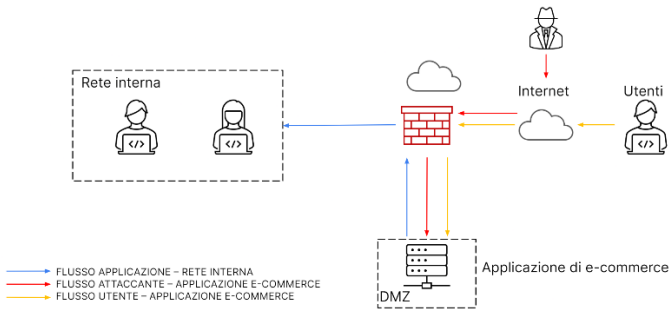
Modulo 5
Esercizio 8

Architettura della rete esaminata:



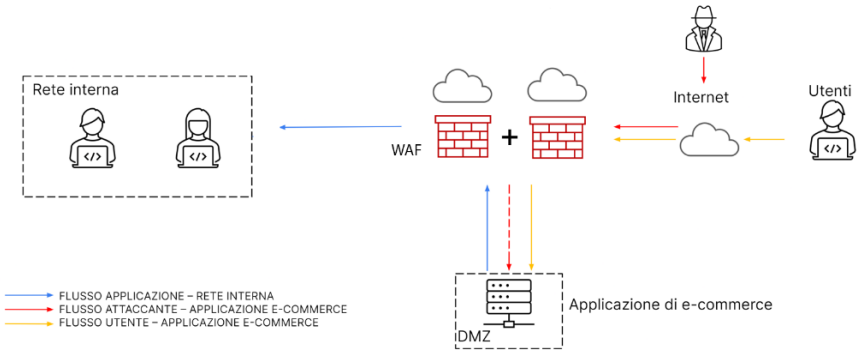
Nella rete presa sotto esame possiamo notare come utenti o persone con scopi malevoli, tramite l'applicazione di e-commerce, possa raggiungere la rete interna.

La struttura ha una DMZ la quale è raggiungibile dalla rete interna.
La DMZ funge da buffer tra la rete interna e la rete esterna, offrendo un primo livello di sicurezza. Le risorse che sono accessibili al pubblico generale, come in questo caso l'applicazione di e-commerce, vengono solitamente posizionate nella DMZ, mentre le risorse interne critiche, come i database e i sistemi di backend, rimangono protette all'interno della rete interna.

Nota:
Bisogna ricordare che se un attaccante riuscisse a compromettere un sistema all'interno della DMZ, non avrebbe automaticamente accesso alla rete interna, poiché ci potrebbero essere ulteriori misure di sicurezza e firewall tra la DMZ e la rete interna.

---

1) Azioni preventive:
Ci viene chiesto di implementare delle misure di sicurezza per difendere l'applicazione web da attacchi SQLi e XSS.
Una fra le tante soluzioni può essere l'aggiunta di un WAF(Web Application Firewall), un dispositivo di sicurezza dedicato a proteggere da attacchi SQLi e XSS.
Per ottenere la sua massima efficacia lo andiamo a collocare fra in nostro firewall esterno e la nostra DMZ.

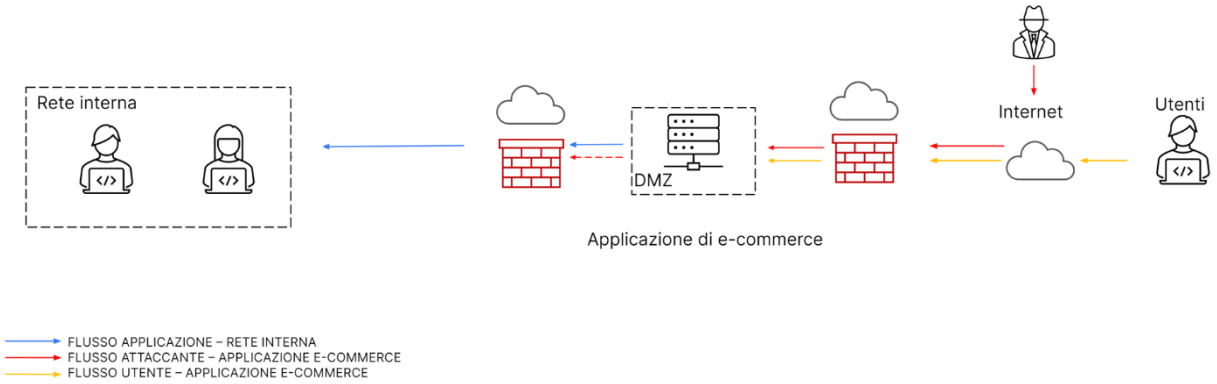


Con questa implementazione siamo andati a rendere più sicura la nostra rete dagli attacchi XSS e SQLi, ma questa misura non garantisce una protezione al 100%. Andrebbero implementate ulteriori soluzioni come l'IDS e l'IPS, la segmentazione dei privilegi ecc..

Nota: La freccia rossa tratteggiata tra il WAF e la DMZ sta ad indicare la possibilità di altre tipologie di attacco.

Azioni preventive 2 soluzione:

Possiamo utilizzare anche una tipologia di struttura di rete differente, dove i due firewall vengono inseriti tra la DMZ e la rete Interna.



Con questa tipologia di struttura andremo ad utilizzare le Group Policy, sfruttando regole molto più specifiche e delineate solo ai gruppi di appartenenza. Disabilitazione di porte e servizi non necessari, monitoraggi sul traffico di rete e sugli end-point.
(Soluzione meno costosa se consideriamo l'acquisto di un WAF).

---

2) Impatti sul business:

L'azienda subisce un attacco DDos che rende l'applicazione offline per 10 minuti facendogli perdere circa 15.000€ al minuto.
Volendo calcolare la perdita monetaria giornaliera possiamo sfruttare una formula matematica.

SLE = AV * EF

dove:
SLE (Single Loss Expectancy) = misura monetaria della perdita al verificarsi dell'evento;
AV (Valore dell'asset) = valore monetario dell'asset
EF (EXposure Factor) = percentuale dell'asset impattato

Avendo chiare queste nozioni possiamo calcolare la perdita monetaria giornaliera dell'azienda a causa dell'attacco DDos.

AV = 1500 * 1440(minuti totali in un giorno) = 2.160.000€
EF = 10(minuti di stop) / 1440 = 0,00694444%

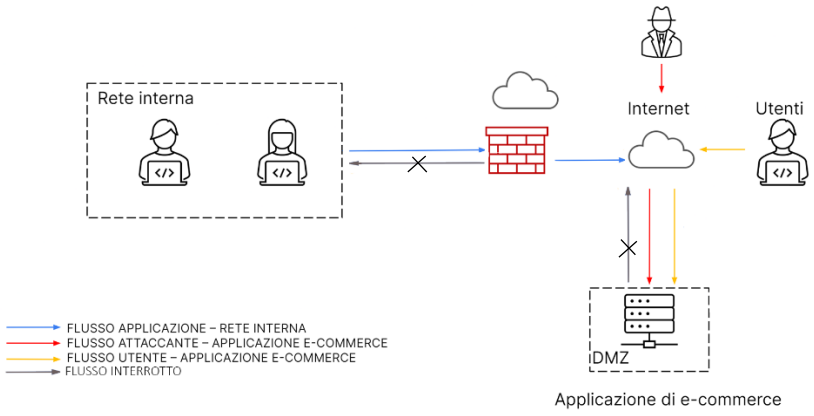
SLE = 2.160.000 * 0,00694444% = 14.999,9904€
Possiamo dire che nell'arco di 10 minuti l'azienda ha perso circa= 15.000€

(Il calcolo poteva essere effettuato anche andando a calcolare il valore (1500) moltiplicandolo per i minuti (10) ottenendo similarmente lo stesso valore)

Azioni preventive:
Per evitare l'interruzione del servizio dovuto ad un attacco DDos possiamo adottare una serie di azioni preventive.
-Implementazione di un firewall per filtrare il traffico in entrata e limitare il numero di connessioni provenienti da un singolo host;
-Implementazione dei sistemi IPS/IDS (ad oggi sono già presenti nei firewall di ultima generazione NGFW) per monitorare e prevenire le intrusioni;
-Implementazione dei Bilanciatori di carico in modo tale da distribuire il traffico in ingresso su più server;
-Riduzione delle porte e servizi non necessari;
- Considerare l'uso di un servizio di mitigazione DDoS fornito da un provider di sicurezza specializzato. Questi servizi sono progettati per rilevare e mitigare gli attacchi DDoS in tempo reale, instradando il traffico malevolo lontano dai tuoi server;
-Aggiornamenti e patching di sicurezza per ridurre le vulnerabilità.

---

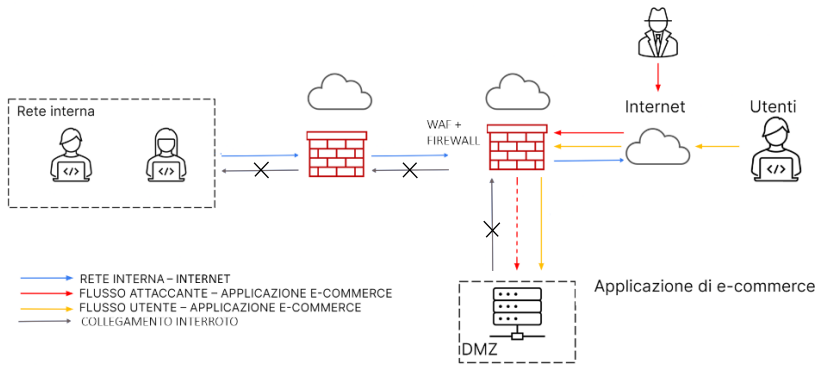
3) Response:
La nostra DMZ è stata colpita da un malware e dobbiamo evitare che si propaghi sulla nostra rete interna. Procediamo con la modifica della struttura della rete andando ad isolare la macchina infetta dalla rete interna.



Facendo ciò abbiamo garantito la continuità del servizio, andando a modificare il firewall con regole più restrittive e bloccando l'accesso della DMZ.
La prossima fase sarà quella di rimozione dell'incidente con lo scopo di eliminare le attività rimaste all'interno della rete o sui sistemi.

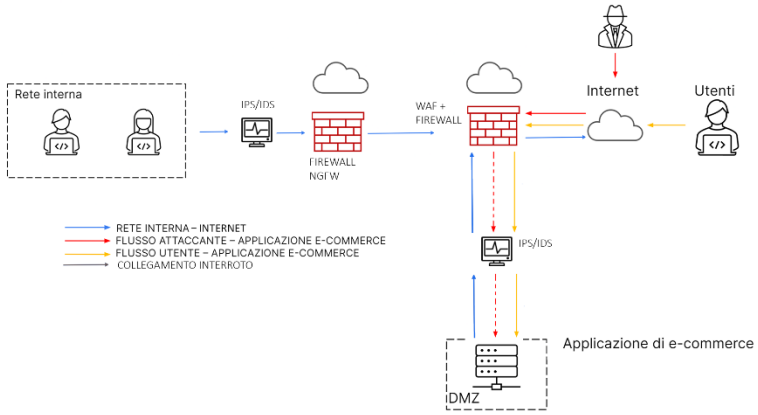
---

4) Soluzione Completa:



---

5) Modifica dell'infrastruttura:



Per migliorare la sicurezza della nostra rete, abbiamo adottato diverse misure:
Abbiamo implementato firewall di ultima generazione per il controllo avanzato del traffico.
Sono stati aggiunti sistemi di rilevamento (IDS) e prevenzione (IPS) delle intrusioni.
La nostra rete è stata riorganizzata per proteggere la rete interna anche in caso di attacco alla DMZ.
Abbiamo chiuso le porte e i servizi non necessari, riducendo le potenziali vulnerabilità.
Un bilanciatore di carico è stato introdotto per migliorare le prestazioni e mitigare gli attacchi DDoS.
In futuro si può considerare l'aggiunta di un server proxy per ulteriori livelli di protezione.