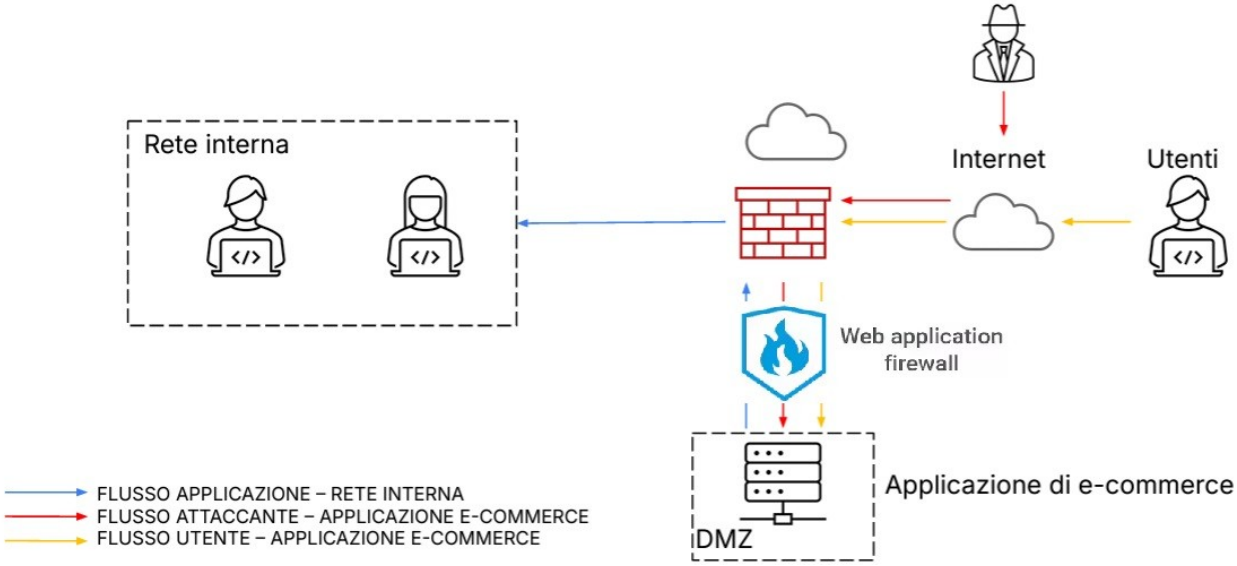
Benchmark M5 – Daniele Rufo

Security Operations

1 – Azioni preventive

Per proteggere l'applicazione web da attacchi come SQLi o XSS sarebbe opportuno introdurre nell'architettura di rete un WAF- Web Application Firewall.
Un WAF può essere hardware, virtuale (software-based), o cloud-based. La scelta varia a seconda della necessità dell'organizzazione e del tipo di infrastruttura che possiede. Visto il giro di affari della compagnia, descritto nella traccia, un WAF di tipo hardware risulta essere la più efficace tra le soluzioni poiché garantisce un controllo diretto con una latenza minima.
Il WAF va posizionato davanti la DMZ quindi al suo esterno così da filtrare il traffico diretto a tutti i server presenti al suo interno (nel nostro caso solo uno). Nel caso i server all'interno della DMZ fossero molteplici questa soluzione potrebbe richiedere un'ulteriore implementazione per supportare a livello di prestazioni il WAF, che si troverebbe a gestire molto traffico.
La figura seguente mostra l'implementazione.



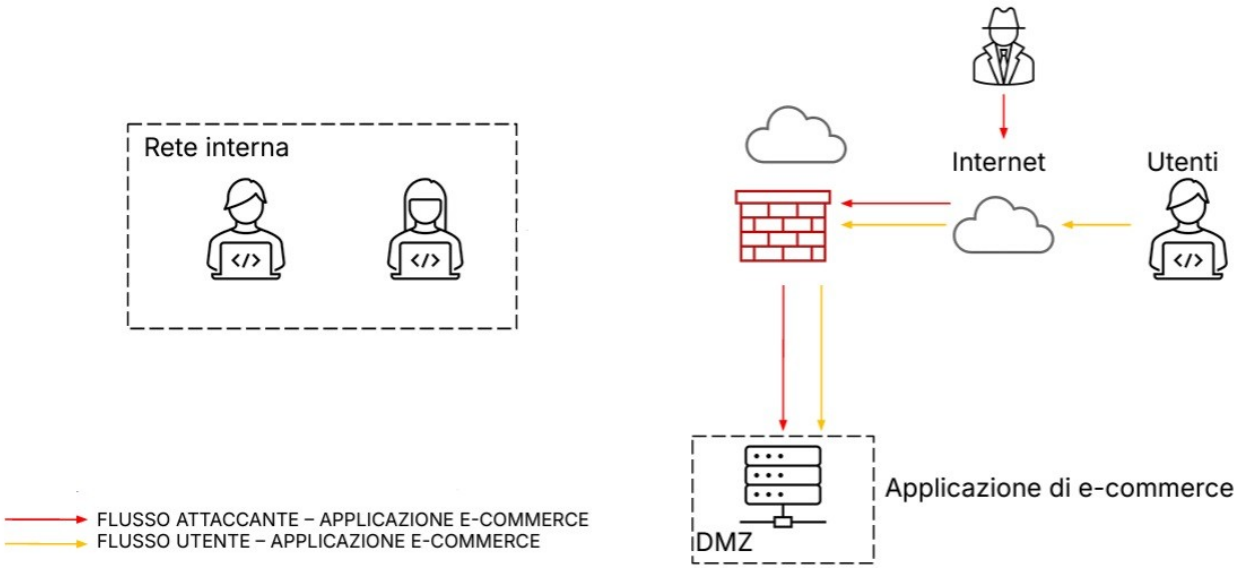
Alternativa sempre valida rimane la prevenzione fatta sul lavoro di tutto il team, soprattutto degli sviluppatori. Infatti la sanitizzazione dell'input utente per garantire sicurezza ed evitare injection indesiderate rimane un *must*, oltre a rispettare ed eseguire le *best practice.*

2 – Impatti sul business

La web application rimane fuori uso per 10 minuti e considerati i dati forniti è possibile calcolare l'impatto finanziario che ammonta a 15000 euro. Va considerato l'impatto che il disservizio può avere sulla clientela e la sua fidelizzazione, in questo caso 10 minuti non sono molti ma è sempre un fattore da considerare per questo tipo di incidenti.
In termini di azioni preventive contro attacchi DDoS diverse sono le strade da seguire, spesso complementari, segue un breve elenco:

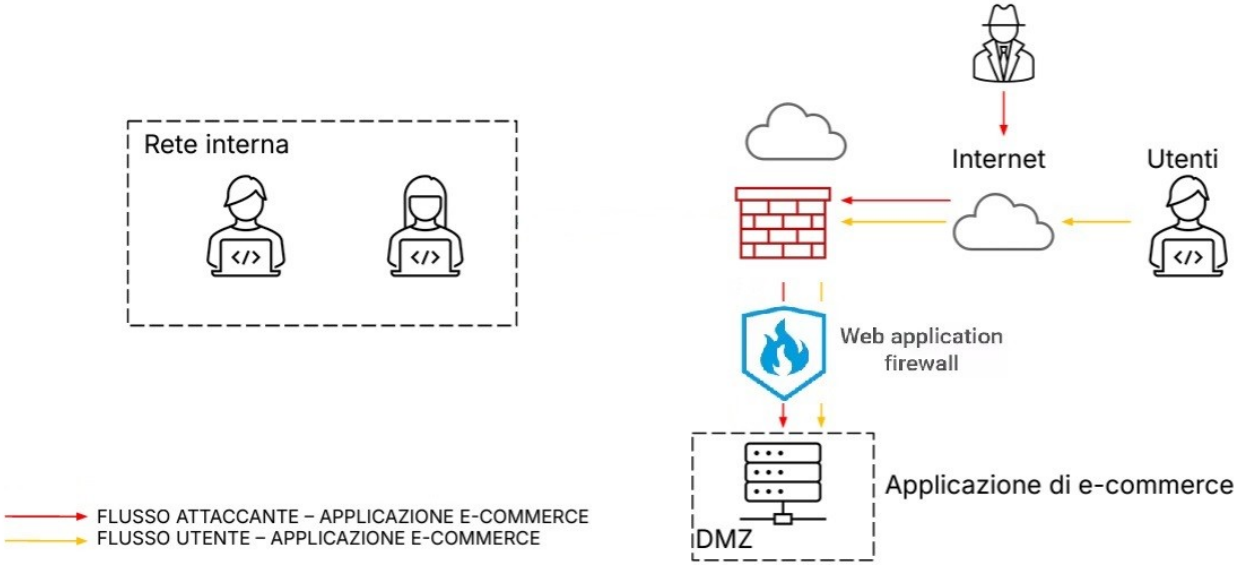
- la ridondanza e distribuzione del traffico aiutano a evitare o quantomeno mitigare attacchi del genere. A tale scopo vengono usate le Content Delivery Network che aiutano a distribuire il traffico.
- Configurare il WAF per limitare il numero di richieste in entrata in un determinato tempo.
- Implementare ulteriormente l'architettura ed, oltre al WAF, inserire sistemi IDS/IPS.

3 – Response
La rete risulta già segmentata, ma in questo caso è necessario ISOLARLA. Questa tecnica di response consiste nel tagliare la comunicazione tra la macchina infetta e la rete interna. In questo modo l'attaccante potrà ancora avere accesso alla macchina infetta ma non più alla rete interna.
Lo scopo è ovviamente quello di proteggere la nostra rete interna ed evitare che il malware si replichi e che l'attaccante sfrutti la macchina compromessa per tentare un accesso (magari provando poi una privilege escalation per ottenere permessi di root e prendere controllo dell'intero sistema).
La figura sotto mostra come sia totalmente assente la connessione tra web app e rete interna.



Questa tecnica fa parte di una serie di 3 azioni di risposta (segmentazione, isolamento e rimozione) che vengono applicate generalmente a cascata. Si parte dalla segmentazione che è quella meno invasiva per poi muoversi a cascata verso isolamento, spiegato in figura, e rimozione. Quest'ultimo è l'approccio più aggressivo e comporta il completo isolamento della macchina infetta che ora non solo non comunica con la rete interna, ma non comunica affatto. L'attaccante non avrà più accesso alla stessa.

4 – Soluzione completa
La figura sotto rappresenta l'unione della fasi di prevenzione e risposta, per questo l'architettura proposta varia da quella inizialmente fornita.



5 – Ulteriore Implementazione
Come già evidenziato nelle azioni preventive al punto 2, una strategia, sicuramente più aggressiva per la compagnia ed anche per le sue finanze, è l'installazione di un *Intrusion Prevention System* (generalmente noto come IPS) di tipo hardware. Farà da complemento perfetto al WAF non solo monitorando il traffico ma mettendo in atto delle response iniziali che mitigano, o evitano, l'attacco.