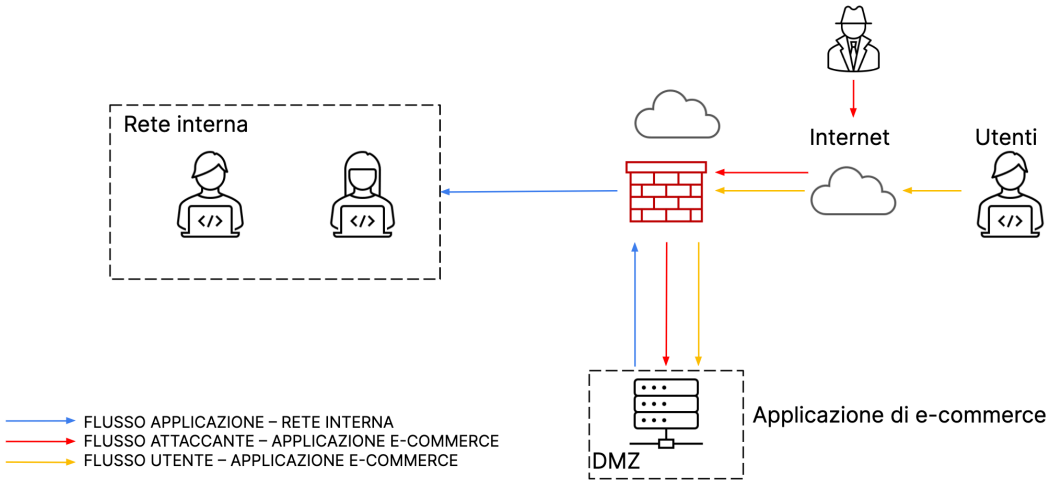
PROGETTO MODULO 5

Traccia:

1) ***Azioni preventive****: azioni preventive per difendere l'applicazione web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato.*
2) ***Impatto sul Business****: considerando che l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che la rende non raggiungibile per 10 min. Calcolo impatto sul business dovuto alla non raggiungibili del servizio, tenendo conto che in media ogni minuto gli utenti spendono 1.500€ sulla piattaforma e-commerce.*
3) ***Response****: l'applicazione Web viene infettata da un malware. La priorità è che il malware non si propaghi sulla rete, senza rimuovere l'accesso da parte dell'attaccante alla macchina infettata.*
4) ***Soluzione Completa****: unione dei disegni dell'Azione Preventiva e della Response.*
5) ***Modifica "più aggressiva" dell'infrastruttura****.*

Architettura di rete:

L'applicazione di e-commerce 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

Considerato che un **SQLi** potrebbe consentire all'aggressore di inserire comandi SQL dannosi attraverso input web, in modo da poter accedere, modificare o cancellare dati nel database dell'applicazione e-commerce.
Mentre con un **XSS** l'aggressore potrebbe insilerei script dannosi nei dati visualizzati sul sito, rubando informazioni degli utenti o interagendo sul sito a loro nome.

Essendoci delle **policy sul firewall** che rendono la rete interna raggiungibile dalla **DMZ** ("*zona demilitarizzata*" ovvero una zona intermedia tra una rete interna sicura e una rete esterna non sicura, come internet. La DMZ in un'applicazione e-commerce funge da filtro di sicurezza che protegge il server principale in cui ci sono dati e transazioni sensibili) è più importante rafforzare le difese in quanto introducono un potenziale punto di vulnerabilità.

Le ***Azioni Preventive*** che si potrebbero adottare possono essere:

- **Validazione e Sanitizzazione dei Dati in Ingresso**: assicurarsi che tutti i dati provenienti dagli utenti siano validati e sanificati, in modo da filtrare e scartare i dati dannosi o non validi prima di elaborarli.

- **Revisione del Codice (analisi del codice)**: dove si esamina il codice sorgente di un'applicazione per individuare errori, vulnerabilità (che potrebbero consentire attacchi *SQLi* e *XSS*) o problemi di sicurezza
- **Parametrizzazione delle Query SQL**: è un ulteriore misura che può prevenire *SQLi*. In quanto impedisce al malintenzionato di iniettare comandi dannosi perché i parametri sono trattati come dati e non come parte della query *SQL*.

Questo elimina il rischio di interpretazione errata del input dell'utente come comandi *SQL*. Una query con valori specifici per "*username*" e "*password*" verranno passati come parametri e l'applicazione si assicurerà che siano trattai in modo sicuro.

Di conseguenza un attaccante non può iniettare comandi *SQL* dannosi in quanto non può influenzare direttamente la struttura della query.

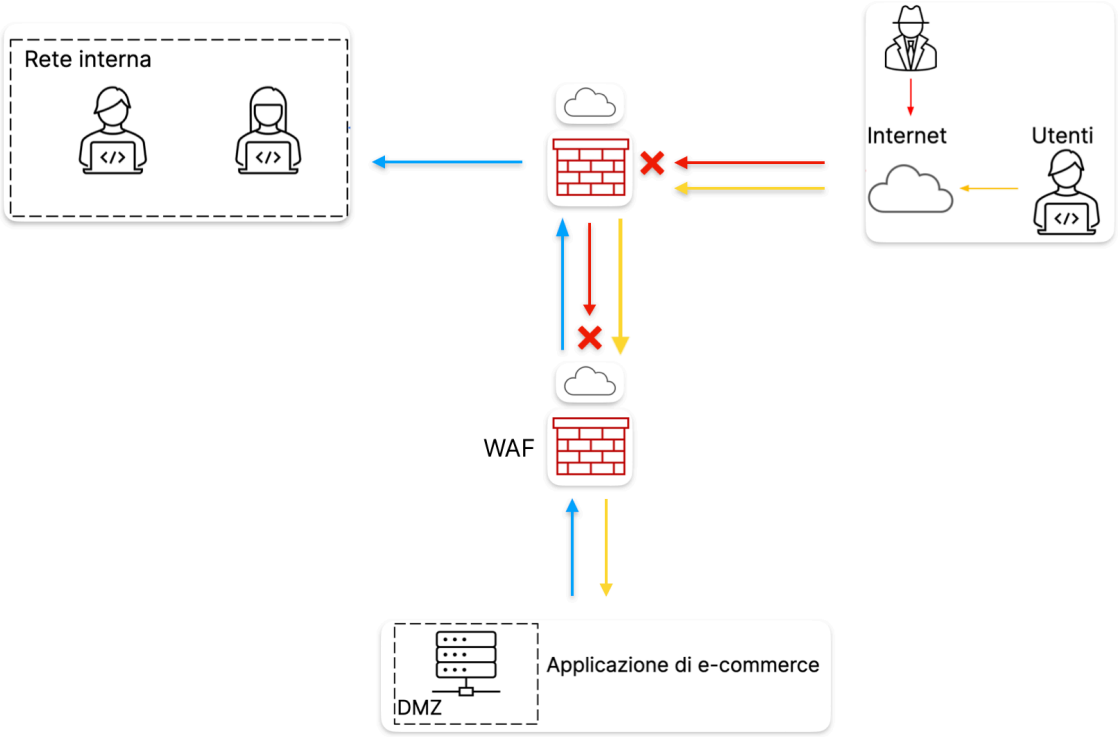
- **Utilizzare un Firewall Applicativo (WAF)**: Analizza il traffico *HTTP/HTTPS* in ingresso. Un **WAF** è progettato specificatamente per proteggere applicazioni web da minacce dirette quindi può aiutare a rilevare e bloccare tentativi di attacchi *XSS, SQLi* e attacchi *DDoS* mirati alle applicazioni.

Consiste nell'installazione e configurazione di un dispositivo o un software che agisce come intermediario tra il traffico web in ingresso e l'applicazione web stessa.

Offere una protezione mirata alle applicazioni web piuttosto che alla rete in generale.

Si può utilizzare un firewall di rete per proteggere quindi l'infrastruttura di rete e i servizi di base, e un WAF per proteggere le applicazioni web.

- **Aggiornamento Costante**: mantenere aggiornati con le ultime patch di sicurezza tutti i componenti dell'applicazione, inclusi i server web, il database il software del server per correggere vulnerabilità conosciute.
- **Scansione di sicurezza periodica**: per identificare vulnerabilità potenziali.
- **Accesso minimale dalla DMZ alla Rete Interna**: limitare rigorosamente l'accesso dalla DMZ alla rete interna solo alle porte e i servizi strettamente necessari. Configurare il firewall per impedire qualsiasi traffico non autorizzato.
- **Monitorare e Registrare gli eventi**: attuare un sistema di monitoraggio e registrazione degli eventi per rilevare tentativi di attacco e rispondere prontamente.



2) Impatto sul Business

Calcolo l'impatto sul business dovuto alla non raggiungibilità del servizio a causa di un attacco DDoS, usando la formula:

Single Loss Expectancy = AssetValue x ExposureFactor

SLE = AV x EF

AV = 1.500 € x 10min = *15.000 €*

***SLE** = 15.000 € x 1 = 15.000 €*

Tendo conto che:

- ***Asset Value (AV)*** = corrisponde alla perdita di entrate durante l'attacco DDoS.
  Quindi **AV = *"Spesa media per minuto" x "Minuti di inattività"***
- ***Exposure Factor (EF)*** = il *Fattore di Esposizione* è una misura che indica quanto del valore totale di un Asset si prevede di perdere a causa dell'incidente. O meglio quanto è dannoso l'incidente per l'Asset. ***EF potrebbe essere 1***, in quanto si prevede di perdere l'intero valore dell'Asset, ovvero tutte le entrate che si sarebbero ottenuto durante quei 10 min, a causa dell'attacco.

EF = 1

Azioni preventive che si potrebbero applicare:

- **Monitoraggio costante**: per rilevare segni di un attacco *DDoS* in tempo reale.
- **Backup**: eseguire regolari copie di backup dei dati e dei sistemi in modo che, se l'attacco danneggiasse qualcosa, si può ripristinare rapidamente.
- **Bilanciamento del carico con il Failover Cluster**: usando più server per distribuire il traffico in modo uniforme, così se anche uno dei server è sotto attacco, gli altri possono ancora gestire il traffico.
- **Firewall DDoS**: configurare un firewall con regole apposite per rilevare e bloccare il traffico dannoso legato agli attacchi *DDoS*. (**per esempio**: monitorare il volume di richieste in arrivo da una singola origine o rilevamento di un alto numero di richieste HTTP da una singola origine, oppure il firewall può richiedere una verifica della legittimità con un Captcha per assicurarsi che le richieste siano effettuate da utenti legittimi e non da bot dannosi).
- **Valutare l'adozione di IPS o IDS**: sono due tipi di sistemi di sicurezza informatica utilizzati per monitorare e proteggere le reti e i sistemi da intrusioni o attacchi informatici.

IPS (*Intrusion Prevention System*) = è una versione più avanzata dell'***IDS***, rileva gli attacchi e con esso si possono prevenire e bloccare attivamente, prima che abbiano successo.

IDS (*Intrusion Detection System*): è principalmente un sistema di rilevamento e allerta che informa degli attacchi, non esegue quindi azioni dirette.

- **Incident Response Plan (IRP) :** preparando un *Piano di Risposta agli Incidenti,* per essere in grado di rispondere prontamente. Si potrebbe valutare l'implementazione di un *SOC* o un servizio di sicurezza gestita, ovviamente in base alle esigenze dell'applicazione e-commerce, al bilancio e la complessità delle operazioni per determinare il livello di supporto necessario.

3) Response

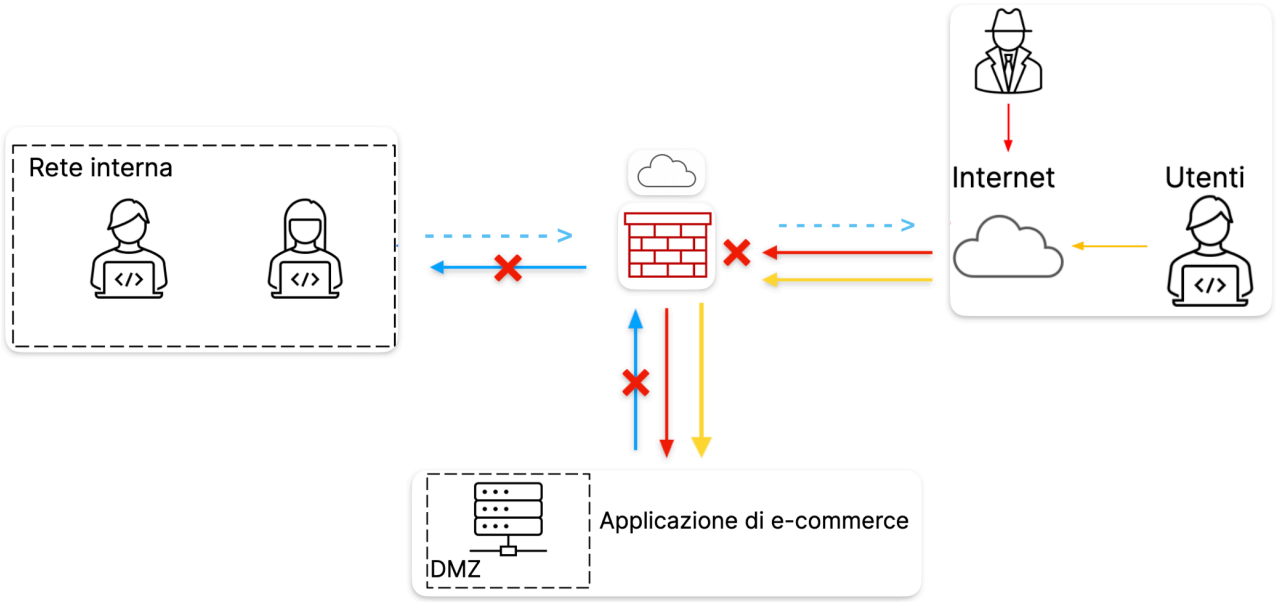
La priorità principale è impedire la propagazione del malware nella rete intera, mentre si accetta temporaneamente che l'attaccante mantenga l'accesso alla macchina infettata nel DMZ.

Quindi si potrebbe seguire un approccio di Contenimento.

La Rete Interna è già *Segmentata* (una ***strategia di Contenimento***), in quanto l'applicazione web (infettata dal malware) è già separata dalla Rete Interna tramite la DMZ

Si ha la possibilità di:

- creare una ***Rete di Quarantena***, utilizzando anche regole specifiche per il Firewall in modo che il malware non possa comunicare con altri dispositivi nella rete.

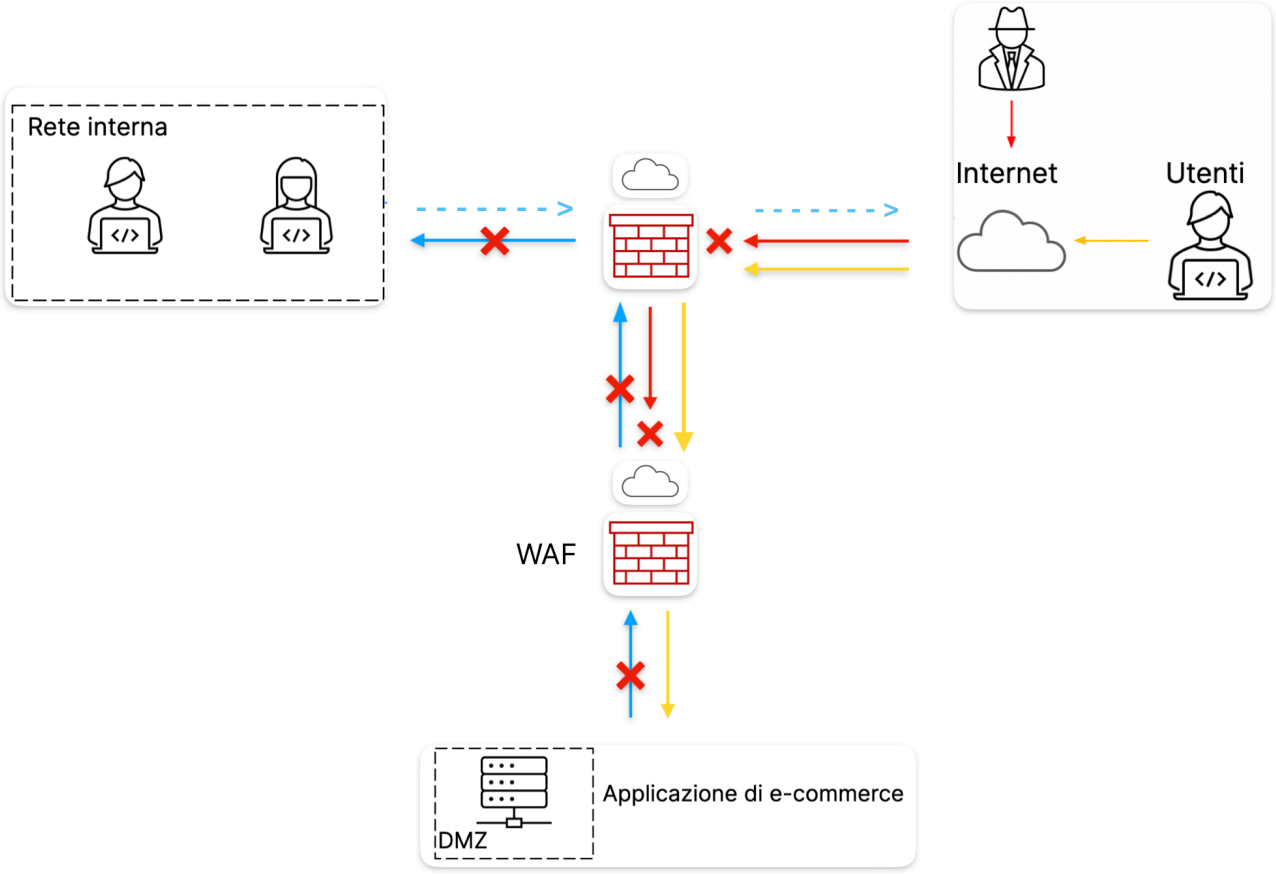


- ***Mitigare e Prevenire***: potendo fare l'Analisi del malware, isolando la copia di esso e quindi analizzarla in un ambiente sicuro per capire come funziona e comprendere le intenzioni dell'attaccante.

Legenda:
- - - -> freccia blu tratteggiata indica che la rete interna è connessa a internet passando dal firewall.
- —> freccia blu non ha più l'accesso al server dell'applicazione e-commerce.

4) Soluzione Completa

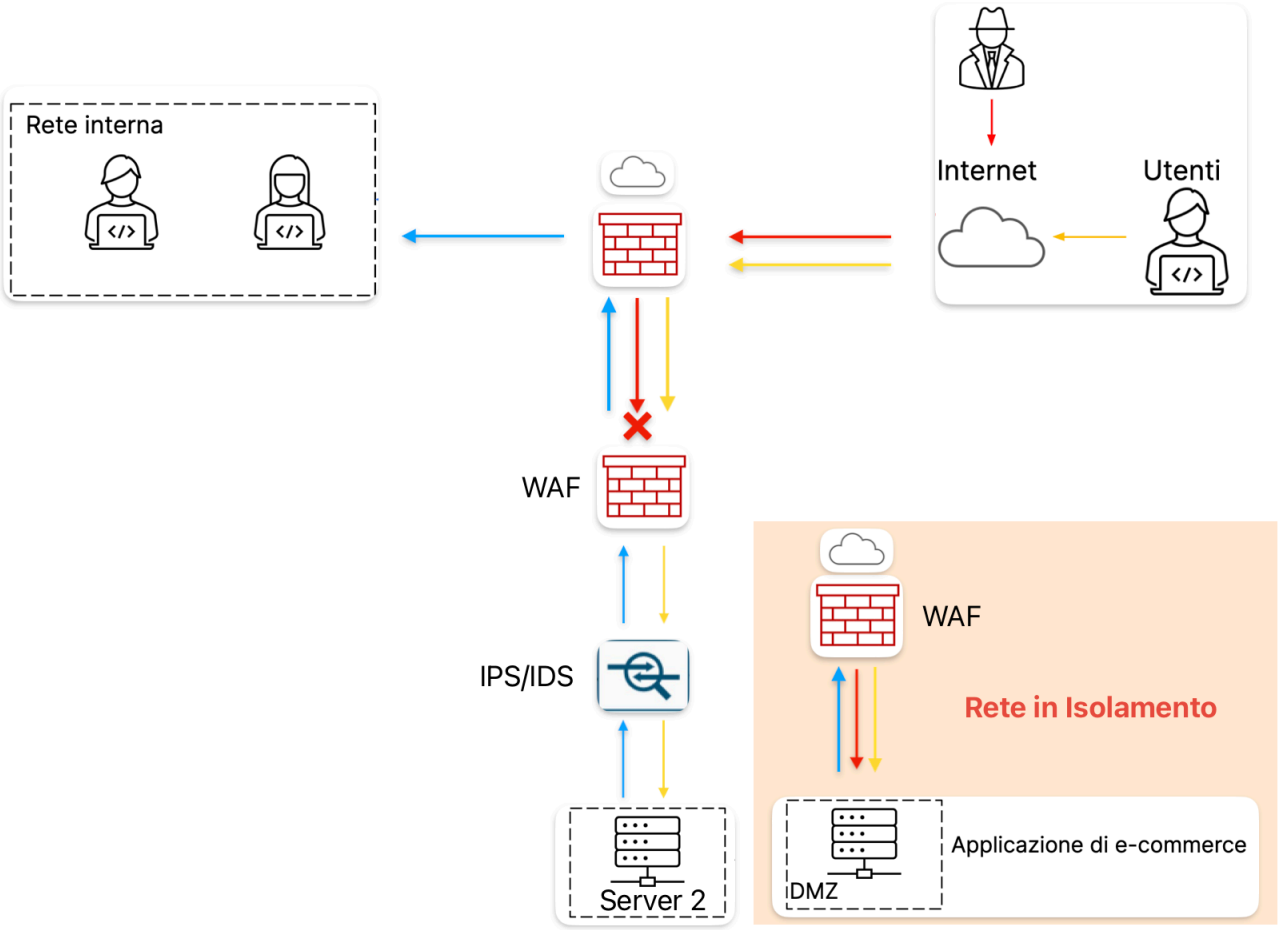
Unione dell'Azione preventiva e della Response



5) Modifica più aggressiva dell'infrastruttura

Si potrebbe optare per un contenimento maggiore, utilizzando la ***tecnica dell'isolamento***, che consiste nella completa disconnessione del sistema infetto dalle rete, per restringere appunto ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.

Integrata all'uso di un WAF, un IPS o IDS o entrambi e un bilanciamento del carico con più server con il Failover Cluster.



Failover cluster