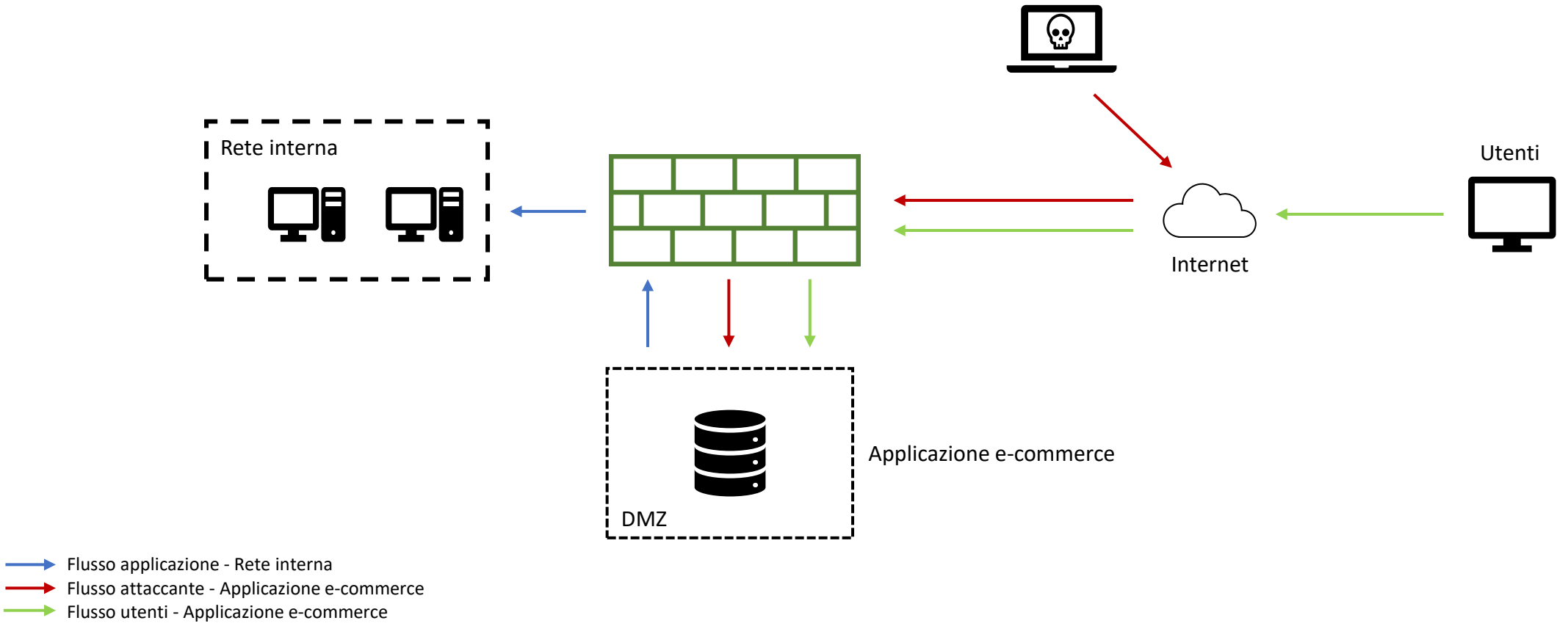
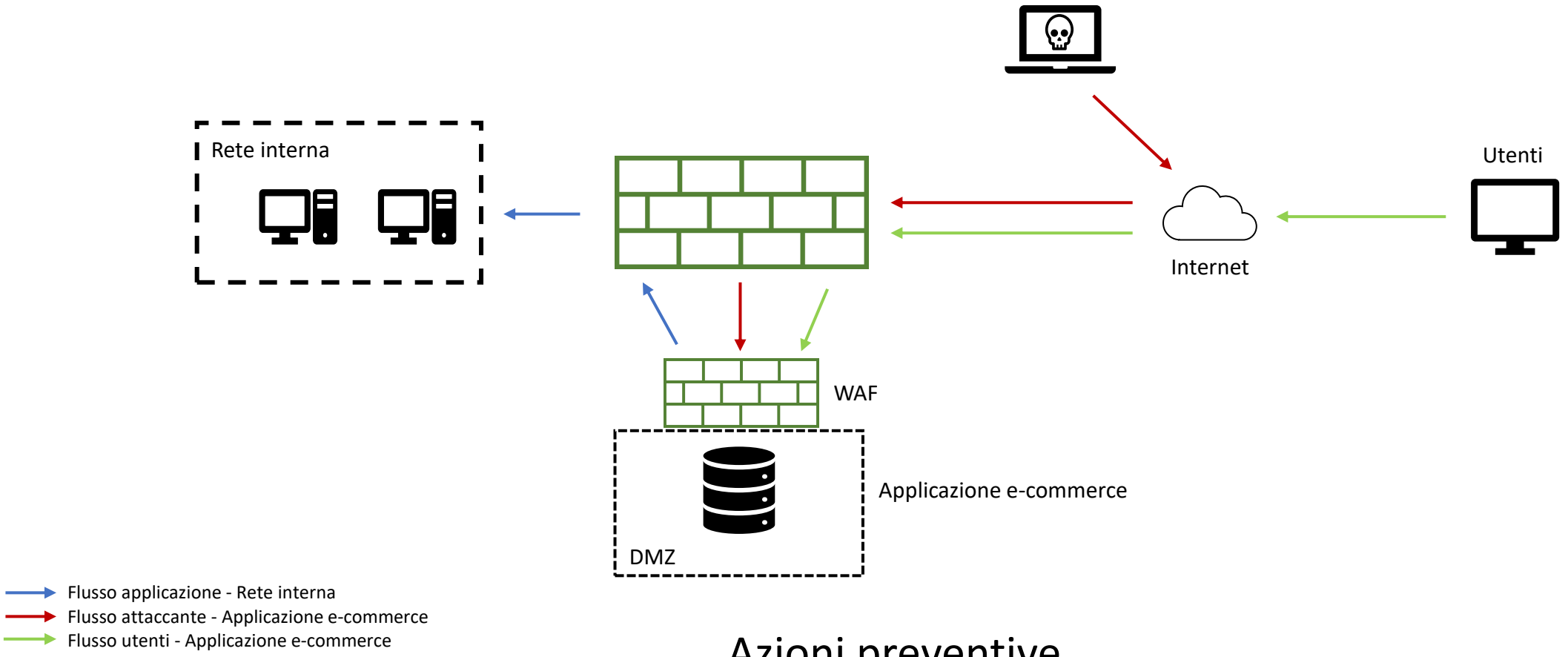
L’applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi, se il server DMZ viene compromesso, potenzialmente, un attaccante potrebbe raggiungere la rete interna



Orlando Tangari

Per difendere l'applicazione da attacchi di tipo SQLi o XSS da parte di un utente malintenzionato,
si ricorre all'uso dell'***Web Application Firewall***, dispositivi di sicurezza dedicati per limitare le azioni di un utente su una web app.



Azioni preventive

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

Calcolo dell’impatto sul business dovuto alla non raggiungibilità del servizio per ***10 minuti*** considerando che, in media, ogni minuto gli utenti spendono ***1500€*** sulla piattaforma di e-commerce.

1500€ · 10 minuti= 150000€

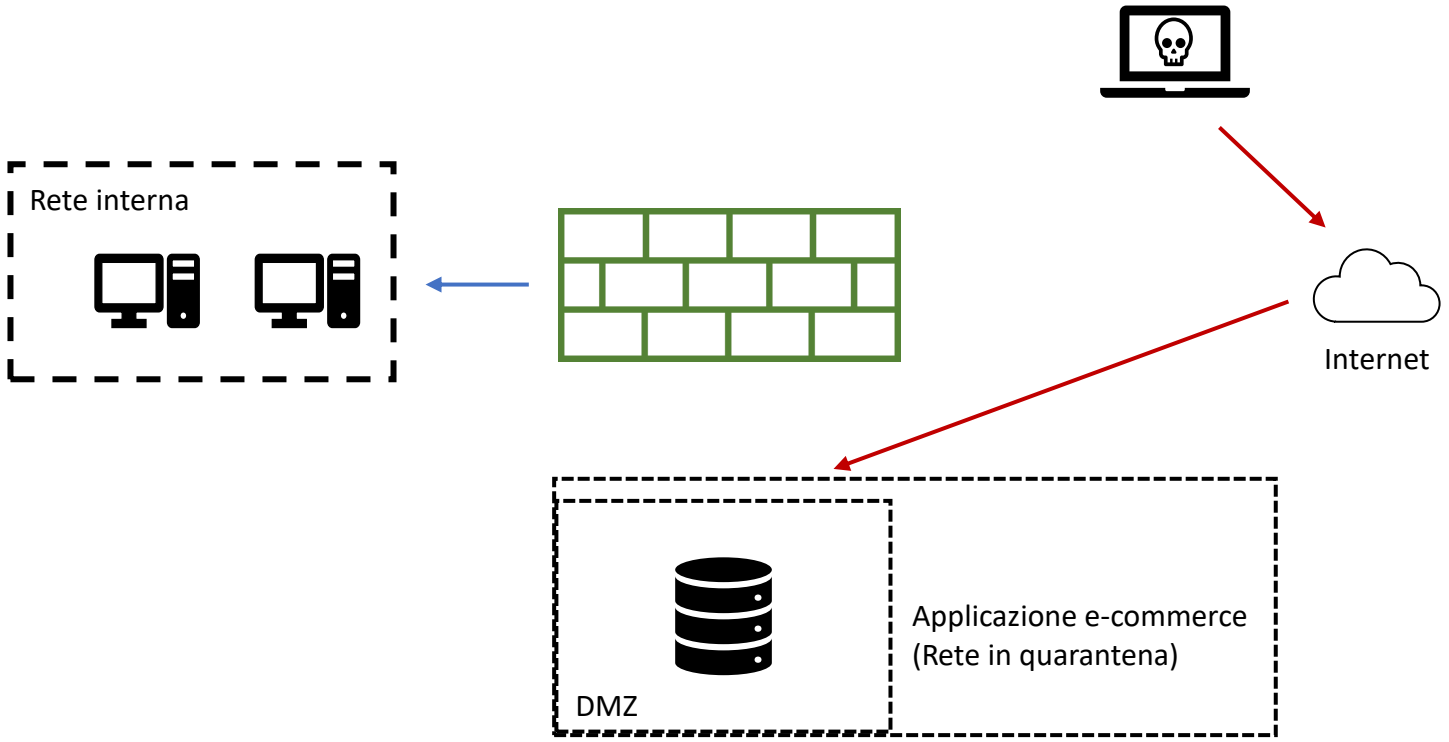
In 10 minuti si perdono 150000€.

Impatti sul business

L’applicazione Web subisce un attacco di tipo DDoS dall’esterno che la rende non raggiungibile per *10 minuti*.

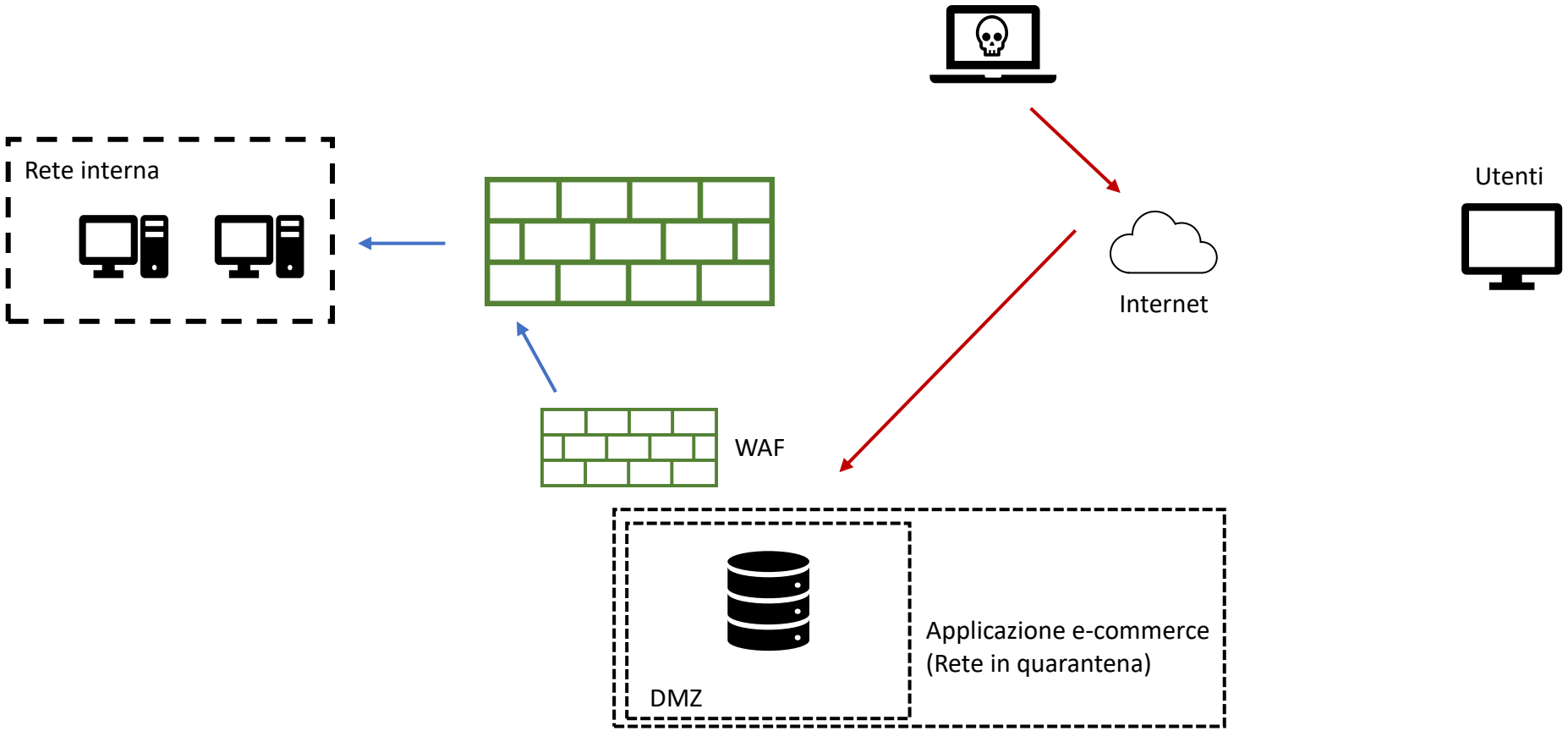
La priorità e non far propagare il malware sulla rete interna senza essere interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

Per un contenimento maggiore si usa la tecnica dell'*isolamento*, che consiste nella completa disconnessione del sistema infetto dalla rete interna.



Response

Applicazione Web infettata da un malware.



Soluzione completa