REPORT DI SICUREZZA

INDICE

1. AZIONI PREVENTIVE

Per difendere l’applicazione Web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS) è possibile implementare le seguenti azioni preventive:

SQL Injection:

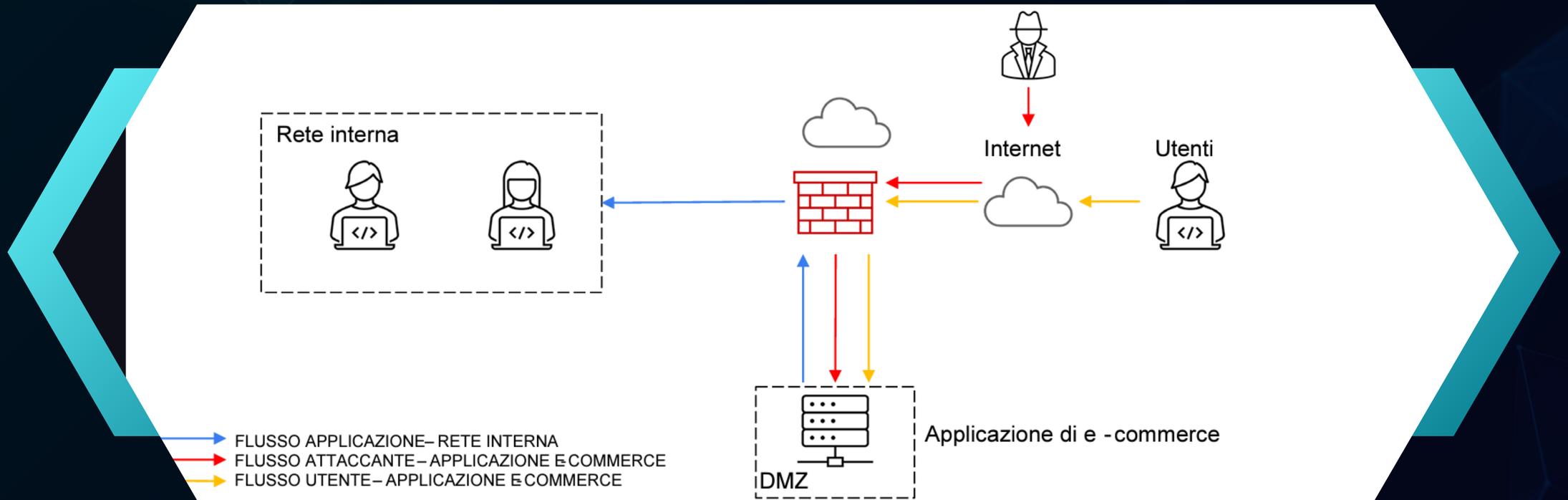
- Parametrizzazione delle query: Utilizzare query SQL parametrizzate anziché concatenare stringhe di query.
- Validazione degli input: Validare e sanificare tutti gli input dell'utente per rimuovere o neutralizzare caratteri pericolosi.
- ORM (Object-Relational Mapping): Utilizzare ORM che gestiscono correttamente le query SQL evitando l'inserimento di codice malevolo.
- WAF (Web Application Firewall): Implementare un WAF per filtrare e monitorare il traffico HTTP.

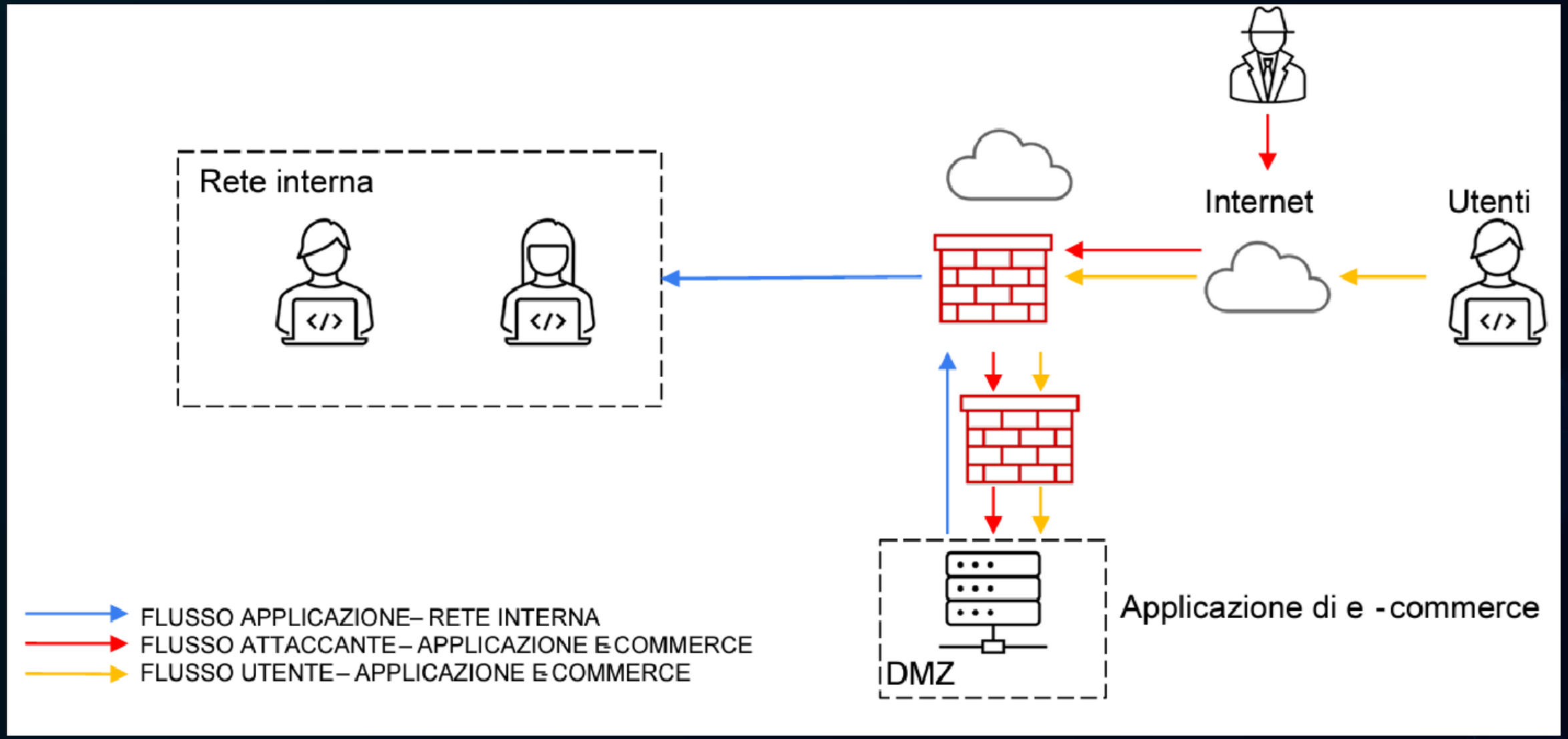
Cross-Site Scripting (XSS):

Sanificazione degli input: Sanificare tutti gli input e output per rimuovere o neutralizzare script pericolosi.
HTTP headers di sicurezza: Utilizzare HTTP headers come Content Security Policy (CSP) per limitare le fonti di script.
Framework di sicurezza: Utilizzare framework e librerie che offrono protezione contro XSS.

Nella figura viene mostrata l’attuale archiettettura di rete, per risolvere il problema degli attacchhi SQL i e XSS ho proposto di aggiungere un WAF tra Internet e l'applicazione di e-commerce.

Un Web Application Firewall (WAF) è un sistema di sicurezza progettato per monitorare, filtrare e bloccare il traffico HTTP/HTTPS diretto a un'applicazione web. Il suo scopo principale è proteggere le applicazioni web da vari tipi di attacchi che sfruttano vulnerabilità note nelle applicazioni stesse.




Rete interna
Internet
Utenti
DMZ
Applicazione di e -commerce
FLUSSO APPLICAZIONE– RETE INTERNA
FLUSSO ATTACCANTE– APPLICAZIONE E-COMMERCE
FLUSSO UTENTE– APPLICAZIONE E-COMMERCE

2. IMPATTI SUL BUSINESS

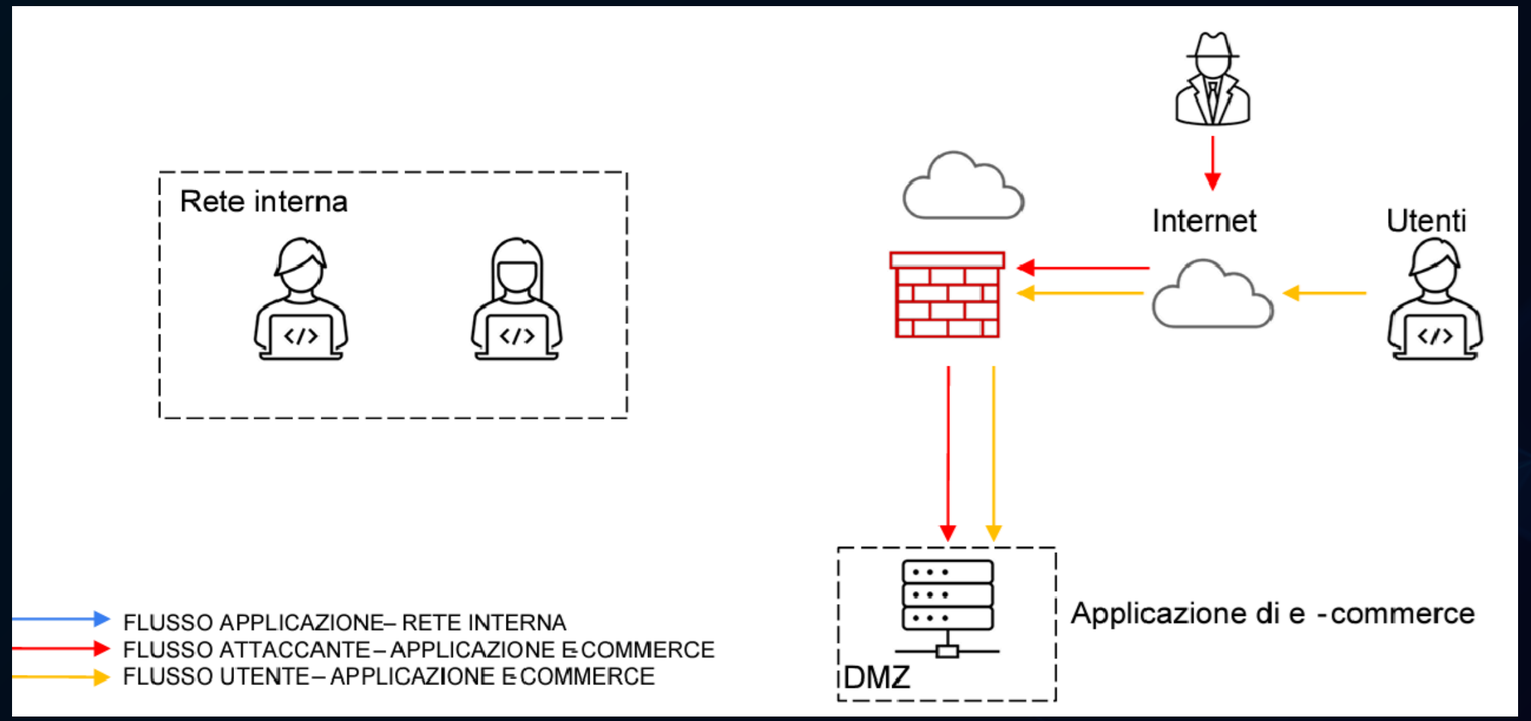
Un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti ha il seguente impatto economico:
Se ogni minuto gli utenti spendono 1.500 €, l’impatto è:
Impatto=10minuti×1.500€/minuto=15.000€

AZIONI PREVENTIVE PER MITIGARE DDOS

Bilanciare il carico utilizzando il load balancer per distribuire il traffico su più server, implementare il CDN (Content Delivery Network) per distribuire il contenuto e ridurre il carico diretto sui server e servizi anti-DDoS

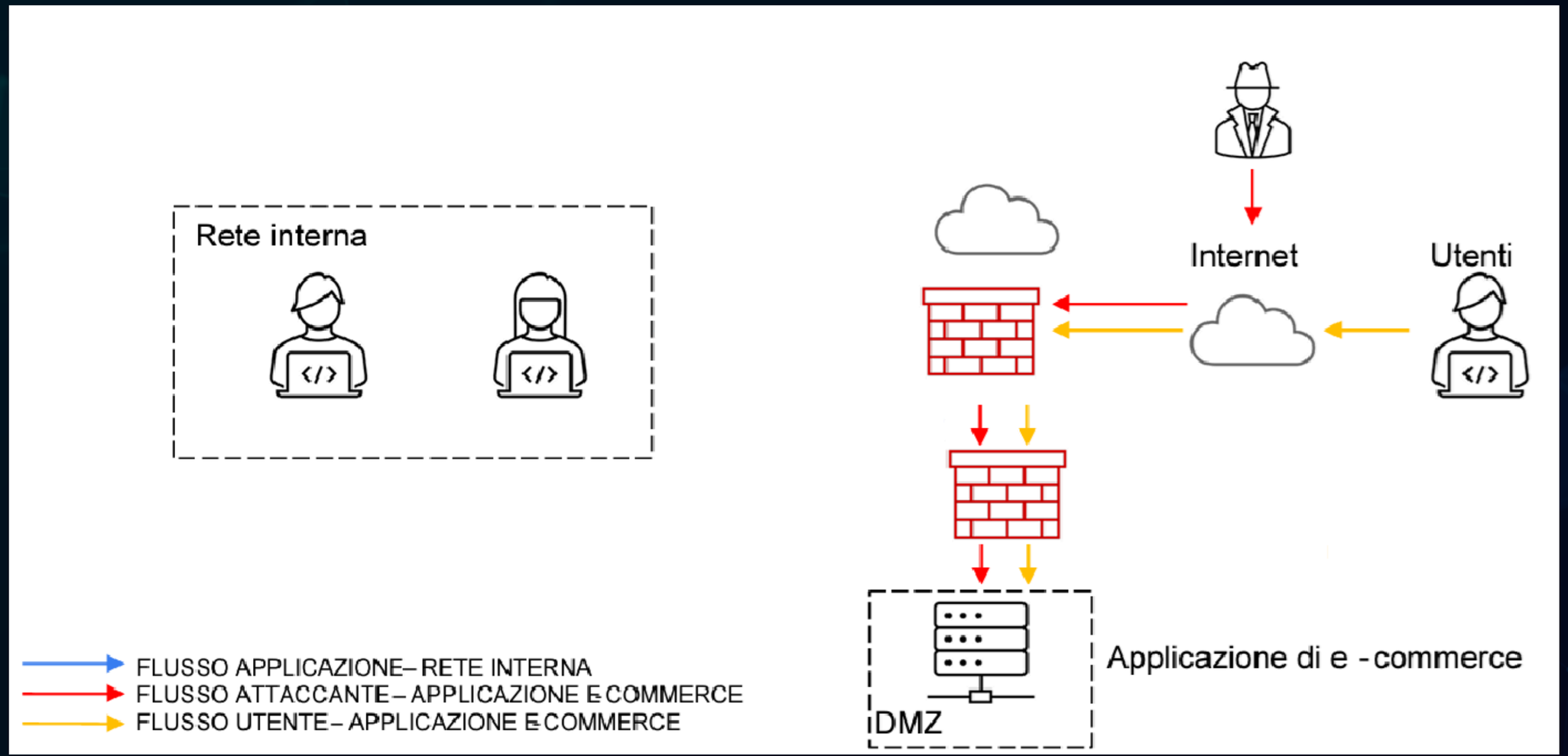
3. RESPONSE

Se l’applicazione Web viene infettata da un malware, la priorità è impedire la propagazione del malware nella rete interna.
Per farlo bisogna isolare il sistema infetto scollegandolo dalla rete interna per impedire la diffusione del malware e implementare strumenti di monitoraggio per rilevare e analizzare ulteriori attività malevole.



Visto che dalla DMZ è possibile raggiungere la rete interna bisogna isolarla in modo che l’attacante non riesca ad entrare anche in essa.

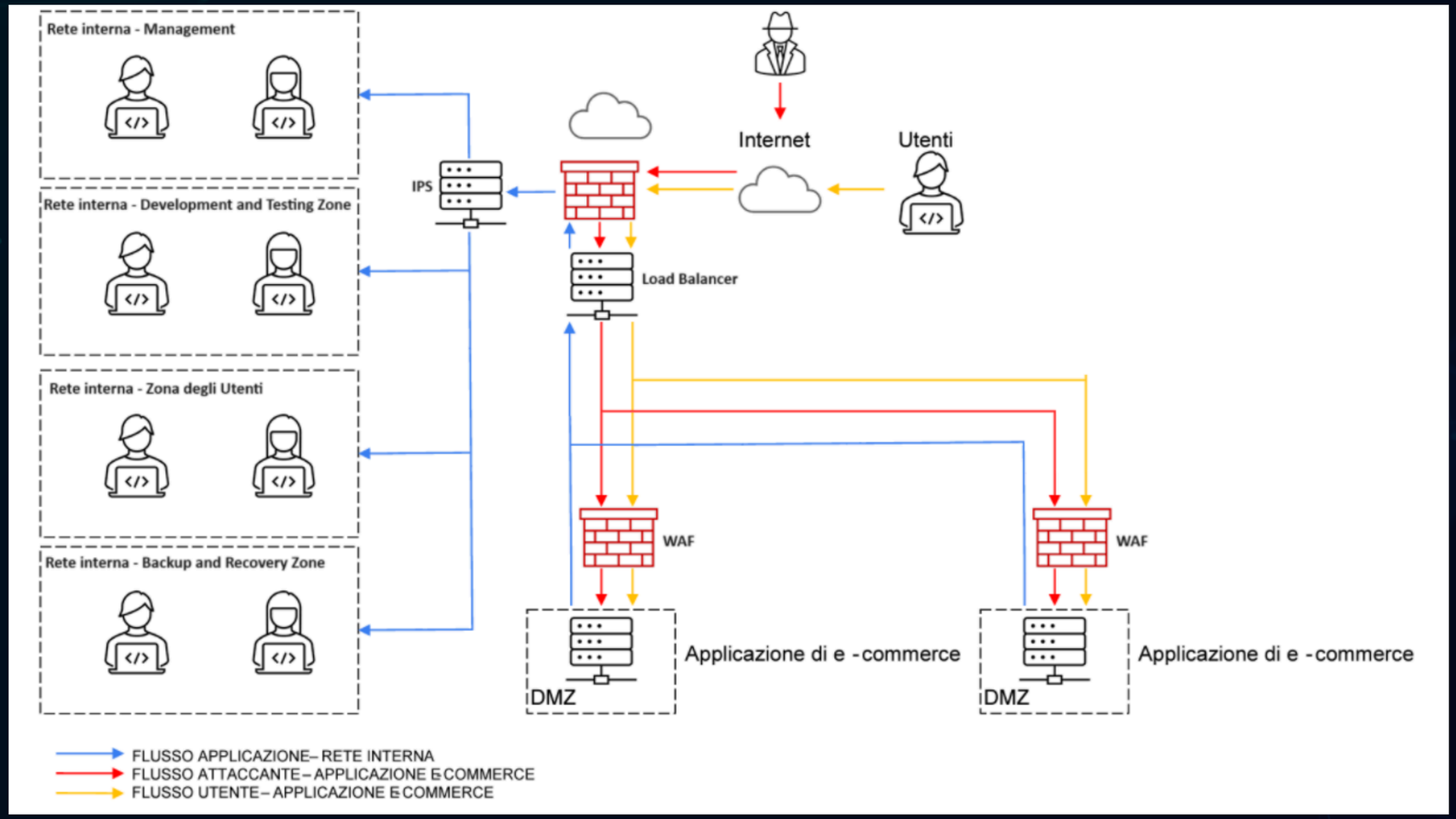
4. SOLUZIONE COMPLETA



5. MODIFICA DELL'INFRASTRUTTURA

Ho deciso di apportare le seguenti modifiche per rendere più sicura la rete aziendale:

1. Ho diviso la rete interna in più sottoreti in modo da migliorare la sicurezza isolando le diverse parti della rete e contenere potenziali attacchi limitando l'accesso tra le subnet.



2. Ho agginto un IPS per rilevare e prevenire tentativi di intrusione e attacchi malevoli rilevando comportamenti sospetti in tempo reale.

3. Un WAF per protegge le applicazioni web da attacchi specifici come SQL injection e XSS e filtrare e monitorare il traffico HTTP/HTTPS diretto alle applicazioni web.

4. Un Load Balancer per distribuire il traffico tra diversi server per evitare sovraccarichi e prevenire attacchi DoS e DDoS, inoltre migliora la disponibilità e le prestazioni delle applicazioni web.

Questi cambiamenti rendono la rete più robusta e resiliente agli attacchi, migliorando al contempo la gestione e la sicurezza complessiva delle risorse aziendali.