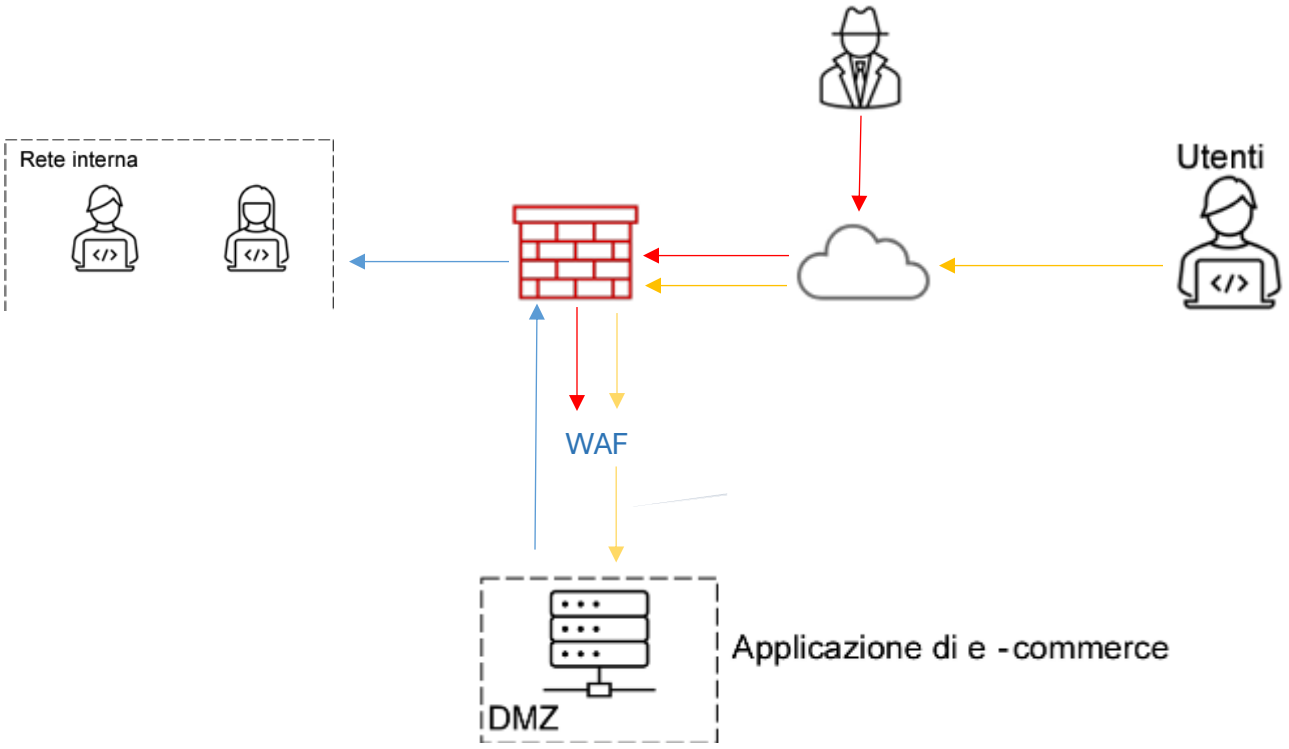
SOLUZIONE TRACCIA

1.Un'azione preventiva per evitare attacchi XSS e SQLi su una applicazione web da parte di malintenzionati potrebbe essere implementare un Web Application Firewall (WAF), ponendolo o tra il firewall convenzionale e la dmz (come in figura), o tra internet e il firewall convenzionale.

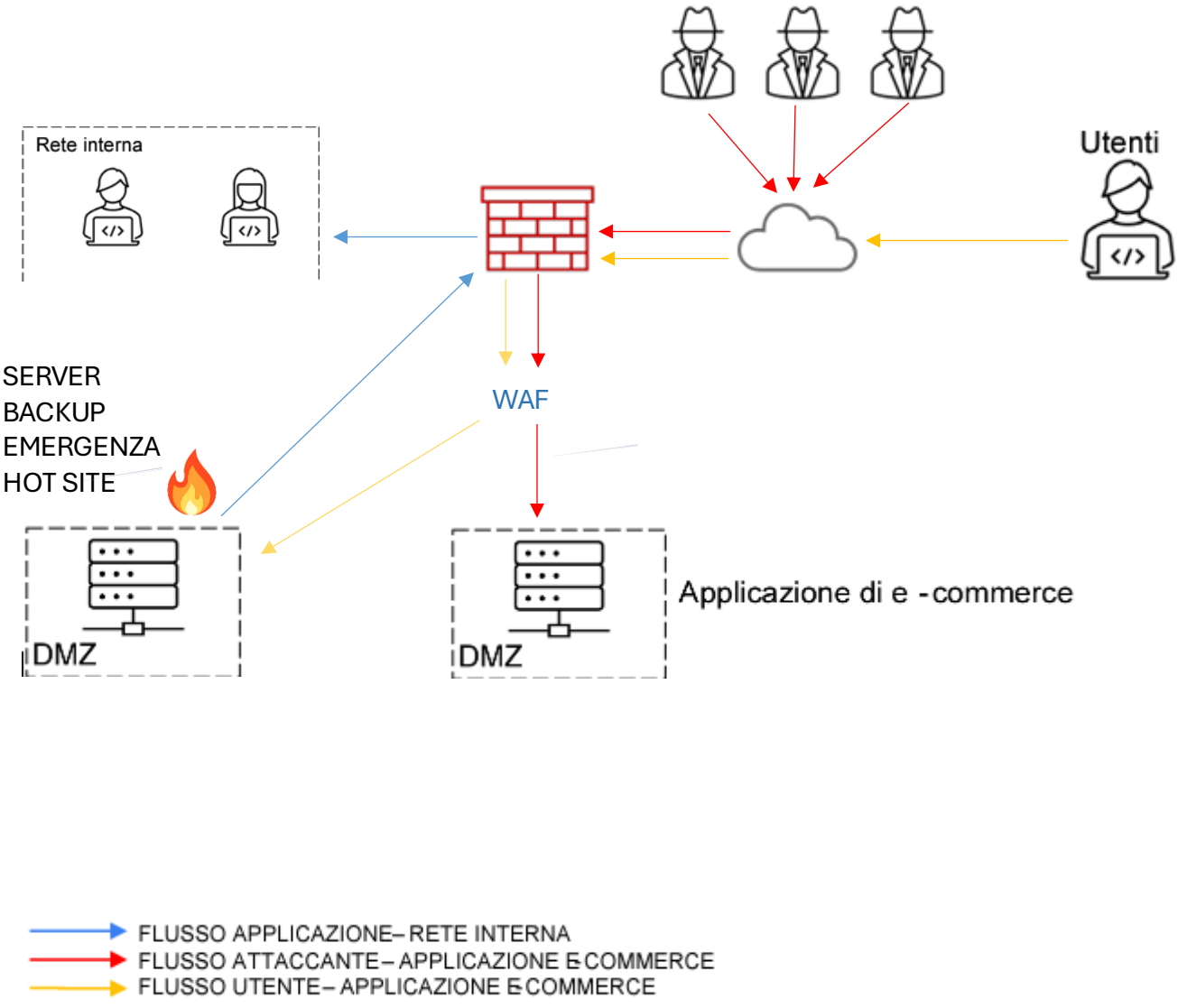


FLUSSO APPLICAZIONE– RETE INTERNA
FLUSSO ATTACCANTE– APPLICAZIONE E-COMMERCE
FLUSSO UTENTE– APPLICAZIONE E-COMMERCE

2. Se l'applicazione web subisce un attacco DDoS che rende la stessa non raggiungibile per 10 minuti, e che in media gli utenti spendono 1500€ al minuto sulla piattaforma, possiamo stimare il danno con una semplice formula matematica:

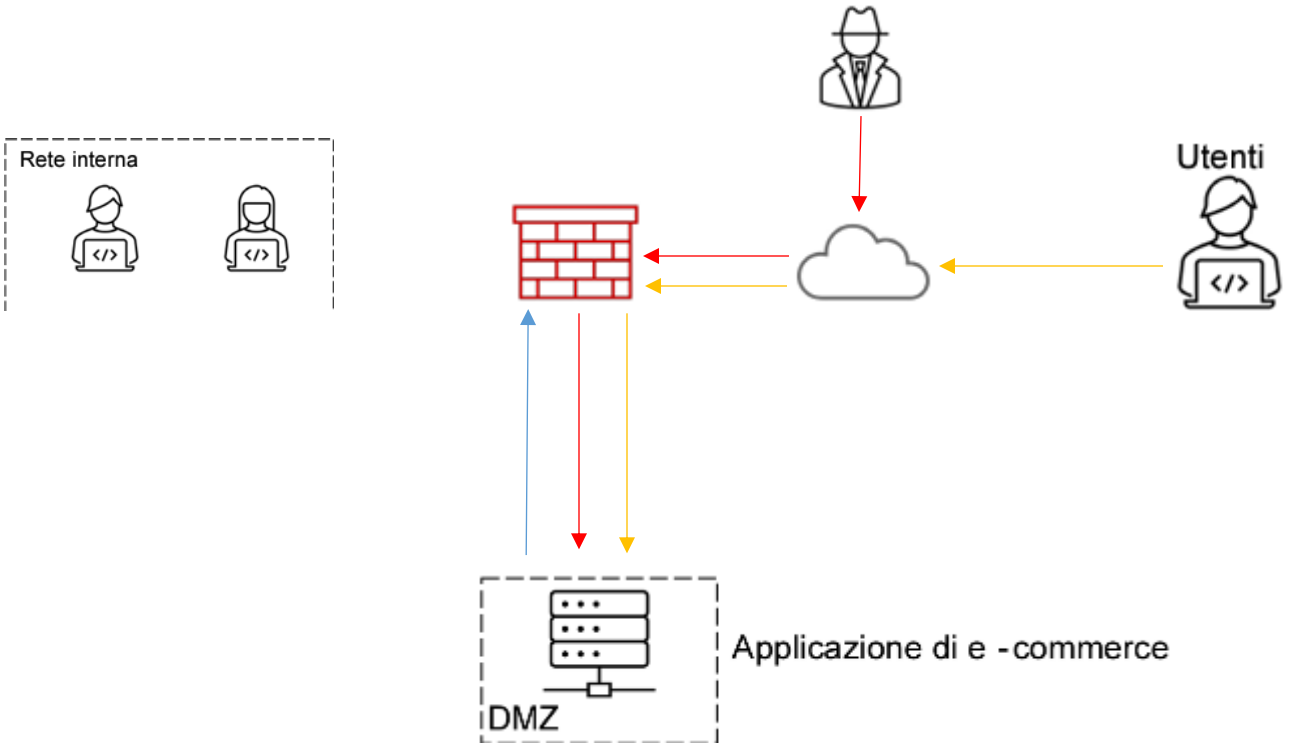
1500€ x 10 min = 15000€

Il danno ammonta a 15000 euro complessivi. Per limitare tutto ciò, si potrebbe "spalmare" le richieste su più server, oppure avere un server di backup, nel caso in cui il principale venga in questo caso ddossato, oppure vada per un qualsivoglia motivo offiline, per garantire così la business continuity. Un altro metodo che potrebbe aiutare molto, sarebbe la limitazione di richieste da un indirizzo IP. In questo caso, però, riusciamo a limitare solo un attacco Dos, proveniente da un singolo IP, e non un DDoS.

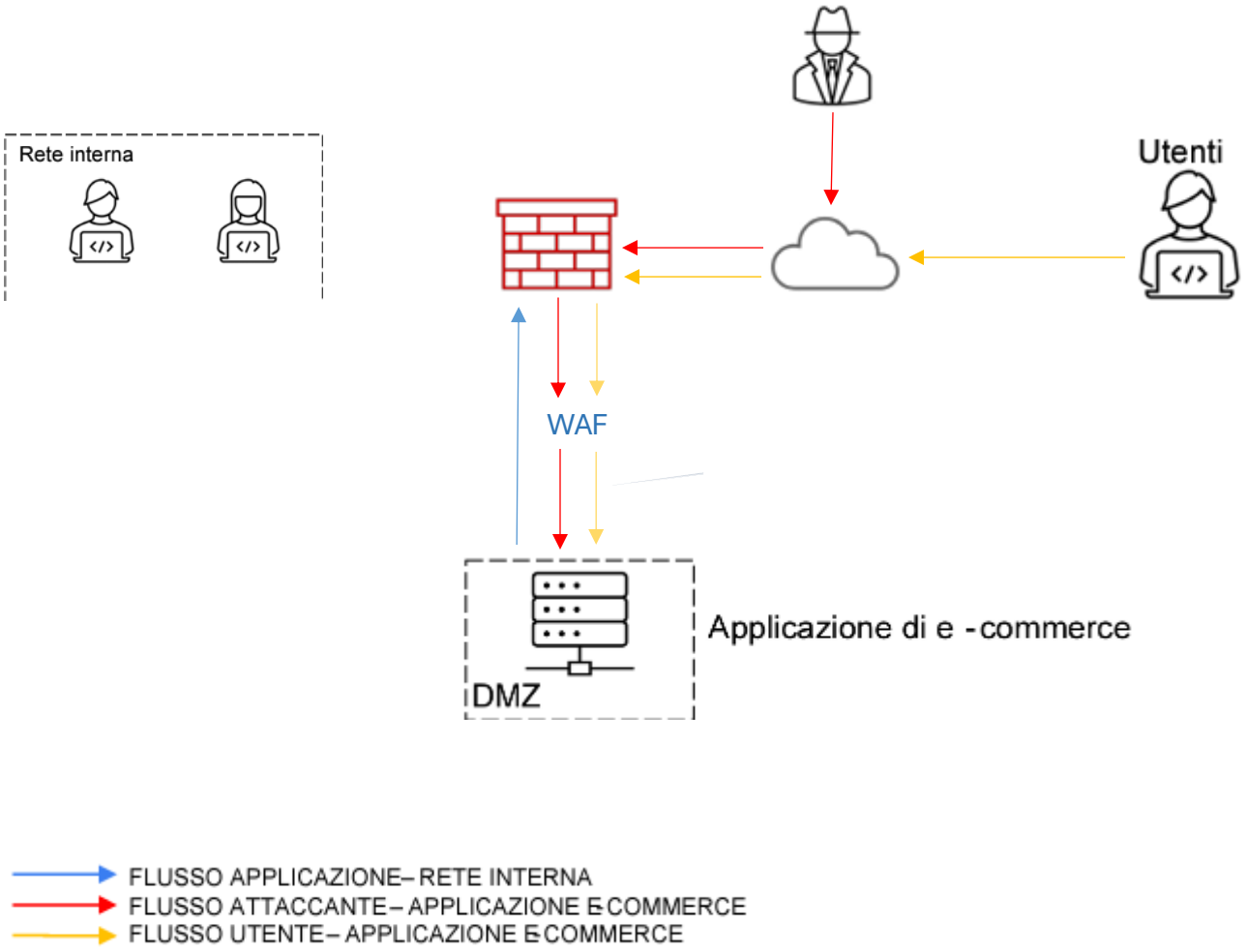


3. Il malware infetta l'applicazione di e-commerce. Non deve in alcun modo raggiungere la rete interna.

Per questo motivo la isoliamo dalla rete interna. Da traccia non ci interessa isolare l'accesso dell'attaccante. Procediamo all'isolamento della rete interna, modificando le regole di policy del firewall.



4. soluzione completa, con implementazione punto 1 e 3



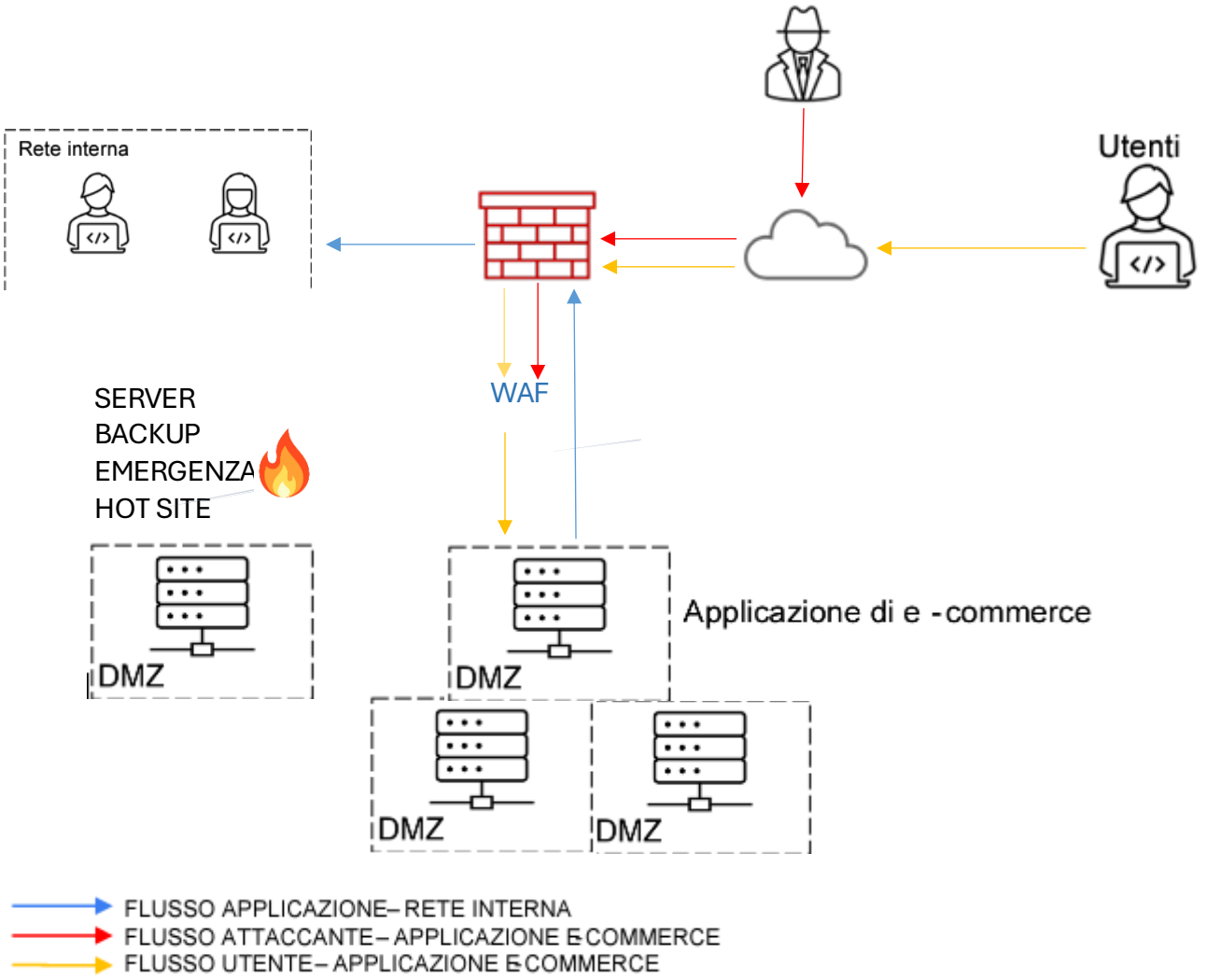
5. soluzione più “aggressiva”:

-utilizzo di eventuali IPS/IDS (esempio, limitazione richieste da parte di singolo IP per prevenire DoS)

-Utilizzo di più web server, per bilanciare il carico di richieste.

-Ridondanza, con uso della tecnica di “failover cluster”: utilizzo server backup nel caso in cui il web server vada offline. In caso di nessun problema di ottimizzazione spazio, si preferisce il full backup. Se si dispone di un grande potere economico, si può organizzare il server di backup in hot site, così da garantire la continuità del servizio.

-Un’altra opzione più economica consiste nel fare un backup sul cloud e utilizzare un Disaster Recovery as a Service (DRaaS), che numerose compagnie, come Amazon Web Services, mettono a disposizione. Tuttavia, la continuità del servizio non è garantita, ma le basse spese di gestione, visto che il servizio si paga solo in caso di utilizzo, sono un plus.



BONUS

Dalle analisi effettuate, siamo giunti alla conclusione che questi due malware appartengono alla famiglia degli Spyware, in quanto raccolgono svariate informazioni del computer attaccato.

Nello specifico, il primo malware raccoglie informazioni di sistema, andando a creare una copia di tutto ciò, che fa passare sottobanco come fosse un backup dello stesso, modifica le policy di esecuzione della powershell, fa uno scan dei software installati sul pc, e infine modifica le permissions di alcuni file o di intere directory.

Il secondo, invece, a prima vista sembra un normale download del browser Edge, ma ad un occhio più attento non sfugge la sorgente, ovvero un drive, cosa alquanto sospetta per un download di un prodotto ufficiale Microsoft. In effetti, il software, oltre che a leggere le specifiche del browser, droppa eseguibili windows legittimi, sostituendosi a questi ultimi, e disabilita il SEHOP (Structured Exception Handeler Overwrite Protection), che consiste in una tecnica utilizzata per prevenire la possibilità di attacchi che sfruttino la tecnica dello Structured Exception Handler (SEH) Overwrite, ovvero la sovrascrittura di un blocco di codice preposto alla gestione delle eccezioni che possono verificarsi durante la normale elaborazione di un'applicazione.

Per evitare di incappare in queste spiacevoli situazioni, si consiglia di scaricare dal web solo prodotti verificati, e che abbiano una sorgente affidabile (Attenzione ai Drive!).
Inoltre, avere un antivirus aggiornato e un firewall funzionante aiutano molto nel contrastare questo tipo di attacchi.