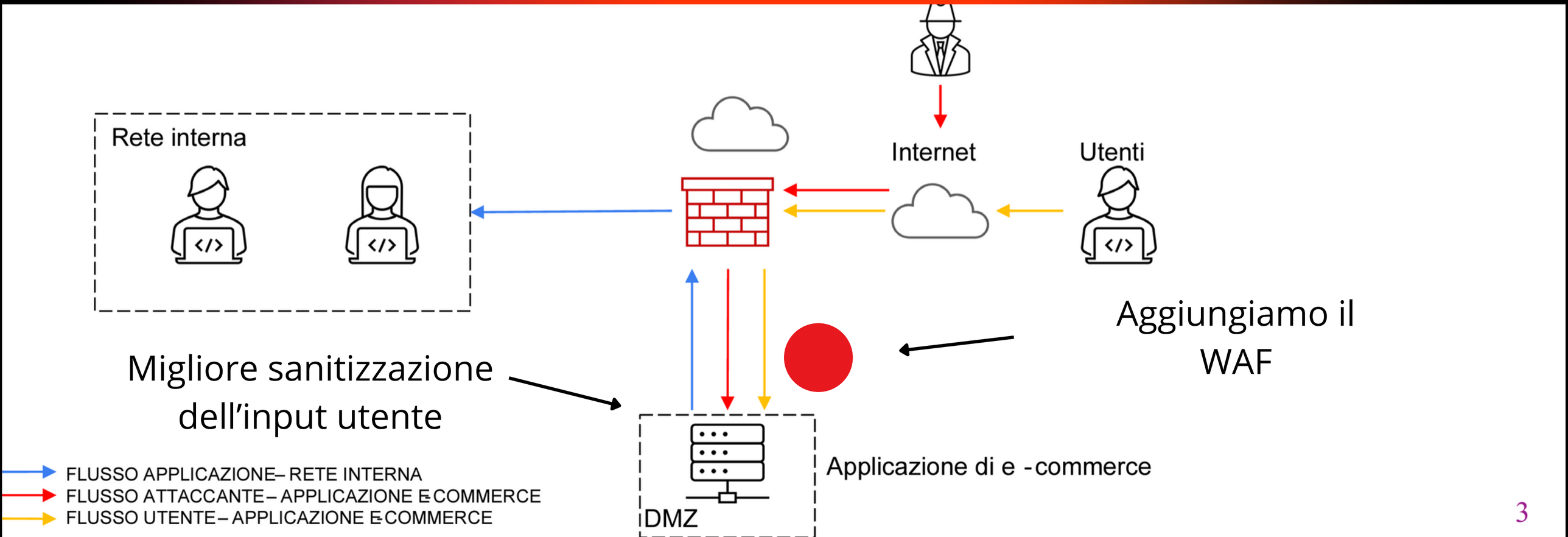
Punto 1:
azioni preventive

Un modo per prevenire attacchi XSS oppure di SQL Injection è quello di implementare una sanitizzazione migliore per gli input inseriti dall'utente sull'applicazione web.
Inoltre possiamo aggiungere un WAF (web application firewall) per filtrare il traffico verso il webserver.



Punto 2:
impatto sul business di un attacco DDoS

I danni economici causati da un attacco DDoS esterno dalla durata di 10 minuti sono di 15.000 € dato che in media gli utenti del sito spendono 1500 € al minuto.

Per prevenire questo tipo di attacco, possiamo implementare diverse soluzioni:

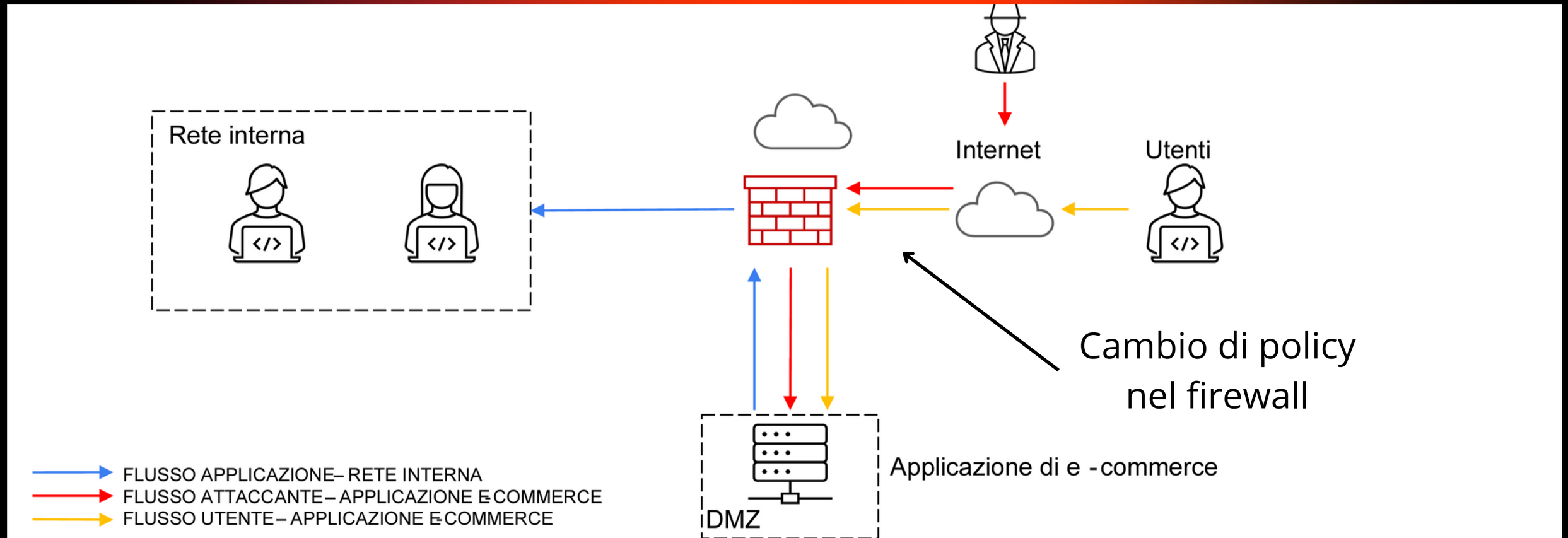
1) Aggiungere un Load Balancer, in modo da aumentare la resistenza al sovraccarico del web server.

2) Aggiungere un sistema di alert, in modo da poter ricevere notifiche in caso di attività anomale e rispondere agli attacchi DDoS in tempo reale.

3) Aggiungere un limite massimo alle richieste che possono essere fatte al web server da un dispositivo in un certo lasso di tempo, in modo da non sovraccaricarlo.

Punto 3:
response

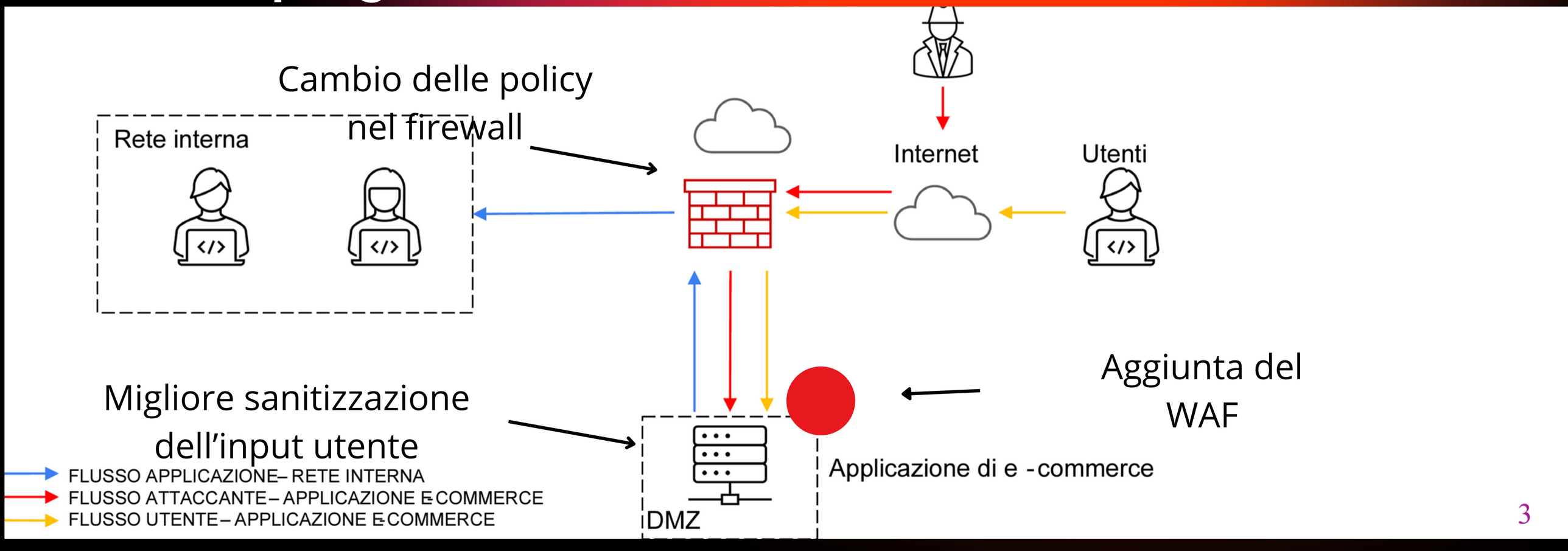
Per non far propagare il malware nel resto della rete, va chiuso qualsiasi contatto tra il web server e la rete interna dell'azienda.
In questo caso specifico, il web server si trova in una DMZ, quindi è isolato dalla rete interna, però mantiene dei contatti a causa delle policy sul firewall, quindi per isolare il web server bisogna cambiare le policy attualmente in uso nel firewall.



Punto 4: soluzione completa

Mettendo insieme le soluzioni del punto 1 e del punto 3 otteniamo:

Migliore sanitizzazione dell'input utente sul web server.
Aggiunta di un WAF per filtrare il traffico.
Cambio delle policy attualmente in uso nel firewall.



Punto 5:
Modifica «più aggressiva» dell'infrastruttura:

Se abbiamo un budget più ampio e vogliamo anche la difesa da attacchi DDoS più altre misure aggiuntive, possiamo aggiungere alla soluzione del punto 3 :

Uno o più Load Balancer come supporto contro gli attacchi DDoS.

Un sistema di alert con IDS/IPS Per una maggiore protezione generale.

Acquisto ed utilizzo di un tool SIEM come Splunk per una maggiore sicurezza.