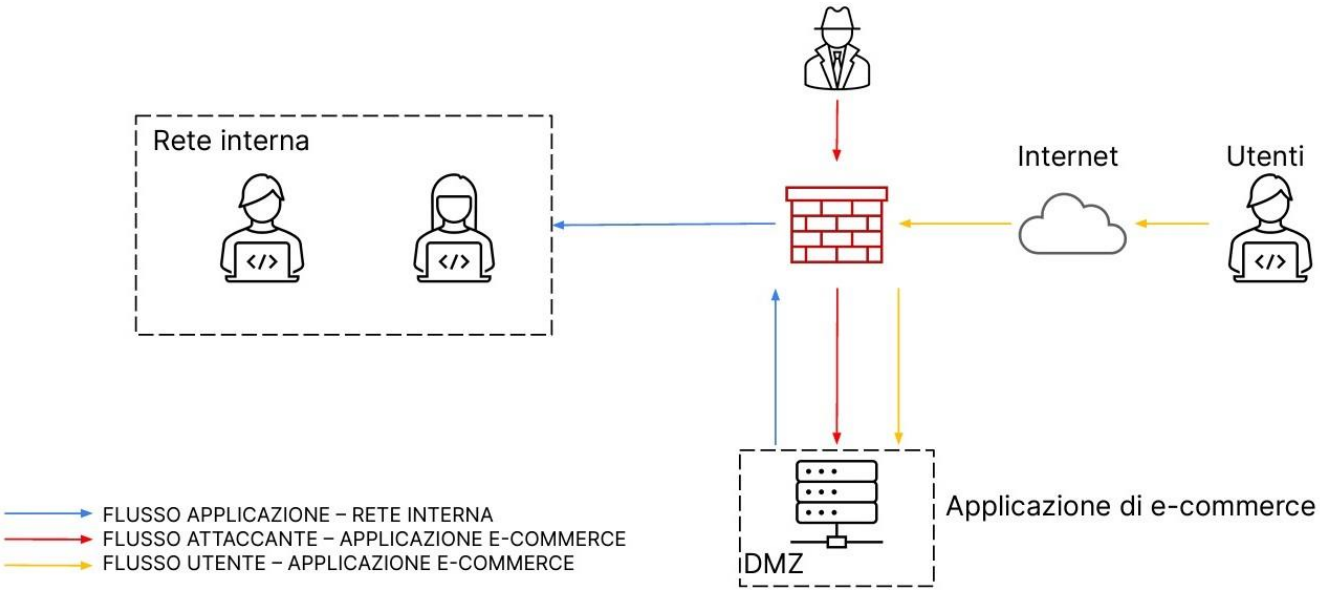
Progetto S9/L5

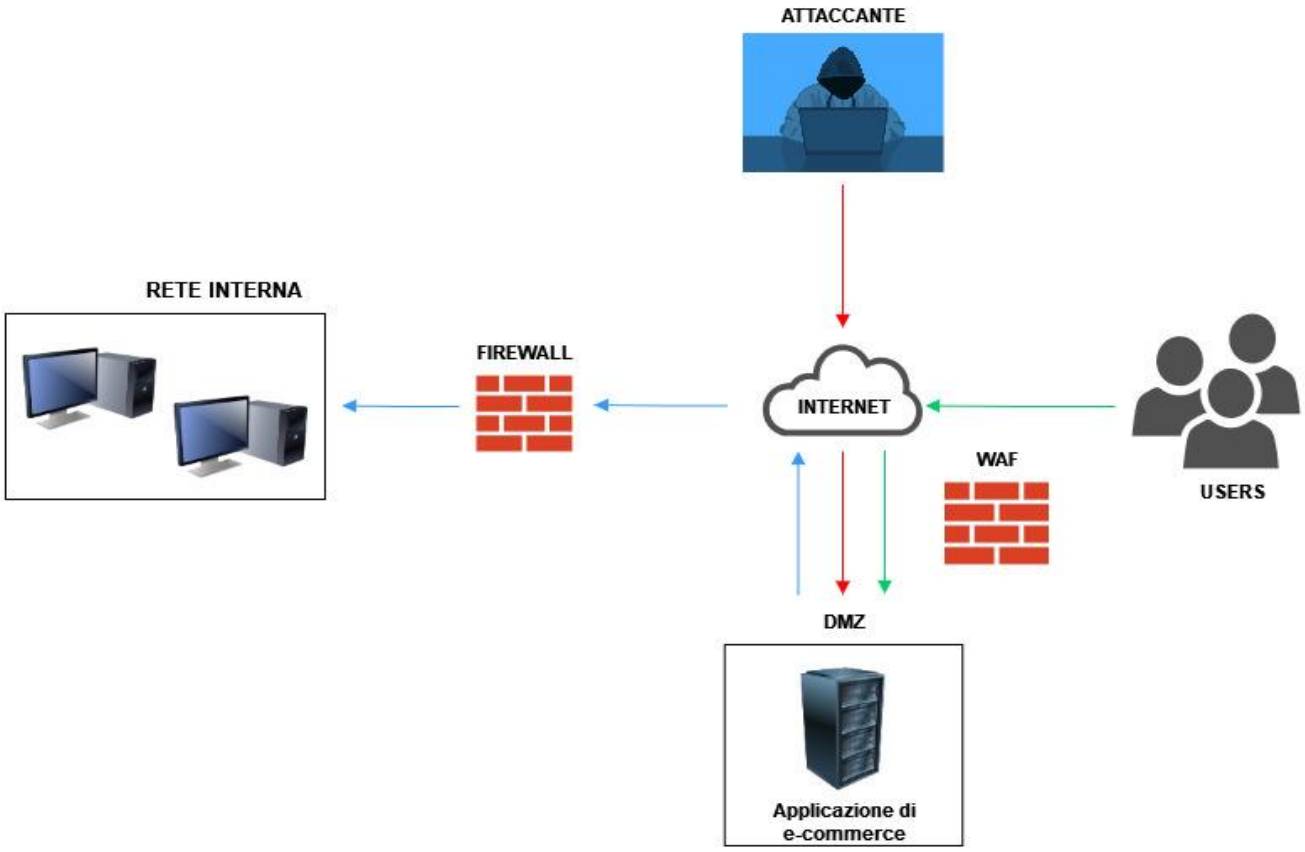
Per questo progetto ci viene richiesto di:

- Attuare azioni preventive per difendere una Web Application da attacchi di tipo SQLi o XSS
- Calcolare l'impatto sul business sulla base dei dati forniti nel progetto
- Ridurre gli impatti a seguito dell'infezione di un Malware sulla Web Application

Architettura di rete



Quesito 1



Come possiamo vedere dall'immagine la prima azione preventiva che va presa in considerazione è l'inserimento del WAF (Web Application Firewall), ulteriore sistema di difesa oltre al Firewall, che va a "difendere" tutta l'area da eventuali attacchi. Il WAF ha, infatti, la funzione aggiuntiva di leggere il contenuto dei pacchetti per stabilire se tale contenuto è malevolo oppure no ed eventualmente bloccarne l'ingresso.
Altre azioni sono:

- limitare l'accesso alla DMZ solo ai clienti autorizzati
- monitorare costantemente il traffico in entrata e in uscita della DMZ per individuare eventuali anomalie
- mantenere i server e le applicazioni sempre aggiornati
- eseguire regolarmente il backup dei dati in modo che, in caso di attacco, siano comunque al sicuro
- eseguire test di sicurezza

Per quanto riguarda la prevenzione sugli attacchi SQLi, che rappresentano una seria minaccia alla sicurezza dei database, è consigliato:

- non accettare script in input e quindi sanare sempre i dati inseriti
- assicurarsi che i dati inseriti dagli utenti rispettino i criteri di validità
- mantenere il software del database e delle applicazioni costantemente aggiornato per usufruire delle correzioni di sicurezza più recenti
- utilizzare procedure di monitoraggio che, osservando prestazioni, stato e integrità di un sistema, vanno appunto a monitorare eventuali attività sospette o a rilevare potenziali minacce
- condurre regolarmente test di sicurezza e penetration testing sulle applicazioni per individuare eventuali vulnerabilità prima che possano essere sfruttate

Per la prevenzione sugli attacchi XSS è consigliato:

- Accettare solo dati che rispettino i criteri di validità previsti, filtrare, dunque, ogni input che sembri sospeto o non valido
- Mantenere aggiornato il software, compreso il sistema operativo, il server web, il framework e le librerie utilizzate. Come già detto le versioni più recenti spesso includono correzioni di sicurezza.
- Effettuare scansioni automatiche per identificare potenziali vulnerabilità XSS nel codice sorgente delle applicazioni

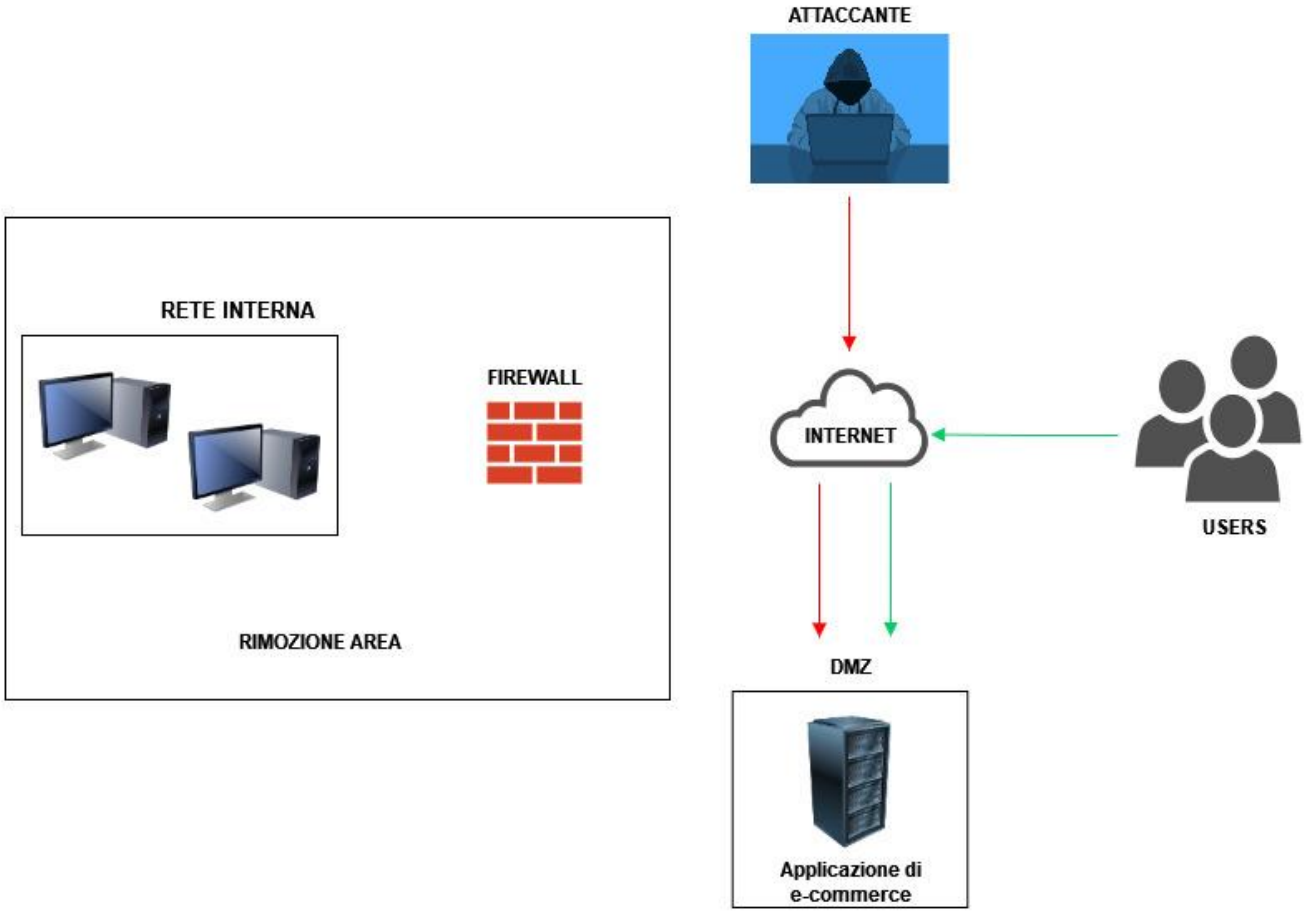
Quesito 2

L'applicazione non è raggiungibile per 10 minuti. Calcolando che l'impatto sul business è di 1.500 euro ogni minuto, il danno subito sarà di **15.000 euro**. Ovviamente, considerando un impatto di 1.500 euro al minuto, l'azienda in questione ha un fatturato elevato, dunque il danno sembra essere limitato.

Azioni preventive che si possono adottare:

- Utilizzare un firewall DDoS può aiutare a rilevare e mitigare gli attacchi DDoS in tempo reale
- Effettuare test di sicurezza regolari per individuare eventuali vulnerabilità nelle web app
- Pianificare la continuità del servizio in caso di un attacco DDoS, ad esempio utilizzando server di backup
- Aggiornare regolarmente i software
- Monitorare costantemente il traffico in ingresso e in uscita delle web app

Quesito 3



Essendoci stata una infezione da Malware la nostra priorità è quella che lo stesso non si propaghi sulla nostra rete. Pertanto la soluzione migliore per evitarlo è la **RIMOZIONE** dell'intera rete interna da tutto il resto. La rimozione del sistema infetto consiste nello staccare i cavi, il dispositivo (o, in questo caso l'area) sarà isolato totalmente, sia dagli altri dispositivi che dalla rete internet. Questa soluzione si attua in situazioni particolarmente problematiche, è utilizzata soprattutto quando si tratta di proteggere dati sensibili o critici (o, nel nostro caso, per evitare che il Malware si propaghi all'intera rete). Viene chiamata air gap, cioè una misura di sicurezza che implica la separazione fisica tra due sistemi informatici o reti

Facciamo presente che in questo modo gli utenti prenderanno il Malware, cosa che potrebbe provocare anche una cattiva pubblicità all'azienda stessa.