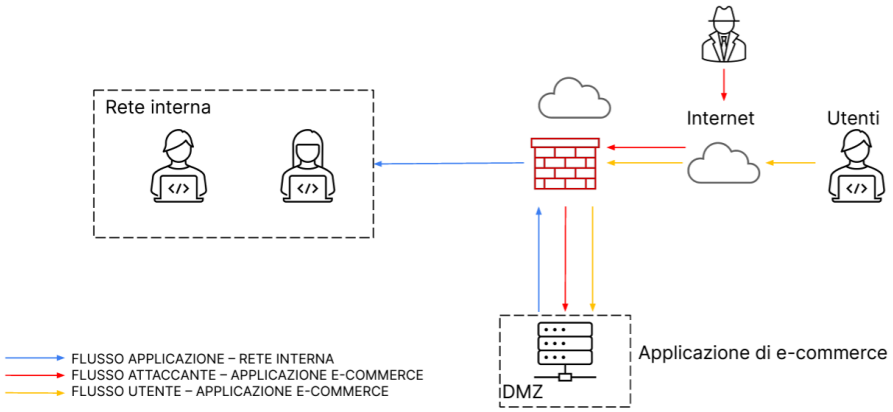
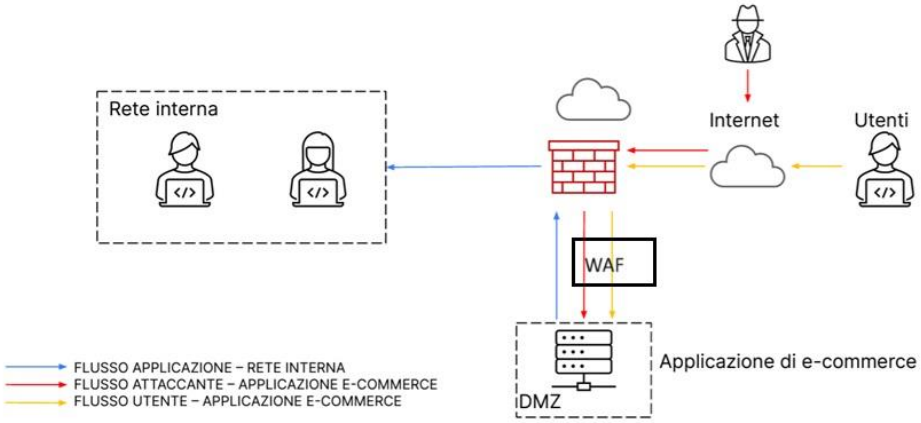
PROGETTO

Il progetto richiede di rispondere ad alcuni quesiti facendo riferimento alla figura seguente:



La figura rappresenta la rete di un'applicazione di e-commerce. L'applicazione deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

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?**
   Gli attacchi SQLi (SQL injection) sono un tipo di attacco che consente di eseguire istruzioni SQL dannose. I malintenzionati utilizzano le vulnerabilità di SQLi per aggirare le misure di sicurezza delle applicazioni, come l'autenticazione e l'autorizzazione di una pagina o applicazione Web, recuperare il contenuto del database e aggiungere, modificare ed eliminare record.
   Gli attacchi XSS (Cross-Site Scripting) invece sono una tipologia di vulnerabilità che consiste nell'iniettare codice malevolo nei browser degli utenti, riuscendo a inserirlo all'interno di un sito web. Una volta che un utente ignaro inserirà un input, si attiverà il codice e l'attaccante potrà visualizzare tutte le informazioni dell'utente. Per prevenire questi attacchi, si potrebbe agire utilizzando un WAF.
   Il WAF (Web Application Firewall) è uno speciale firewall che si occupa specificatamente della protezione delle applicazioni web analizzando il contenuto delle richieste e delle risposte HTTP/HTTPS.
   Come si può notare dalla figura, impostando particolari parametri e usando un WAF in quel punto, è possibile bloccare l'accesso alla DMZ e filtrare solo particolari tipi di traffico

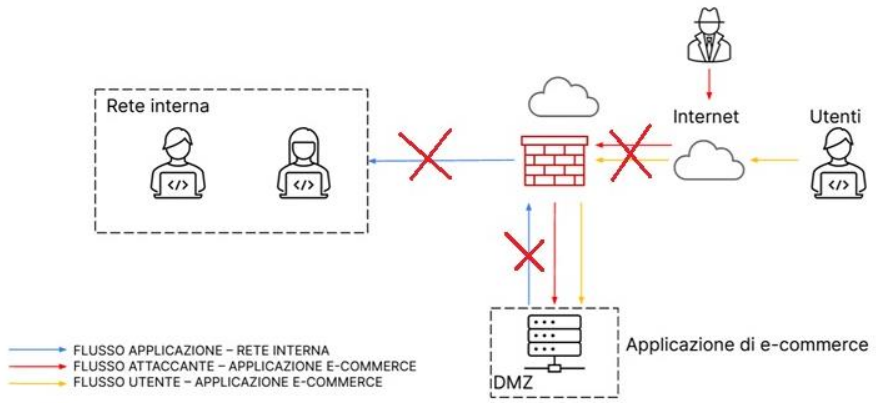


2) **Impatti sul business: L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare.**
Gli attacchi DDoS (Distributed Denial of Service) sono un attacco il cui fine è rendere inutilizzabile un sito web o una risorsa di rete inondandolo di traffico dannoso, in modo tale da sovraccaricare il bersaglio di traffico dati e impedire il corretto funzionamento e l'accesso degli utenti. Questo può causare anche perdite finanziarie e danni alla reputazione. Per rispondere al quesito, dobbiamo semplicemente prendere quanti soldi gli utenti spendono al minuto e moltiplicarli per i minuti persi. La formula quindi è questa:

soldi spesi*tempo perso
1.500*10=15.000

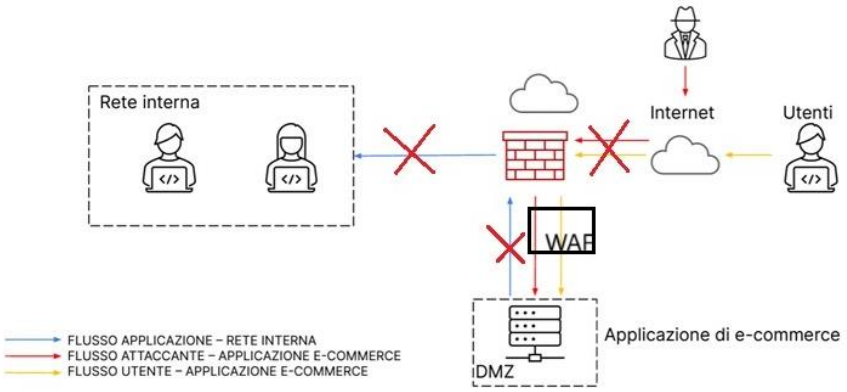
Quindi, l'impatto avuto sul business è di 15.000 euro. Eventuali azioni preventive che si possono applicare possono essere utilizzare un'infrastruttura di rete robusta in grado di gestire grandi quantità di traffico, utilizzare un servizio anti-DDoS, ovvero servizi che possono filtrare il traffico malevolo prima che raggiunga l'infrastruttura di rete e l'utilizzo di un firewall.

3) **Response: L'applicazione Web viene infettata da un malware. Impedire che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.**
Il malware è un software maligno che si infiltra in un sistema informatico per causare danni, come rubare informazioni, danneggiare file o controllare dispositivi altrui. Per risolvere questo quesito, la miglior soluzione è utilizzare una tecnica di isolamento. Questa tecnica consiste nella disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante e limitando la capacità di minacce come malware di diffondersi all'intera rete.

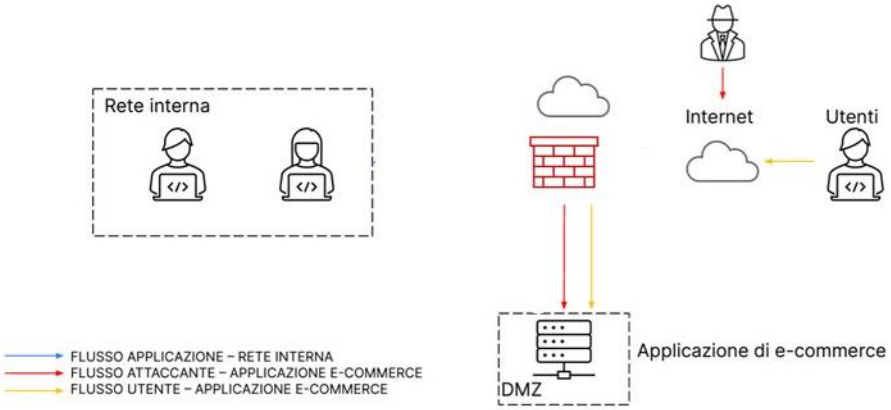


Come si può vedere dall'immagine, gli utenti e l'attaccante avranno ancora l'accesso ad internet, ma il sistema è stato disconnesso dalla rete, questa impossibilità è rappresentata con le x rosse.

4) Soluzione completa: Unire i disegni dell'azione preventiva e della response



Unendo le immagini dopo l'applicazione del WAF e l'isolamento della rete avremo come risultato l'impossibilità di raggiungere la rete interna



L'app comunque continuerà a funzionare perchè se ne sarà fatta una di backup che continuerà a comunicare con la rete interna