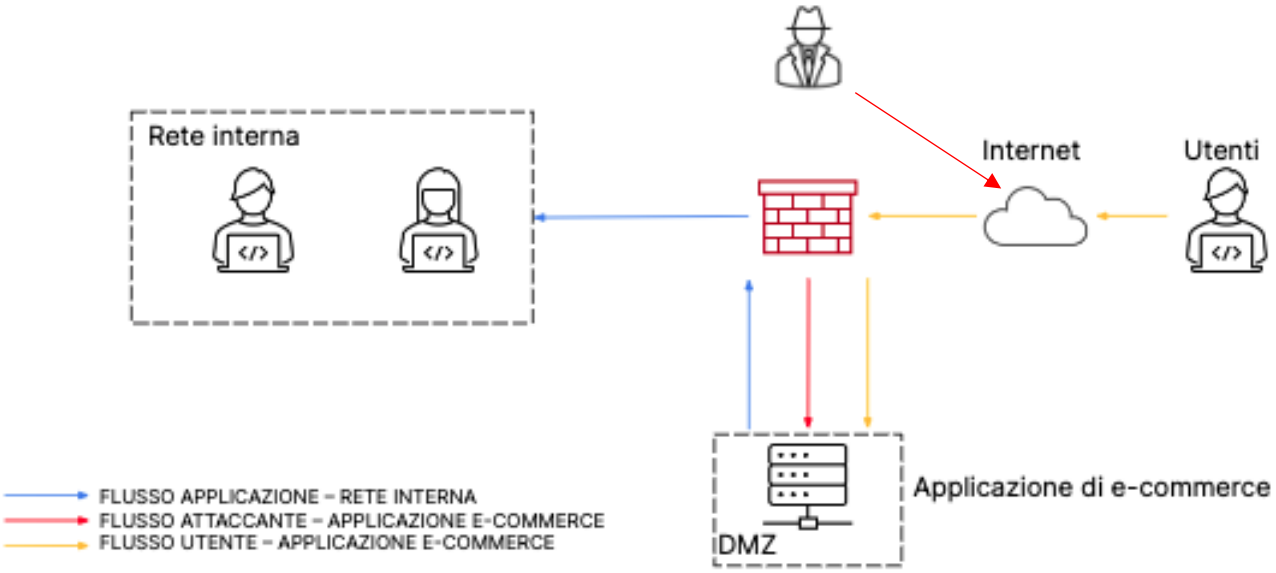
REPORT PROGETTO

FRANCESCO PERSICHETTI

La nostra applicazione di e-commerce è così composta



Dove la nostra rete interna può essere raggiunta dalla DMZ per via delle policy sul firewall; quindi, se quest'ultimo venisse compromesso un possibile attaccante potrebbe entrare nella rete interna. Per migliorare la seguente struttura, implementiamo i seguenti task:

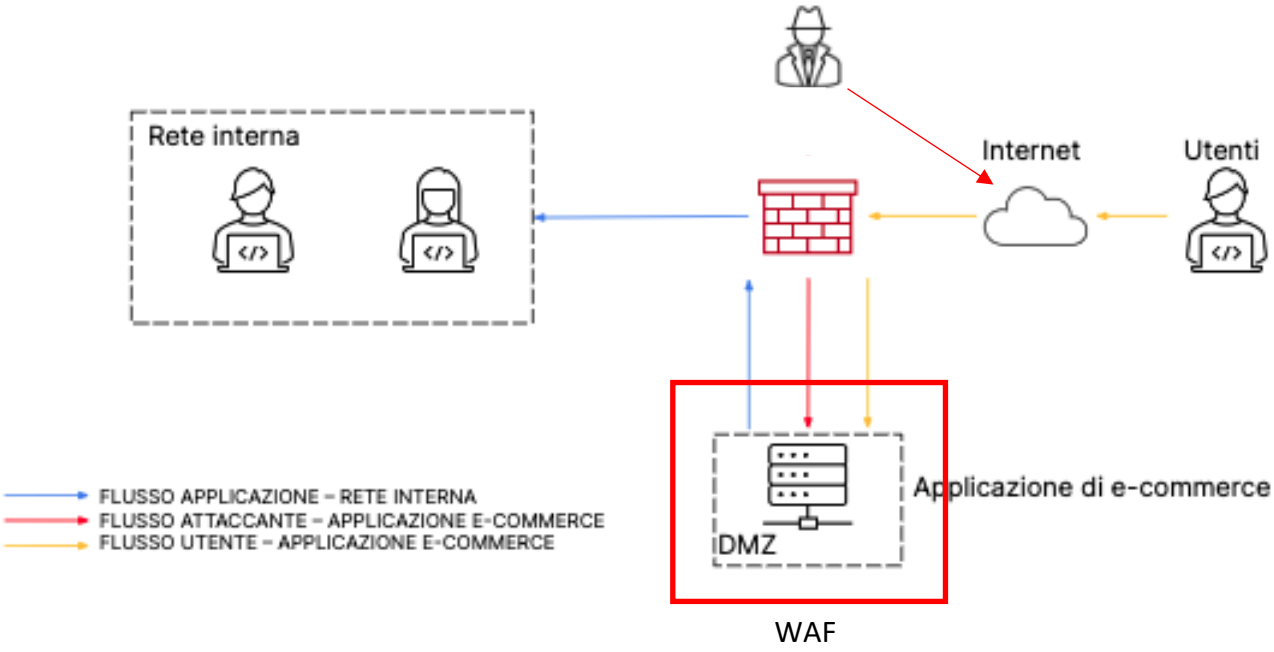
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
   Modificate la figura in modo da evidenziare le implementazioni

2. **Impatti sul business**: 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.

3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response

1.
Per prevenire attacchi di tipo SQLi oppure XSS sulla nostra applicazione Web introduciamo un ulteriore firewall specifico per le applicazioni web, il “WAF” posizionato come mostrato di seguito

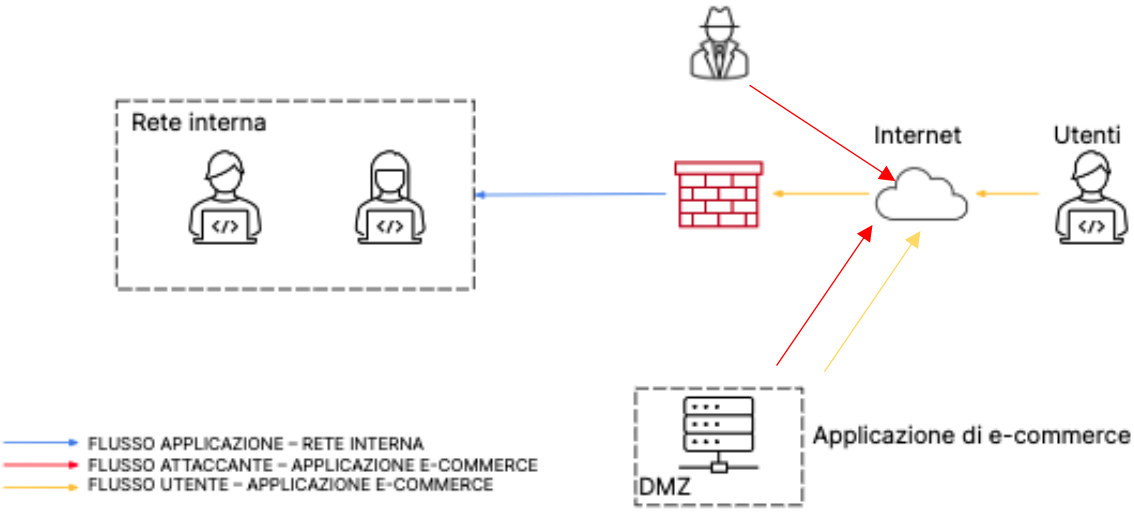


2.
Nel momento in cui un malintenzionato riesce a entrare e lanciare un attacco DDos che manda in down l’ e-commerce per 10 minuti, calcolo il danno economico a livello di business che il sito subisce considerando che in media guadagna 1.500€ al minuto. Il calcolo sarà:

1.500€ x 10 = 15.000€

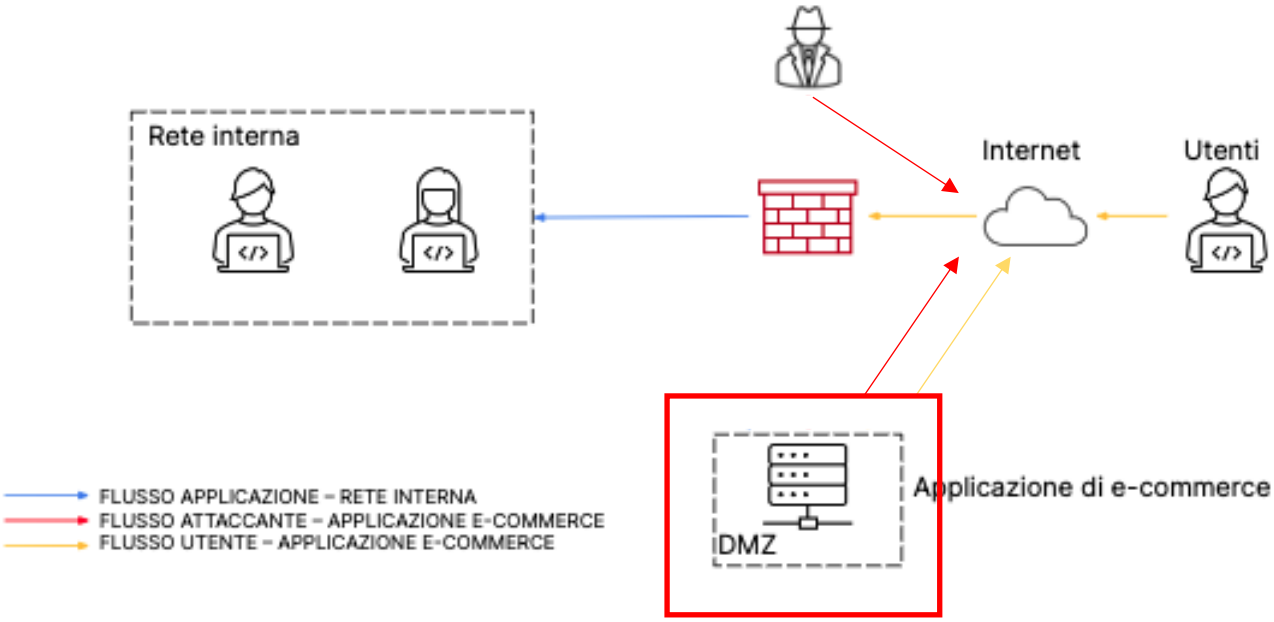
Quindi l’impatto economico finale di questo attacco durato 10 minuti è di 15.000€

3.
Una volta sotto attacco bisogna isolare il sistema infetto dal resto della connessione interna, senza preoccuparci del fatto che l’attaccante possa continuare a risiedere sulla macchina attaccata. Visto che la macchina in questione è la nostra applicazione web che è già distaccata dalla nostra rete interna perché è all’interno della DMZ, basta togliere la comunicazione che ha con la rete interna per evitare ulteriore contagio



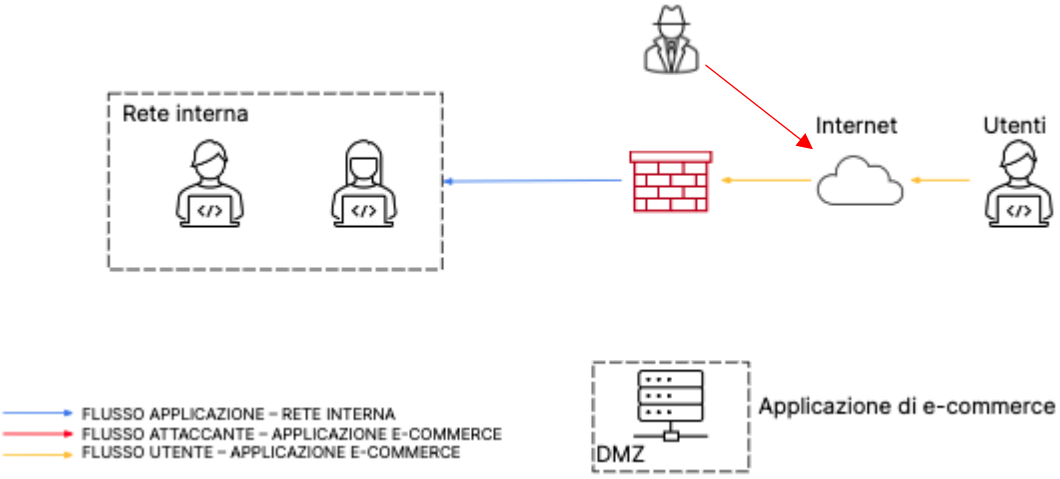
Così facendo gli utenti potranno comunque interpellare il nostro sito, mantenendo attivo il servizio critico

4.
La soluzione finale verrà così:



WAF

5.
Un ulteriore opzione più drastica e invasiva potrebbe essere quella di mettere la nostra applicazione completamente in “quarantena” staccandola anche da internet e quindi di conseguenza anche dal controllo dell’attaccante per poter sanificare il sistema dal malware iniettato



Ciò comprende ovviamente il completo down della nostra applicazione, comportando quindi disagi per gli utenti ma soprattutto un impatto negativo per il business dell’azienda, ma si ripristinerebbe la situazione iniziale con l’aggiunta di aver modificato e reso più sicure le aree precedentemente vulnerabili in modo da non essere più attaccata o quanto meno non nello stesso punto.