolto il flusso Applicazione che permeteva di connettere la basedati alla rete interna.

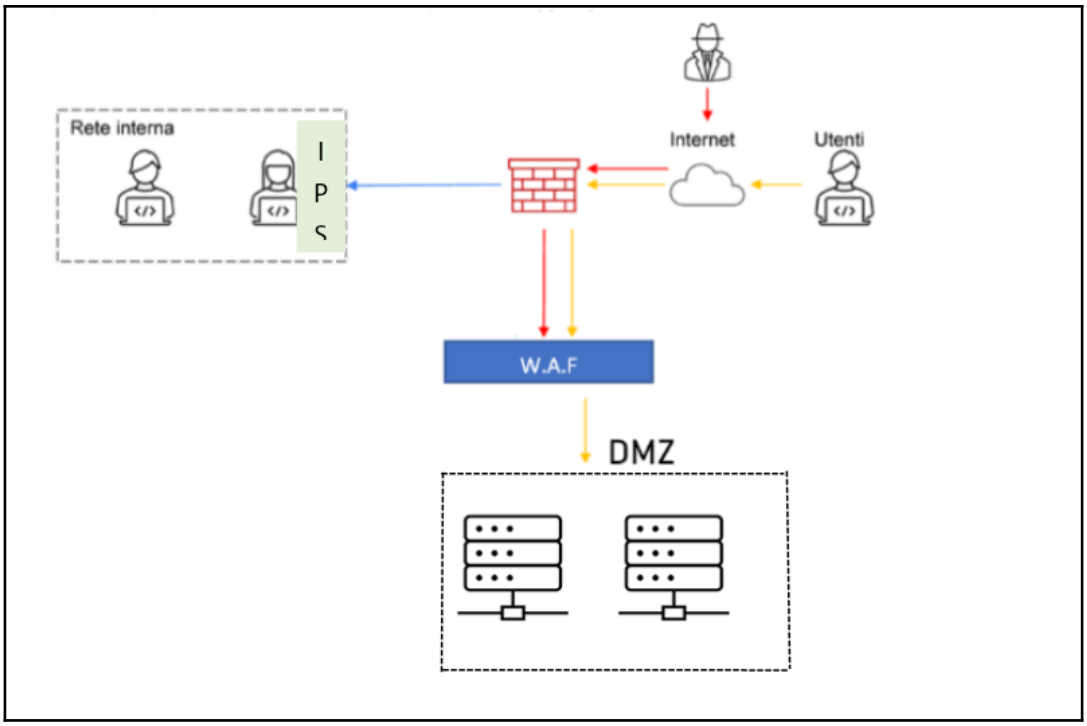
**4-) Unire i designi dell'azione preventiva e della response(1-3)**



# PROGETTO S9-L5

Qua abbiamo unito 1 e 3; abbiamo tolto il flusso di applicazione che permeteva di connettere la rete interna e il database. Avremo potuto lasciare il flusso di applicazione, visto che il WAF blocca gia l'attaccante ,ma per rispettare l'isolamento l'abbiamo tolto.

**5-) Modificazione dell'infrastruttura integrando altri elementi di sicurezza.**




Come altro elemento di sicurezza abbiamo inserito un IPS e un secondo database.

**IPS** in questo caso deve permettere di monitorare il traffico di rete in tempo reale e identificare e prevenire attività sospette o dannose che potrebbero costituire una minaccia per la sicurezza delle reti e dei sistemi informatici.

E il secondo database servirebbe di supporto se il principale ha un problema o se si rovina.

# PROGETTO S9-L5