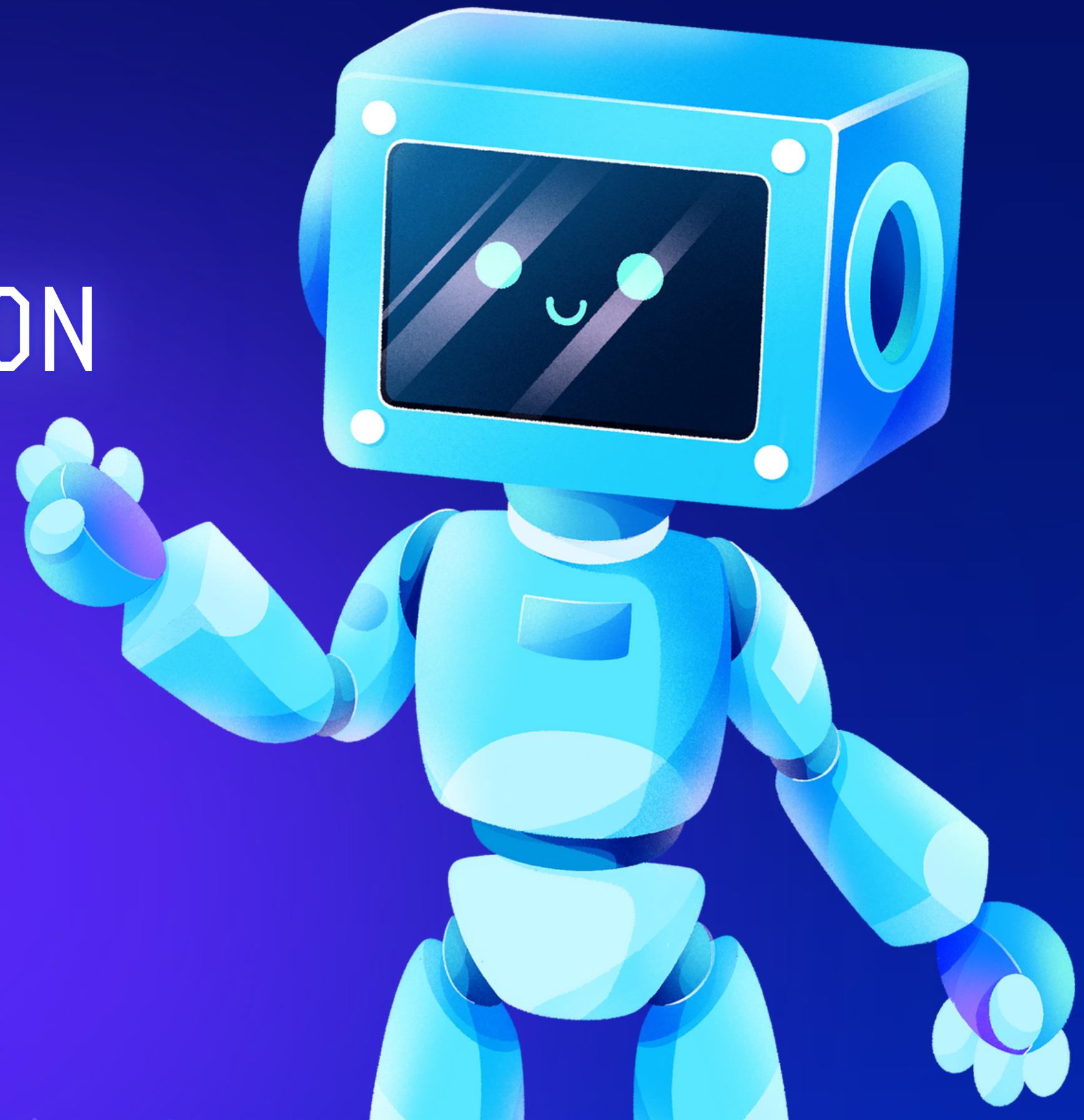
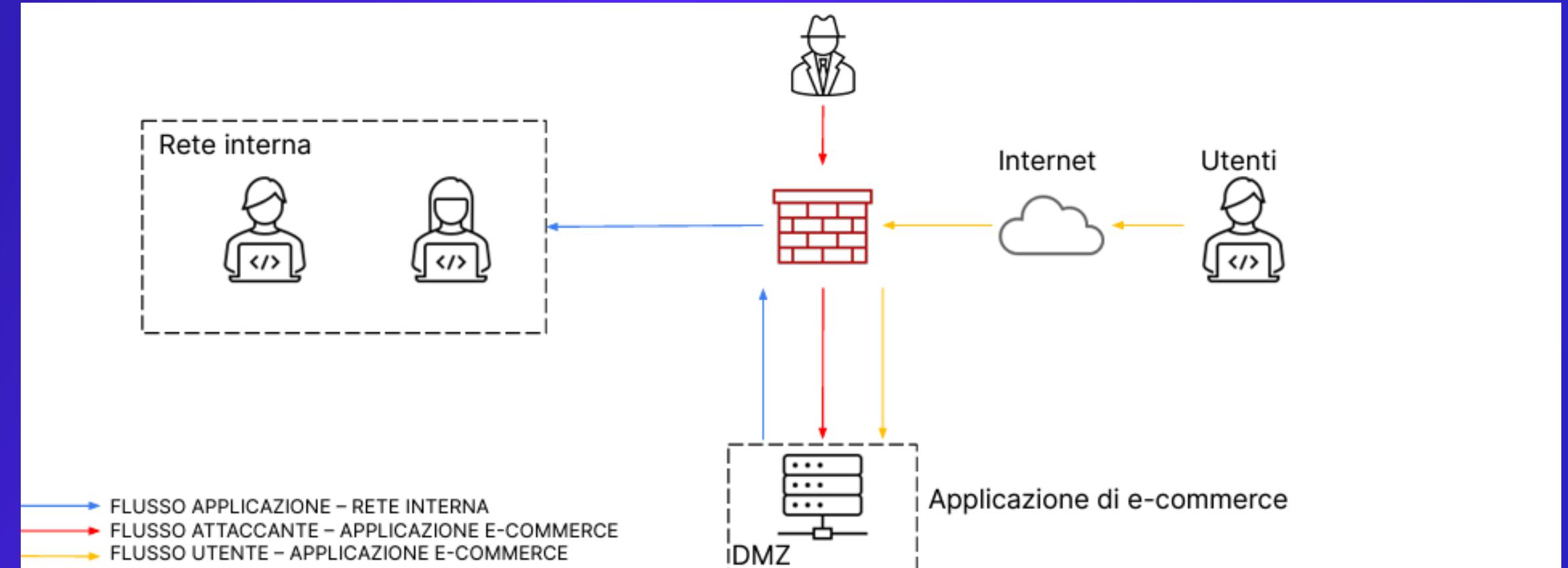


SECURITY OPERATION CENTER

Ernesto Robles

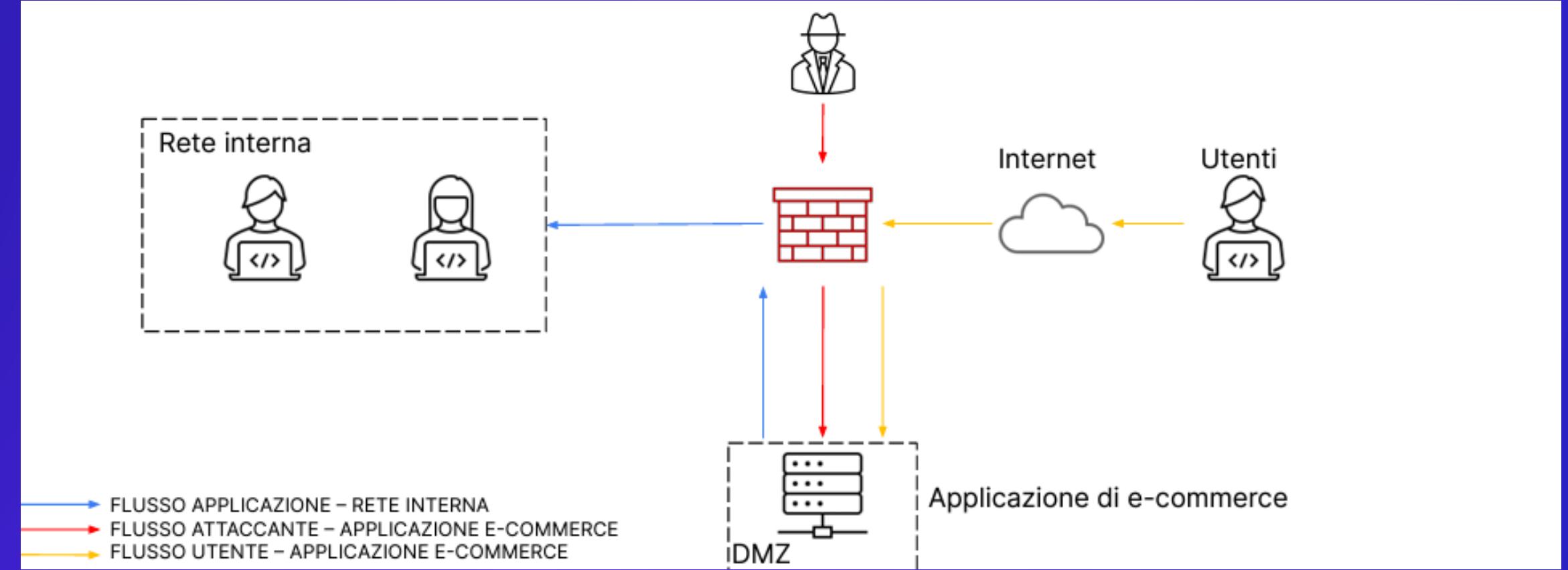




Data la seguente immagine possiamo immaginare una condizione come la seguente:

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.

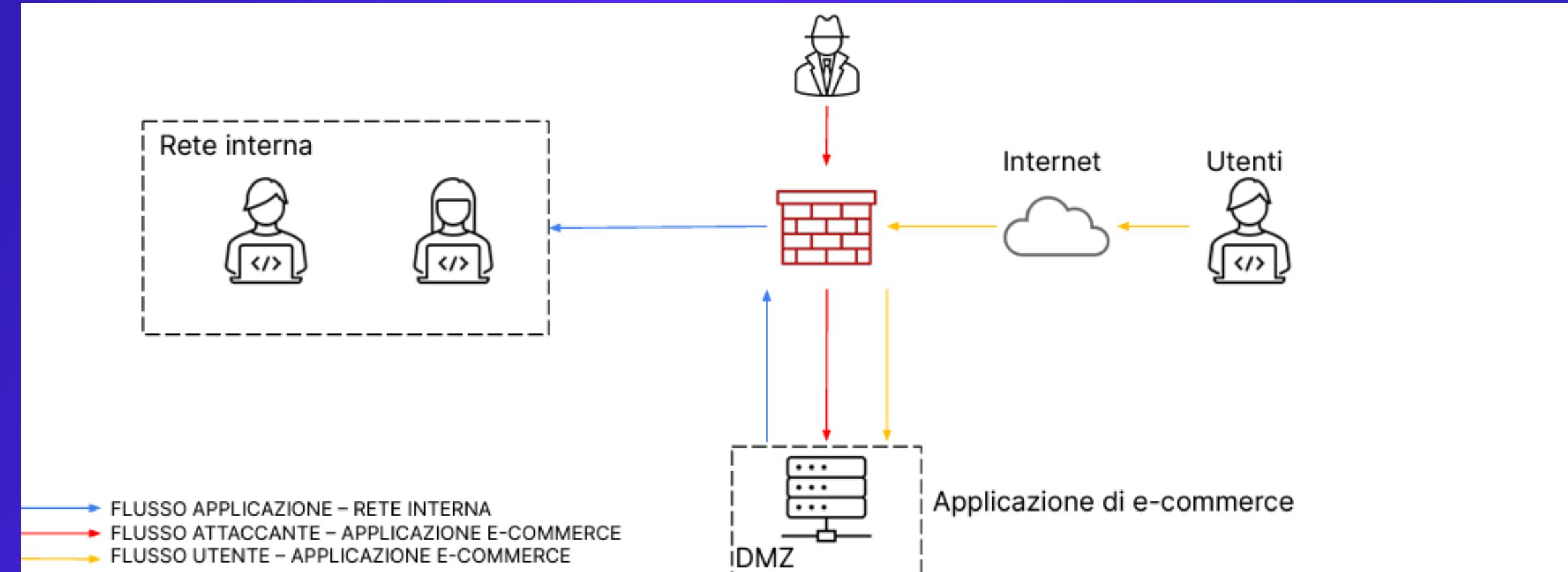


In base allo situazione prima esposta vengono effettuate delle azioni a risposta di possibili scenari quali:

Azioni preventive che si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato.

Impatti sul business nell'eventualità che l'applicazione Web subisca un attacco di tipo Ddos dall'esterno che renderebbe l'applicazione non raggiungibile per 10 minuti.

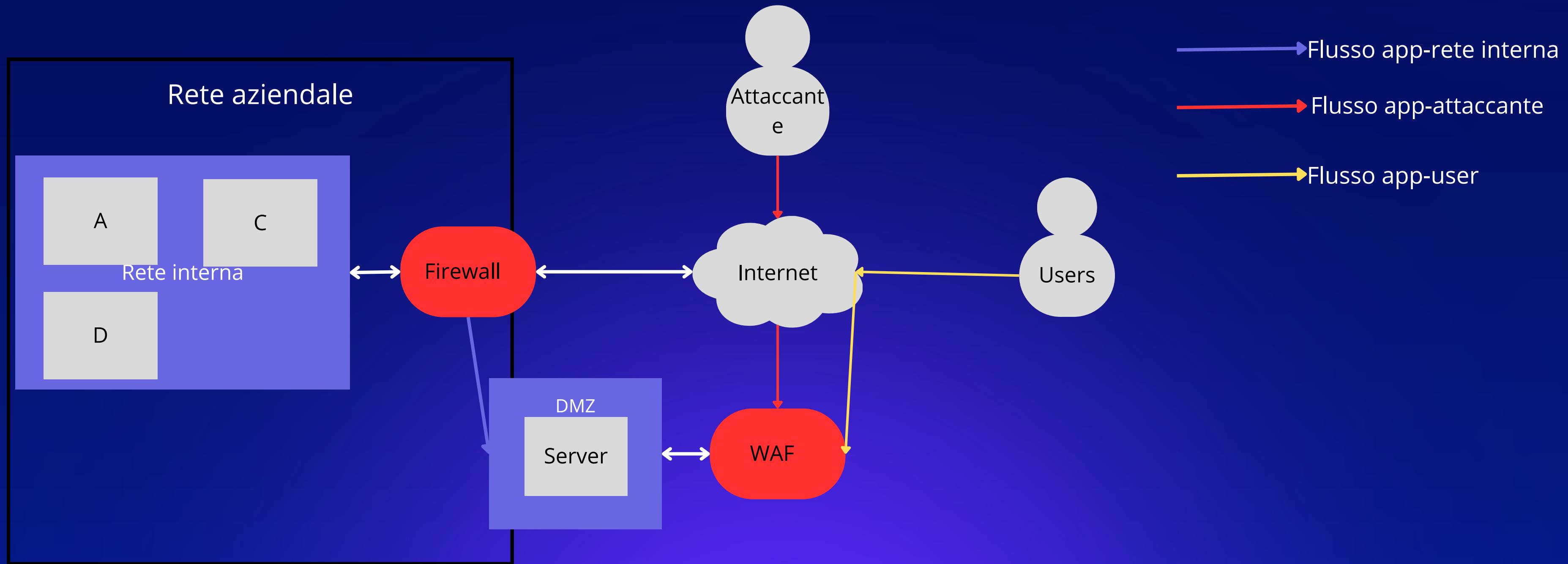
Response nell'eventualità che l'applicazione Web venga infettata da un malware.



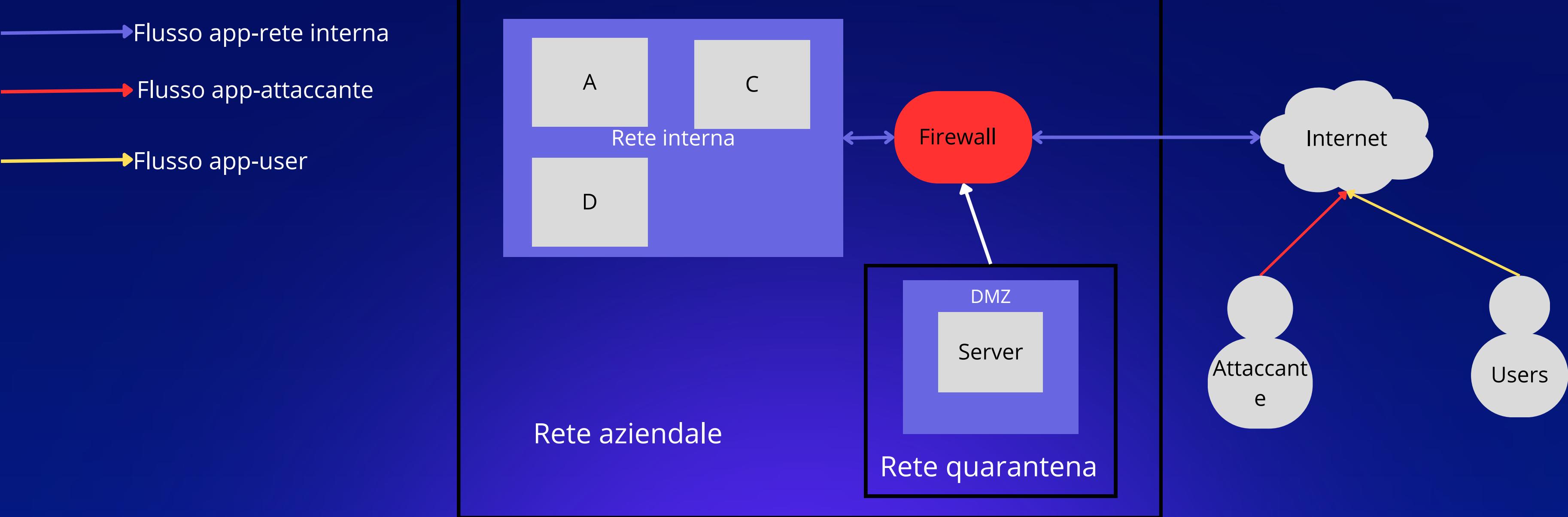
Il BIA (Business impact analysis) ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte.

Consideriamo uno scenario in cui l'applicazione Web subisce un attacco di tipo Ddos dall'esterno che rende l'applicazione non raggiungibile per 10 minuti, sapendo che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.. Possiamo calcolare l'impatto quantitativo sul business dovuto alla non raggiungibilità del servizio. andando a AV= valore dell'asset. T= durata dell'indisponibilità. SLE= single loss expectancy.

$$SLE = AV \cdot T = (1500/1) \cdot 10\text{min} = 15000\text{\$}$$

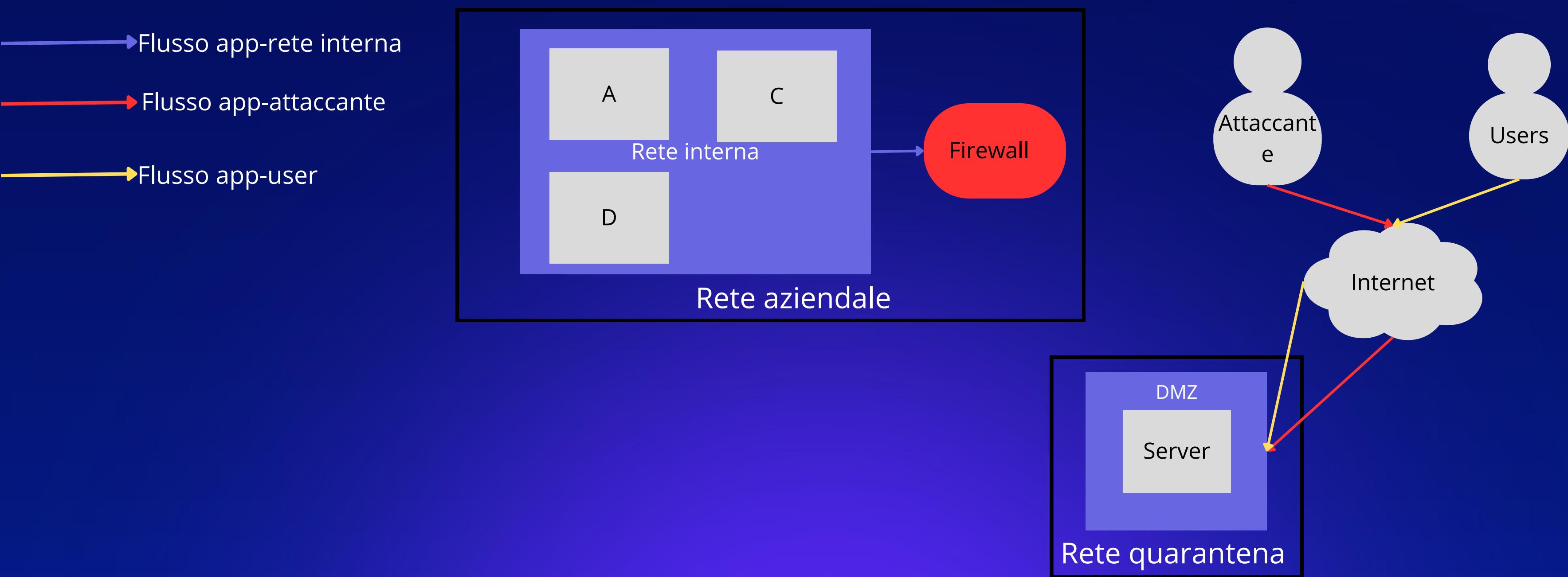


Nello scenario in cui un attaccante effettui attacchi di tipo SQLi oppure XSS come si evince dallo schema modificato per scongiurare il rischio di un attacco SQLi è stato aggiunto un WAF (Web Application Firewall) a difesa del nostro servizio esposto sulla rete, che viene configurato per filtrare e validare i parametri di input ricevuti dall'utente includendo la verifica dei caratteri speciali e delle strutture di query SQL nei dati inseriti, analizza inoltre il traffico in tempo reale alla ricerca di script dannosi e filtra tali contenuti prima che raggiungano l'applicazione web o vengano restituiti agli utenti.



In questo scenario l'applicazione Web è stata infettata da un malware la priorità è non lasciare propagare il malware sulla rete interna ed in un primo momento potremmo non essere interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata

Per difendere la rete interna usiamo la tecnica della segmentazione, particolarmente utile anche nella fase di contenimento di un incidente in corso. La segmentazione permette di dividere una rete in diverse LAN o VLAN. In questo caso viene creata una rete ad hoc, che viene chiamata generalmente rete di quarantena, grazie alle configurazioni a livello network il malware risulterebbe così separato dal resto della rete ed incapace di riprodursi.



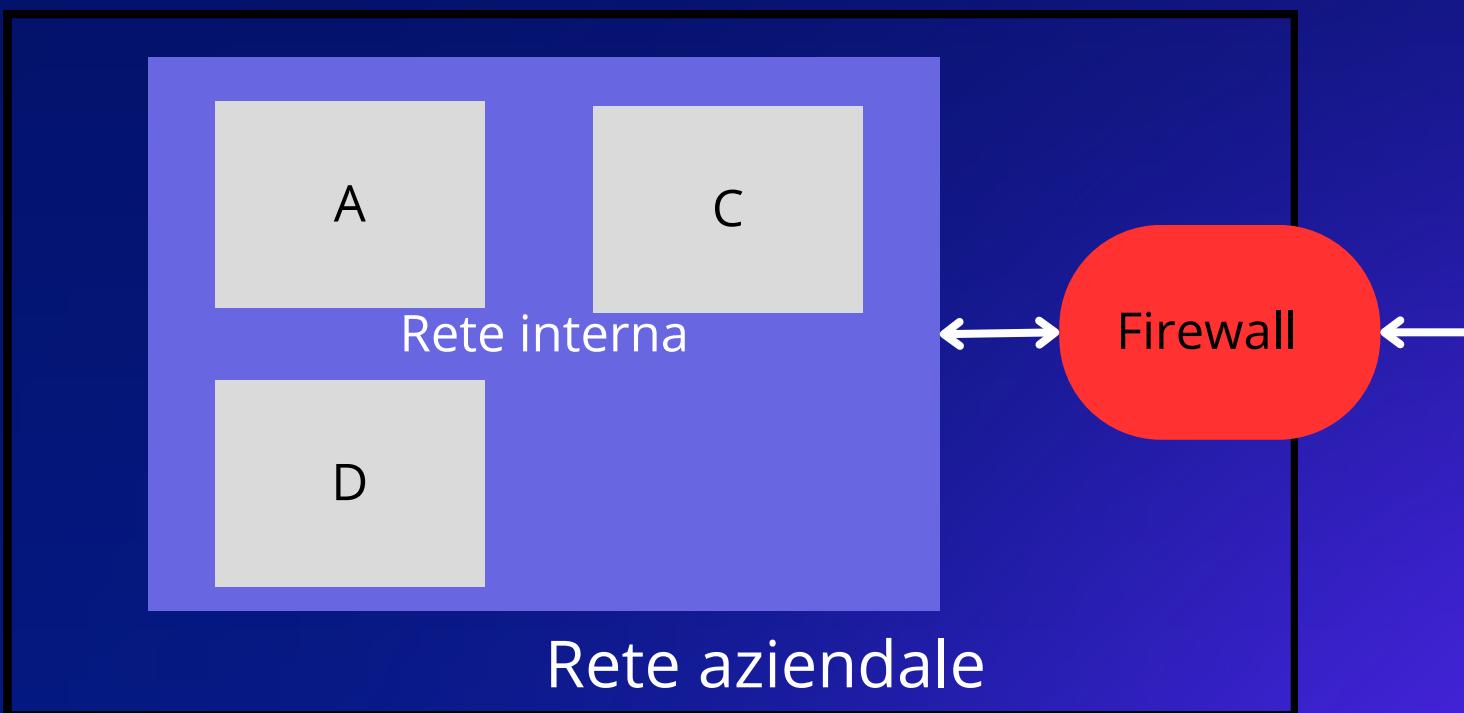
In questo scenario l'applicazione Web è stata infettata da un malware la priorità è non lasciare propagare il malware sulla rete interna ed in un primo momento potremmo non essere interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata

Per difendere la rete interna usiamo la tecnica dell'isolamento viene creata una rete ad hoc, che viene chiamata generalmente rete di quarantena e si disconnette completamente il sistema infetto dalla rete per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante, il quale però ha ancora accesso al sistema attraverso internet.

Flusso app-rete interna

Flusso app-attaccante

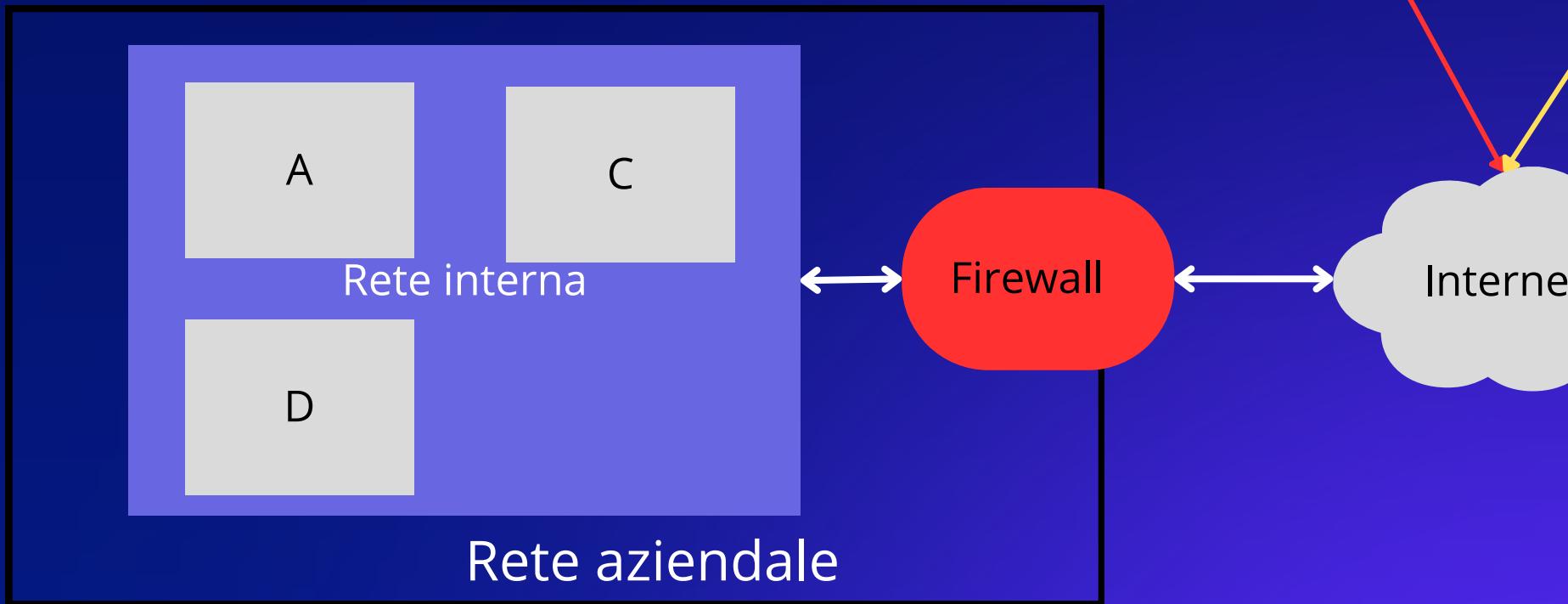
Flusso app-user



In alcuni casi l'isolamento non è ancora abbastanza perciò si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet come è qui raffigurato. In questo modo l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.

Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, si passa alla fase di recupero che consiste nel ristabilire la normale operatività delle applicazioni e dei servizi, ad esempio il recupero dei dati e delle informazioni perse perse, l'applicazione delle patch dove disponibili, revisione delle politiche dei firewall, IPS e IDS in questa fase si cerca di evitare che lo stesso attacco possa avere successo nuovamente in futuro.

- Flusso app-rete interna
- Flusso app-attaccante
- Flusso app-user



Se i sistemi, server e host fossero stati compromessi da un attaccante durante un attacco vanno considerati non più affidabili e di conseguenza ripuliti a fondo prima di essere utilizzati nuovamente. Per farlo si usano le tecniche di reconstruction o rebuilding. ●

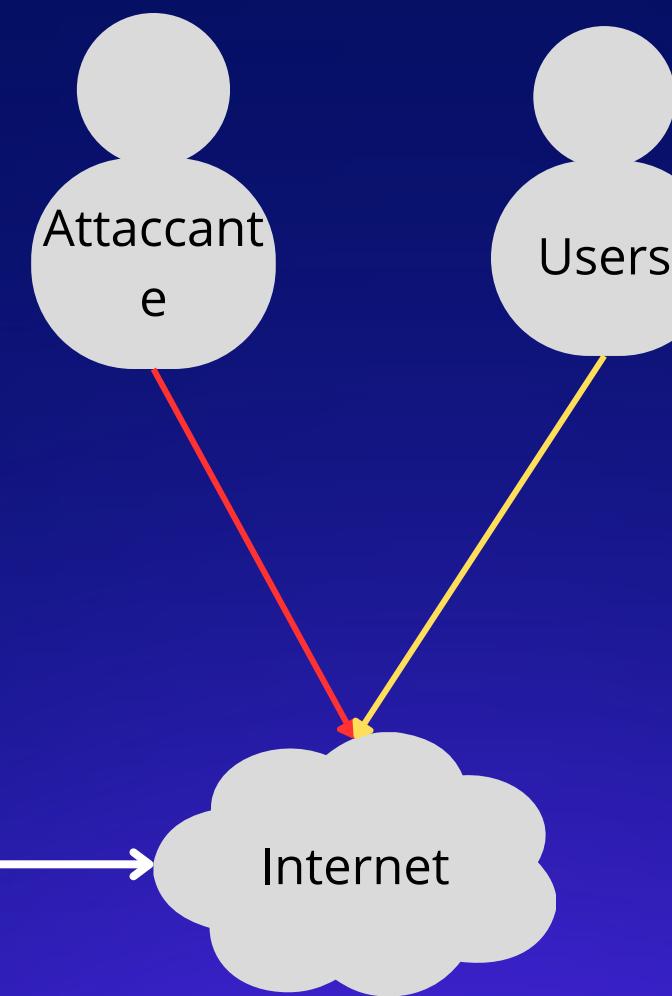
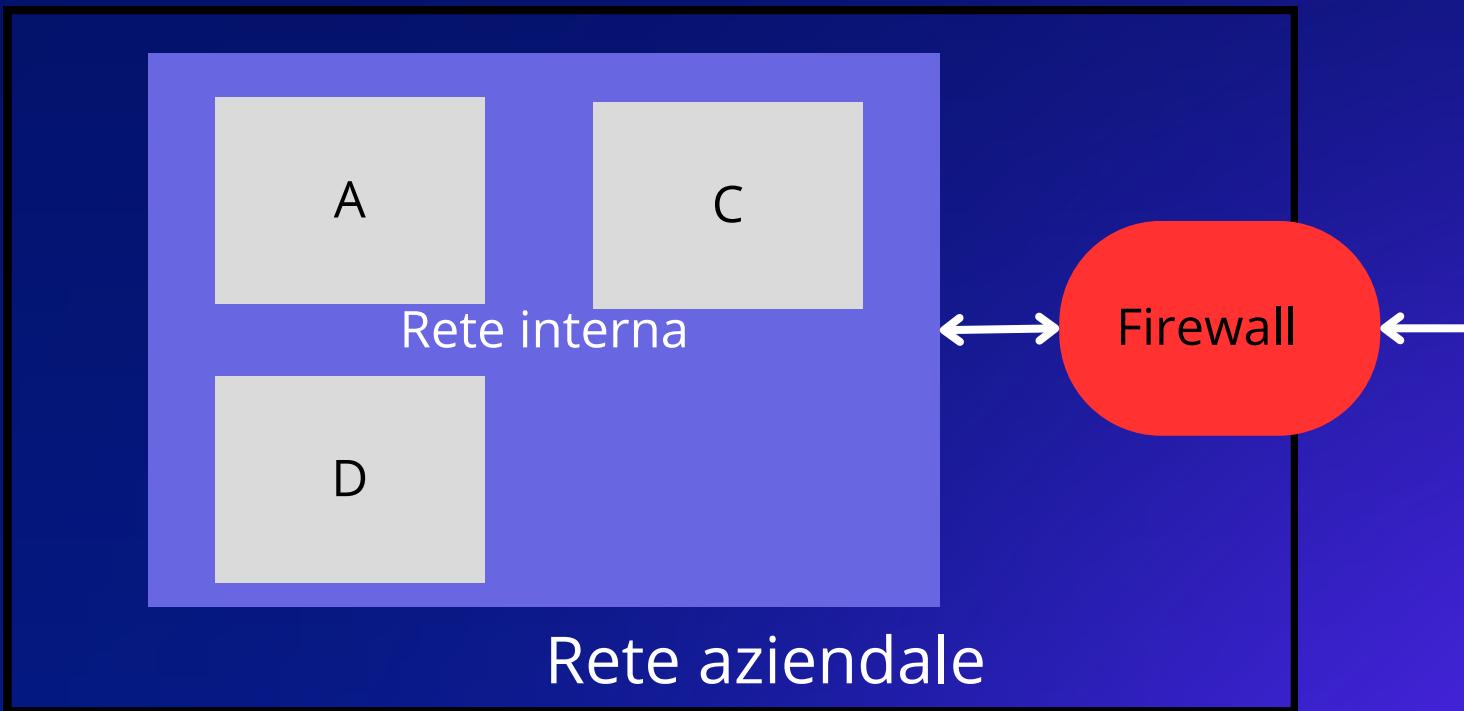
Reconstruction: mira a recuperare quelle parti ancora affidabili di un sistema compromesso. ●

Rebuilding: mira a ricostruire interamente un sistema impattato considerato non più affidabile.

Per la gestione dei media contenenti informazioni sensibili abbiamo tre opzioni:

Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche logiche. Si utilizza un approccio di tipo **read and write** dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale

- Flusso app-rete interna
- Flusso app-attaccante
- Flusso app-user



Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili, oltre ai meccanismi logici e fisici appena visti si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. E' sicuramente il metodo più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.