W20D4 – Pratica

Epic Education Srl

Difesa da SQLi/XSS
Attacco DDos
Response
Soluzione completa
Modifica aggressiva

Simone Giordano

27/11/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Esercizio

Traccia

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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.

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 in questa problematica.*

Response: l'applicazione Web viene infettata da un malware.
La vostra priorità è che il malware non si propaghi sulla vostra 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.

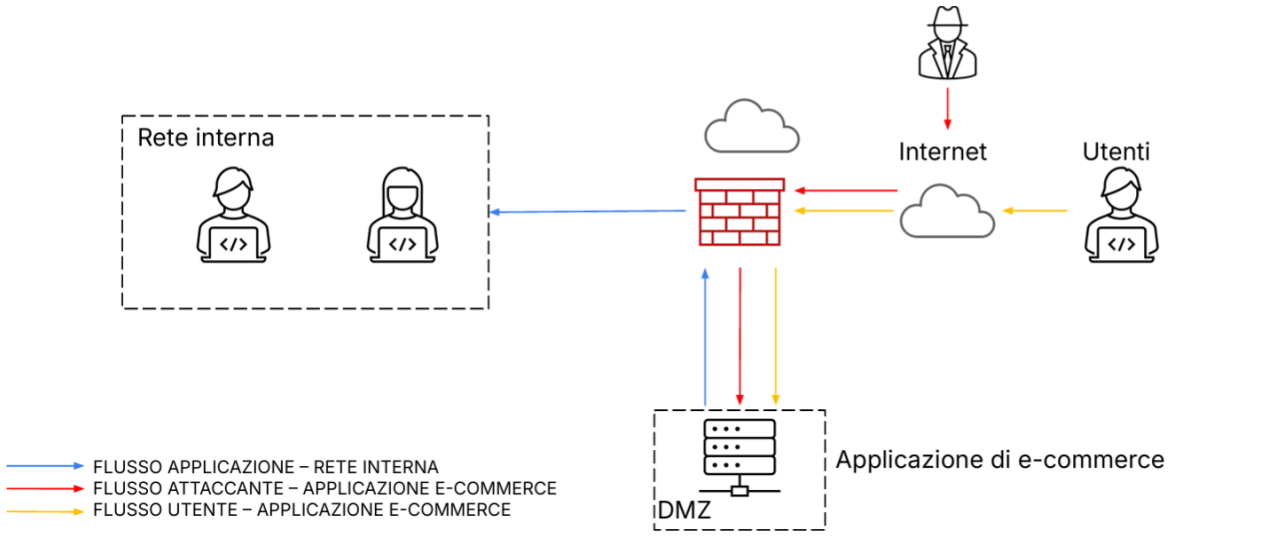
Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2).

Architettura di rete

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

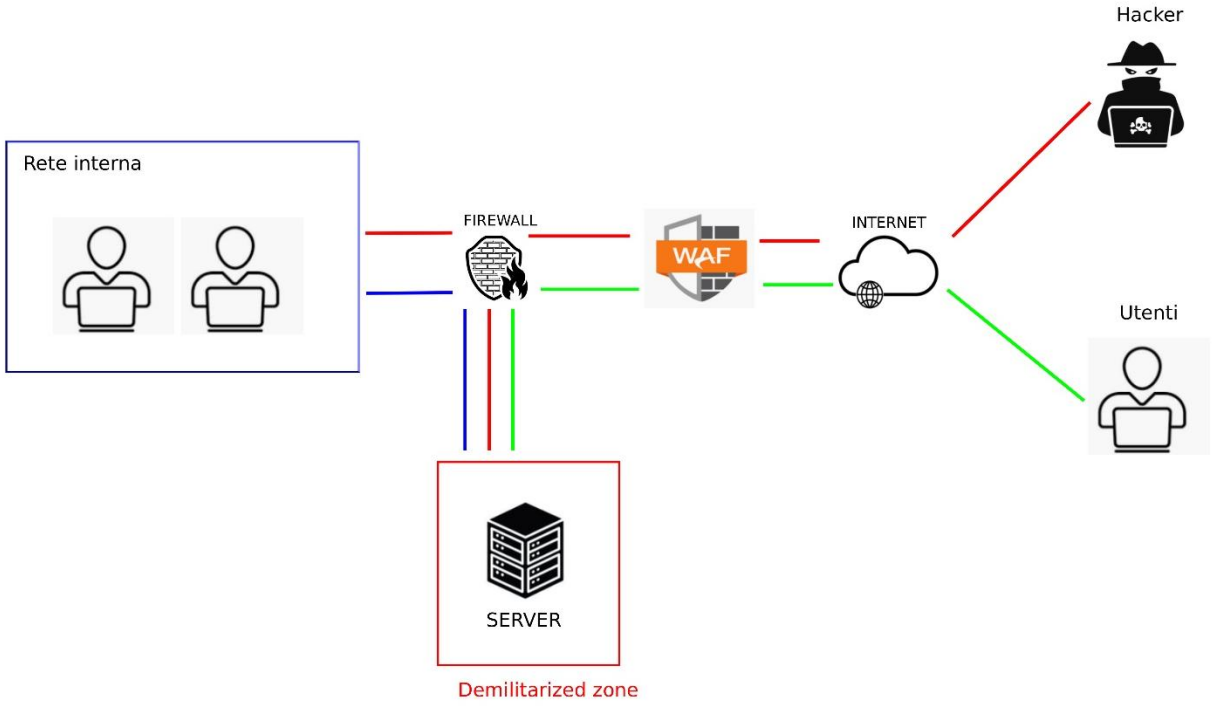
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Difesa App Web da SQLi o XSS

Azioni preventive

Inserire un WAF tra il firewall e il server che effettua l'hosting della WebApp. Il WAF è un firewall specifico per applicazioni web (Web Application Firewall), che opera a livello 7 (applicazione) del modello OSI. In questo caso il WAF deve proteggere il traffico che entra nella Web App e identificare eventuali SQLi e XSS.



Attacco DDoS

Impatti sul business

Moltiplicando la spesa media per minuto, pari a 1.500 €, per il tempo in cui l'applicazione non è raggiungibile, si ottiene l'impatto economico del disservizio. Nel caso di 10 minuti di downtime, la perdita stimata è di 15.000 €.

Spesa al minuto	Stop applicazione (minuti)	Impatto sul business
1.500 €	10	**15.000 €**

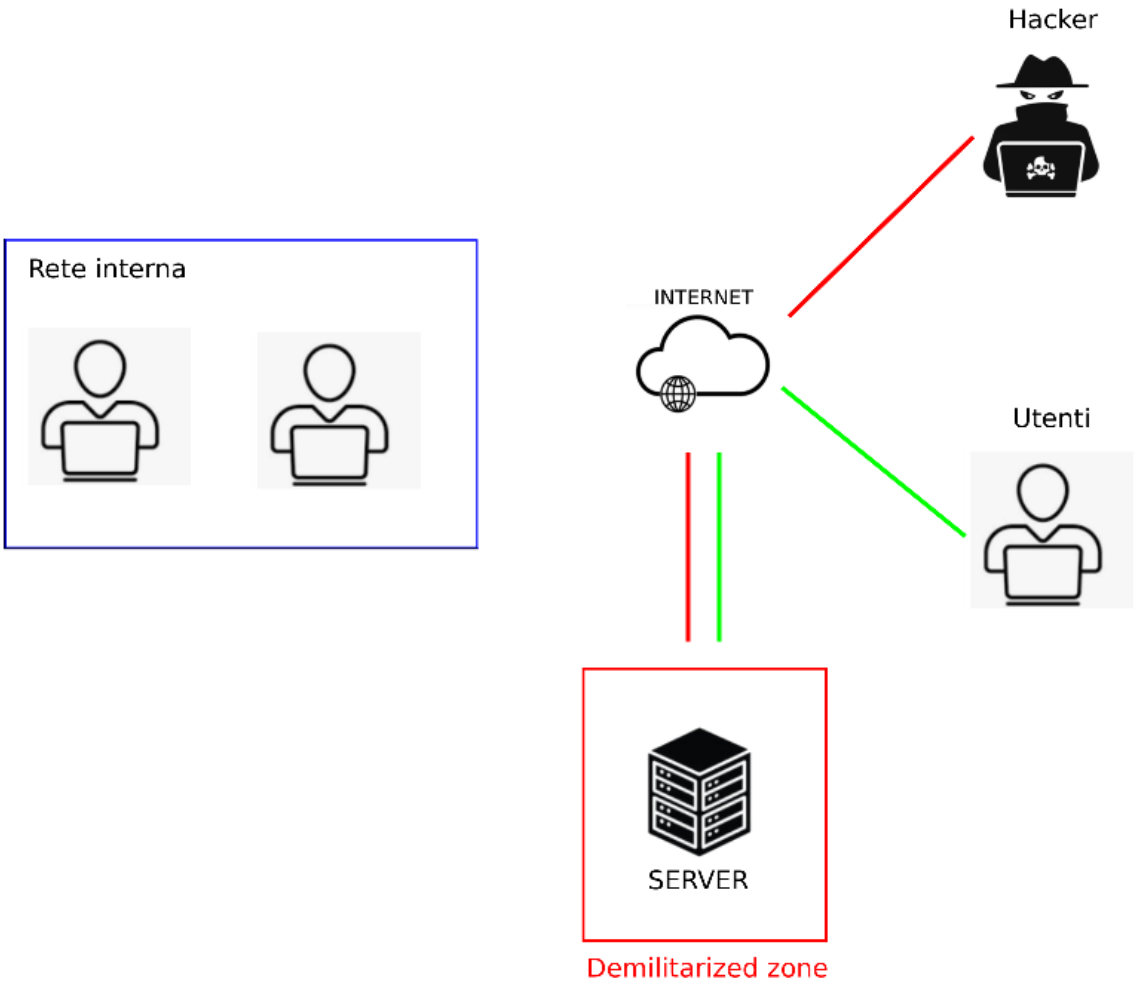
Valutazione azioni preventive

L'introduzione di un WAF rientra nelle misure preventive, poiché contribuisce anche alla mitigazione degli attacchi DDoS. Tra le soluzioni che possono essere integrate con un WAF troviamo:

- **Load balancing**, per distribuire il traffico su più server e ridurre il rischio di sovraccarico.
- **Server geo-distribuiti**, posizionati in punti diversi per garantire continuità del servizio e assorbire meglio picchi di traffico o attacchi mirati.
- **Monitoraggio dello stato delle prestazioni delle macchine tramite il SIEM.** Un eventuale aumento repentino delle prestazioni potrebbe indicare un attacco DDoS**.**

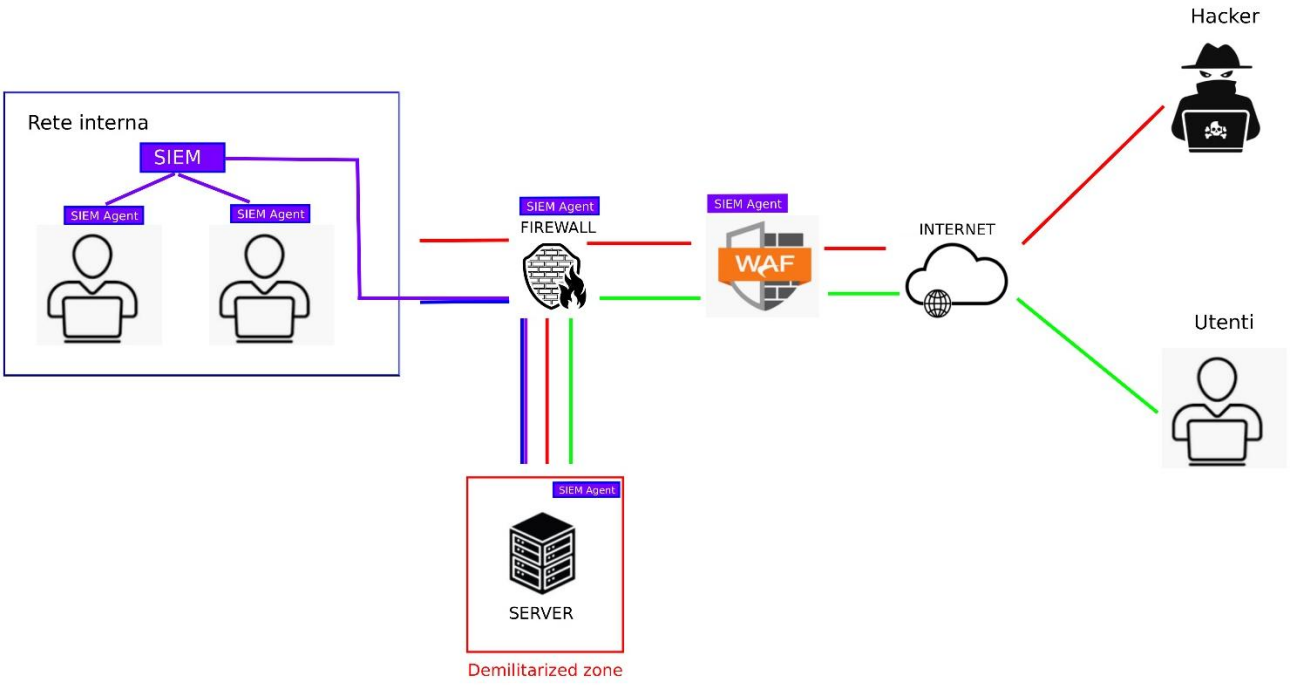
Response

Per evitare che il malware si propaghi nella rete interna è necessario isolarla completamente, rimuovendo il firewall che la collegava al server con l'applicazione, quindi il WAF e il collegamento al SIEM ma mantenedo il collegamento a internet in modo che gli utenti possano continuare ad accedere al servizio, incluso l'utente malintenzionato.



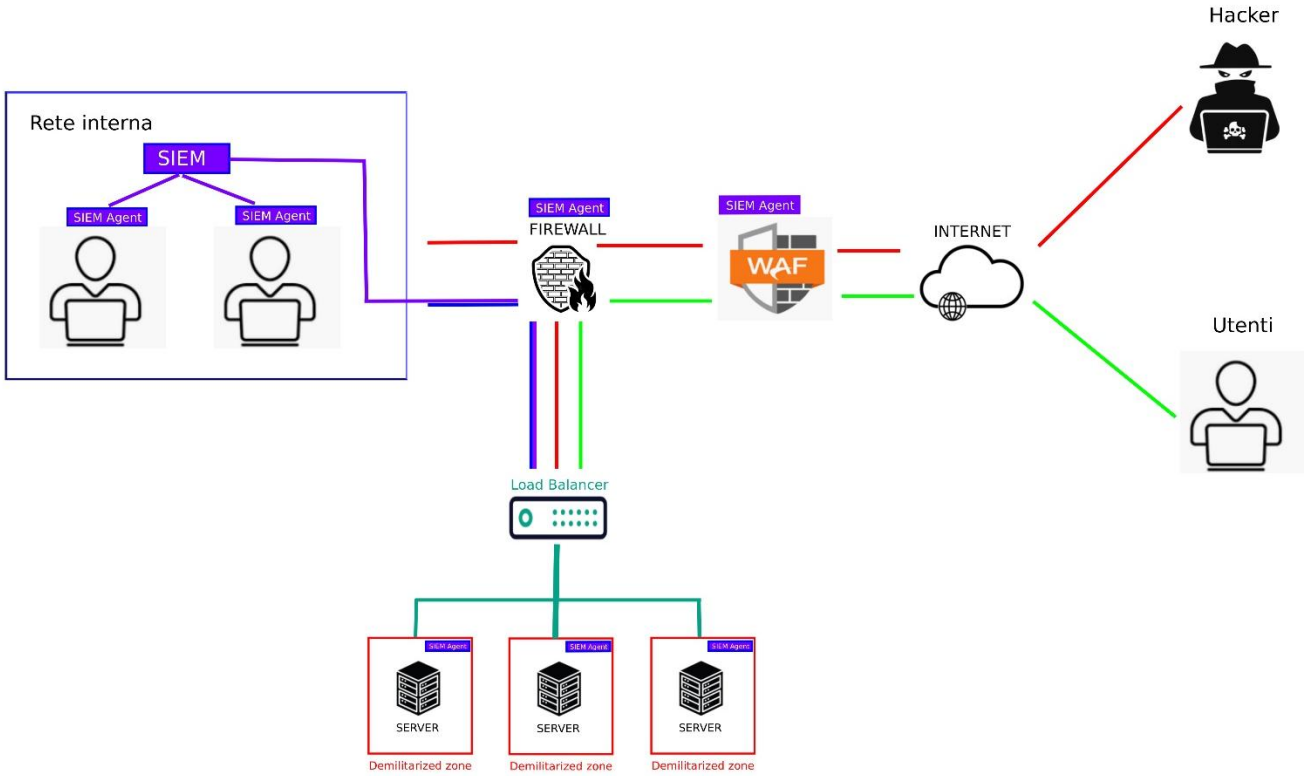
Soluzione completa

Inserire un SIEM installando il relativo agent sul server, sulle macchine della rete interna, sul firewall e sul WAF per ricevere e monitorare tutte le informazioni che arrivano dai vari agent e agire in caso di comportamenti sospetti.



Modifica “più aggressiva” all’infrastruttura

- Inserimento di un load balancer per distribuire il carico su più server per prevenire eventuali sovraccarichi e/o attacchi Dos/DDoS.
- Installazione dei server in aree geografiche diverse, per garantire il servizio in caso uno dovesse andare giù.
- Sanitizzazione input utente.
- Penetration Test su codice sorgente.
- Inserimento di honeypot nella Web App per attirare eventuali utenti malintenzionati e studiarne i comportamenti.



- Sanitizzazione input utente
- Penetration test