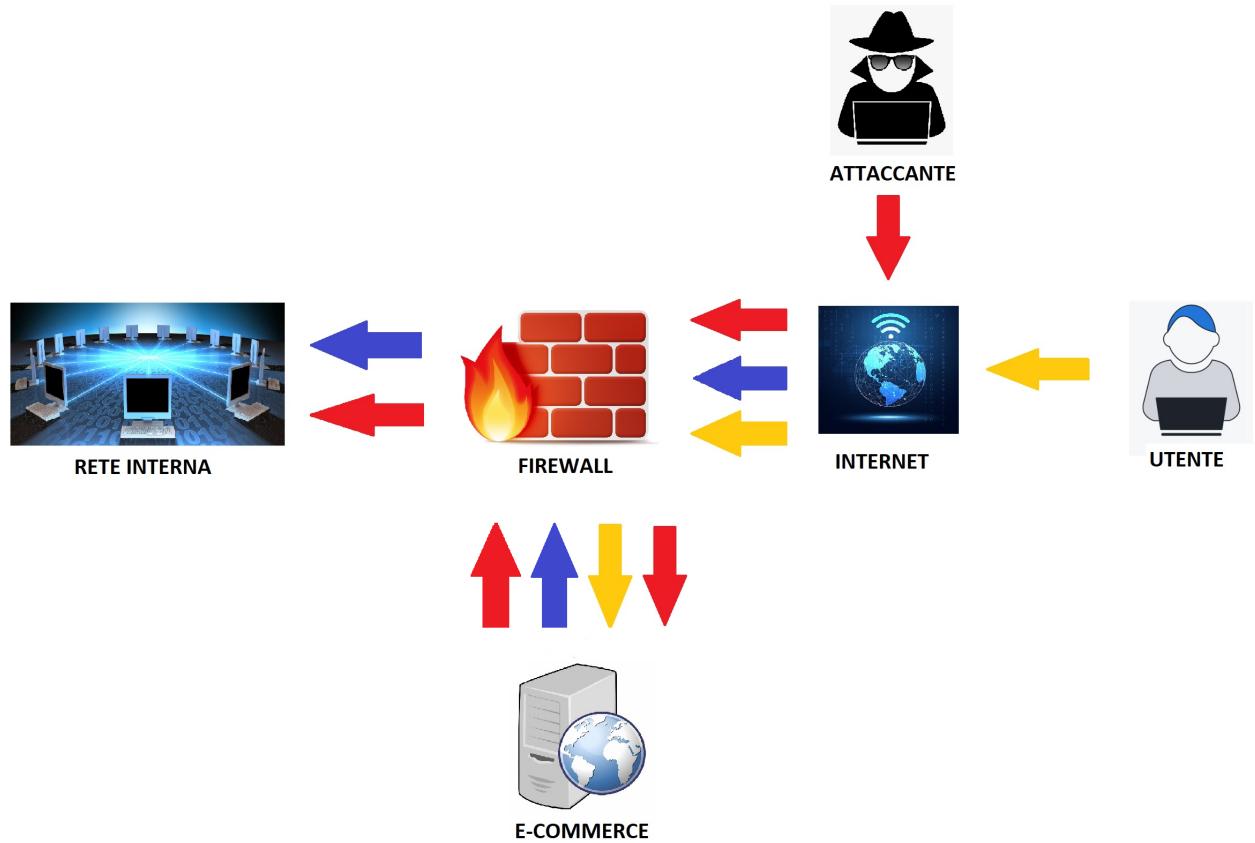


Progetto Week 9 - SOC

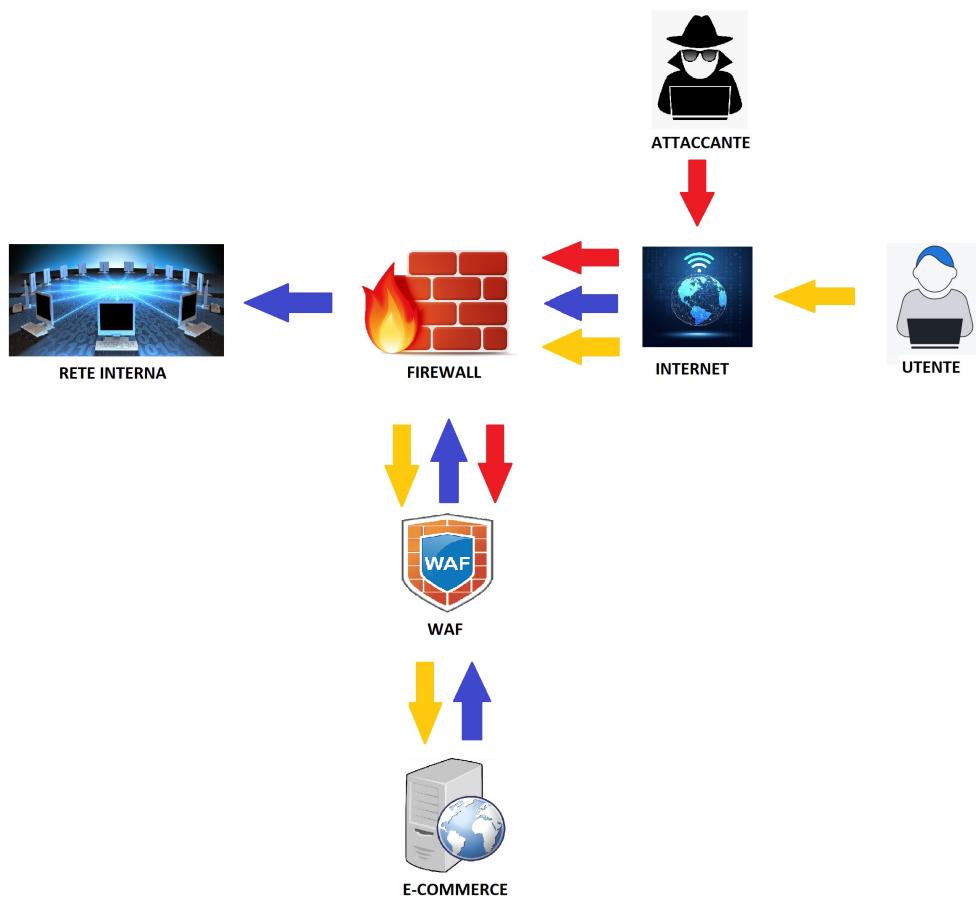
Dall'architettura di rete in figura si evince che:

- gli utenti possono collegarsi alla piattaforma e-commerce;
- Un attaccante non può accedere direttamente alla rete interna perché bloccato dal firewall, ma può entrare nella piattaforma, compromettere il server e passare dall'area DMZ (dove c'è l'applicazione web) alla rete interna.



1- Azioni preventive per difendere l'app web da attacchi SQLi o XSS

L'implementazione di un **firewall applicativo (WAF)** può aiutare a mitigare il rischio di attacchi di tipo SQL injection o XSS sull'applicazione web e-commerce presente nella DMZ. Il WAF analizza il traffico HTTP in entrata e in uscita per identificare eventuali attacchi web e bloccarli prima che raggiungano l'applicazione web, motivo per cui va collocato tra l'utente esterno e l'applicazione web e-commerce.



Un WAF non è una soluzione completa e dovrebbe essere integrato con altre misure di sicurezza:

Gestione rigorosa degli accessi: tramite l'utilizzo di password complesse, autenticazione a due fattori, certificati digitali o altri meccanismi di autenticazione. Inoltre, è importante definire chiaramente i diritti di accesso per ogni utente, in modo che ciascuno possa accedere solo alle risorse a cui ha diritto.

Validazione dei dati in ingresso: si riferisce alla verifica che i dati inseriti dagli utenti siano validi e conformi alle aspettative. Ad esempio, quando un utente inserisce dei dati, è importante verificare che gli stessi siano del tipo e della lunghezza corretti e che non contengano caratteri sospetti o pericolosi, come codici SQL o script dannosi.

2- Calcolo dell'impatto sul business nel caso in cui l'app subisse un DDoS

Sapendo, dai dati della traccia, che:

- per 10 minuti il servizio non sarebbe disponibile
- ogni minuto gli utenti spendono in media 1500 €

Ricaviamo facilmente l'informazione che ogni qual volta si verifichi una fattispecie del genere, l'azienda perderebbe circa 15000 € in 10 minuti.

$$10 \text{ min} * 1500 \text{ €} = 15000 \text{ €}$$

La soluzione più efficace è senz'altro quella di utilizzare un **firewall dotato di un servizio di mitigazione DDoS** in grado di identificare e bloccare il traffico DDoS prima che raggiunga il sito web. Ad esempio **Cloudflare** agisce come intermediario tra il sito web e i suoi visitatori, filtrando il traffico in ingresso e bloccando le minacce di sicurezza, tra cui gli attacchi DDoS.

Inoltre sarà opportuno predisporre delle azioni preventive, volte ad aumentare il livello di sicurezza:

- **Effettuare controlli regolari sugli end point, ovvero:** assicurarsi di avere configurazioni corrette dei sistemi e policy giuste sui firewall; effettuare i processi di patch management, per mantenere aggiornati tutti i sistemi; effettuare pen-test per implementare le remediation action con il supporto di tool adeguati.
- **Incrementare l'attività di monitoring dei log** (file che tracciano gli eventi e contengono informazioni sulle attività che un utente svolge su un sistema). Tale operazione sarebbe facilitata se si utilizzasse un **SIEM** (tool che possono accentrare, analizzare i log e configurare gli alert automaticamente)
- **Configurare il firewall in modo corretto**, ovvero in modo tale da limitare il traffico in ingresso alle sole porte necessarie per il sito web e-commerce. In questo modo, il traffico non necessario viene bloccato, riducendo il rischio di attacchi DDoS. Ad esempio, configurando correttamente il WAF, già proposto come soluzione nel 1° quesito, sarà molto più difficile subire attacchi DDos.

E' altresì fondamentale, viste le cifre economiche in ballo, predisporre azioni, volte a perseguire la continuità operativa e che possano tornare utili anche in caso di altri disastri, qualsiasi sia la loro natura:

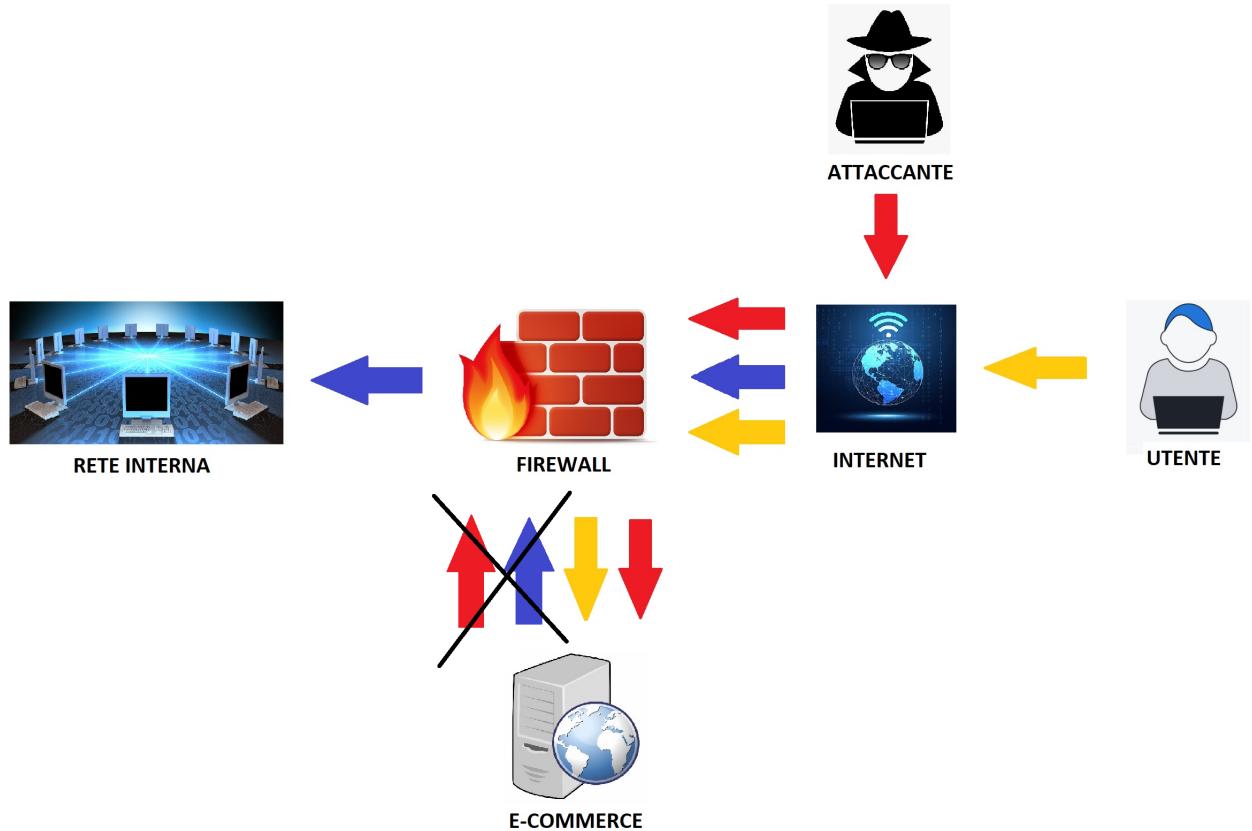
- **Effettuare spesso Backup:** è importante avere un sistema di backup dei dati e dei server, in modo da poter ripristinare la situazione in caso di attacco DDoS.
- **Eliminare SPOF** (Single Point of Failure) per aumentare la resilienza dei sistemi

3- Response nel caso in cui l'app web venga infettata da un malware

Più precisamente ci è chiesto di evitare che il malware si propaghi sulla rete, permettendo all'attaccante di continuare ad accedere alla macchina infettata.

La soluzione consigliabile è quella di **contenimento, isolando l'app web**, ovvero disconnettendola completamente.

Data l'architettura di rete, ci si può limitare a **configurare il firewall in modo corretto**, ovvero creando una policy che impedisca il traffico in uscita.



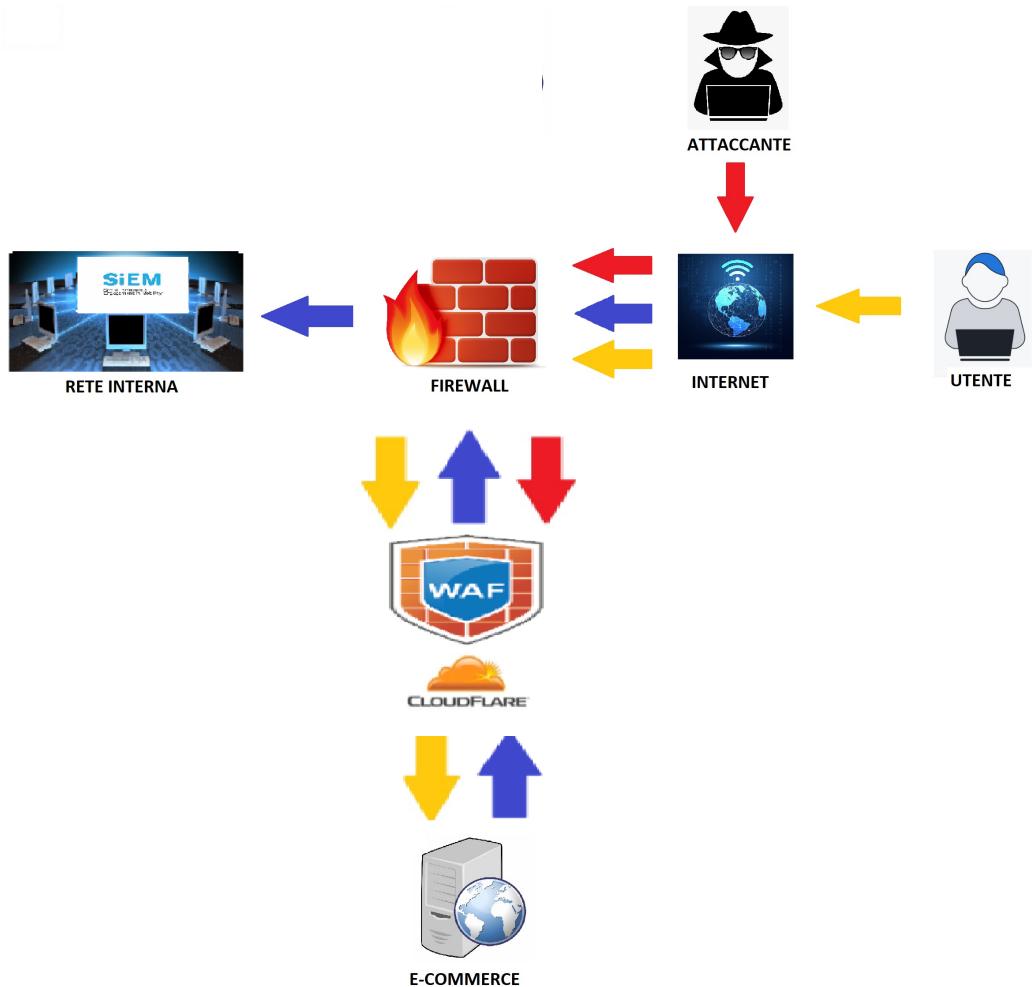
4 - Soluzione completa

Mettendo insieme i pezzi, per implementare una soluzione basilare ed economica, sarà sufficiente acquistare un firewall WAF

SPESE:

I prezzi di questi firewall possono variare da poche centinaia a diverse migliaia di euro al mese, a seconda della complessità del progetto e del livello di supporto richiesto. Il consiglio ricade su Cloudflare con un abbonamento business o enterprise. Con circa **170 €/mese** si può dunque mettere in sicurezza la rete.

Free	Pro	Business	Enterprise
Per progetti personali o per hobby che non sono business-critical.	Per siti Web professionali che non sono business-critical.	Per le piccole imprese che operano online.	Per applicazioni mission-critical fondamentali per la tua attività.
\$ 0 / mese	\$ 20 / mese	\$ 200 / mese	Personalizzato
Fatturazione mensile dei componenti aggiuntivi	fatturati \$ 240 all'anno o \$ 25/mese fatturati mensilmente	fatturati \$ 2.400 all'anno o \$ 250/mese fatturati mensilmente	Fatturazione annuale



5 - Modifica "più aggressiva" dell'infrastruttura

Ulteriori migliorie dell'infrastruttura di rete, in definitiva, possono essere le seguenti:

- **Utilizzare un honeypot** può essere una soluzione efficace per trarre in inganno eventuali attaccanti e rilevare eventuali intrusioni. Ciò permetterebbe agli amministratori di avere informazioni sulla tipologia e sull'origine degli attacchi.

SPESE:

Per un server honeypot di alta qualità, si può considerare l'acquisto di un VPS (Virtual Private Server), che costa 100 € al mese

Per una soluzione di medio-alto livello, propongo il Raspberry Pi 4 Modello B, uno dei modelli più recenti e potenti, il cui prezzo varia da 45 a 75 €/mese, a seconda della quantità di memoria RAM e dello spazio di archiviazione.

Consiglio momentaneamente di provare con un modello precedente, come il Raspberry Pi 3 Modello B+, che offre prestazioni più che accettabili all'accessibilissimo prezzo di **35 €/mese**.

- **Aumentare la ridondanza dei server con un failover cluster**, al fine di garantire la continuità operativa, ad esempio, durante un attacco DDoS. Un failover cluster è un gruppo di server che lavorano insieme per garantire l'alta disponibilità dei servizi, in modo che se un server viene compromesso, l'altro server può sostituirlo.

SPESE:

In generale, i costi per un failover cluster possono variare notevolmente (da qualche centinaio a diverse migliaia di €/mese) a seconda delle funzionalità desiderate.

I fornitori di hosting di alta qualità sono OVH, Hetzner e DigitalOcean.

Ad esempio, un server dedicato di fascia alta come l'Intel Xeon E5-2630 v4 con 64GB di RAM e 2TB di spazio di archiviazione di Hetzner può costare circa **300-400 €/ mese**, mentre un server simile presso OVH può costare circa 500-600 €/mese.

- **Utilizzare un load balancer**, dotato di due porte di WAN per collegare due provider diversi e una lan, a cui si legherà il firewall. E' opportuno, ovviamente, che ci siano due router, ciascuno con il proprio accesso WAN, per connettersi a due diversi provider di servizi Internet e dotate di IP pubblico per fornire accesso agli utenti. Questa soluzione permetterebbe di separare il traffico in due reti distinte e, al contempo, fornire ridondanza in caso di guasto di una delle due connessioni.

SPESE:

Il costo di un router può variare a seconda della marca, del modello e delle funzionalità desiderate. Ad esempio, un router di fascia media può costare circa **50-100 €**, mentre un router di fascia alta può costare oltre 200 euro.

L'abbonamento a un provider di rete può variare a seconda del provider, ma il range è sicuramente compreso tra i 20 € e i **50 €/ mese**.

Un load balancer hardware può costare da centinaia a migliaia di euro, a seconda delle specifiche. Sul costo dello stesso bisognerà anche considerare il supporto tecnico e la manutenzione. In generale, in vista della funzione, non calcolerei una spesa inferiore ai **200 €/ mese**.

Qualora vengano implementate tutte le misure proposte, i costi per le migliori nell'architettura di rete ammonterebbero a un **totale di circa 800 €/mese**. Sommando questa spesa a quella del WAF possiamo preventivare una **spesa complessiva di circa 1000 €/ mese**.

