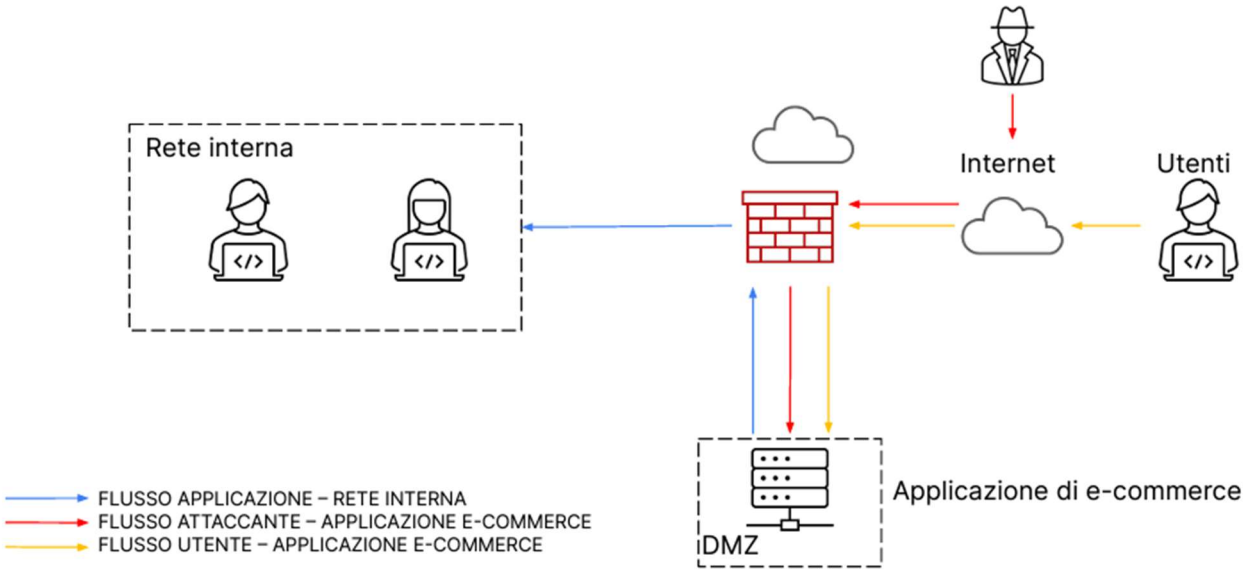
**ESERCITAZIONE FINE MODULO 5**
**BARRECA MONICA**




**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**

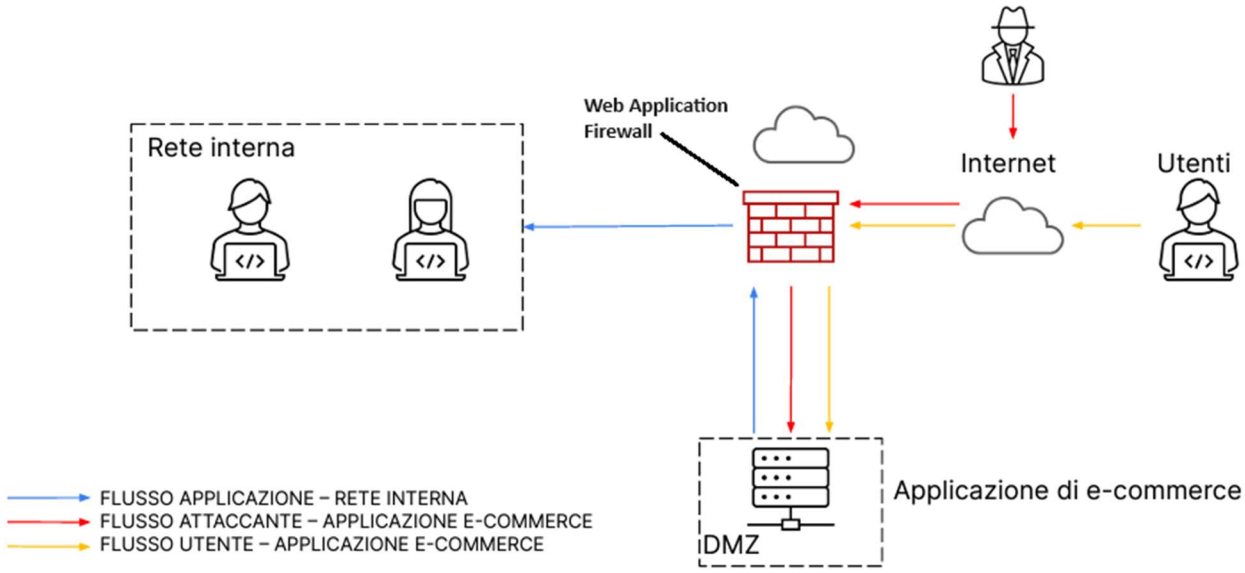
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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

5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

1. **Azioni preventive:**
   Sicuramente una delle azioni preventive da utilizzare è un Web Application Firewall, dispositivo di sicurezza apposito per proteggere la web application da attacchi di tipo SQL Injection o XSS (Cross Site Scripting).
   In via preventiva sarebbe il caso anche di sviluppare adeguatamente la web application in previsione di queste tipologie di attacco: è importante andare a verificare che nel codice sorgente non vi siano delle potenziali vulnerabilità che possano essere sfruttate da un attaccante. Quindi sarebbe utile fare un'analisi del codice sorgente statico in prima battuta, e magari anche dinamico in seconda battuta per effettivamente verificare se vi sono anomalie in fase di esecuzione del programma.

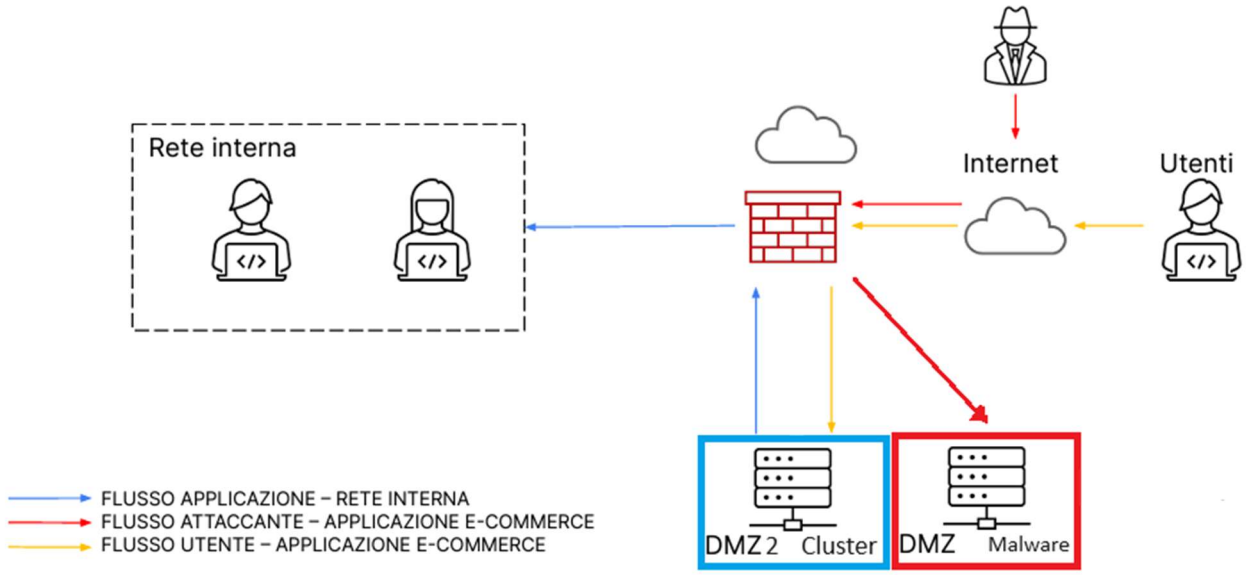
**ESERCITAZIONE FINE MODULO 5**
**BARRECA MONICA**



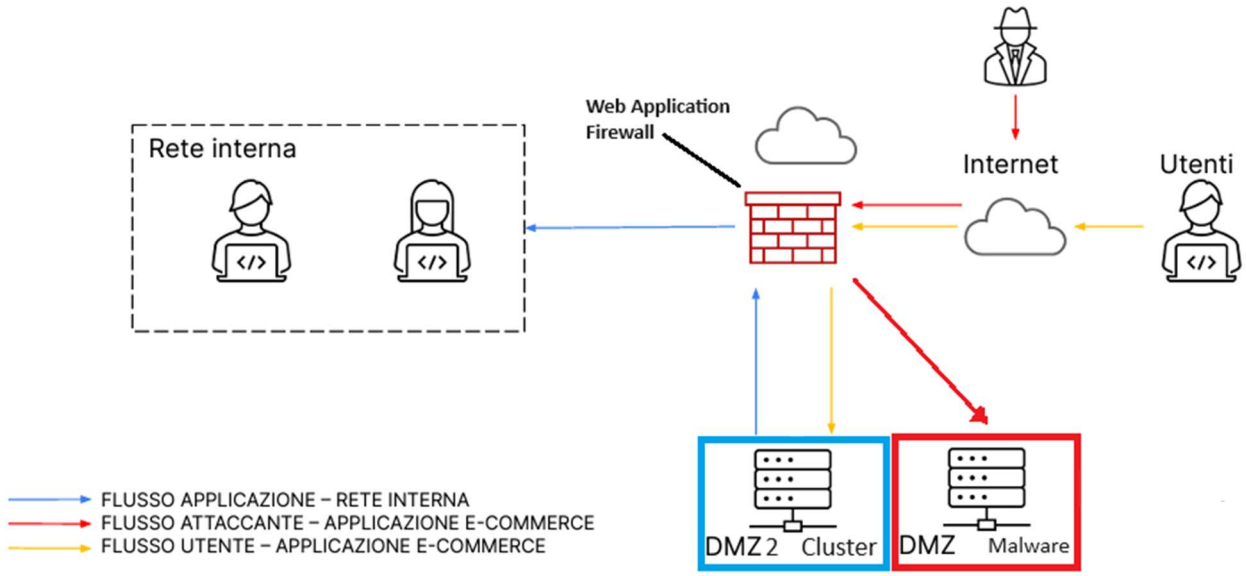

2. **Impatti sul business:**
   Per attacco di tipo DDoS, si intende in pratica che più macchine stanno attaccando contemporaneamente la nostra web application. Nel caso previsto dalla traccia, il mero calcolo da fare per risalire all'impatto reale sul business è:
   **1.500,00 €/min * 10 minuti = 15.000,00 € (potenzialmente persi)**
   Però, in via preventiva si potrebbe pensare a un failover cluster, quindi avere un'altra macchina che svolge esattamente lo stesso ruolo, in modo tale che, se la prima smette di funzionare, la seconda subentri automaticamente.
   A seconda del budget a disposizione, si potrebbe pensare ad un approccio di tipo cold/hot site, oppure affidarsi a terzi con il DRaaS.
   Unitamente a queste azioni si potrebbe utilizzare anche un sistema di prevenzione e rilevamento delle minacce (IPS) che monitora il traffico in cerca di anomalie sospette e in via preventiva supporta anche delle azioni automatiche per bloccare le intrusioni.

3. **Response:**
   Nel caso specifico richiesto dalla traccia, l'opzione migliore sarebbe l'isolamento della DMZ dalla rete interna. Stiamo parlando della fase di contenimento in caso di incidente.
   Ipotizziamo anche che vi sia un cluster backup della nostra DMZ, così che da un lato gli utenti e la rete interna non abbiano accesso al server infetto, ma possano comunque utilizzare il servizio, mentre l'attaccante continua comunque ad avere accesso al server infetto.
   Successivamente, vi sono le fasi di rimozione e recupero:
   - La rimozione prevede un'analisi approfondita della macchina al fine di rimuovere eventuali backdoor, ripulire dischi o dispositivi di archiviazione esterna eventualmente danneggiati.
   - Nella fase di recupero invece si cerca appunto di recuperare dati e informazioni perse, si applicano patch per correggere eventuali sistemi obsoleti, si rivedono le politiche di firewall e sistemi di monitoraggio, con lo scopo di evitare che lo stesso incidente si verifichi di nuovo in futuro.

**ESERCITAZIONE FINE MODULO 5**
**BARRECA MONICA**

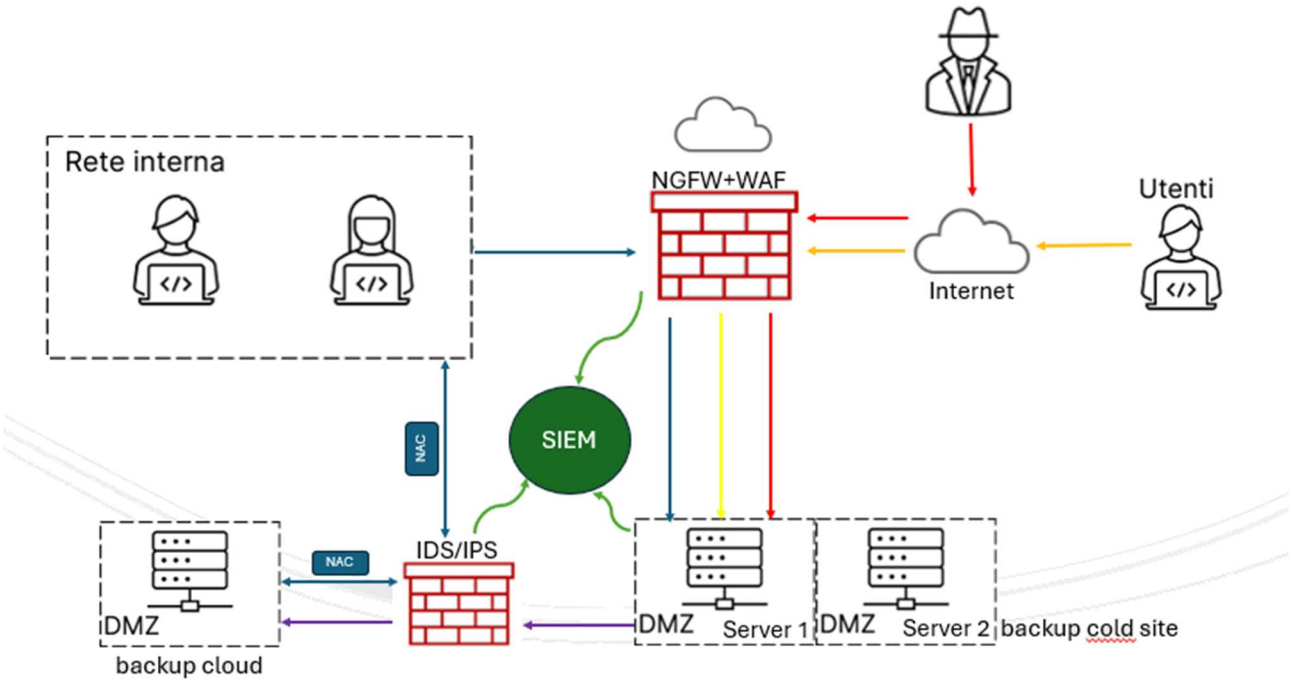



**4: Soluzione completa**



**ESERCITAZIONE FINE MODULO 5**
**BARRECA MONICA**

## 5: Modifica “più aggressiva” dell’infrastruttura




Budget permettendo, si potrebbe implementare l’infrastruttura con ulteriori modifiche più “aggressive”:

1. Utilizzo di un next generation firewall combinato con un web application firewall così da non limitarci al solo controllo dei pacchetti attraverso le regole policy, ma essere in grado anche di mantenere le informazioni sullo stato delle connessioni, avere un’analisi approfondita dei flussi e avere anche la protezione per eventuali attacchi SQL Injection e XSS.
2. Avere un secondo server di backup come failover cluster con metodologia cold site, così che, se per qualsiasi motivo il server principale smette di funzionare, il secondo seppur non completamente aggiornato è in grado di prendere il suo posto, mantenendo attivi servizi.
3. Optare per un eventuale terzo server di backup in cloud con metodologia DRaaS, da sincronizzare una volta al mese col server principale, che scambi informazioni solo con la rete interna passando attraverso un ulteriore firewall con controlli NAC e monitoraggio IDS/IPS.
4. Mantenere attivo per tutta l’infrastruttura il monitoraggio dei log (di sicurezza, di sistema, applicativi, firewall e proxy) con invio dei dati al SIEM (Security Information Event Management)
5. Infine eseguire Vulnerability Assessment e Penetrion Testing periodici per verificare che l’infrastruttura non sia violata, così come verificare periodicamente che i sistemi siano aggiornati.