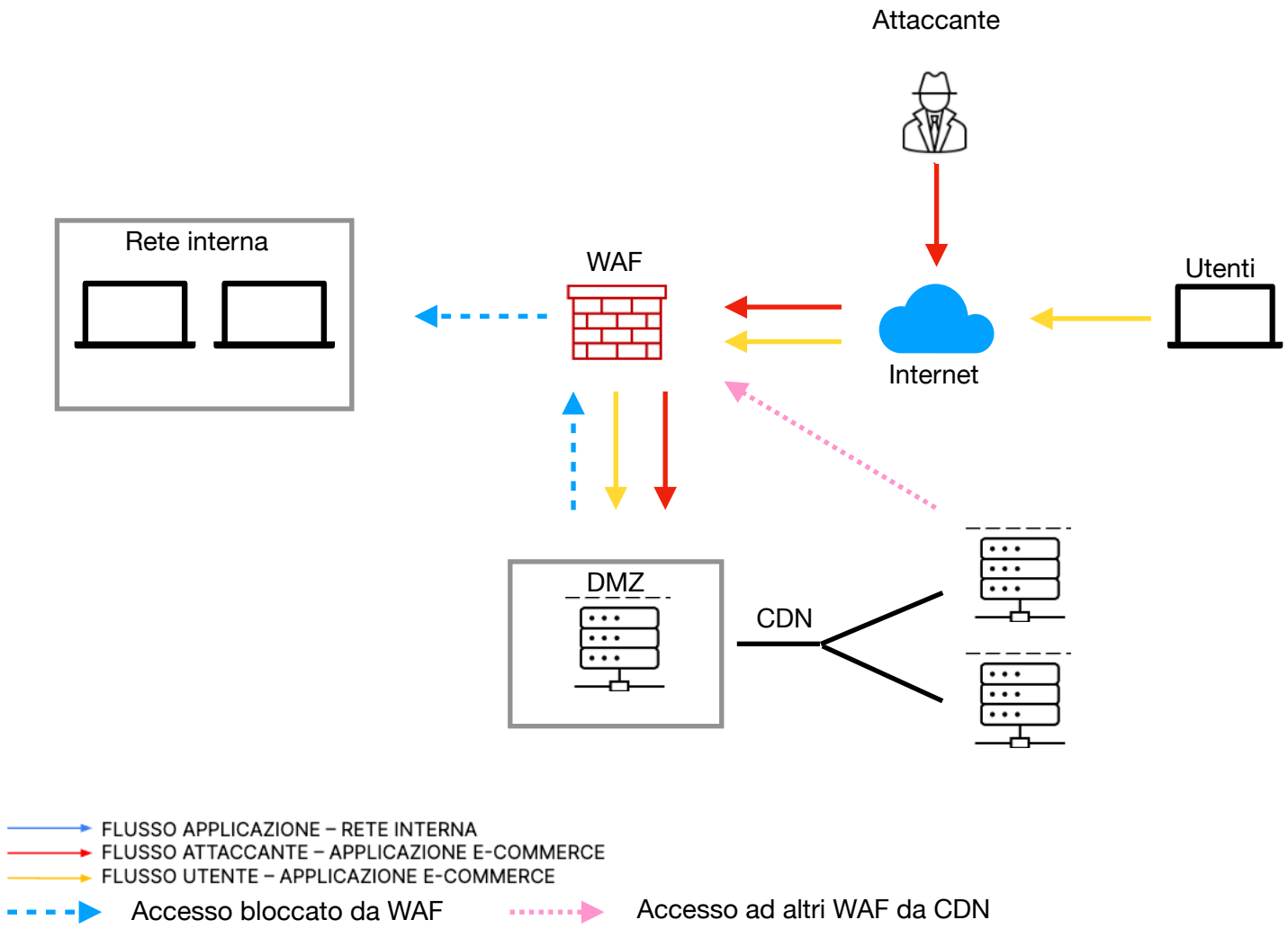
Progetto modulo 5



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

- Come azione preventiva principale è necessario implementare la santificazione dai dati in input lato client

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

- L’impatto a livello economico secondo i dati forniti ed i minuti trascorsi può essere stimato ad una cifra intorno ai 15000 euro
- Come azioni preventive è possibile implementare un WAF che fornisce maggior protezione nei confronti di attacchi DDOS e non solo. Si tratta di Web Application Firewall, gestisce il filtraggio del traffico HTTP/HTTPS inoltre fornisce supporto anche nei confronti di attacchi web come SQLI o XSS.
- Inoltre è possibile come azione preventiva attivare un secondo server e tenerlo quieto, cioè che venga attivato solo in caso di necessità come per un attacco DDOS (failover cluster) per rendere sin da subito il server disponibile ed implementare azioni di rimedio al server principale
- L’utilizzo di una CDN(Content Delivery Network) ovvero una rete di server distribuiti geograficamente progettata per fornire contenuti Web, come pagine Web, immagini, video e altri tipi di contenuti multimediali, in modo più efficiente agli utenti finali, potrebbe essere la situazioni ottimale per gestire un attacco di tipo DDOS
- L’installazione di un WAF può costare all’incirca 5000 E annui mentre l’implementazione di una CDN può costarne altri 3000 E annui. Sommando complessivamente si avrebbe un costo di circa 8000 E annui che potrebbe essere certamente più ragionevole rispetto ad una perdita stimata di 15000 E in 10 minuti a causa di un attacco DDOS che altresì potrebbe verificarsi ancora.

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.

- Creare una policy di firewall che blocca l’accesso tra rete interna e DMZ