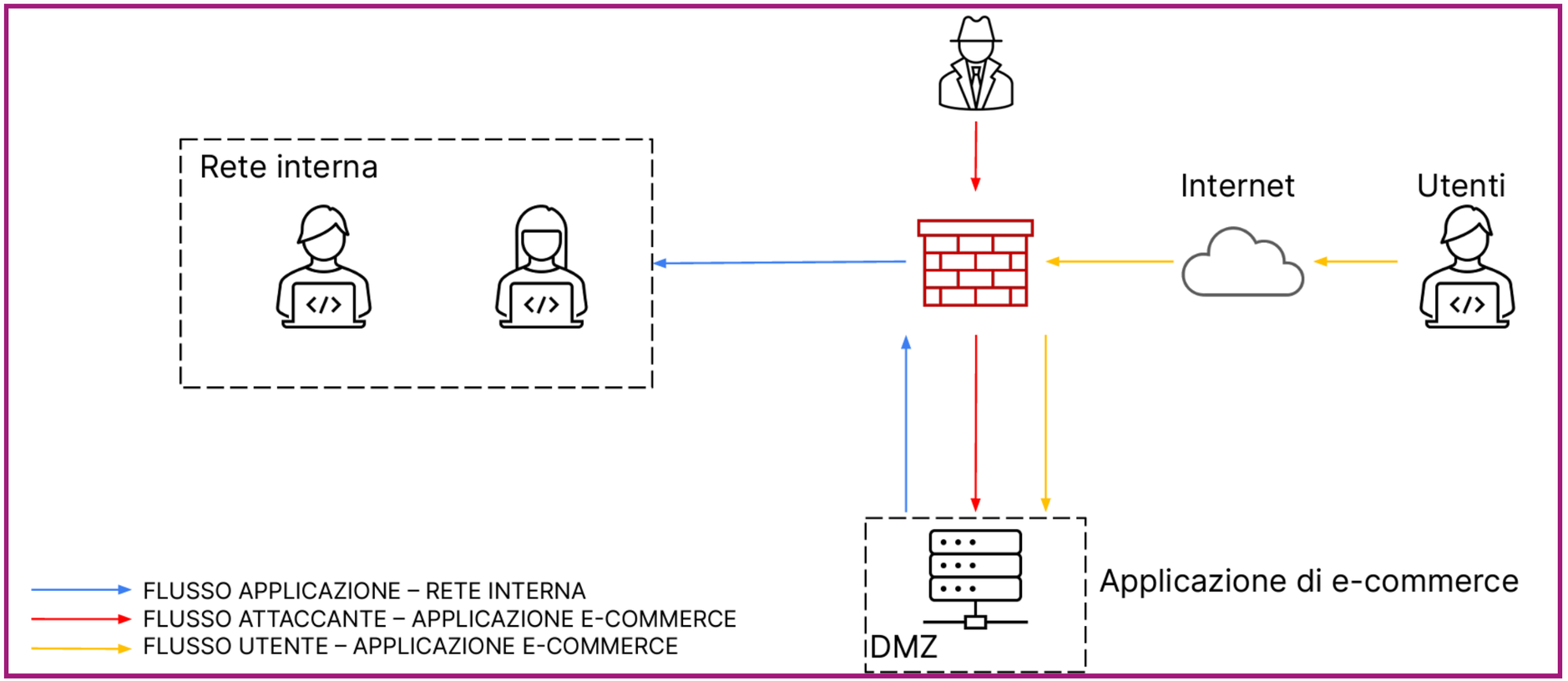
Progetto 24-11 Alessandro Moscetti

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.
- 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.

Architettura di rete proposta



Primo quesito

Azioni preventive per attacchi SQLi e XSS verso il web application server.

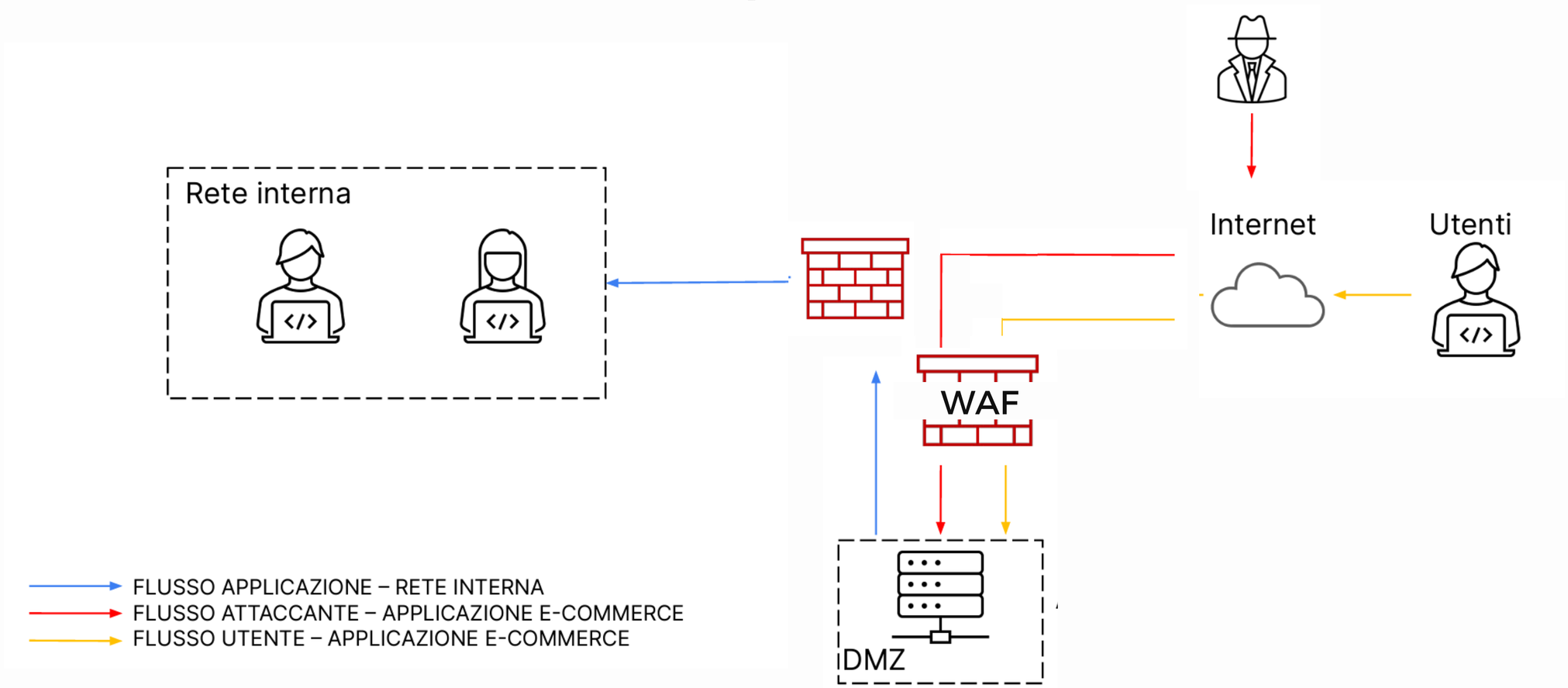
Per azioni preventive riguardanti il livello web:

- 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 riguardanti 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.

Modifica rete primo quesito



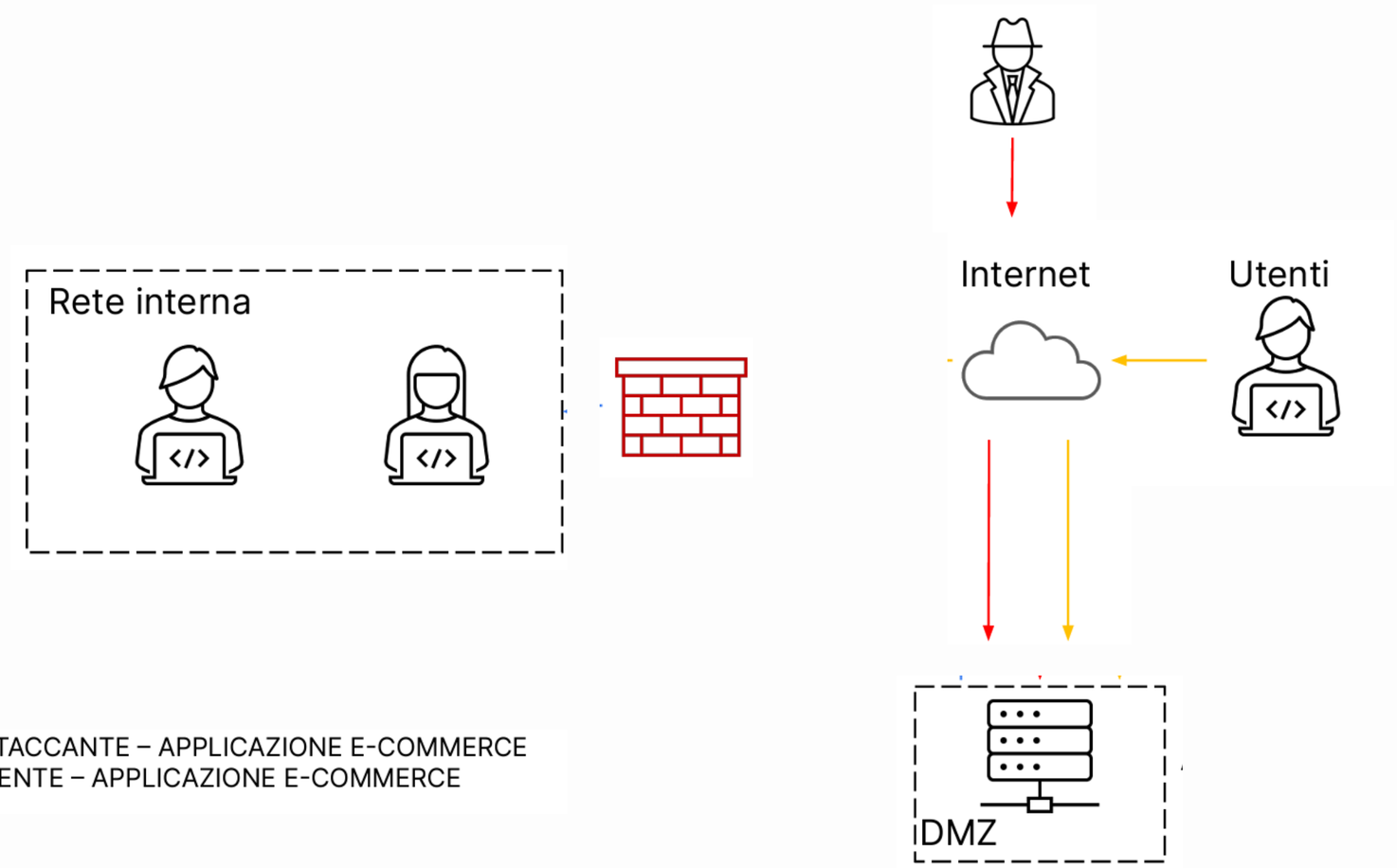
Spiegazione disegno

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.

Secondo quesito

Per calcolare l'impatto sul business subito con l'ipotesi fatta nel quesito andiamo a moltiplicare il guadagno medio al minuto fornito (1500€) per il numero di minuti di servizio non raggiungibile del caso (10 minuti).
Quindi **1500 x 10= 15000€**
Per contrastare un attacco DDos si potrebbe utilizzare un CDN (Content Delivery Network) per distribuire il traffico di rete e/o implementare la ridondanza nella rete come, per esempio, installando un Web Application Server clone in modo di coprire un eventuale down del server primario.

Modifica rete terzo quesito



Spiegazione disegno

Per gestire l'attacco di malware senza rimuovere l'accesso dell'attaccante al server infetto, ho modificato la figura **isolando** tutta la rete interna.
In questo modo, miriamo a prevenire la propagazione del malware sulla rete interna, mantenendo comunque il server infetto accessibile da Internet, quindi raggiungibile sia dall’attaccante che dagli utenti del servizio Web.

Grazie per l’attenzione.