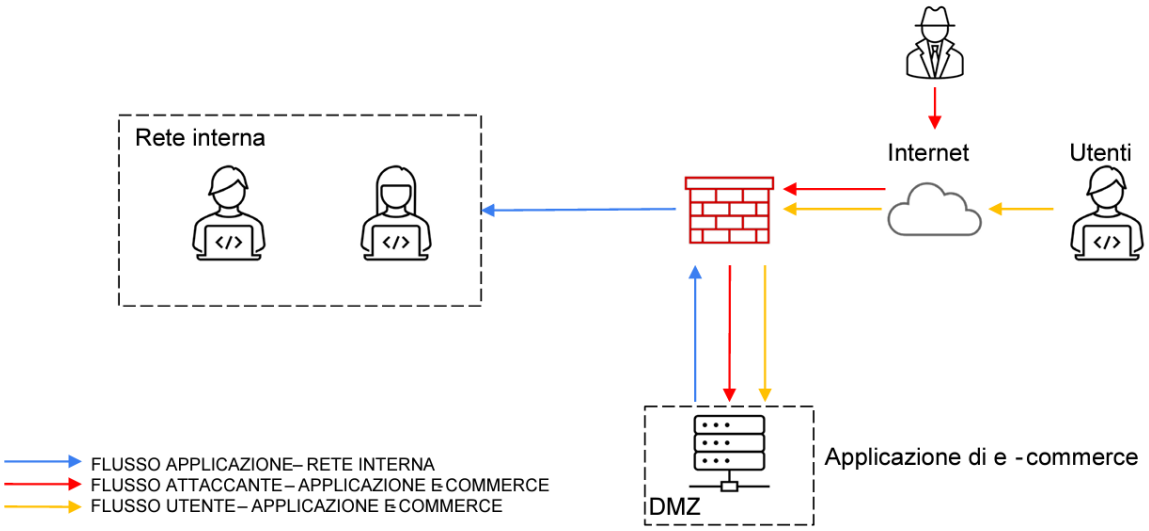
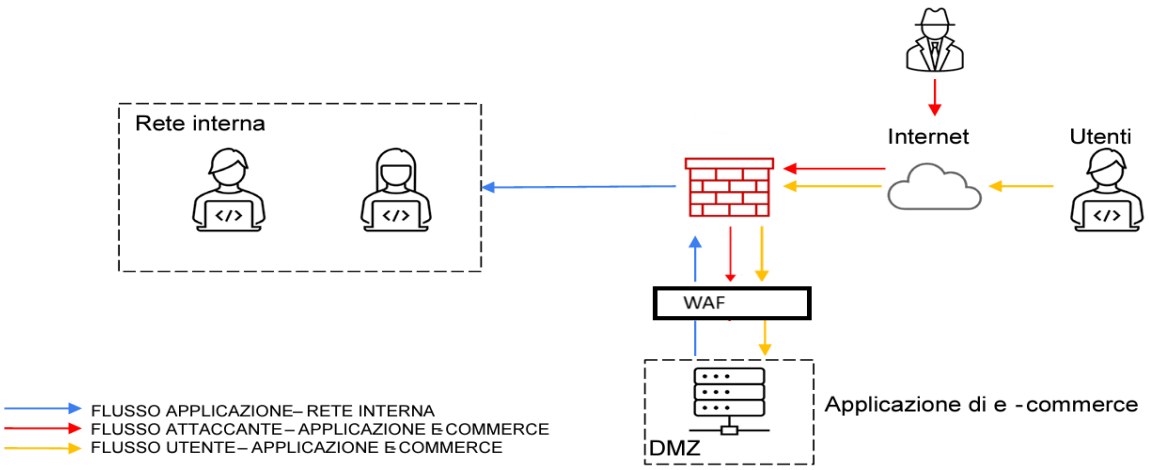
Architettura di rete: L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna:



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.*

Le **azioni preventive** sono misure proattive adottate per prevenire o ridurre al minimo i rischi e le minacce nel nostro caso legate alla sicurezza informatica. Queste azioni sono progettate per evitare che eventi dannosi o indesiderati si verifichino, o per limitare il loro impatto nel caso in cui si verifichino. Le azioni preventive possono includere l'implementazione di politiche, procedure, protocolli, controlli tecnologici, formazione del personale e altre strategie volte a mitigare i rischi e proteggere gli interessi, gli asset o le persone coinvolte. In sostanza, le azioni preventive sono uno sforzo preventivo per evitare problemi anziché reagire ad essi una volta che si sono verificati.

Per difendere l'applicazione web da attacchi di tipo SQLi (Injection SQL) o XSS (Cross-Site Scripting) da parte di un utente malintenzionato ho messo un WAF tra il firewall e la DMZ. L'implementazione di un Web Application Firewall (WAF) tra il firewall e la DMZ rappresenta una decisione strategica fondamentale per garantire la sicurezza e l'integrità di un'applicazione web esposta su Internet. Il WAF agisce come una barriera difensiva aggiuntiva, fornendo filtraggio del traffico, rilevazione di pattern malevoli e protezione contro vulnerabilità conosciute e zero-day. Questa misura contribuisce a mitigare efficacemente il rischio di attacchi di tipo Injection SQL e Cross-Site Scripting da parte di utenti malintenzionati:



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.*

Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco DDoS, possiamo utilizzare la seguente formula:

Impatto sull'attività = (Numero di minuti di indisponibilità) * (Spesa media degli utenti al minuto)

Dato che ogni minuto gli utenti spendono in media 1.500 € sulla piattaforma di e-commerce e l'applicazione è stata non raggiungibile per 10 minuti, il calcolo dell'impatto sull'attività sarà:

Impatto sull'attività = 10 minuti * 1.500 €/minuto = 15.000 €

Quindi, l'impatto sull'attività dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.

Per ridurre l'impatto degli attacchi DDoS e mitigare la non raggiungibilità dell'applicazione, si possono adottare diverse azioni preventive, tra cui:

- **Implementazione di un sistema di mitigazione DDoS**: Utilizzare un servizio o un dispositivo di mitigazione DDoS che possa rilevare e mitigare gli attacchi DDoS in tempo reale, permettendo all'applicazione di rimanere accessibile agli utenti anche durante gli attacchi.

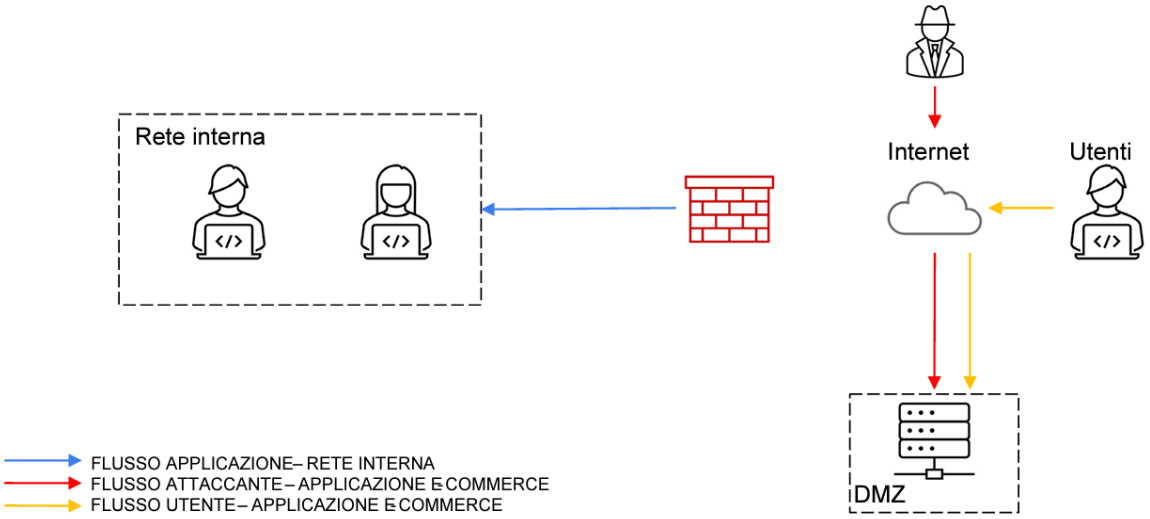
- **Bilanciamento del carico:** Implementare una soluzione di bilanciamento del carico per distribuire il traffico tra più server o infrastrutture, in modo che un eventuale attacco DDoS non sovraccarichi un singolo punto di ingresso.

- **Firewall e filtri di rete**: Configurare firewall e filtri di rete per bloccare il traffico sospetto o proveniente da indirizzi IP noti per essere associati ad attacchi DDoS.

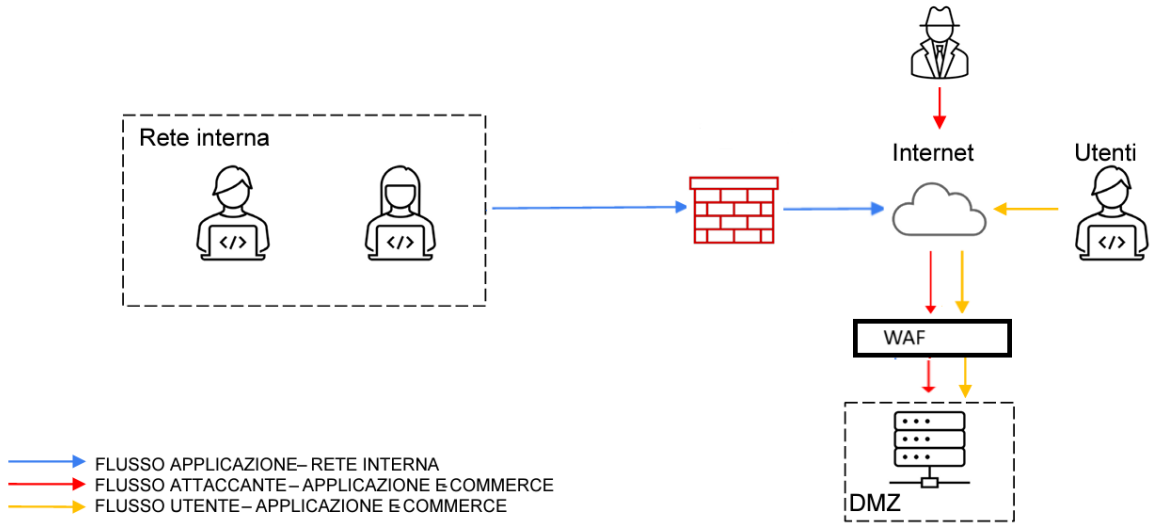
L'implementazione di queste azioni preventive può contribuire significativamente a ridurre l'impatto degli attacchi DDoS sull'attività e a garantire la continuità operativa dell'applicazione di e-commerce anche in presenza di attacchi.

3. ***Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malwarenon si propaghi sulla vostra 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.*

Ho **isolato la DMZ**, il dispositivo infetto, per prevenire la propagazione del malware sulla rete aziendale. Ciò è fondamentale perché l'isolamento della DMZ limita la capacità del malware di diffondersi su altri dispositivi all'interno della rete. Isolare il dispositivo infetto aiuta a contenere l'attacco all'area colpita, proteggendo al contempo il resto dell'infrastruttura e dei dati aziendali. Inoltre, mantenendo l'accesso dell'attaccante alla macchina infetta, si può condurre un'analisi approfondita del malware e delle sue azioni senza interferenze, fornendo informazioni cruciali per comprendere l'attacco e sviluppare contromisure adeguate per prevenirne futuri incidenti:



4. ***Soluzione completa**: unire i disegni dell'azione preventiva e della response(unire soluzione 1 e 3):*



5. ***Modifica "più aggressiva" dell'infrastuttura*** *integrando eventuali altri elementi di sicurezza.*

- L'implementazione di una **connessione Internet di backup** può essere estremamente utile per garantire la continuità operativa in caso di down della prima connessione. Questo è noto come un sistema di failover.

- L'installazione di uno o più Network Attached Storage (**NAS**) potrebbe essere una buona idea per il backup dei dati critici e per fornire una soluzione di archiviazione centralizzata.

- Si potrebbe implementare anche un **IPS** (Intrusion Prevention System), che potrebbe essere una buona aggiunta per rafforzare ulteriormente la sicurezza della rete, soprattutto considerando l'importanza di proteggere l'infrastruttura dalla minaccia delle intrusioni. Si può posizionare l'IPS in punti strategici della rete per massimizzare la protezione e la rilevazione delle intrusioni. Nel nostro caso possiamo posizionare l'IPS tra il WAF e la DMZ, per fornire un ulteriore strato di sicurezza e monitoraggio del traffico in ingresso e in uscita dalla DMZ. In questa configurazione, l'IPS può fornire un controllo supplementare sul traffico che passa attraverso il WAF prima di entrare nella DMZ o di lasciare la DMZ per raggiungere la rete interna. Ciò consente di identificare e prevenire tempestivamente le minacce che potrebbero aver superato il WAF o originarsi all'interno della DMZ.