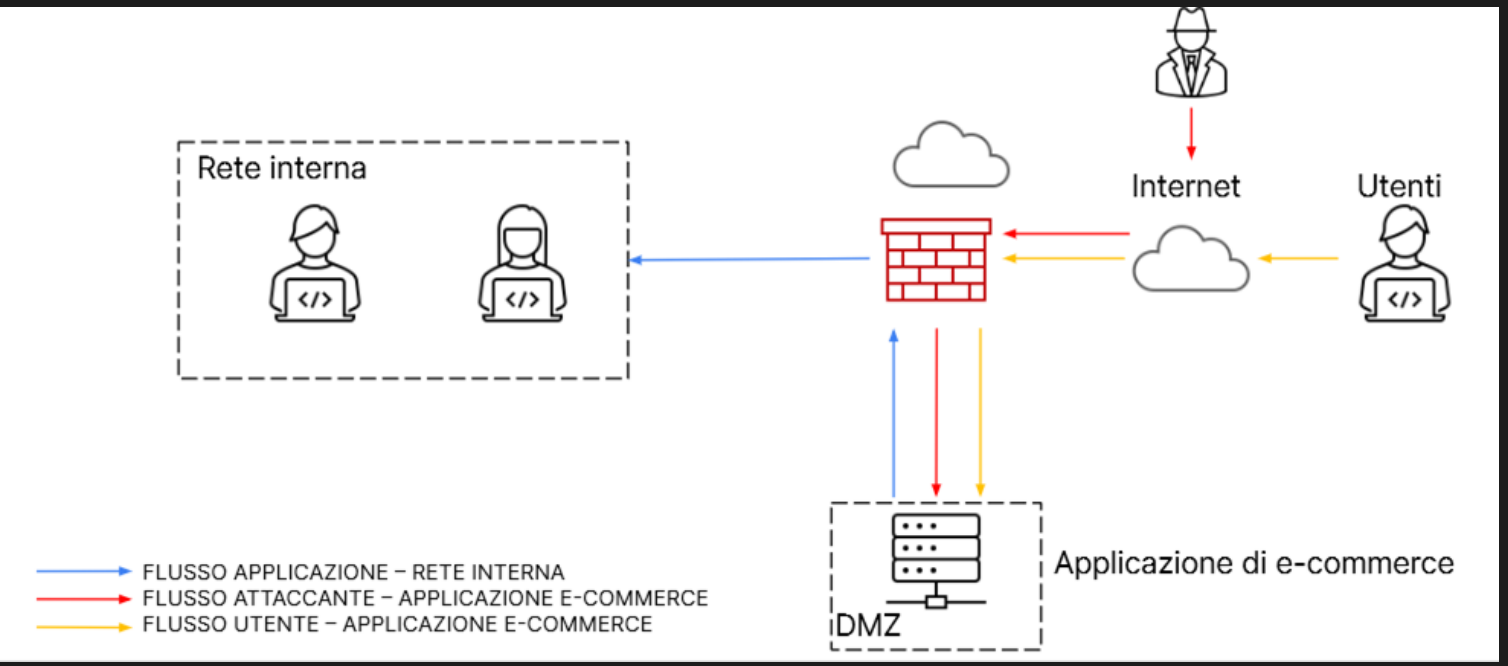
Edoardo Cucca
22/10/2023

Corso CSPT0223

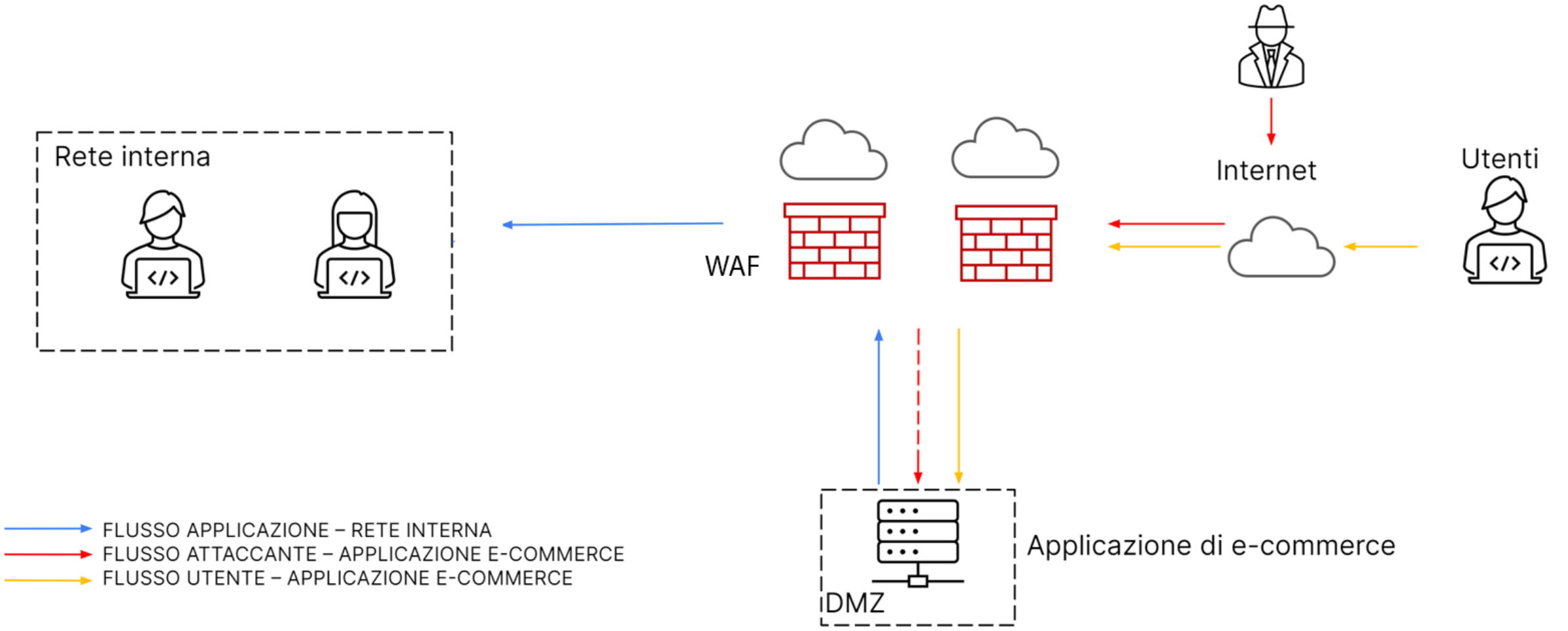
1.1) Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura di sotto in modo da evidenziare le implementazioni



Le soluzioni per limitare attacchi SQLi e XSS possono essere varie, quella alla base è assicurarsi che in fase di programmazione gli sviluppatori abbiano inserito dei controlli di valutazione e sanitizzazione dell input immesso dagli utenti e che quindi vengano gestiti correttamente ,mettendo dei limiti ai caratteri utilizzabili o seguendo magari delle linee guida dettate nel BCP – Business continuity Plan.
Sempre in fase di sviluppo si potrebbero crittografare i dati i dati sensibili limitato cosi eventuali danni.

Un'altra soluzione in aggiunta a quella appena citata è l utilizzo di un WAF – Web application firewall, il cui funzionamento è quello di monitorare , filtrare, bloccare il traffico dati proteggendo le Web App da possibili minacce (specifici per SQLi e XSS)

1.2)L Immagine modificata risulterebbe quindi come di seguito :



2) 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

Per fare un analisi più dettagliata bisogna fare qualche supposizione utilizzando i seguenti parametri :

AV : valore Asset , valore monetario (€ in questo caso)
EF : Exposure Factor – percentuale asset impattato in caso di catastrofe (in questo caso Attacco DDoS)
SLE : Single Loss Expectancy – valore monetario della perdita
ARO : Annualized Rate of Occurrence – numero di volte evento stimate in un anno
ALE : annualized loss expectancy – aspettativa di perdita annualizzata

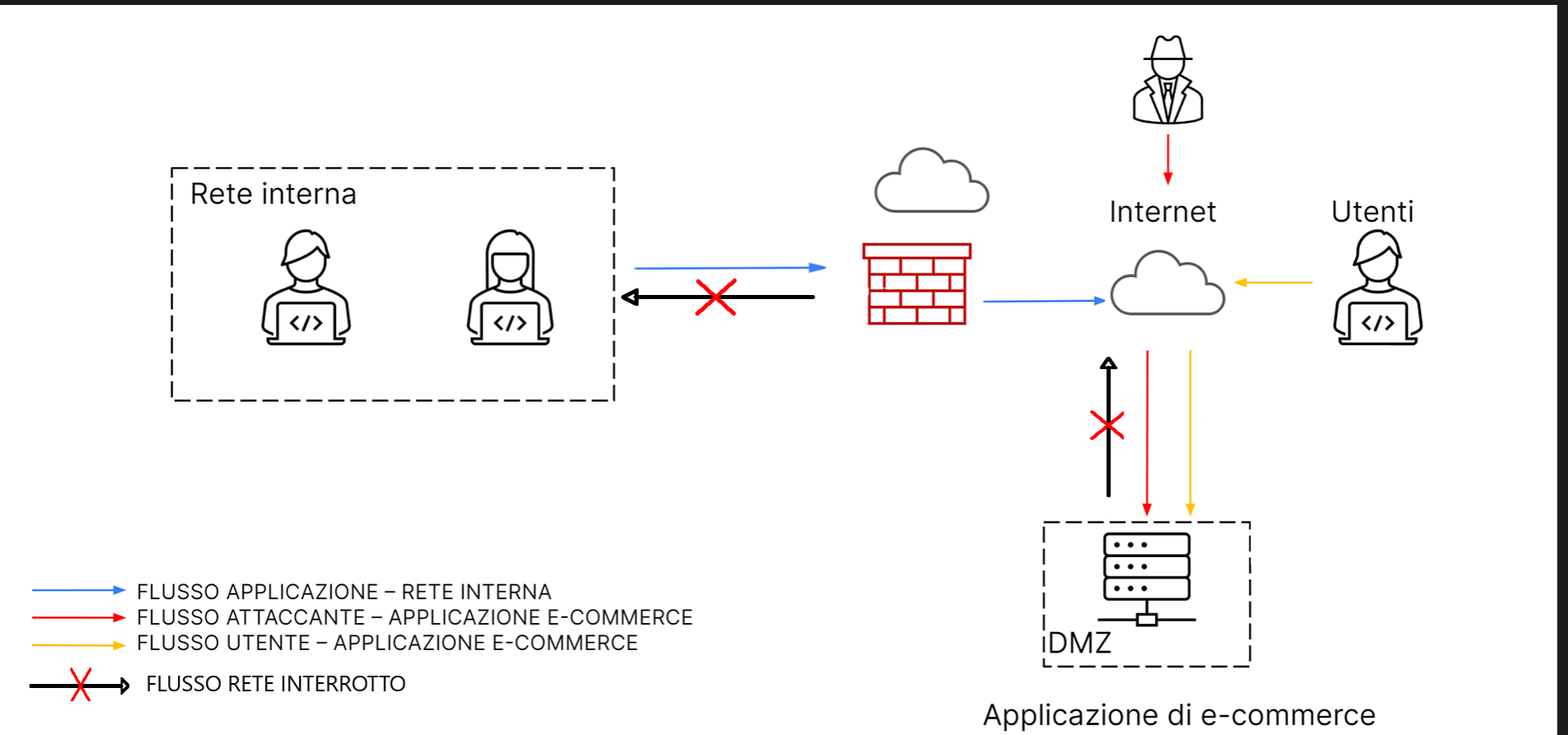
AV minuto = € 1500,00 / min
AV = 1500*1440 (minuti totali in un giornata) = € 2.160.000,00
EF = 10 minuti stop / minuti della giornata = 10/1440 = 0,0069444444%
SLE = AV * EF = 2.160.200,00 * 0,0069444444% = € 14.999,99
ARO = ipotizzato 1 Volta all anno
ALE = SLE * ARO = 14.999,99 * 1 = € 14.999,99
In questo caso ALE e SLE combaciano

3) Response: l'applicazione Web viene infettata da un malware.

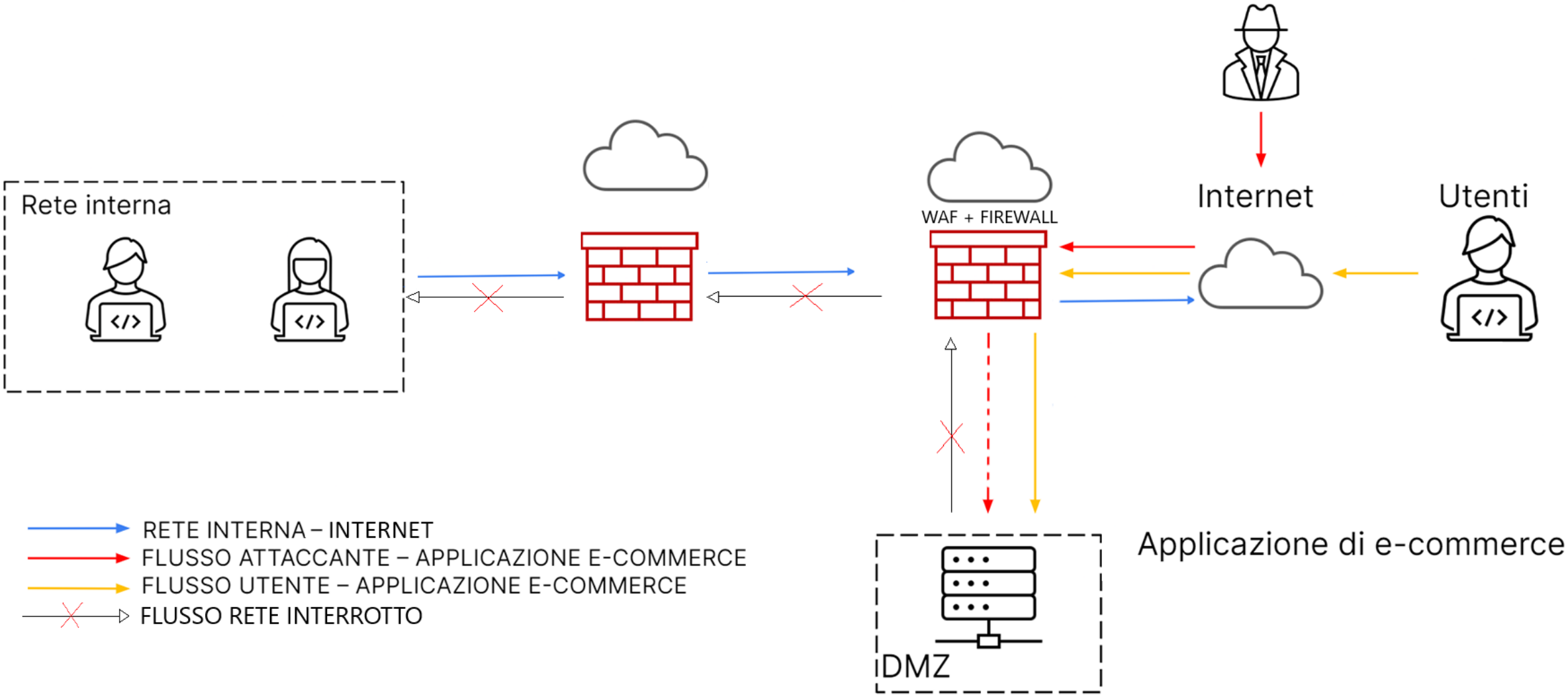
La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

Modificate la figura in slide 2 con la soluzione proposta.

In questo caso la soluzione è abbastanza semplice, avendo una rete già segmentata, ci basta impostare delle regole Firewall in modo tale che le connessioni in uscita dalla nostra Dmz , vengano Bloccate limitando quindi la propagazione del malware

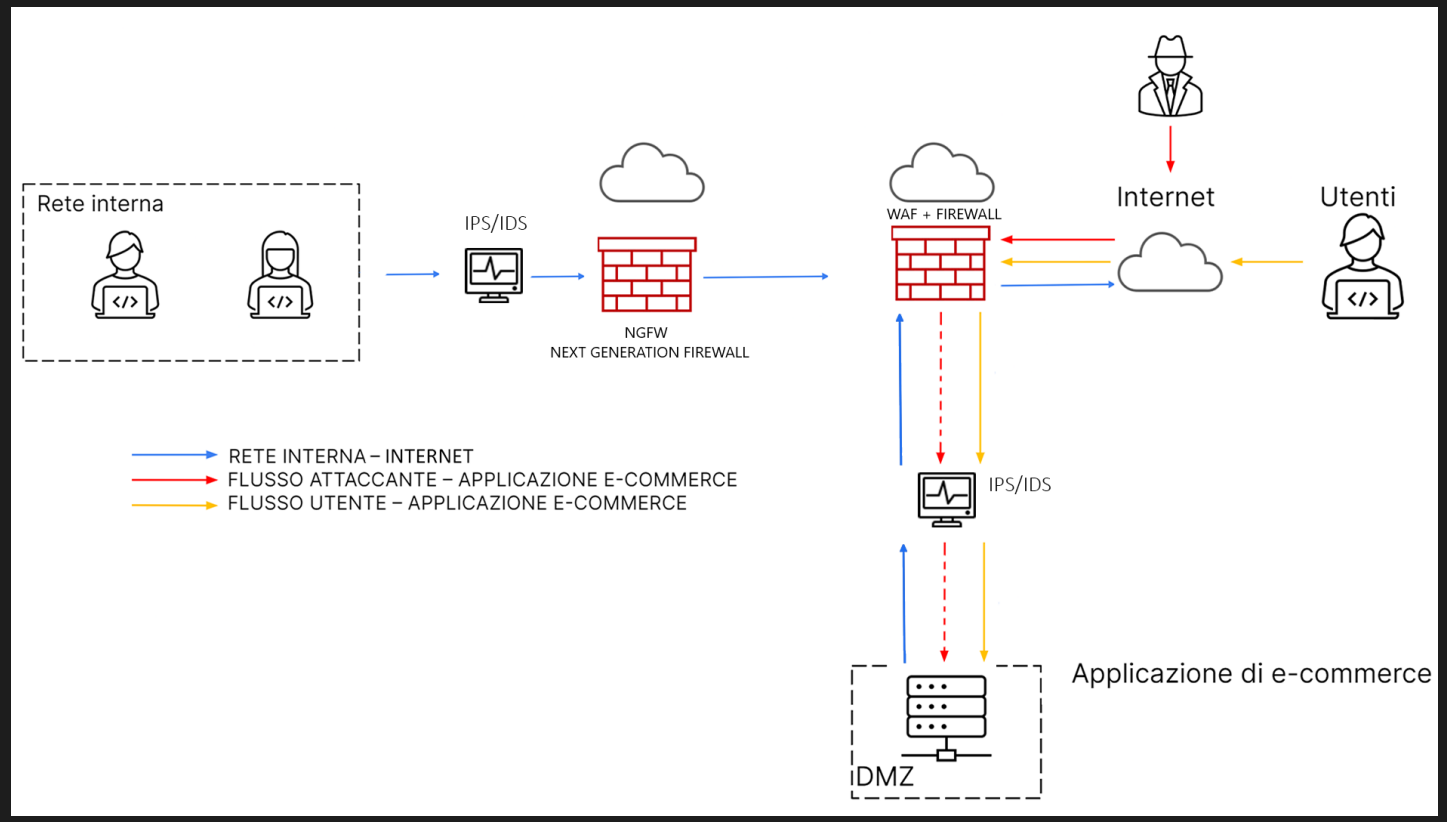


4) Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)



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

Il punto due segnalava come vulnerabilità un attacco di tipo DDoS dall'esterno , quindi per ovviare a questo problema senza limiti di spesa , rendendo quindi la rete il più sicura possibile , ho aggiunto due IPS e due IDS che controllano il traffico ingresso e uscita della rete interna e della DMZ, assicurando che eventuali tentativi di attacco vengano segnalati dall IDS e successivamente bloccati dall IPS .
Un’altra aggiunta è stata il NGFW Next Generation Firewall che include funzionalità di analisi extra e permette di analizzare i flussi basati sull’utente che effettua la connessione.
Sono stati inoltre configurati i 2 firewall andando a bloccare il traffico sulle porte inutilizzate , e di quelle con servizi superflui.



FINE