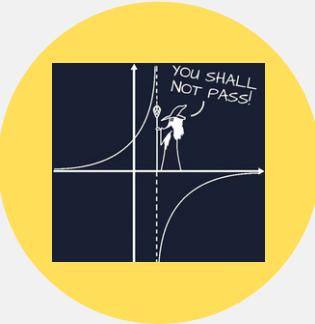


# **Traccia n. 1**

## **Azioni preventive**

# Protezione da attacchi XSS e SQLi

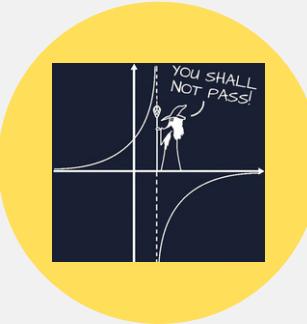


Per evitare danni agli asset ed incidenti di sicurezza a causa di possibili attacchi di tipo **Cross Site Scripting (XSS)** o di tipo **SQL Injection (SQLi)** si potrebbe valutare l'implementazione di un **Web Application Firewall (WAF)** posizionato a difesa del server di e-commerce presente nella **zona demilitarizzata (DMZ)**.

Gli attacchi di tipo **XSS** sono di due tipi:

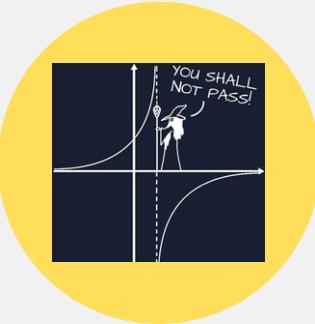
- **XSS Reflected:** questa tipologia di attacco prevede di sfruttare l'attività dell'utente e la capacità dei moderni browser di navigazione web di eseguire del codice al loro interno, per far sì che l'utente clicchi su un link modificato contenente del codice malevolo che portato in esecuzione, si occuperà di rubare dati all'utente, come ad esempio le credenziali per l'accesso ad una pagina web. Gli attacchi di questa tipologia ormai sono rilevabili dai moderni browser e per questo è più difficile che vadano a buon fine. In questi casi viene sfruttata l'ingenuità e l'inconsapevolezza dell'utente.
- **XSS Stored:** questa versione di attacco è la più pericolosa e la più difficile da rilevare. Il codice malevolo in questo frangente, viene direttamente iniettato nella pagina web, sfruttando dei campi di testo che lato back-end non vengono correttamente sanitizzati o non vengono del tutto controllati, come ad esempio i commenti a fondo pagina. Quindi, ogni utente che visiterà la pagina sarà soggetto all'attacco del malintenzionato, e anche lato web server, chi gestisce la pagina farà fatica ad accorgersi che è avvenuta una modifica al codice del sito.

# Protezione da attacchi XSS e SQLi

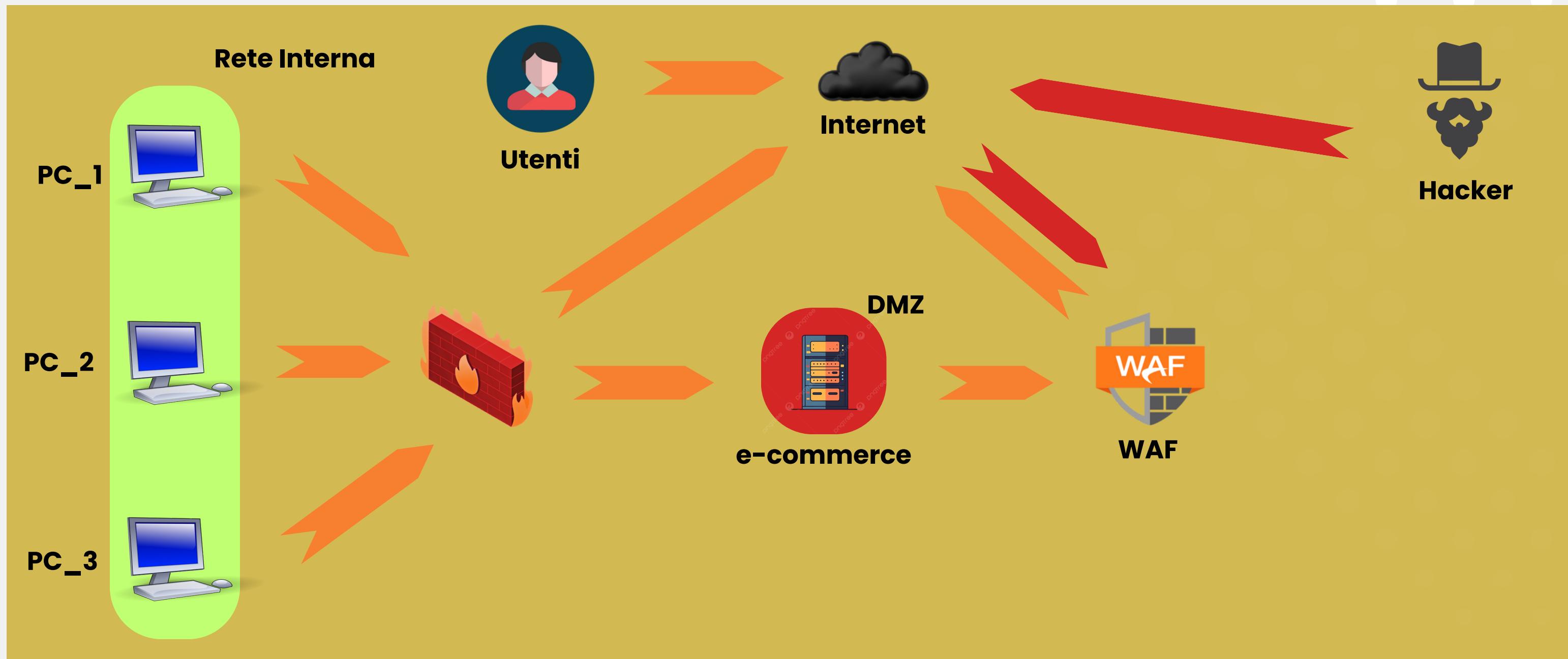


Gli attacchi del tipo **SQLi**, sono definiti anche come attacchi di **command injection**. L'attaccante sfrutta le **query** nel linguaggio **SQL (Structured Query Language)** per ottenere accesso ai dati presenti in un **database SQL**, o addirittura la possibilità di modificarli. In questo modo, se il campo di ricerca del malcapitato sito internet non ha i necessari controlli di sanitizzazione per l'input dell'utente, l'attaccante di turno potrà sfruttare questa vulnerabilità a suo piacimento, facendo sì che il database si comporti in modo anomalo e gli restituisca tutti i dati di cui ha bisogno.

# Protezione da attacchi XSS e SQLi



Ecco come potrebbe essere modificata la struttura della rete originale per aumentarne il grado di affidabilità e sicurezza.



Consegna U3 S9 L5

## **Traccia n. 2**

# **Business Impact**

# Business Impact



Un attacco di tipo **Distributed Denial of Service (DDoS)**, consiste dello sfruttare una rete di macchine dette **zombie**, cioè infette da malware e controllate da remoto tramite un **CC Server (Control and Command Server)**, per avviare una serie infinita di richieste di accesso ad una pagina web specifica, ottenendo così il risultato di saturare la potenza di calcolo del server sul quale è hostata la pagina, ed impedendo la normale fruizione dei servizi erogati dalla stessa agli utenti che si collegano, rendendo di fatto la pagina irraggiungibile. Per creare danni ancora maggiori, di solito i malintenzionati sfruttano le cosiddette **botnet**, ovvero delle enormi reti di macchine **zombie** composte da decine di migliaia di apparecchi connessi alla rete.

Considerando che l'applicazione web dell'azienda è rimasta ferma per ben 10 minuti a causa di questo attacco, e che in media le **entrate per minuto di questa applicazione fruttano 1200€**, si può calcolare che l'azienda **ha già perso 12.000€**. Per evitare che attacchi di questo genere o ancor peggio, di portata ancora maggiore possano verificarsi ancora, serve attuare delle misure preventive di sicurezza.

# Business Impact



Si potrebbe implementare un **failure cluster**, ovvero un server di e-commerce duplicato in modo da avere la **ridondanza** dei sistemi necessari a far funzionare la web app anche in caso di inconvenienti come questi. Quindi al ripresentarsi di un **attacco DDoS**, si potrebbe disconnettere il server primario ed avviare il secondario per mantenere il servizio attivo e non creare alcun disservizio agli utenti della piattaforma.

Un'altra soluzione possibile sarebbe la **riduzione della superficie di attacco** tramite il blocco delle porte nelle quali non ci si aspetta di ricevere alcun tipo di connessione per il corretto funzionamento del servizio.

O ancora si potrebbe optare per una soluzione di **bilanciamento del carico di rete**. Ovvero smistare il traffico tra più web server per rendere molto difficile la possibile saturazione delle risorse hardware a causa di attacchi di questo tipo.

Come ulteriore soluzione, si può considerare l'implementazione di un **Web Application Firewall (WAF)** o di un sistema **IDS/IPS (IntrusionDetection System/Intrusion Prevention System)** per il rilevamento e conseguente blocco di attacchi del genere.

Consegna U3 S9 L5

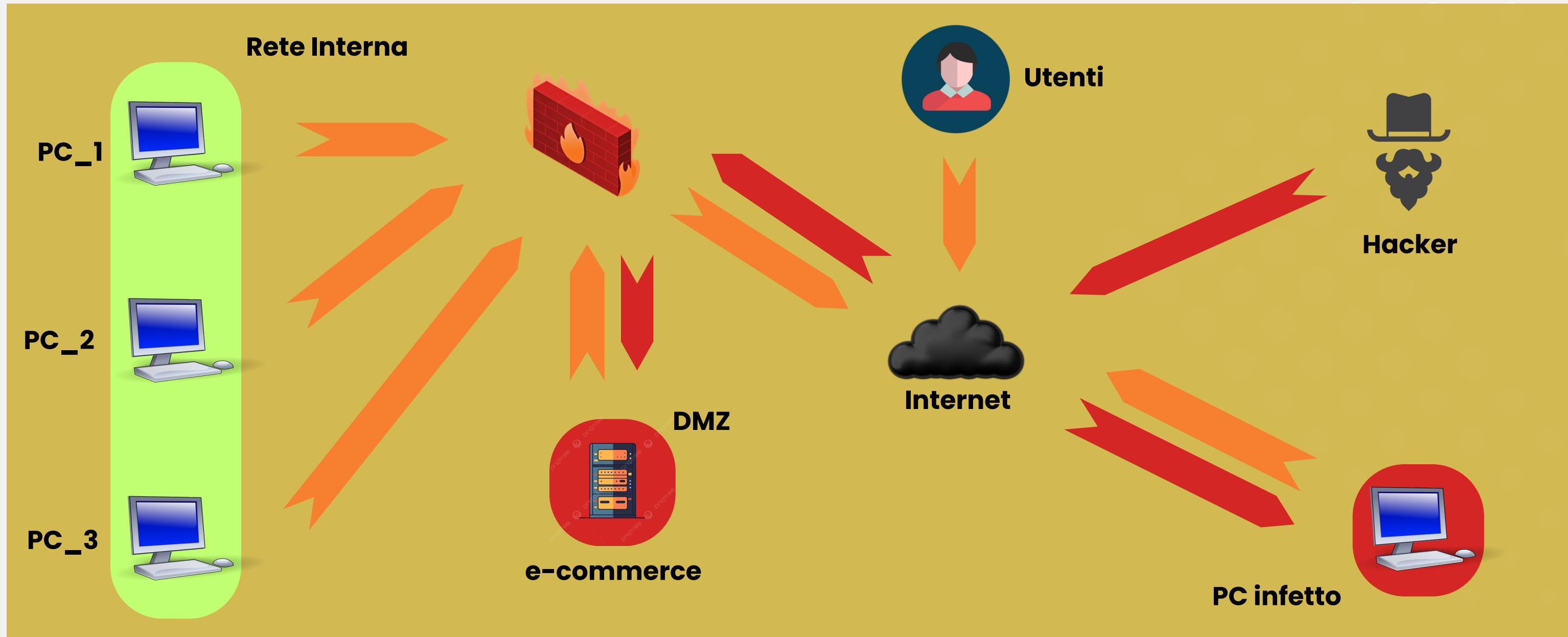
# **Traccia n. 3**

# **Incident Response**

# Incident Response



Per evitare la propagazione del **malware** dalla macchina infetta a tutte le altre connesse alla rete interna, si può scollegarla da essa ma comunque mantenerla connessa ad internet. Questa tecnica è definita di **isolamento**. Agendo in questo modo, l'attaccante avrà ancora pieno accesso al computer infetto tramite la rete.



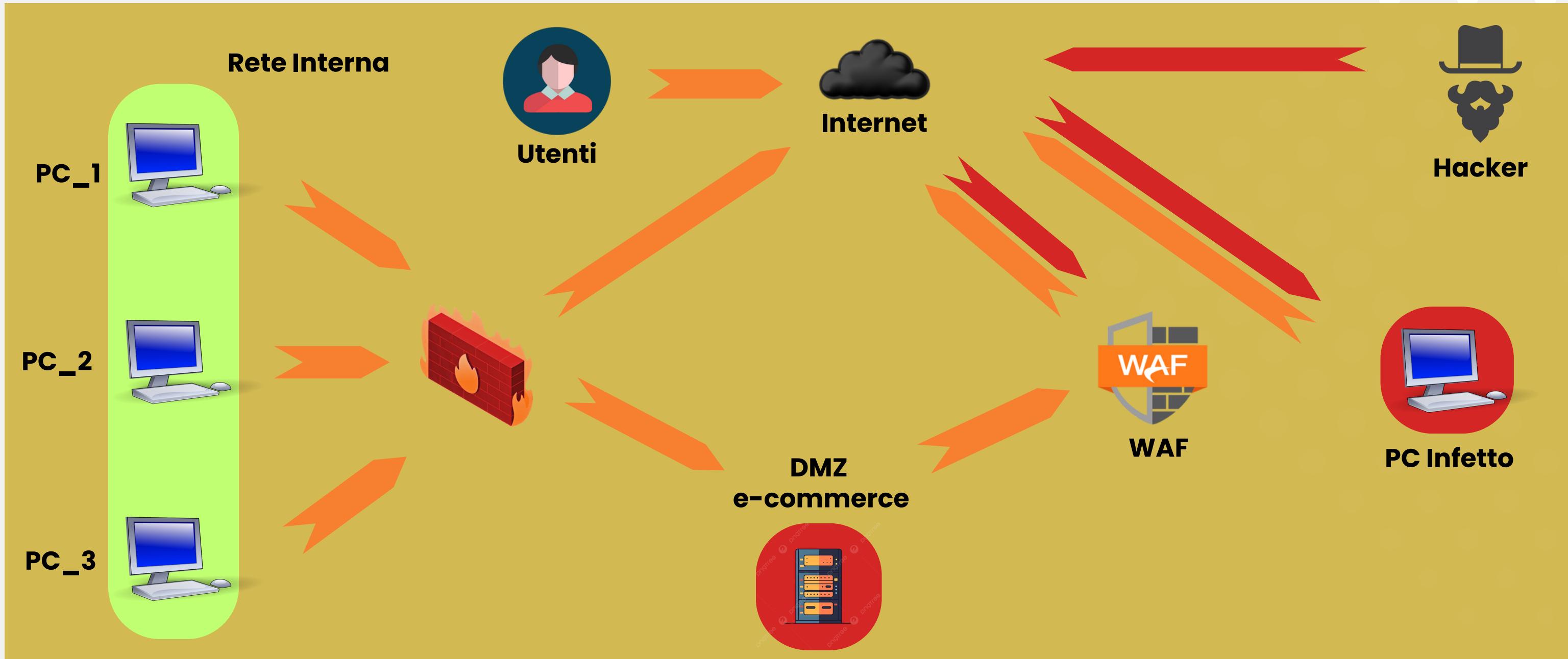
# **Traccia n. 4**

## **Soluzione di rete completa**

# Soluzione di rete completa



Integrando le soluzioni della traccia n.1 e della traccia n.2 abbiamo ottenuto questo schema di rete. E' stato implementato l'**isolamento** della macchina infetta rispetto alla rete interna e a protezione dell'e-commerce è stato inserito un **WAF**.



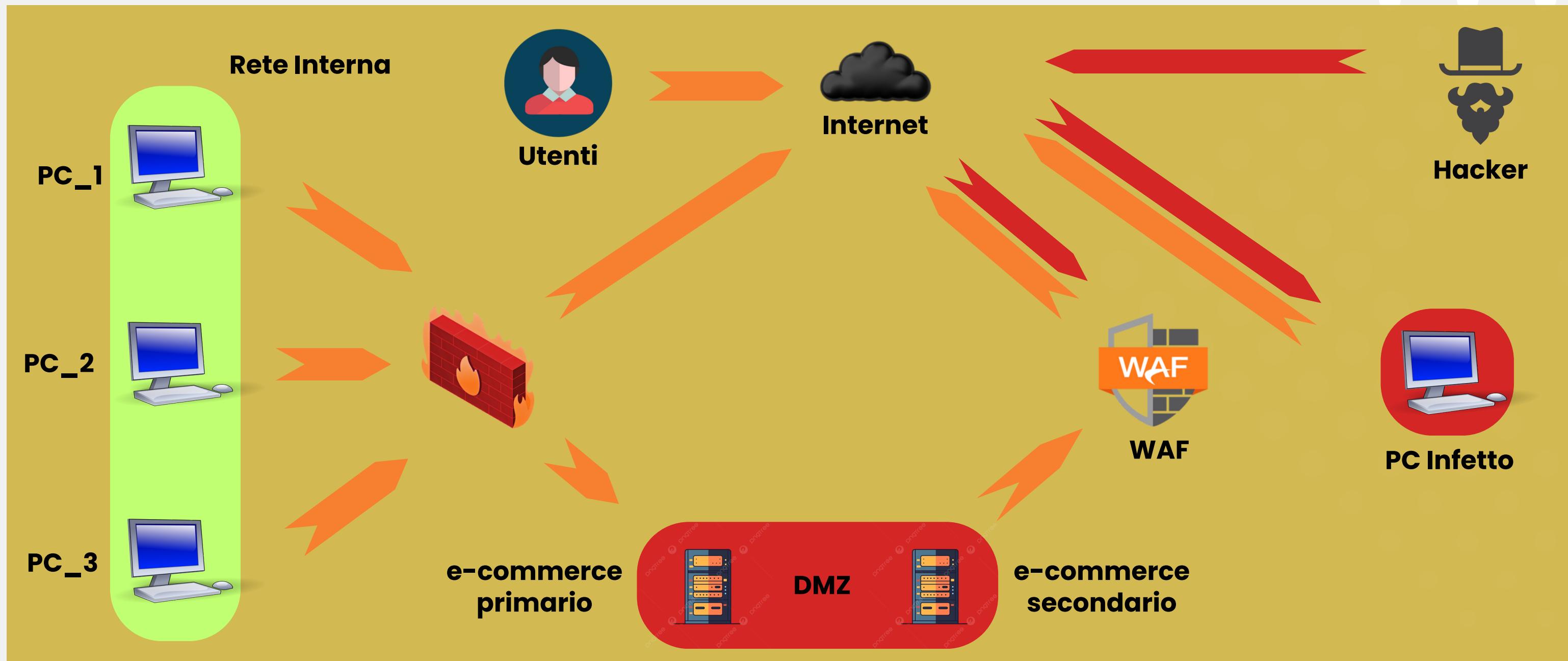
# **Traccia n. 5**

## **Protezione aggressiva della rete**

# Soluzione di rete n.1



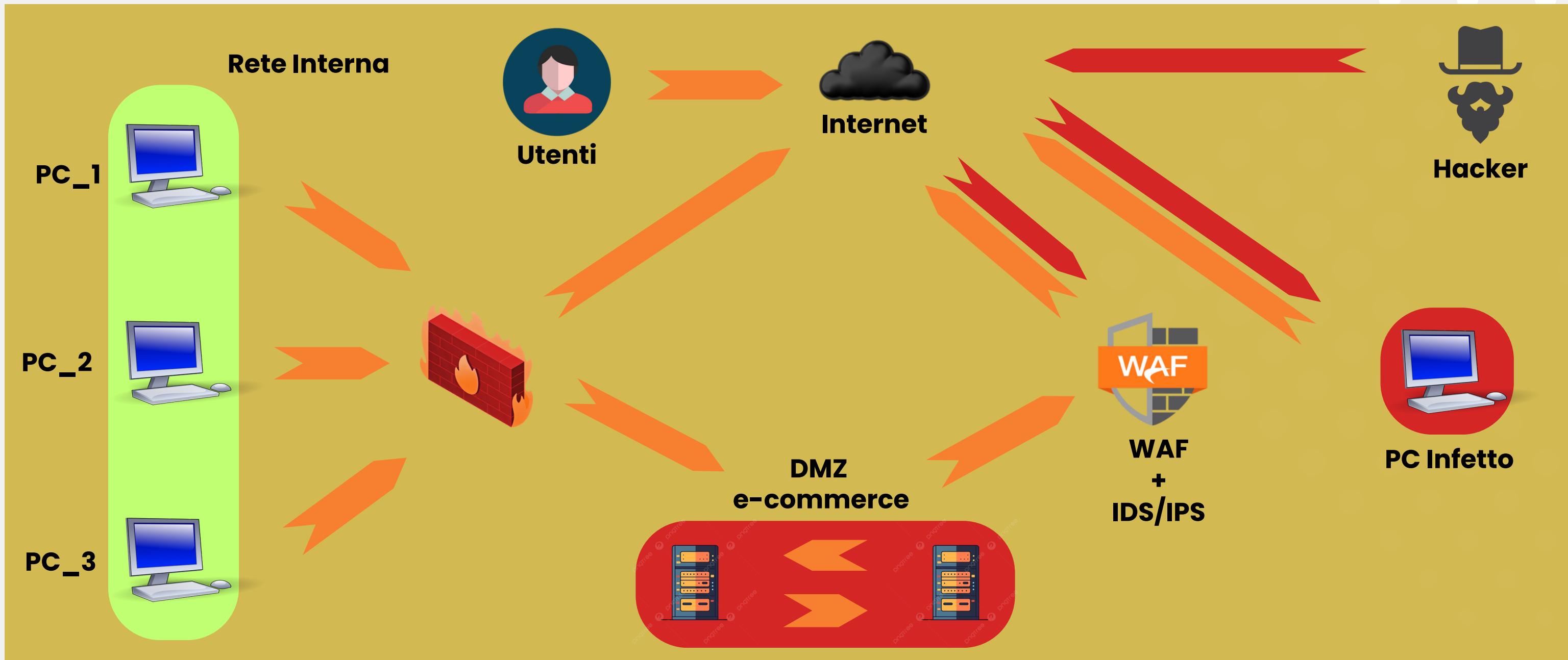
Ecco come potrebbe essere modificata la struttura della rete originale per aumentarne il grado di affidabilità e sicurezza. E' stato implementato un **failure cluster**, ovvero un secondo web server da utilizzare in caso di avaria del server principale entrambi protetti da un **WAF**, e l'**isolamento** della macchina infetta dalla rete interna.



# Soluzione di rete n.2



Per aumentare ulteriormente il grado di affidabilità e sicurezza della rete, è stato implementato il **bilanciamento del carico** su più web server per garantire il corretto funzionamento dell'e-commerce anche in caso di sovraccarico, l'**isolamento** della macchina infetta rispetto alla rete interna, e a protezione dell'e-commerce sono stati inseriti un **WAF** e i sistemi **IDS** ed **IPS**.



**Grazie**

**Gianluca Sansone**