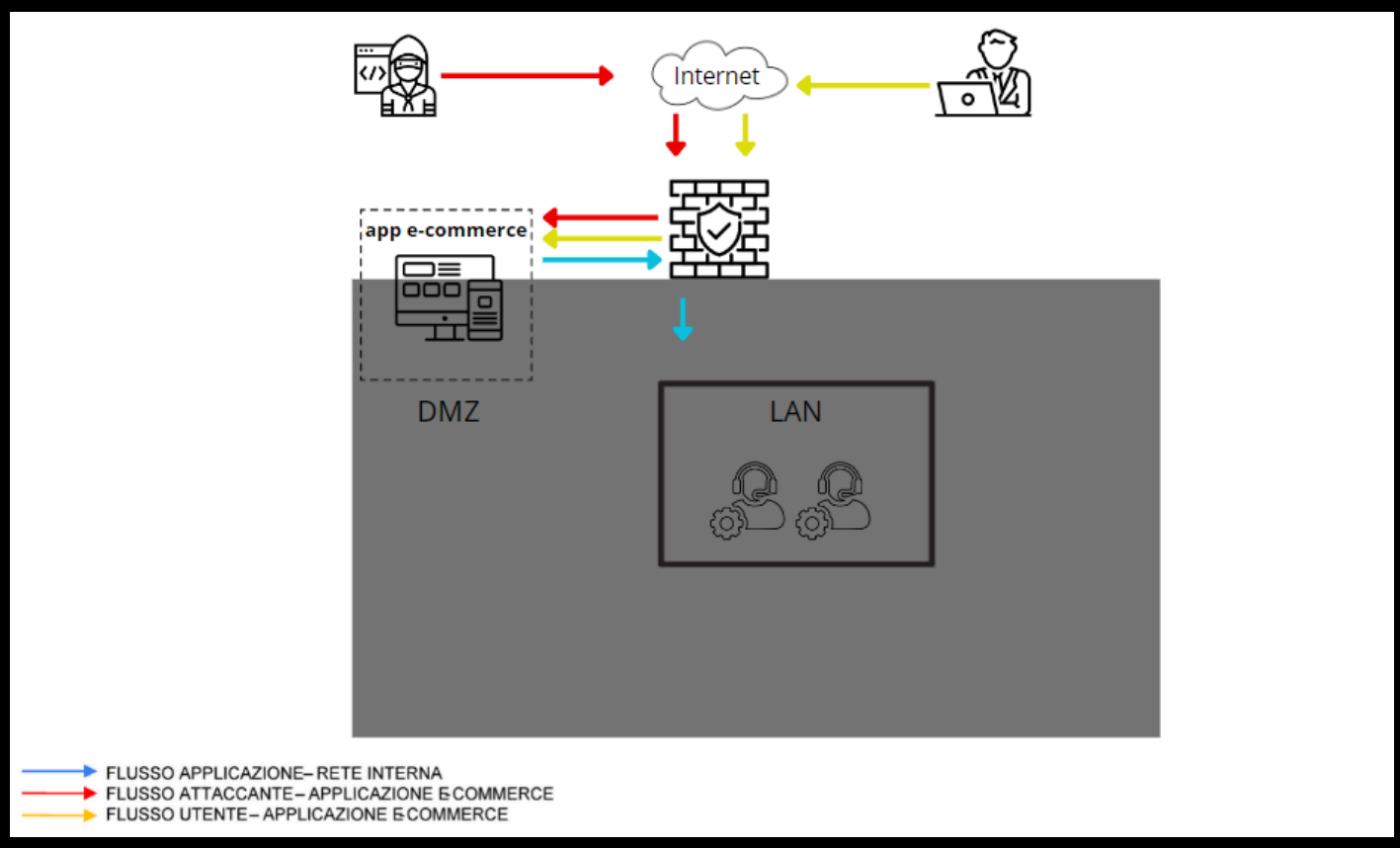
Security Operation

Richiesta: Effettuare delle operazioni di sicurezza.



Sulla base di questa architettura di rete, rispondere ai seguenti quesiti:

1. Prevenzione: Quali misure adottare per proteggere una web app da SQLi e XSS?

2. Impatto economico: : L' applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. Risposta al malware: Come isolare un'app infetta per prevenire la diffusione del malware senza interrompere l'accesso?

4. Soluzione integrata: Unire le soluzioni di preventive e di response dei punti 1 e 3.

5. Miglioramento aggressivo: Quali miglioramenti infrastrutturali implementare con un budget di 7.000€?

1. Azioni preventive
Effettuiamo azioni preventive per prevenire i seguenti attacchi:

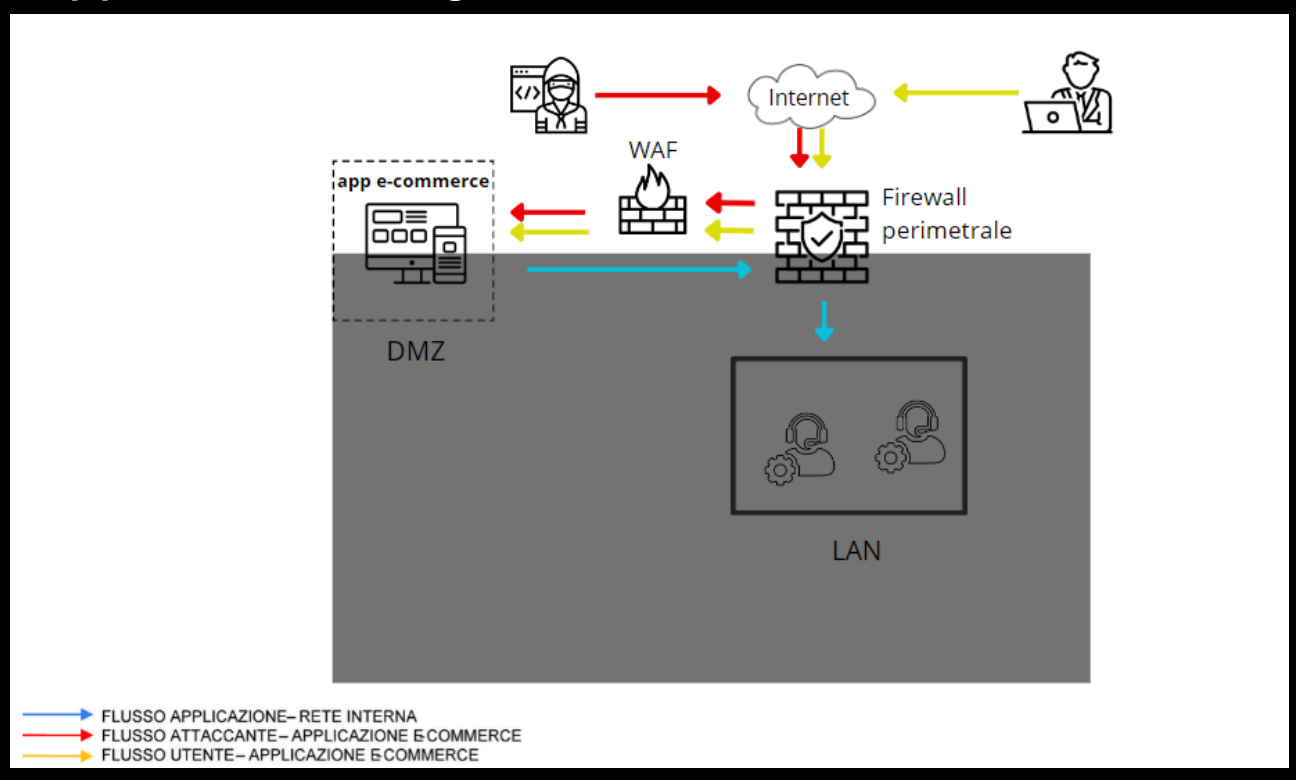
SQLi: Questo attacco (SQL injection) può permettere all'aggressore di visualizzare dati che altrimenti sarebbero stati protetti, come informazioni sugli utenti o altri dati riservati, inserendo attraverso un campo input delle query malevole.

XSS: Il Cross-Site Scripting è un attacco che sfrutta la vulnerabilità di un'applicazione web nell'elaborare input non fidati.

Prevenzione SQLi

1. Validazione dell'Input: Assicurarsi che tutti gli input forniti dagli utenti siano validati lato server per tipo, lunghezza, formato e range.
2. WAF: Si implementa un Web Application Firewall che possa bloccare e rilevare SQLi.

Rappresentazione grafica:



Prevenzione XSS

1. Aggiornamento e Patching: Mantieni il software aggiornato con le ultime patch di sicurezza.
2. Validazione input e WAF: Così come l'SQLi, anche questo attacco può essere contrastato con l'utilizzo di queste pratiche, come la configurazione di un Web Application Firewall che blocchi tentativi di XSS e la modifica del codice che prevede la sanitizzazione dell'input.

Impatti sul business

Durante l’attacco di DDoS si sono perse entrate pari a 15’000$

Impatto economico = Guadagno medio al minuto x Durata dell'attacco
Quindi:
Impatto economico = 1.500€/minuto x 10 minuti = 15.000€

Per mitigare gli attacchi DDoS, è importante adottare una serie di strategie preventive come:

1. Server di bilanciamento: Utilizzare più server in modo da bilanciare il carico delle richieste, in caso di attacco, il traffico può essere reindirizzato o bilanciato tra diversi nodi per evitare sovraccarichi.

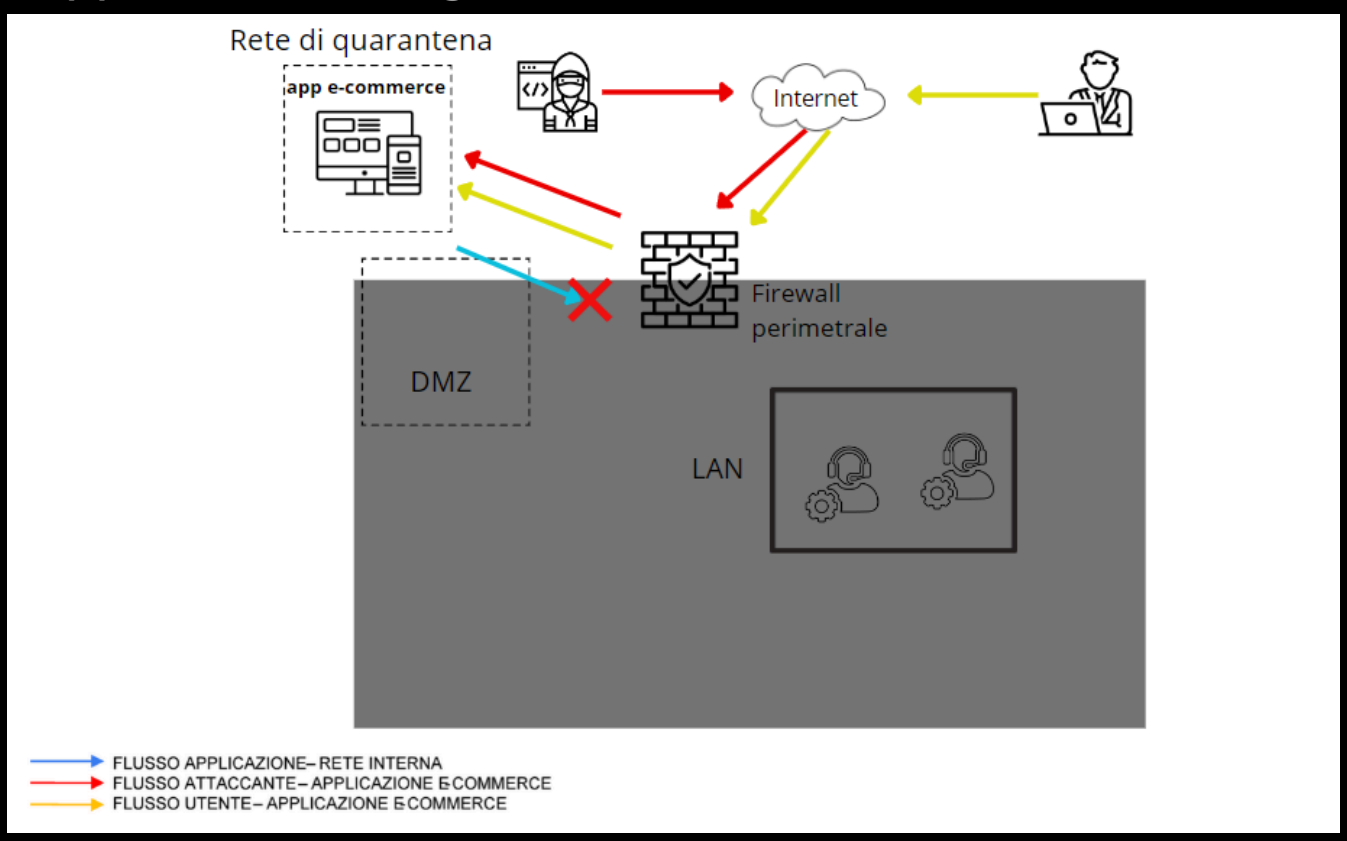
2. Web Application Firewall: Il WAF può aiutare a filtrare il traffico indesiderato prima che raggiunga la tua applicazione web.

3. Rate Limiting: Impostare limiti sul numero di richieste che un utente può fare in un determinato intervallo di tempo per prevenire il sovraccarico del server.

Response

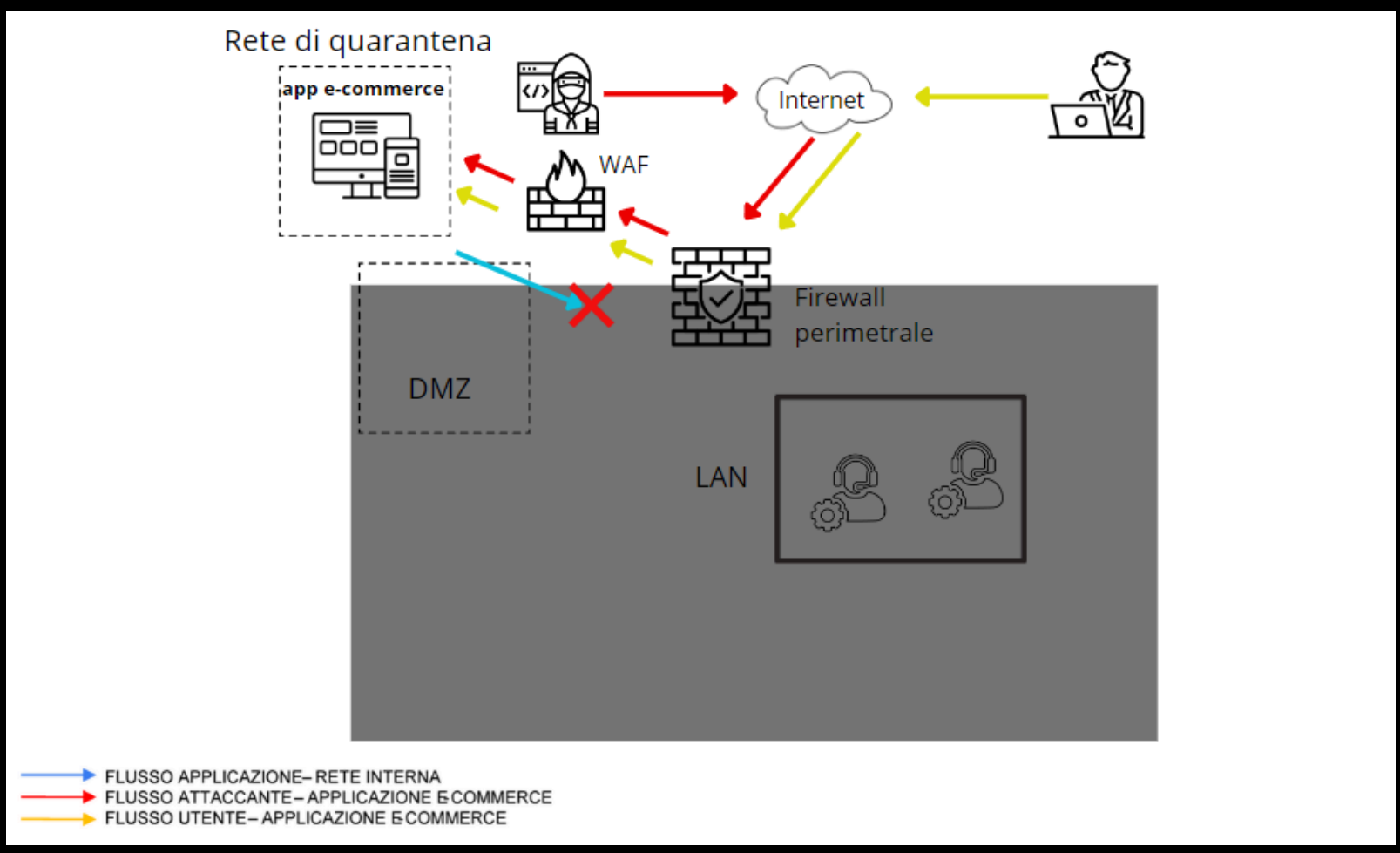
Una volta che il malware ha infettato il server, nel caso in cui non siamo interessanti a rimuovere l’accesso da parte dell’hacker, possiamo procedere attraverso l’isolamento del server in una rete di quarantena, in modo che non raggiunga la rete interna.

Rappresentazione grafica:



Soluzione completa

Adesso che abbiamo implementato azioni preventive e di response, procediamo a rappresentare la struttura finale:



Infrastruttura “aggressiva” della rete

Per migliorare ulteriormente il livello di sicurezza della rete, basandoci su un budget di 7’000 euro, possiamo implementare:

1. Sistema di Rilevamento e Prevenzione delle Intrusioni (IDS/IPS): Un IDS/IPS può monitorare il traffico di rete per attività sospette e agire per bloccare gli attacchi.

2. Software di Backup e Recupero: Assicurarsi di avere un buon sistema di backup e recupero in caso di incidenti, in modo da non perdere importanti dati in caso di attacchi come ransomware.

3.Web Application Firewall (WAF): Abbiamo visto attraverso le azioni preventive l’importanza di avere un WAF all’interno dell’infrastruttura di rete.