Report azioni preventive e impatto sul business

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

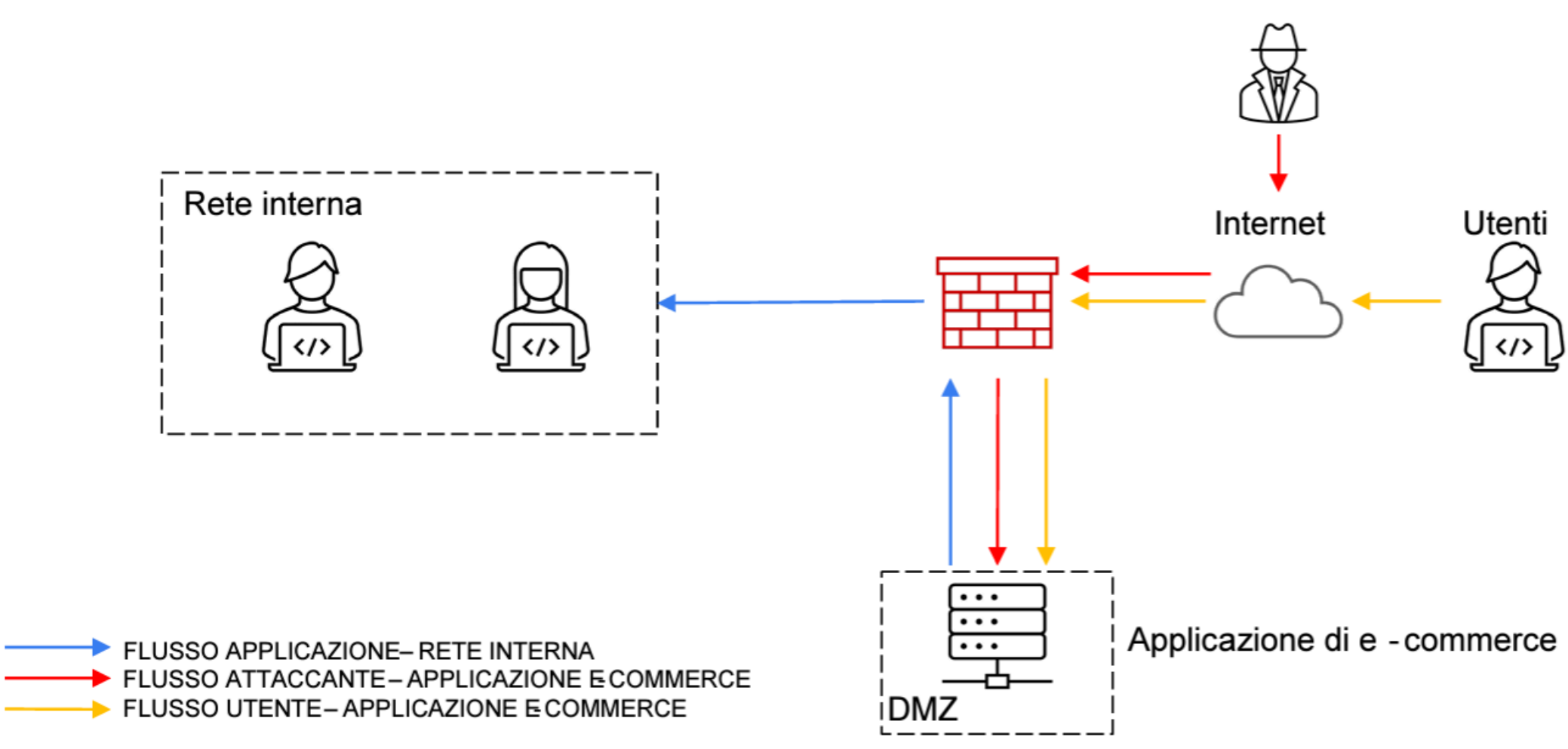
1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica

2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

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 .

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

5. Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (**integrando anche una soluzione al punto 2**) Budget 5000-10000 euro. Eventualmente fare più proposte di spesa.



1) Azioni Preventive per Difendere un'Applicazione Web da Attacchi SQLi e XSS

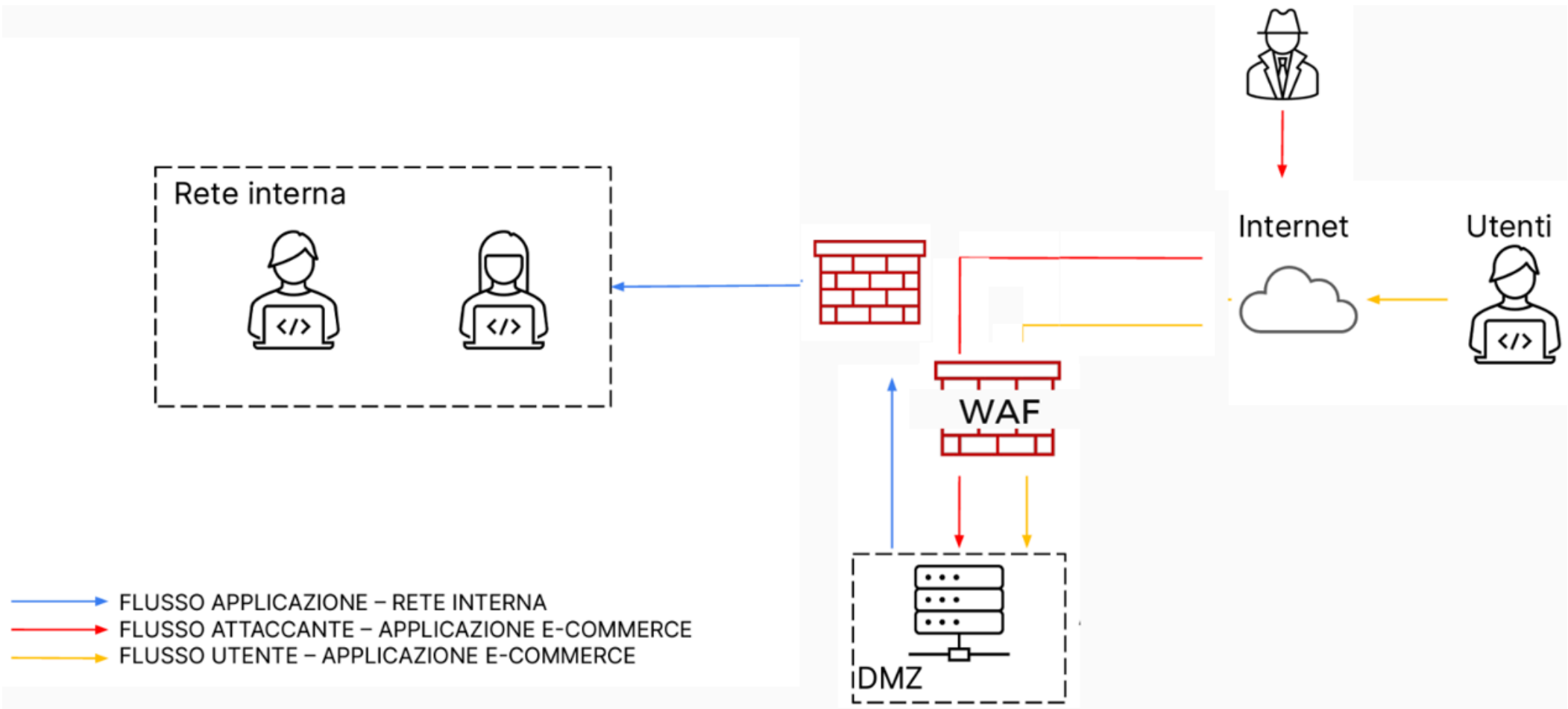
Gli attacchi **SQL Injection (SQLi)** e **Cross-Site Scripting (XSS)** sono due delle minacce più comuni e pericolose per le applicazioni web. Entrambi sfruttano vulnerabilità nell'input gestito dall'applicazione per eseguire azioni malevole. Ecco alcune misure preventive che puoi adottare per proteggere la tua applicazione da questi tipi di attacchi:

Per azioni preventive riguardanti il livello web:

- sanificazione dell'input utente.
- utilizzi di parametri SQL sicuri che evitano manipolazioni dannose da parte degli utenti.
- aggiornamento dei software.
- fornire formazione ai programmatori sull'importanza di gestire correttamente gli input utente per evitare vulnerabilità.
- testare tramite penetration testing periodici.

Per azioni preventive riguardanti il livello di rete:

- utilizzare sistemi di sicurezza come **WAF (Web Application Firewall)**, **IDS/IPS (Intrusion Detection System/Intrusion Prevention System)**, e monitoraggio dei file per rilevare e prevenire attacchi.
- aggiornamento dei software.
- formazione al personale riguardante la sicurezza informatica.
- eseguire regolarmente backup dei dati sensibili per garantire la disponibilità e il ripristino in caso di attacco.
- testare tramite penetration testing periodici.
- azioni preventive per attacchi SQLi e XSS verso il web application server.



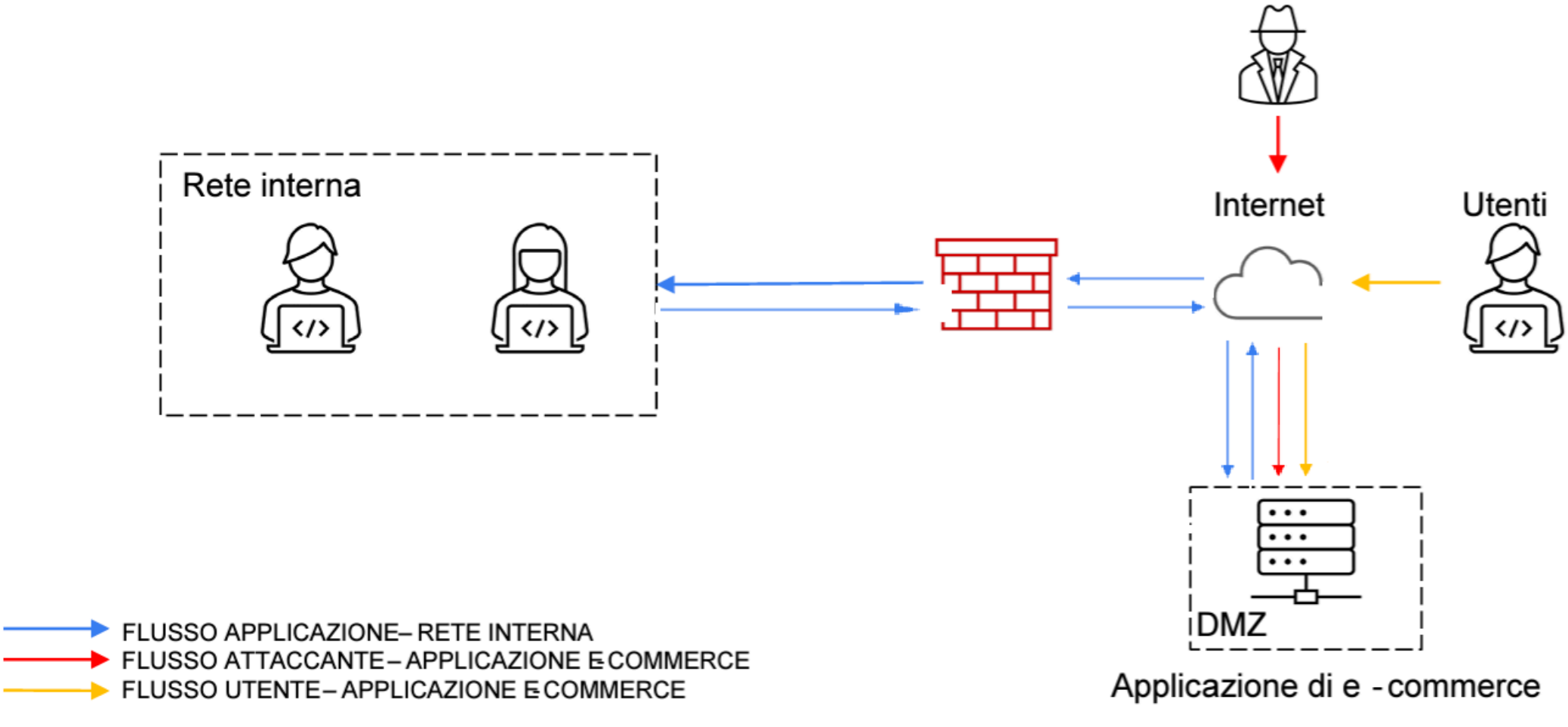
Spiegazione disegno

Ci veniva richiesto di modificare il disegno fornito per prevenire attacchi di tipo SQLi o XSS. Sono andato quindi ad aggiungere un **WAF (Web Application Firewall)** tra la **DMZ** in questione e Internet. Il **WAF**, come suggerisce il nome, è un tipo di **firewall** progettato appositamente per le applicazioni web e le sue funzionalità possono variare in base alla configurazione e al dispositivo utilizzato. Configurato nella maniera opportuna è un ottimo punto di partenza per prevenire questi tipi di attacco.

2) Impatti sul business

Per calcolare l'impatto sul business subito con l'ipotesi fatta nel quesito andiamo a moltiplicare il guadagno medio al minuto fornito (1200€) per il numero di minuti di servizio non raggiungibile che in questo caso sono (10 minuti). Quindi, il calcolo che andremo ad eseguire sarà il seguente: 1200 x 10= 12000€.

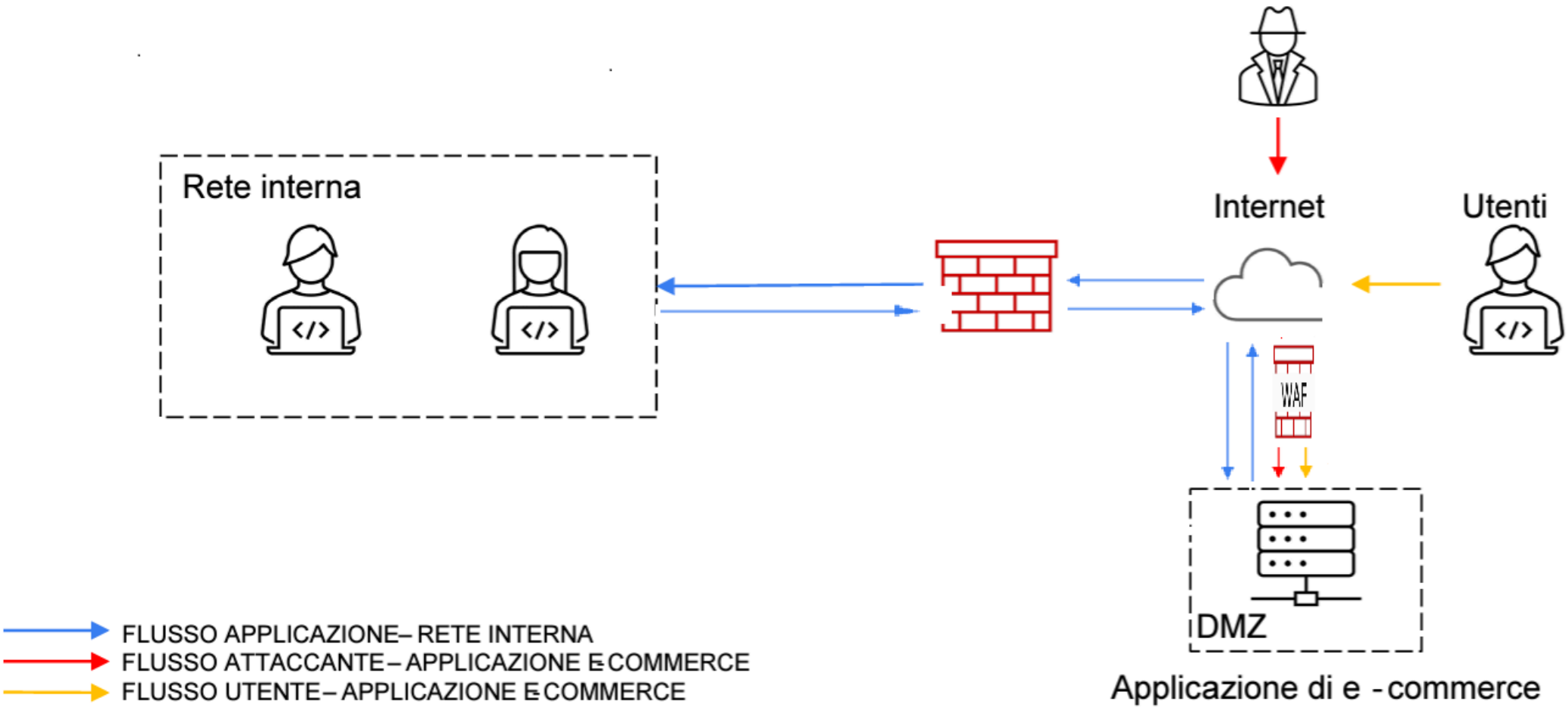
3) Response con modifica della rete



Spiegazione disegno

Per gestire l'attacco di malware senza rimuovere l'accesso dell'attaccante al server infetto, evitando al contempo che la rete interna non venisse infettata ma lasciando comunque la possibilità di comunicazione tra la rete interna e la DMZ. ho configurato una sottorete secondaria in modo tale da impedire all'attaccante di penetrare e infettare anche la rete interna dell'azienda.

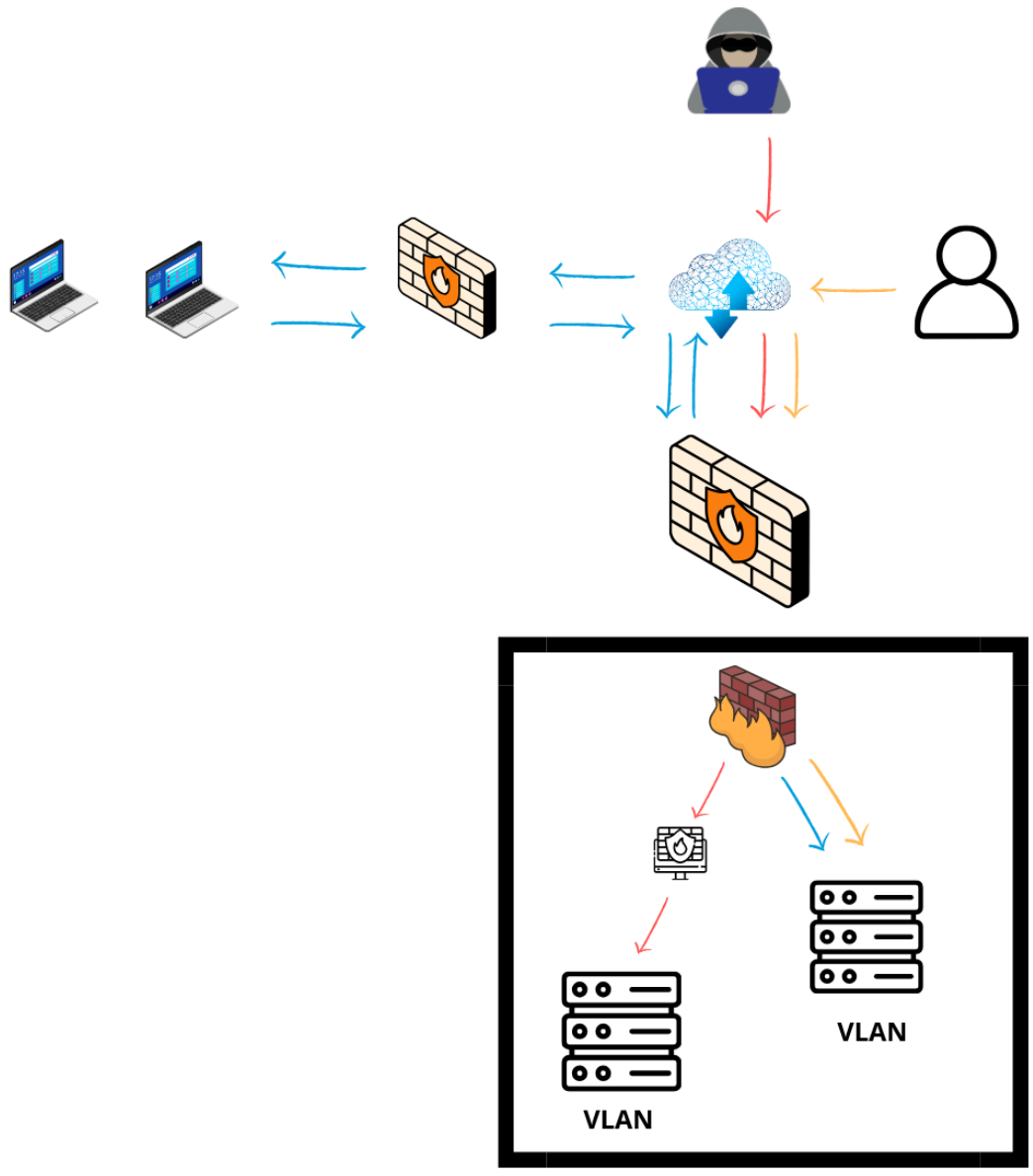
4) Soluzione completa



Spiegazione disegno

Implementazione del **WAF** per monitorare, filtrare e bloccare il traffico HTTP e HTTPS in modo tale da proteggere l'applicazione web di nostro interesse da attacchi mirati.

5) Modifica «più aggressiva» dell’infrastruttura



Aggiunta di un **honeypot** affinchè l’attaccante venga attirato verso la nostra trappola con l’aggiunta ulteriore di un **firewall** e un **honeywall** per filtrare e monitorare il traffico in entrata e in uscita.

Stima dei costi totali

- **Soluzione con Server Fisici:**
  - honeypot: $1,000 - $3,000
  - firewall: $500 - $5,000
  - honeywall: $1,000 - $3,000
  - **totale:** $2,500 - $11,000

- **Soluzione con VM:**
  - honeypot: $600 - $1,800
  - firewall: $0 - $1,500
  - honeywall: $600 - $1,800
  - **totale Annuale:** $1,200 - $5,100