

Benchmark M5

esercitazione finale modulo 5

Ignazio Saba

TRACCIA

rispondere ai seguenti quesiti:

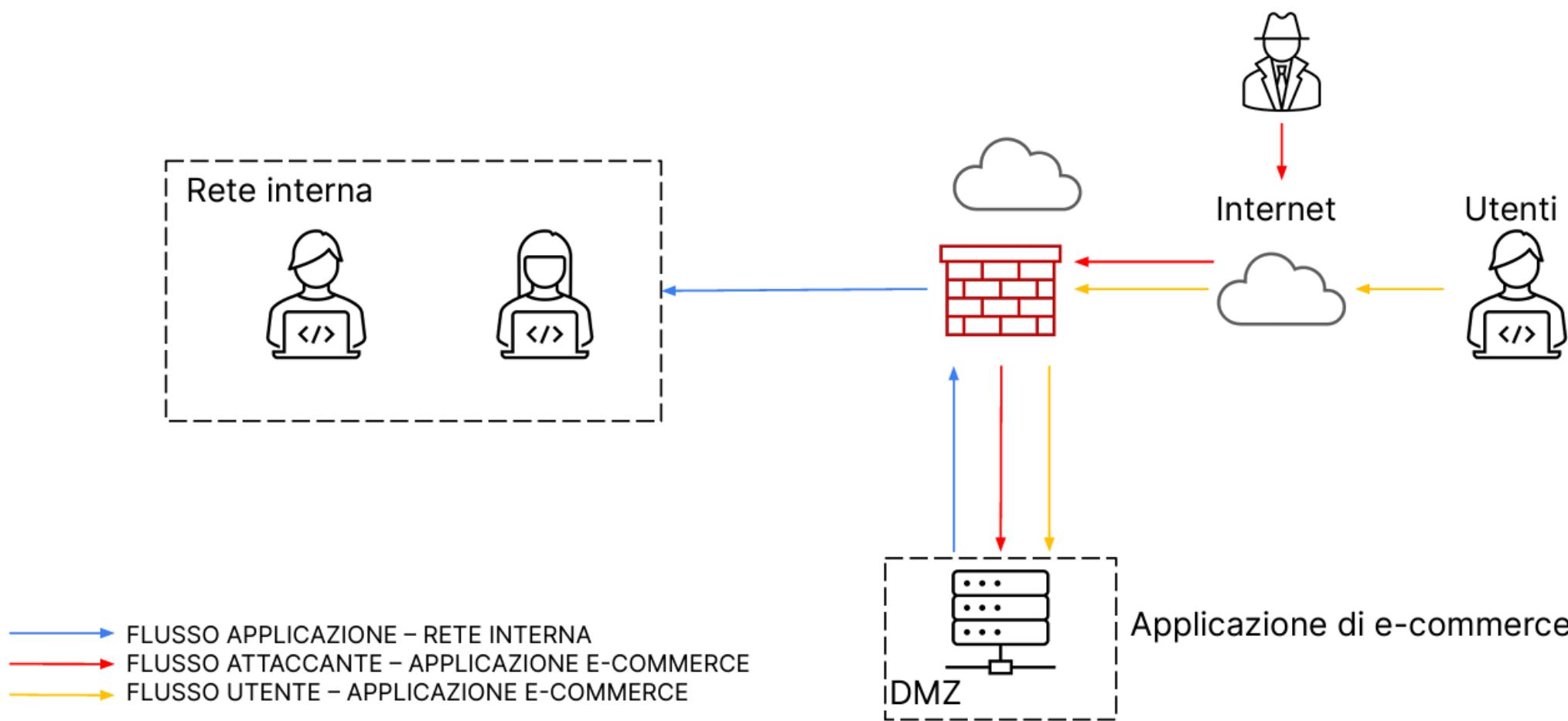
- 1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
- 2. Impatti sul business: l'applicazione Web subisce un 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
- 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 (se necessario/facoltativo magari integrando la soluzione al punto 2)

TRACCIA

Architettura di rete:

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

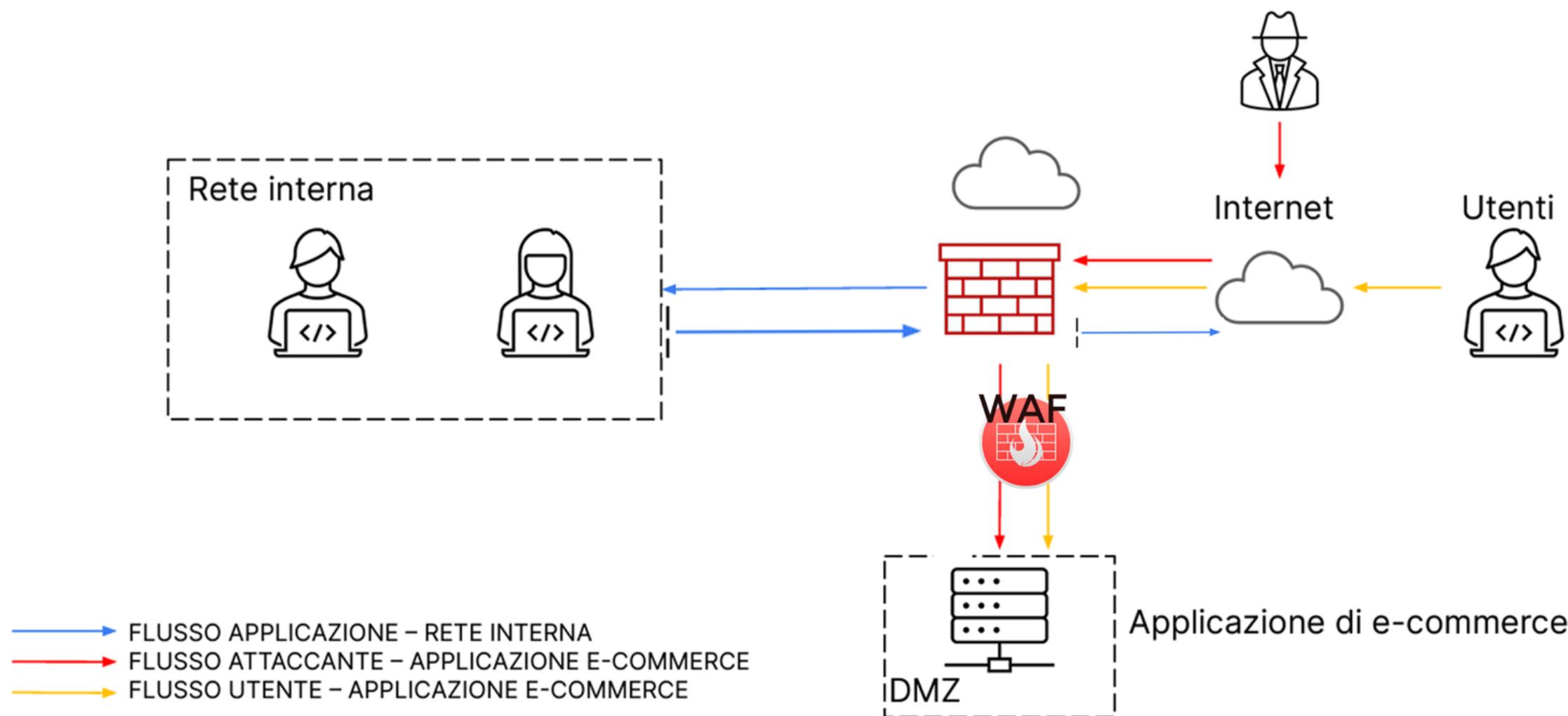
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



AZIONI PREVENTIVE

aggiungiamo un web application firewall (WAF) per proteggere la nostra web app da attacchi SQL injections e xss

facciamo eseguire da una ditta certificata ISO 27001 sia Vulnerability Assessment che Penetration Test, così da verificare se ci sono vulnerabilità conosciute e valutarne i rischi, costi e nel caso risolverli



IMPATTI SUL BUSINESS

per calcolare il danno subito durante il down dell'e-commerce dobbiamo moltiplicare la perdita al minuto per i minuti di down

perdita al minuto = 1500€ minuti di down = 10

PERDITA COMPLESSIVA

$1500 \times 10 = 15000\text{€}$

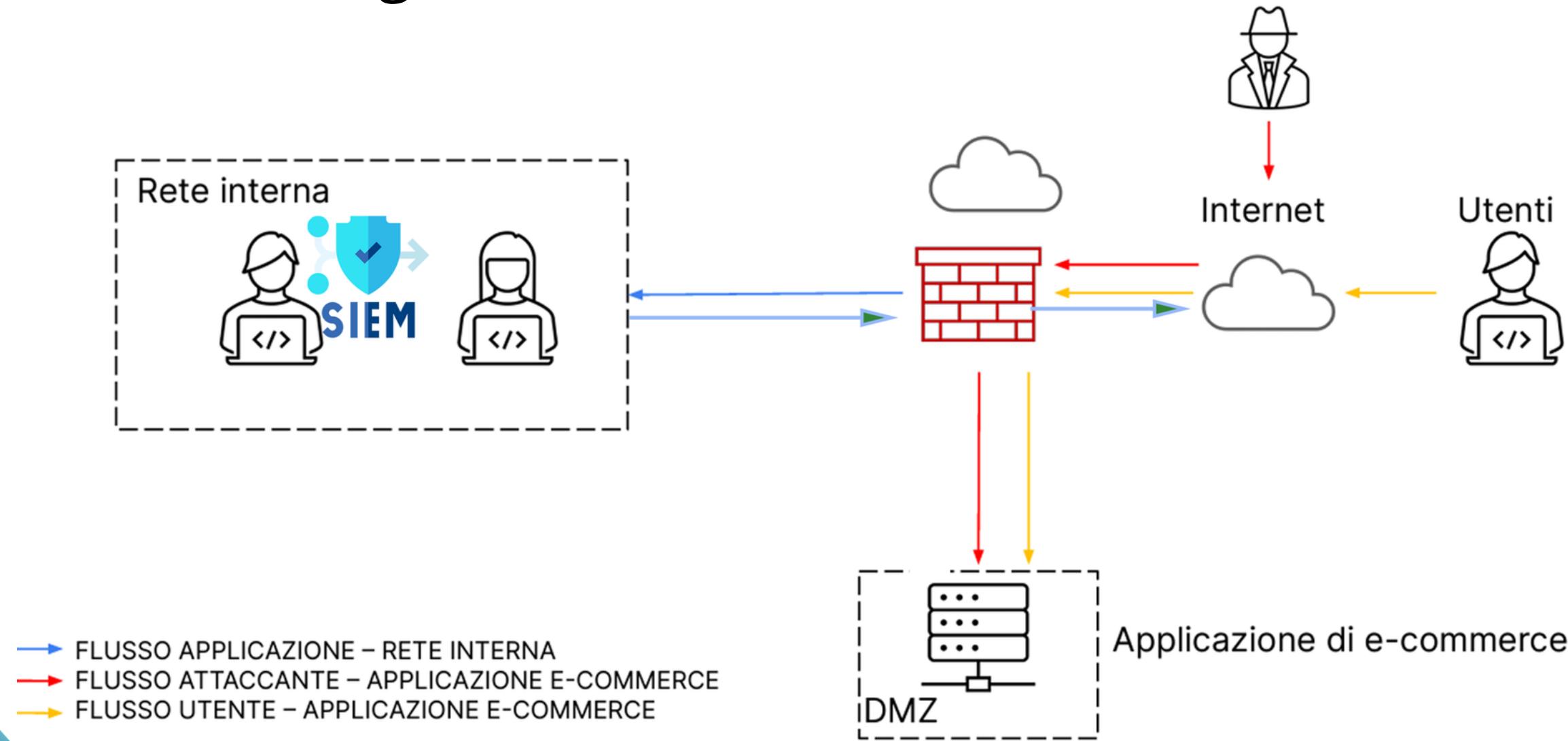
IMPATTI SUL BUSINESS

per ovviare a problemi di down sarebbe opportuno dotarsi di un sistema di backup hot site in modo tale da garantire una continuità del servizio e il mantenimento dei dati senza discrepanze.

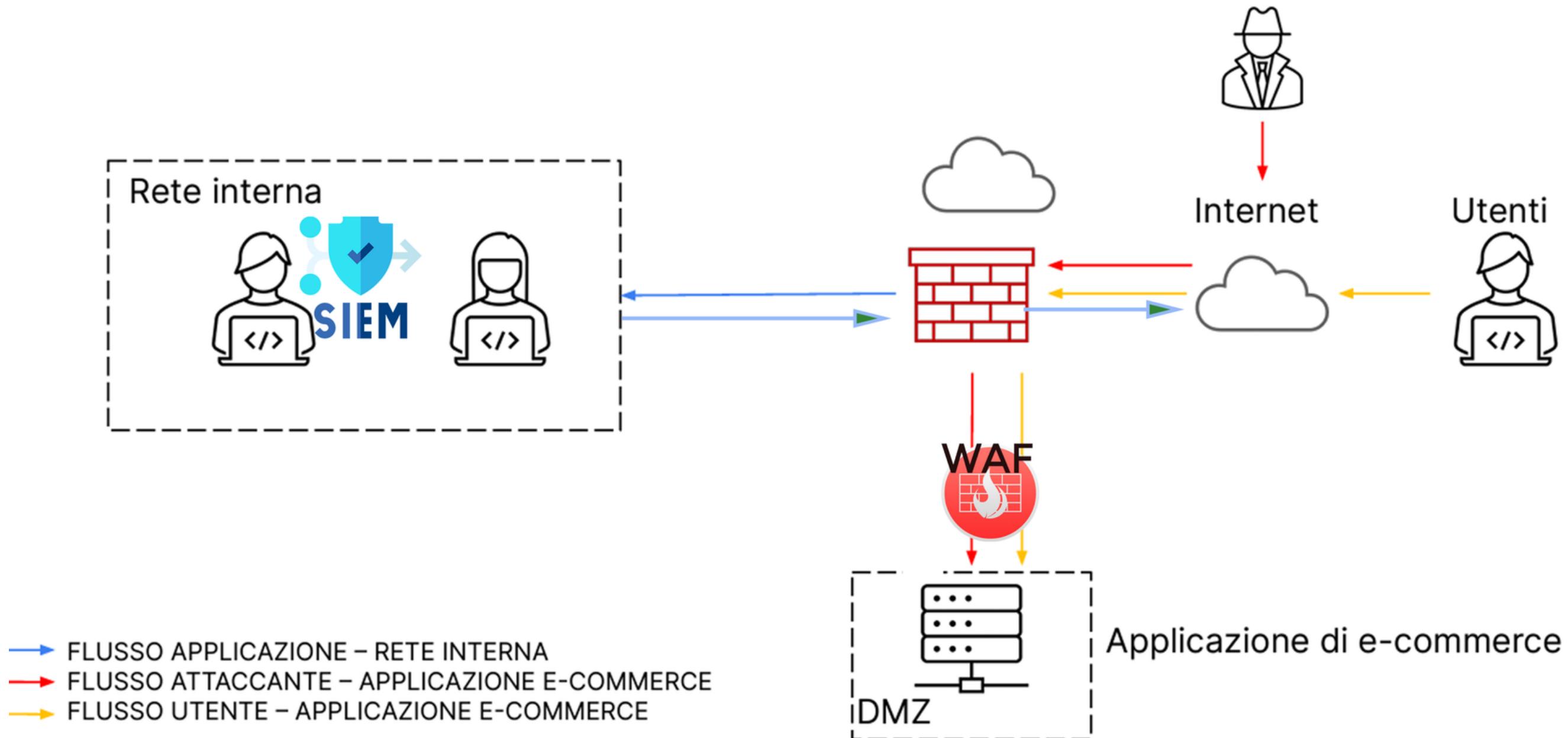
Inoltre si potrebbe optare per una soluzione cloud.
Così da poter sfruttare le soluzioni di sicurezza e disaster recovery messe a disposizione dal host, avendo sia delle copie di backup sempre disponibili e delle soluzioni facilmente scalabili in caso di aumento del flusso di utenti

RESPONSE

isoliamo con regole firewall la DMZ dalla rete interna.
installiamo un SIEM sui computer aziendali in modo da tenere monitorata
l'integrità e sicurezza dell'intera infrastruttura IT



SOLUZIONE COMPLETA



MODIFICA DELL'INFRASTRUTTURA

