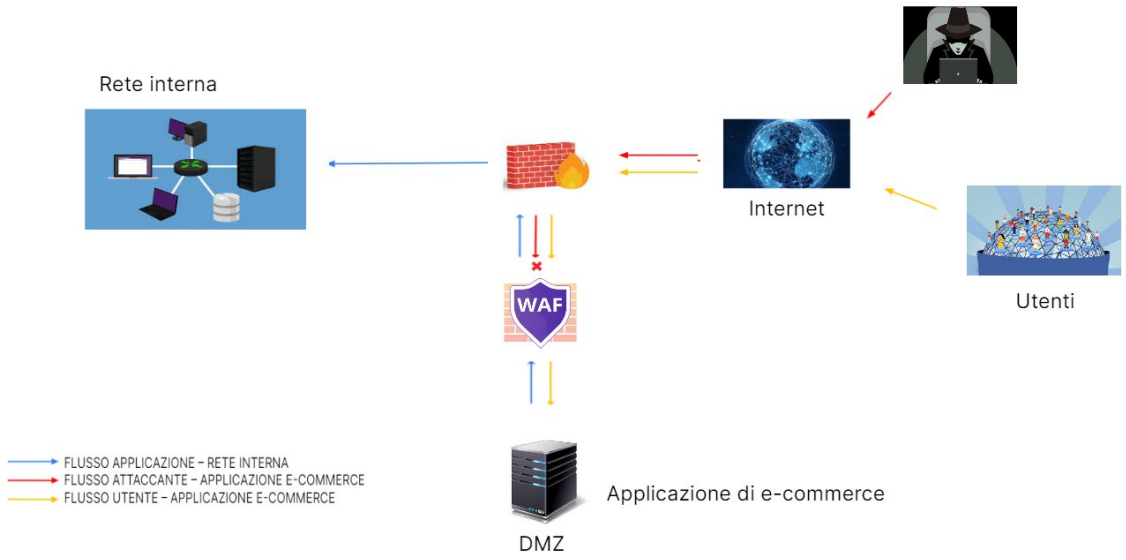
ANALISI DEI LOG – CASO REALE

Punto 1: azioni preventive

Per difendere l'applicazione di e-commerce da attacchi di tipo SQLi oppure XSS da parte di un malintenzionato è possibile implementare una WAF.
WAF significa "Web Application Firewall" ed è un tipo di firewall che si concentra sulla protezione delle applicazioni web, nello specifico è un sistema che monitora e controlla il traffico tra un'applicazione web e l'esterno, impedendo l'accesso non autorizzato, bloccando attacchi di sicurezza, filtrando il traffico dannoso e proteggendo i dati sensibili dell'applicazione.



Punto 2: impatti sul business

Considerando che in media gli utenti spendono circa 1.500,00€ sulla piattaforma di e-commerce, un attacco DDoS che rende irraggiungibile l'applicazione per 10 minuti, reca un **danno di 15.000,00€**. Questo valore potrebbe variare in base alla durata effettiva dell'attacco. In ogni caso, un attacco di tipo DDoS può avere conseguenze significative per la reputazione dell'azienda, oltre ai danni economici diretti e indiretti.

Esistono diverse soluzioni per mitigare il rischio di attacco DDoS e ridurre l'impatto sul business in caso di un attacco effettivo. Alcune delle possibili soluzioni possono essere:

1. Utilizzare una soluzione anti-DDoS di terze parti o fornita dal provider di hosting per filtrare il traffico DDoS e proteggere l'applicazione web.

2. Aggiornare regolarmente l'applicazione web e il software del server per ridurre le vulnerabilità e mitigare il rischio di exploit.

3. Implementare una rete CDN (Content Delivery Network) per distribuire il traffico in modo più uniforme e ridurre l'impatto di un attacco DDoS.

4. Limitare il numero di connessioni che un singolo indirizzo IP può stabilire con l'applicazione web per mitigare il rischio di un attacco DDoS.

5. Monitorare costantemente il traffico del sito web utilizzando strumenti di monitoraggio del traffico per identificare rapidamente eventuali attività sospette.

6. Creare un piano di risposta agli incidenti che definisca i passaggi da seguire in caso di un attacco DDoS, compreso il coinvolgimento di un team di sicurezza dedicato, l'isolamento dell'applicazione web colpita e la comunicazione con gli utenti.

Punto 3: response

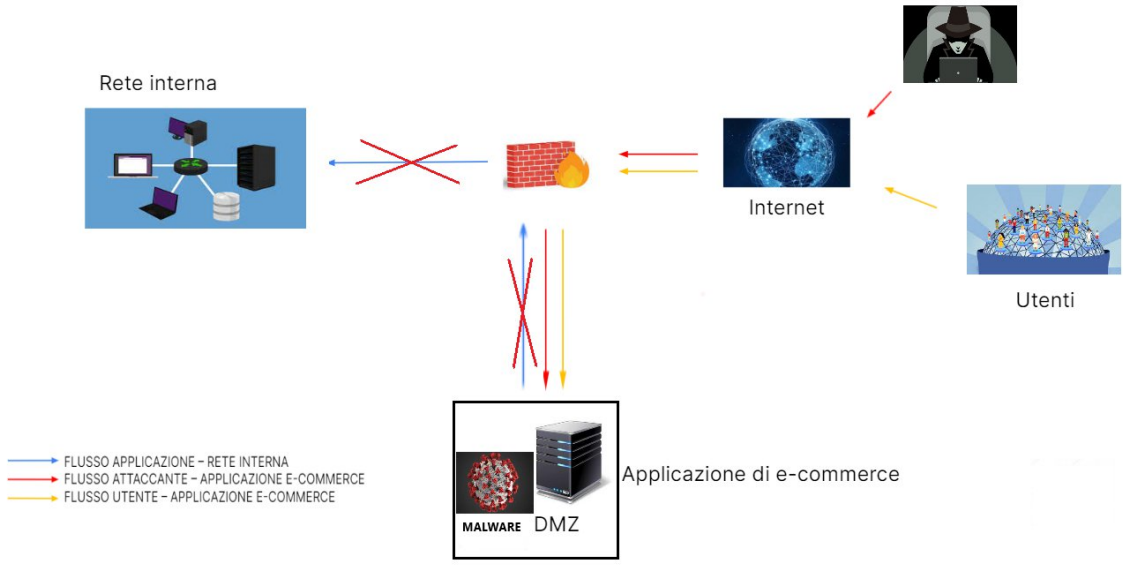
L’applicazione web viene infettata da un malware.
Il nostro obbiettivo è quello di non permettere al malware di propagarsi sulla nostra rete senza rimuovere l’accesso da parte dell’attaccante alla macchina infettata attraverso “l’isolamento”.

L’isolamento è una misura di sicurezza che prevede la separazione dei dispositivi infetti dalla rete principale per impedire la diffusione del malware. Questi sono alcuni passi che potremmo seguire:

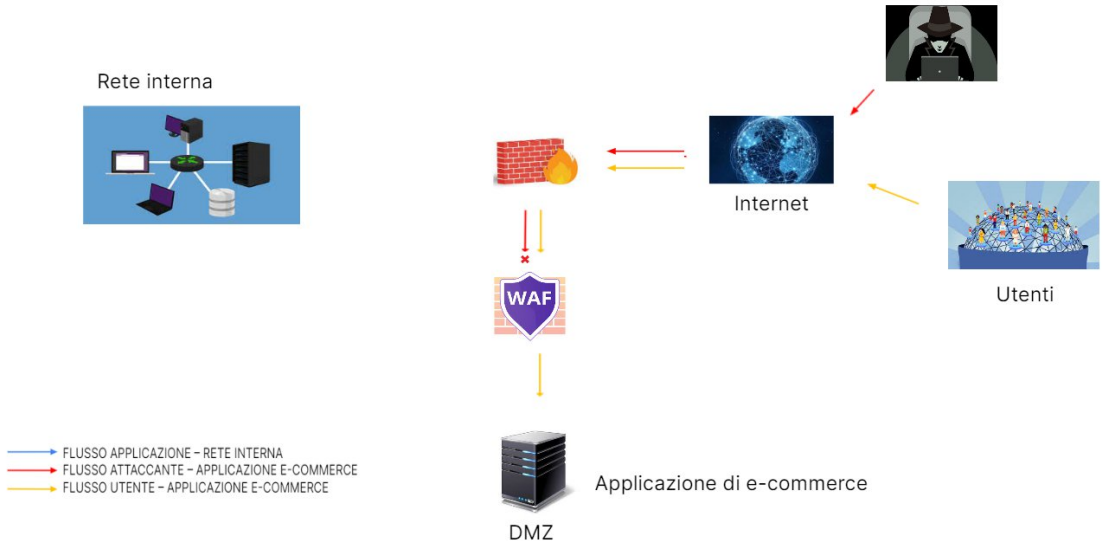
1. Attraverso l'utilizzo di una VLAN separata, di un firewall o di un dispositivo di isolamento di rete andiamo ad isolare i dispositivi infettati.

2. Una volta che i dispositivi infetti sono stati isolati dalla rete principale, è possibile procedere all'analisi del malware. Ciò può aiutare a identificare il tipo di malware e le sue funzionalità, nonché a sviluppare un piano di risposta.

3. Una volta completata l'analisi del malware e sviluppato un piano di risposta, è possibile procedere al ripristino dei dispositivi infetti. Ciò può includere l'eliminazione del malware, l'installazione di patch di sicurezza e il ripristino dei dati da backup.



Punto 4: soluzione completa.



Punto 5: soluzione aggressiva

Come accennato nel punto 2, per mitigare il rischio di attacchi DDoS e malware possiamo implementare una rete CDN attraverso *Cloudflare*. Di seguito troviamo alcune delle funzionalità principali di Cloudflare:

1. *CDN*: Cloudflare offre una rete di distribuzione di contenuti che aiuta a migliorare la velocità di caricamento del sito web e a ridurre la latenza. Il servizio CDN di Cloudflare distribuisce i contenuti del sito web su una rete globale di server, in modo che i visitatori del sito possano accedervi dal server più vicino a loro.

2. *Protezione DDoS*: Cloudflare protegge i siti web dagli attacchi DDoS utilizzando tecniche di mitigazione avanzate per bloccare il traffico di attacco prima che raggiunga il sito web. Ciò include la filtrazione del traffico, la limitazione delle connessioni, l'analisi comportamentale e l'implementazione di regole personalizzate di sicurezza.

3. *Firewall*: Cloudflare offre un firewall che aiuta a proteggere il sito web da attacchi di sicurezza come SQL injection, cross-site scripting (XSS) e altri tipi di attacchi.

4. *SSL/TLS*: Cloudflare offre un certificato SSL/TLS gratuito per proteggere la connessione tra il sito web e i visitatori del sito web. Ciò aiuta a proteggere le informazioni degli utenti e a garantire che la connessione sia sicura.

5. *Analisi del traffico*: Cloudflare offre strumenti per l'analisi del traffico del sito web, tra cui informazioni sulle visite al sito web, il tempo di permanenza sul sito web e le pagine più visitate. Queste informazioni possono aiutare a ottimizzare il sito web e migliorare l'esperienza dell'utente.

In aggiunta al servizio CDN è possibile aumentare la resilienza e la tolleranza agli errori del sistema attraverso la **ridondanza.**

L'aggiunta di componenti critici in un sistema al fine di eliminare eventuali SPOF (single point of failure) è una pratica comune nella progettazione di sistemi altamente affidabili. Un SPOF è un componente che, se fallisce, può causare l'interruzione dell'intero sistema. Aggiungere componenti critici aiuta a creare un sistema ridondante, in cui ogni componente critico può assumere le funzioni di un componente guasto e mantenere il sistema operativo.

Altri esempi di componenti critici che possono essere aggiunti a un sistema per eliminare gli SPOF includono alimentatori di emergenza, controller di storage ridondanti, connessioni di rete ridondanti, server web in cluster e così via.

Tuttavia, è importante notare che l'aggiunta di componenti critici può aumentare i costi e la complessità del sistema. Pertanto, è necessario valutare attentamente i rischi, i costi e i benefici dell'aggiunta di componenti critici in base alle esigenze specifiche del sistema.

Nell'immagine sottostante è stato inserito il servizio di Cloudflare, inoltre come soluzione preventiva ancora più aggressiva è stato aggiunto un altro server che è possibile configurare come backup del primo. In caso di guasto del primo server, il secondo server può assumere le funzioni del primo e mantenere il sistema operativo.