# Incident response Plan

Nel nostro esercizio di oggi dovremmo condurre delle azioni preventive in caso di un attacco **SQLi** e **XSS** sulla nostra web app da parte in un attaccante, verificare l'impatto sul Business in caso di un attacco **DDoS** ed evitare la propagazione del **Malware** che ha infettato la nostra rete.

## Azioni Preventive

Per prevenire un attacco **SQLi** e **XSS** potremmo effettuare diverse tecniche di difesa:

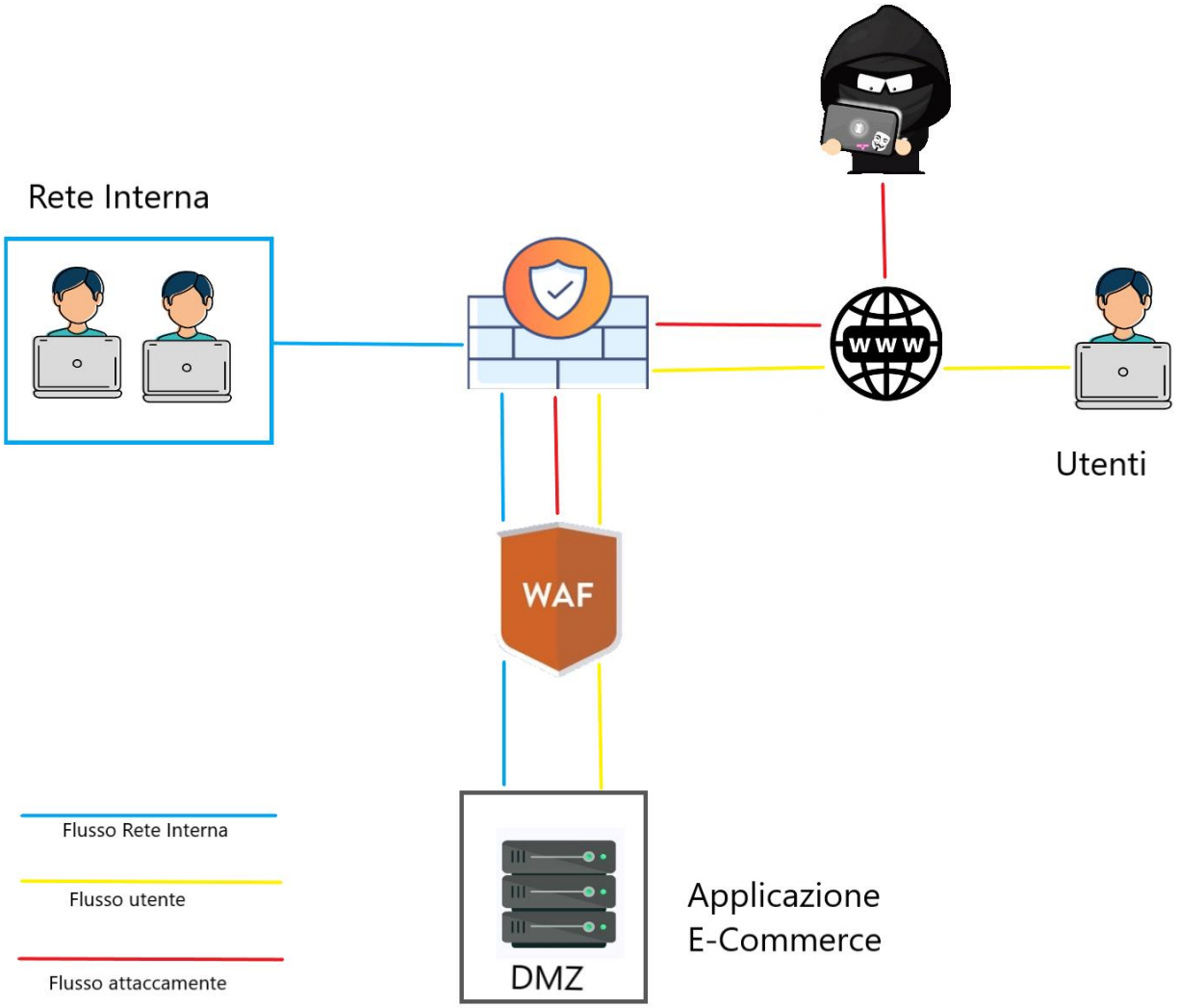
- **Web Application Firewall ( WAF )**

Il WAF viene posizionato a protezione delle nostre applicazioni web. Il dispositivo procederà, quindi, all'analisi del traffico HTTP/HTTPS, passante verso i nostri servizi web esposti sulla rete e attraverso l'utilizzo di firme apposite, di regole logiche e di whitelist/blacklist deciderà se tale traffico può essere ritenuto lecito o malevolo. Nel caso in cui il traffico risultasse malevolo, il WAF genererebbe un alert, a disposizione degli analisti, riportante le caratteristiche dell'attacco. Tale traffico malevolo, chiaramente, verrà bloccato. Il traffico normale, invece, verrebbe reindirizzato alla corretta applicazione web.

- **Blocco dei caratteri**

Questo permetterà di bloccare la modifica, come ad esempio la lunghezza, nei campi di dove viene richiesto di inserire un input. Modifiche che vengono usate per inserire stringhe malevoli.

Nell'immagine possiamo vedere come effettuare la nostra azione preventiva a protezione del nostro E-Commerce. Posizioneremo il **WAF** in modo che potrà analizzare e controllare il traffico dati prima di raggiungere la nostra Web App.




# Impatti sul Business

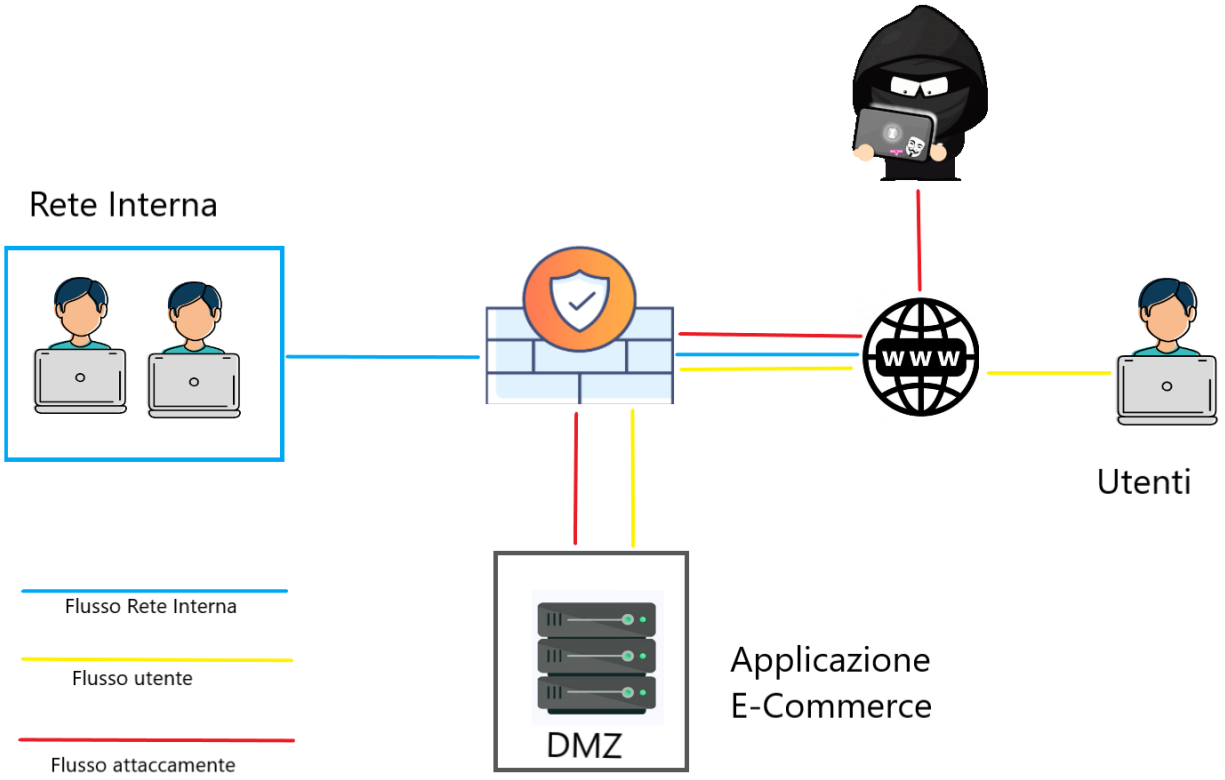
Nel caso la nostra Web Application subisse un attacco **D**istributed **D**enial **o**f **S**ervice ( DDoS ), consiste nel inviare moltissime richieste al Sito fino a renderlo irraggiungibile e quindi senza la possibilità di accedervi.

Questo attacco porterà l'azienda a non essere raggiungere per 10 minuti e tenendo in considerazione che il loro guadagno è di 1.500€  al minuto possiamo constatare che la perdita complessiva in quel lasso di tempo sarà di 15.000€

# Response

Dopo essere stati infettati da un Malware, abbiamo la priorità di far si che quest'ultimo non si propaghi all'interno della nostra rete.

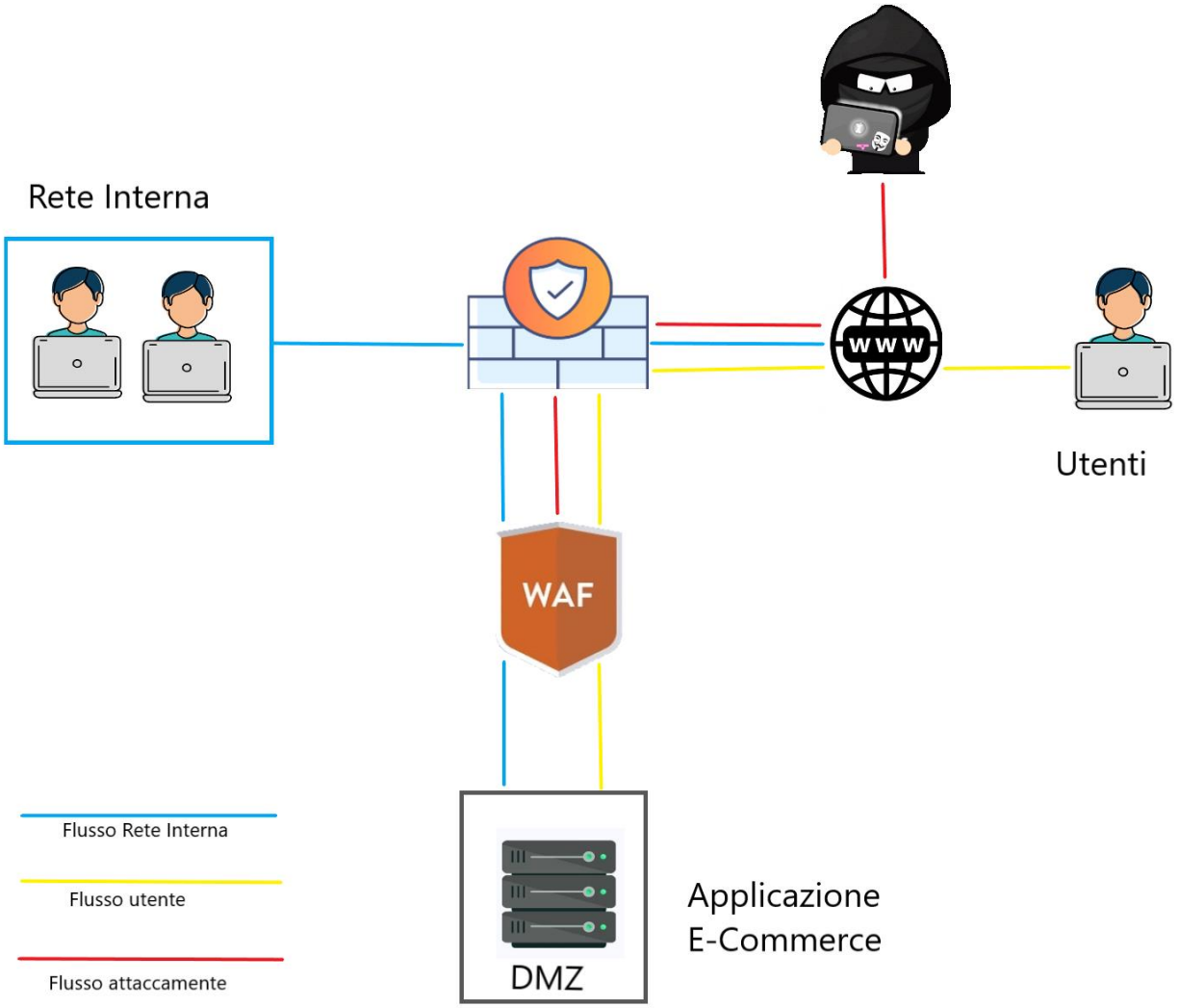
Possiamo utilizzare la tecnica dell'**Isolamento**, ovvero isoleremo la **Web Application** dalla nostra **Rete Interna**, modificando la configurazione del Firewall. In questo modo il nostro E-Commerce rimarrà online e usufruibile dagli utenti, essendo ormai la nostra Web Application infetta sarebbe inutile eliminarle la minaccia, anzi, in questo modo potremmo indagare sulle mosse del nostro attaccante.




# Soluzione Completa

La soluzione definitiva per la protezione della nostra Web Application è quello di inserire un WAF che bloccherà l'accesso all'utente malintenzionate, mentre la rete interna e gli utenti comuni potranno navigare

senza problemi




# Bonus:

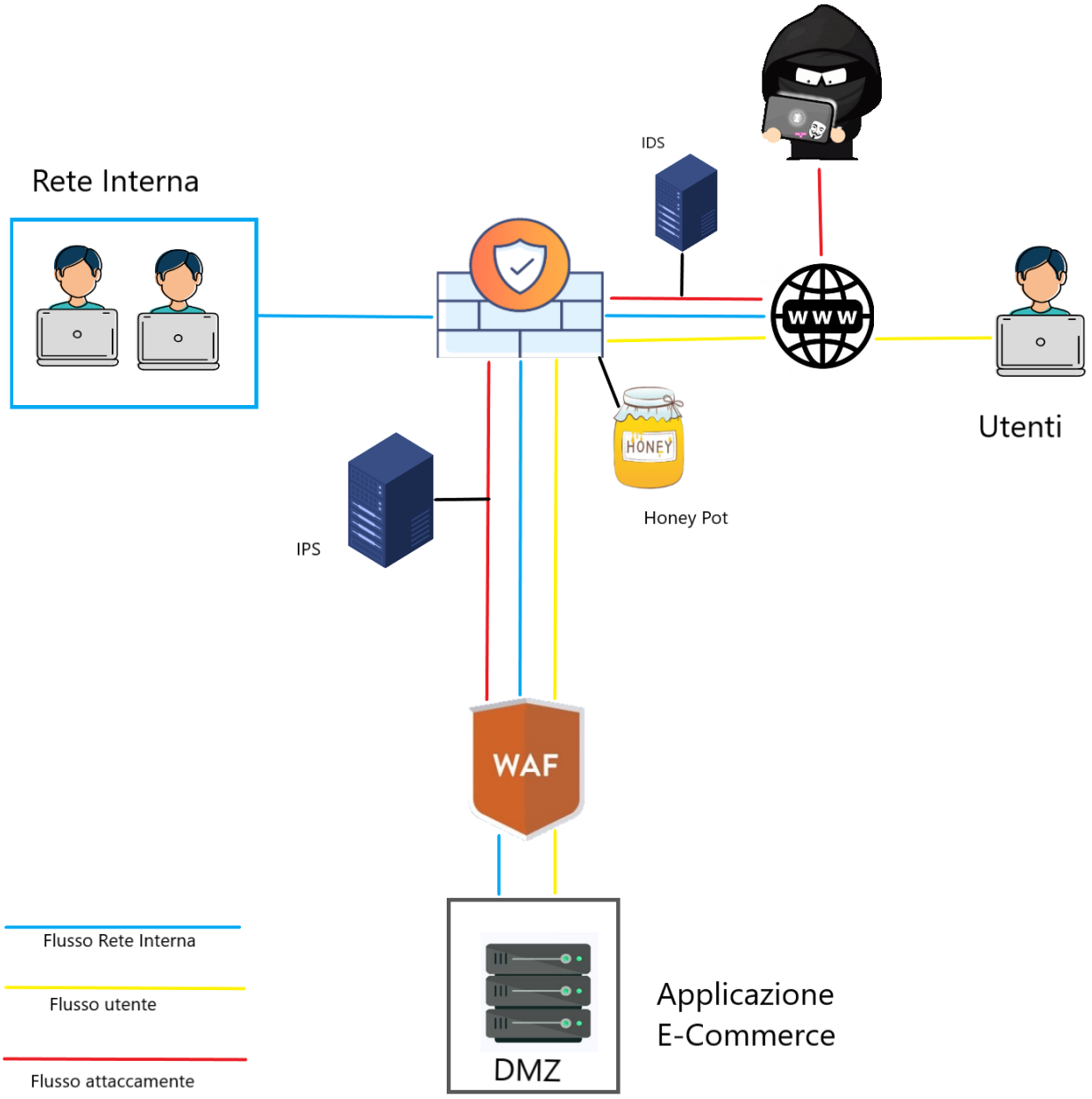
Potremmo implementare la nostra azione di protezione mettendo un **IDS** ( **I**ntrusion **D**etecion **S**ystem ) e un **IPS** ( **I**ntrusion **P**revention **S**ystem ), un **Honeypot, Patching** dei sistemi per aggiornare o migliorare la sicurezza , e creare delle strategie di Backup così da prevenire delle perdite considerevoli in caso di danni.

**IPS** : Sono dei componenti software attivi sviluppati per incrementare la sicurezza informatica di un sistema informatico, individuando, registrando le informazioni relative e tentando di segnalare e bloccare le attività dannose.

**IDS**: E' un sistema di rilevamento delle intrusioni è un dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali.

**HoneyPot**: Un sistema trappola o esca così da attirare verso questo l'attacco informatico

***Ricordiamoci che più sistemi controllato la rete più la latenza sarà maggiore.***


Rete Interna
IDS
WWW
Utenti
HONEY
Honey Pot
IPS
WAF
DMZ
Applicazione
E-Commerce
Flusso Rete Interna
Flusso utente
Flusso attaccamente