



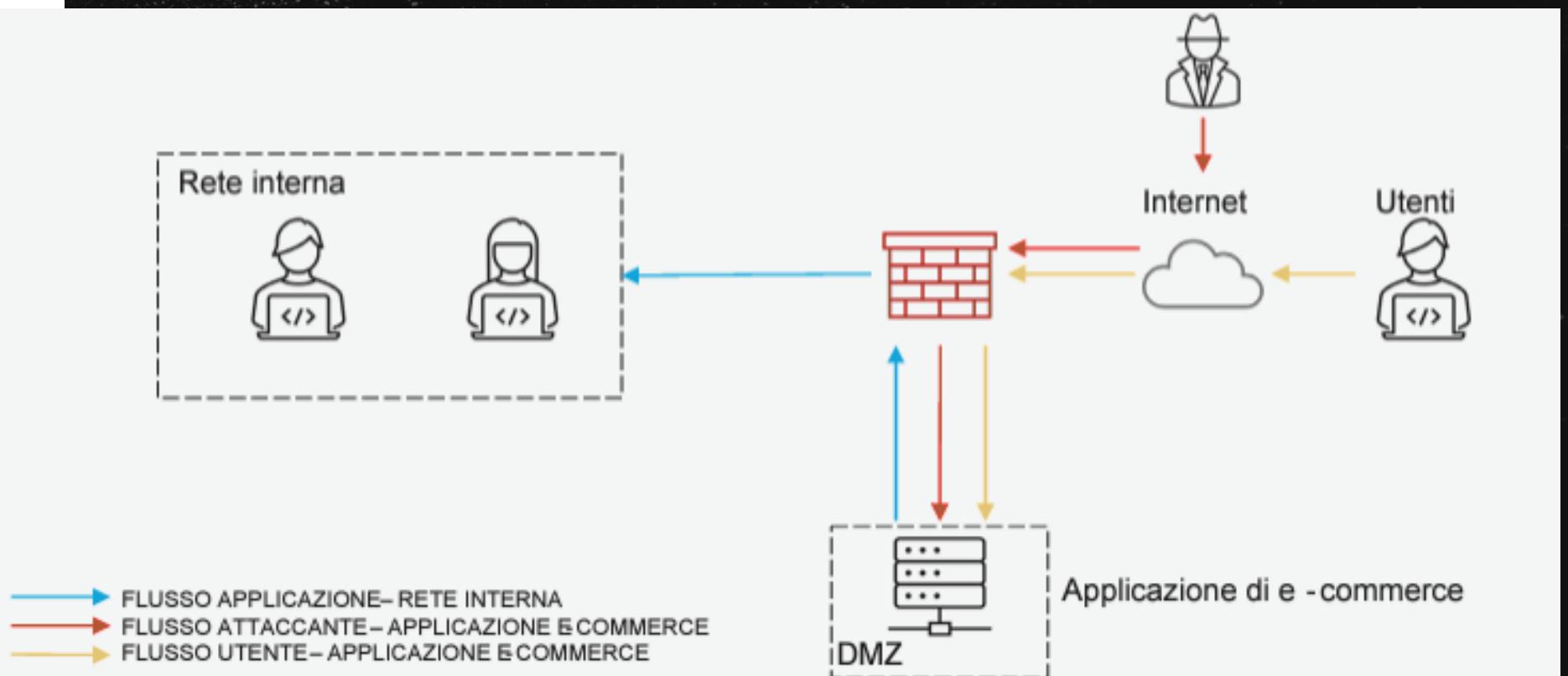
# CYBER SECURITY & ETHICAL HACKING

## Giorno 5 - Progetto

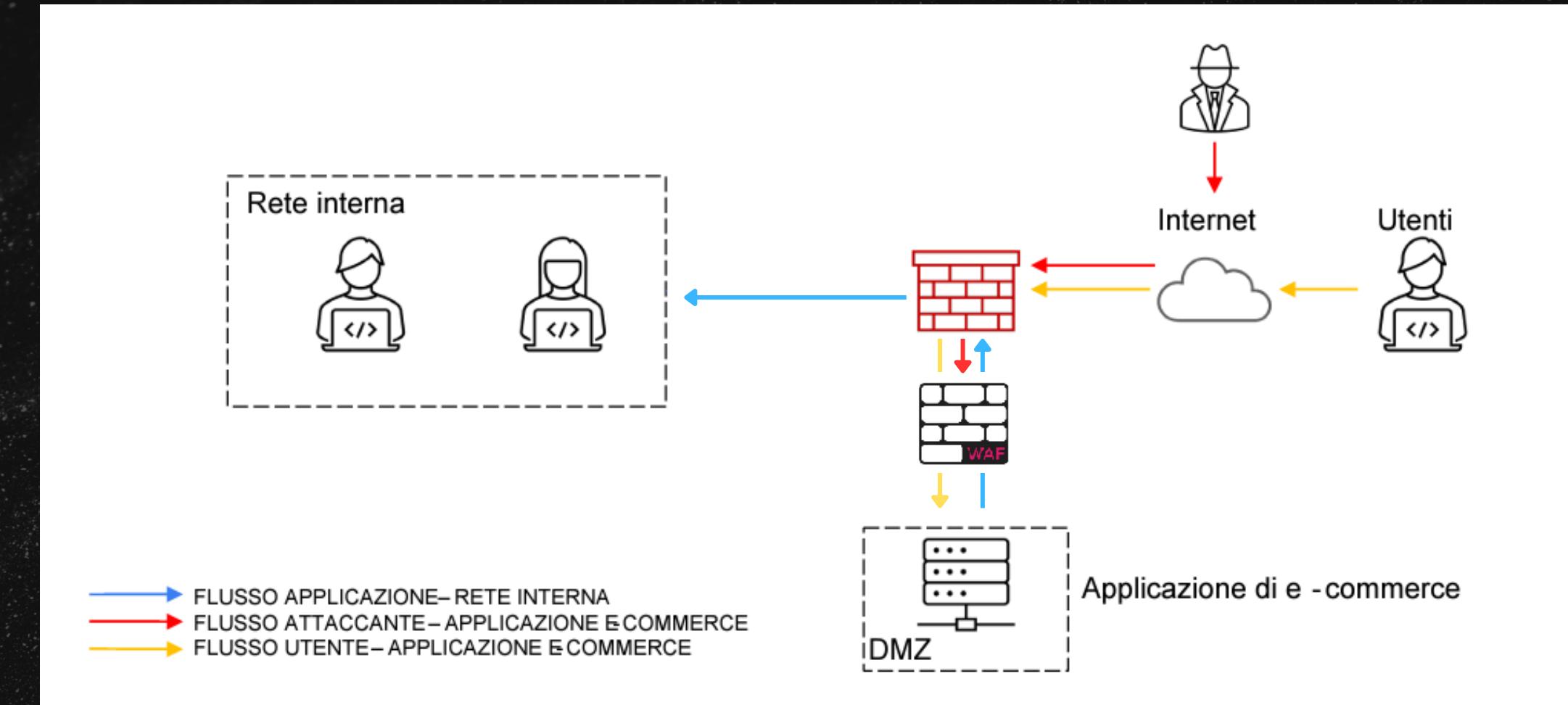
# TRACCIA

Con riferimento alla figura in slide 2, 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:** integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)



# AZIONI PREVENTIVE



## WAF

Un Web Application Firewall (WAF) è uno strumento importante per la sicurezza delle applicazioni web, poiché agisce come barriera protettiva tra l'applicazione e il traffico web. L'implementazione di un WAF e l'adozione di queste azioni preventive contribuiranno a rafforzare la sicurezza dell'applicazione web contro una vasta gamma di minacce online.

## Protezione Contro SQL Injection e XSS:

Utilizzare le funzionalità di protezione integrate del WAF per rilevare e bloccare tentativi di SQL Injection e Cross-Site Scripting. Molte soluzioni WAF offrono regole predefinite per queste minacce comuni.

# IMPATTI SUL BUSINESS

## Calcolo Impatto totale

Durata dell'attacco: 10 minuti

**Spesa media degli utenti al minuto:** 1.500 €

Impatto Finanziario = Durata Attacco x Spesa Media

Impatto Finanziario = 10 min x 1500€/min

Impatto Finanziario = 15.000€

## Azioni Preventive:

**Backup e ripristino:** Eseguire regolarmente backup dei dati e verifica la disponibilità di procedure di ripristino in caso di attacchi che potrebbero danneggiare o compromettere i dati.

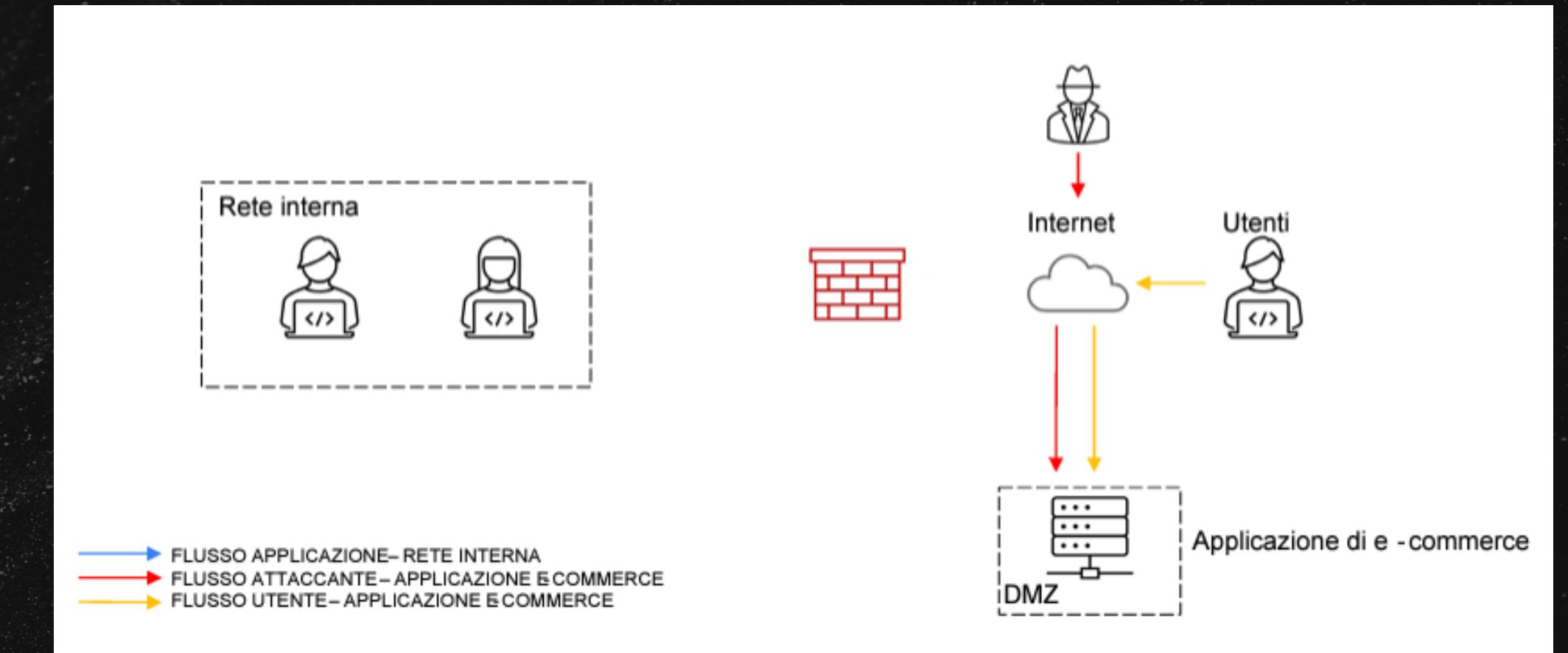
**Monitoraggio e rilevamento anomalo:** Implementare sistemi di monitoraggio che rilevano comportamenti anomali nel traffico e nei pattern di accesso, permettendo una risposta tempestiva.

**Educazione degli Utenti:** Informare gli utenti sulle pratiche di sicurezza, ad esempio l'utilizzo di password sicure e l'attenzione a possibili minacce.

# RESPONSE

## ISOLAMENTO DELLA MACCHINA INFETTA

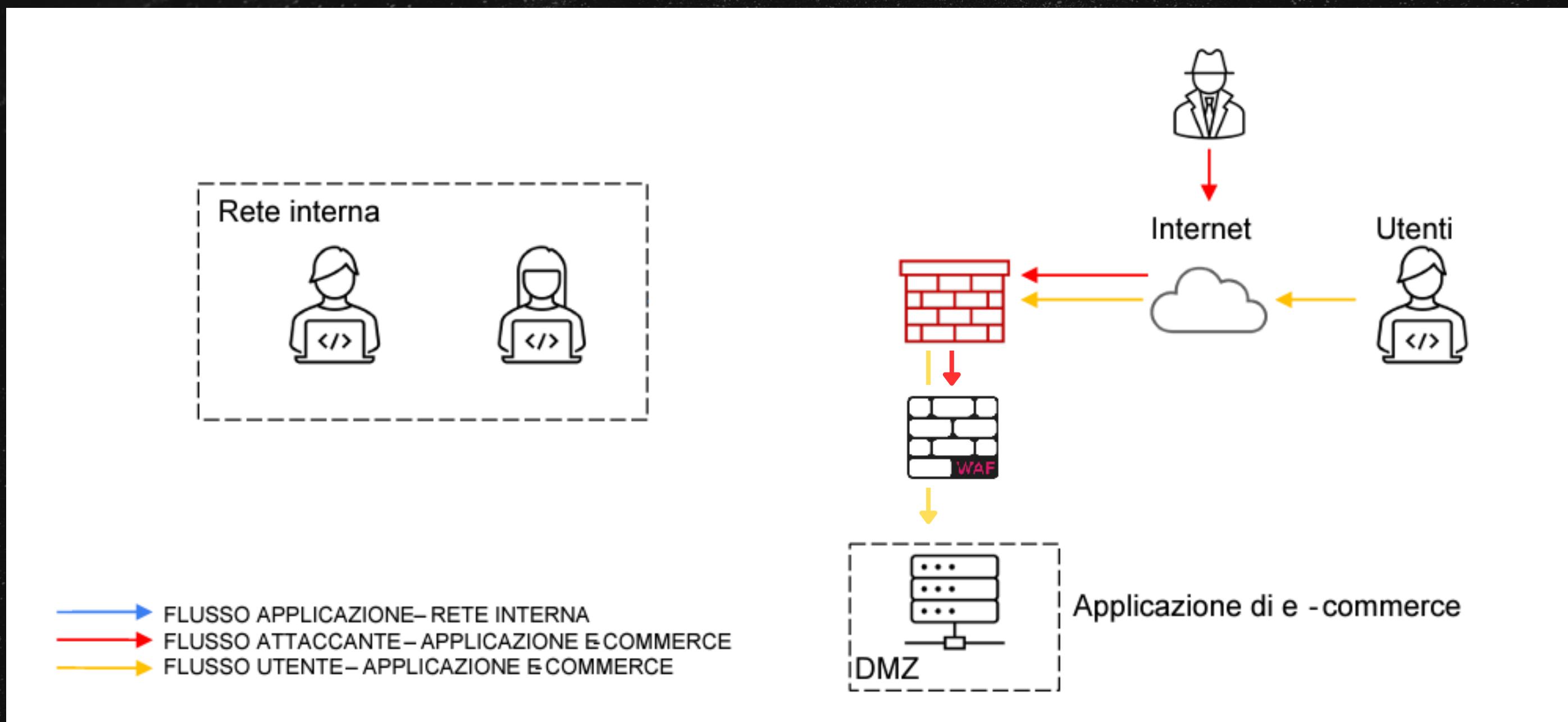
Isolare immediatamente la macchina infettata dalla rete. Questo può essere fatto disconnettendo fisicamente la macchina dalla rete o utilizzando funzionalità di isolamento di rete.



## SCANSIONE ANTIVIRUS E ANTIMALWARE

Utilizzare scanner antivirus e antimalware per individuare e rimuovere il malware dalla macchina infettata. Tuttavia, se l'obiettivo principale è prevenire la propagazione e non disconnettere l'attaccante, la rimozione potrebbe essere ritardata.

# RESPONSE



# **MODIFICA «PIÙ AGGRESSIVA» DELL'INFRASTRUTTURA**

## **Segmentazione della Rete**

La "segmentazione della rete" si riferisce alla pratica di dividere una rete informatica in segmenti più piccoli o "segmenti" al fine di migliorare la sicurezza, la gestibilità e le prestazioni complessive del sistema. Questo approccio è spesso utilizzato per limitare la propagazione di minacce e migliorare la visibilità e il controllo del traffico di rete.

## **IPS/IDS**

IPS (Intrusion Prevention System) e IDS (Intrusion Detection System) sono due componenti critici nella sicurezza delle reti. Entrambi si concentrano sulla rilevazione e, nel caso dell'IPS, anche sulla prevenzione delle intrusioni.

L'IDS è progettato per rilevare attività sospette o potenziali intrusioni nella rete.

L'IPS va oltre l'IDS intervenendo attivamente per prevenire o bloccare attacchi identificati.