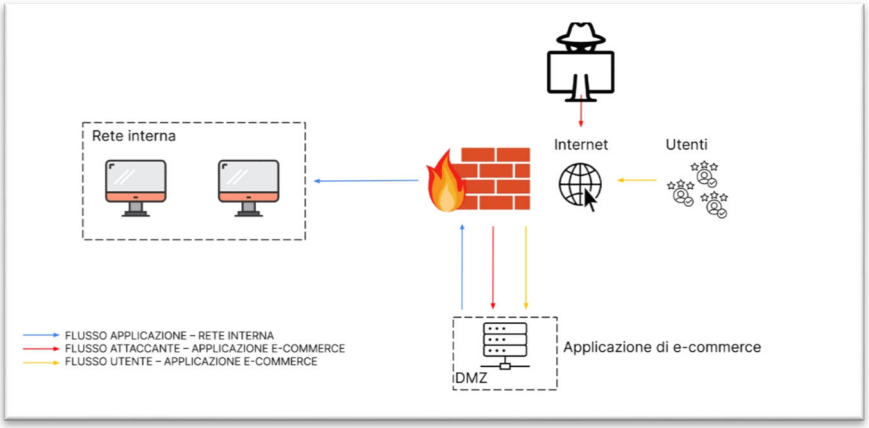
PROGETTO SETTIMANALE

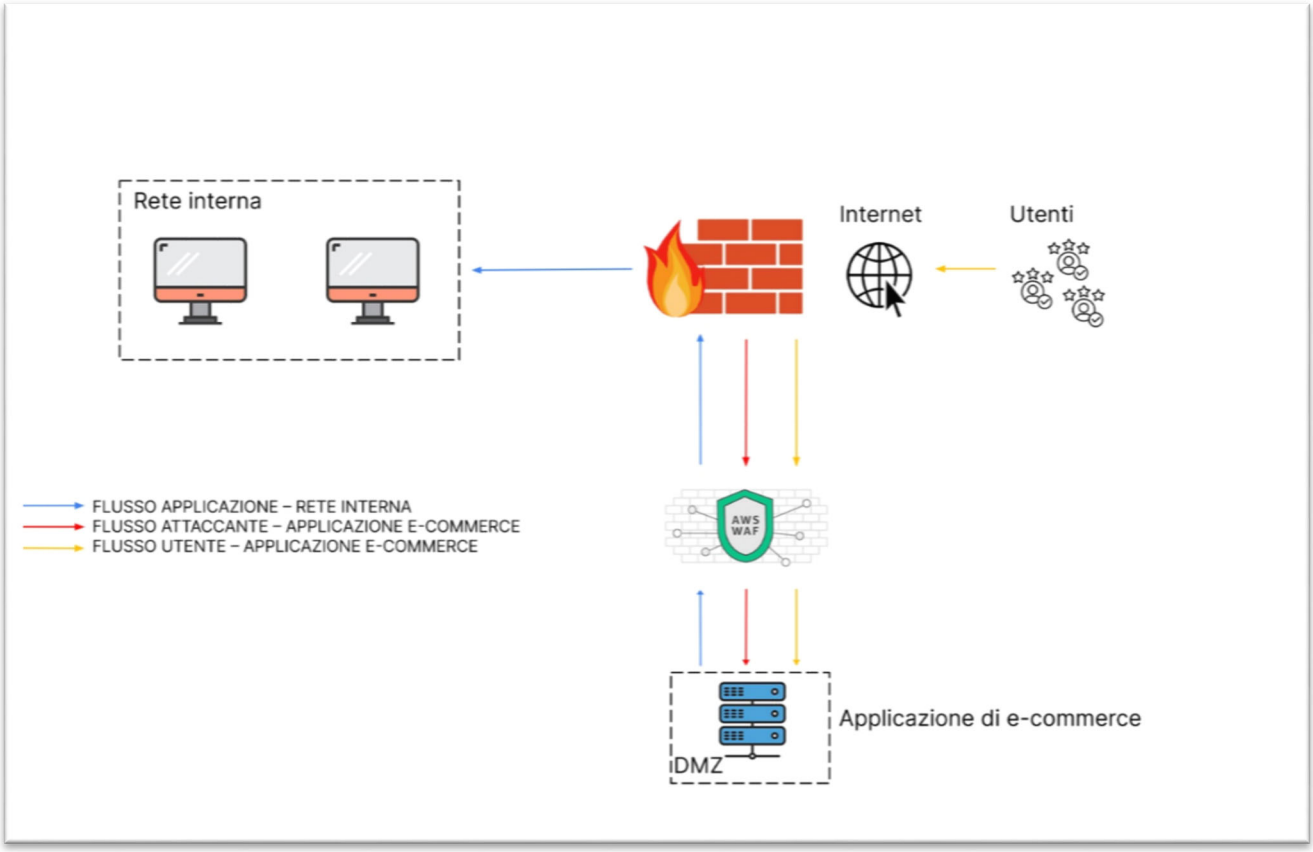
Il progetto di questa settimana consiste nella modifica e nell'implementazione di sicurezza di una web app.

- **AZIONI PREVENTIVE**
- **IMPATTI BUSINESS**
- **RESPONSE**



FASE 1 - AZIONI PREVENTIVE

Nella prima fase abbiamo effettuato delle azioni preventive sulla nostra web app di e-commerce. Per poter prevenire un futuro attacco di tipo SQLi e XSS da parte di un utente malintenzionato, abbiamo apportato delle modifiche alla nostra rete di riferimento



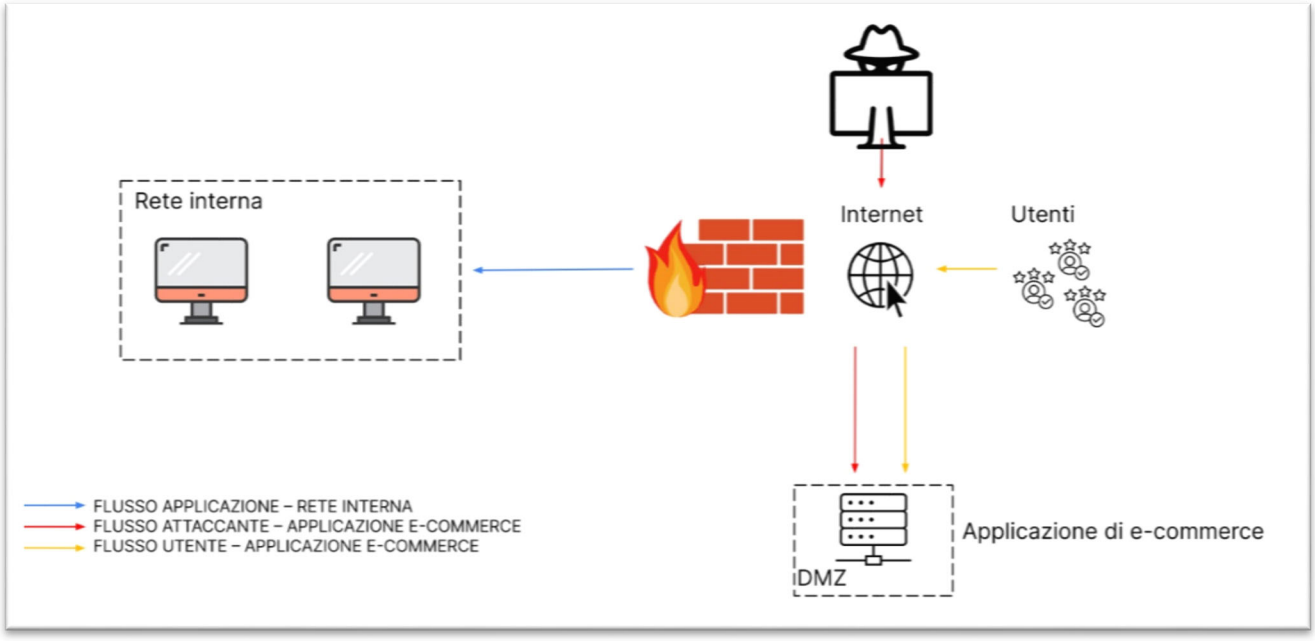
WAF (web app firewall): è una forma specifica di firewall applicativo che filtra, monitora e blocca il traffico HTTP da e verso un servizio web. Ispezionando il traffico HTTP, può prevenire gli attacchi che sfruttano le vulnerabilità note di un'applicazione web, come SQL injection, cross-site scripting (XSS), inclusione di file e configurazione impropria del sistema

FASE 2 - IMPATTI BUSINESS

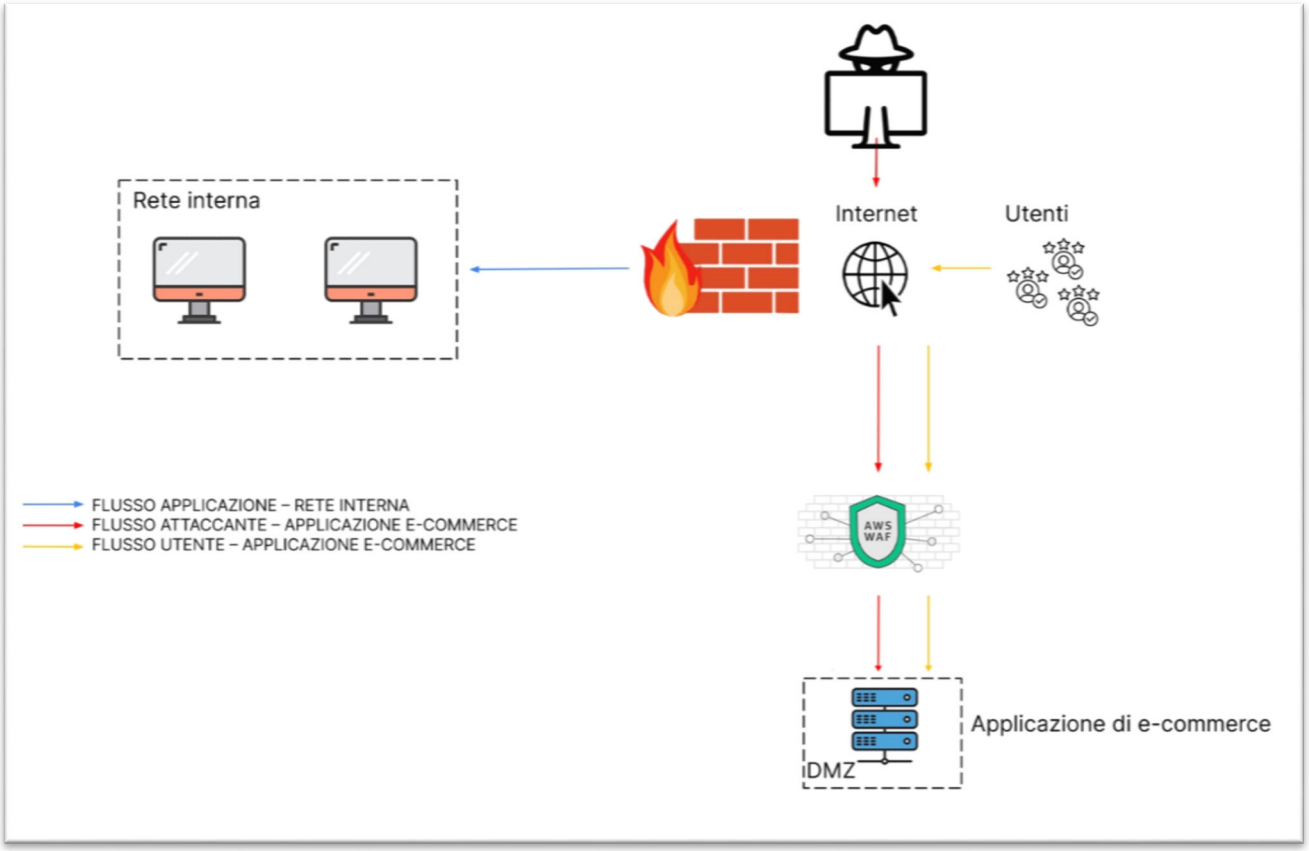
Nella seconda fase invece abbiamo calcolato l'impatto negativo sul nostro business dovuto ad un attacco Ddos. Questo attacco ci ha reso irraggiungibili per 10 minuti. Considerando la nostra perdita è di 1.500 € al minuto, il totale sarebbe du 15.000 € (basta moltiplicare la nostra perdita per i minuti in cui eravamo irragiungibili)

FASE 3 – RESPONSE

Nella terza fase l'applcazione web viene infettata da un malware da parte di un malintenzzionato esterno. Considerando che la nostra priorità è quella di mantenere la web app attiva per i clienti abbiamo adottato il metodo dell'**isolamento.** L'isolamento consiste nel tenere la macchina scollegata dalla rete interna ma sempre collegata verso internet. In questo modo noi possiamo comunque mantenere il servizio attivo e monitorare l'attacco (monitoraggio passivo). Facendo cosi riusciamo evitare che il malware si propaghi anche all'inteno della nostra rete (rete interna).



FASE 4 - SOLUZIONE COMPLETA



BONUS – MODIFICA DELL'INFRASTRUTTURA

Qui possiamo notare delle modifiche apportate alla infrastruttura. Abbiamo aggiunto al nostro WAF anche un 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. Rappresentano un'estensione dei sistema di rilevamento delle intrusioni "*intrusion detection system*, IDS" perché entrambi controllano il traffico e le attività di sistema per identificare l'esecuzione di codice non previsto). Un secondo nodo nella zona DMZ, in modo che se dovesse capitare un altro incidente, il secondo nodo potrebbe continuare a mantenere il servizio mentre il primo nodo viene analizzato. Infine per poter rendere ancora più sicura la rete interna è stato aggiunto un firewall perimetrale, posto sul confine di una rete in modo da filtrare tutto il traffico che questa scambia con l'esterno.