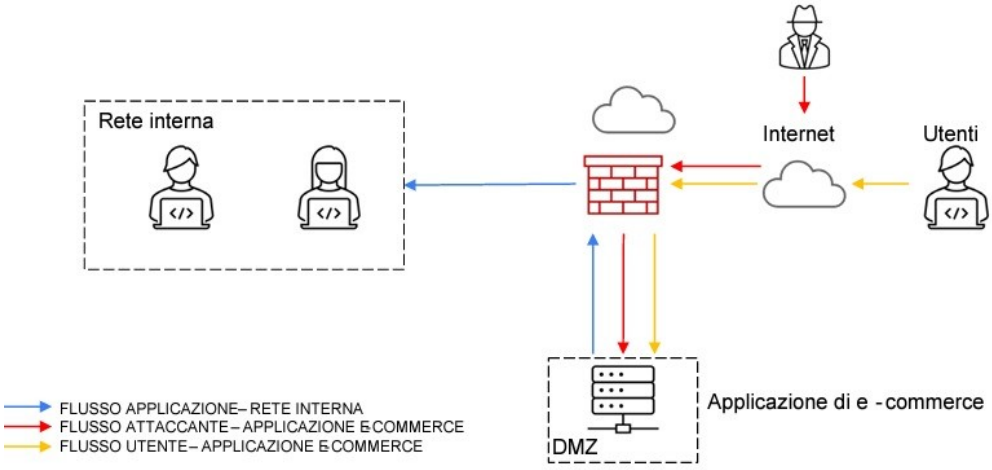
Progetto settimana 9 Daniele D'Esposito

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.



Con riferimento alla figura , 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

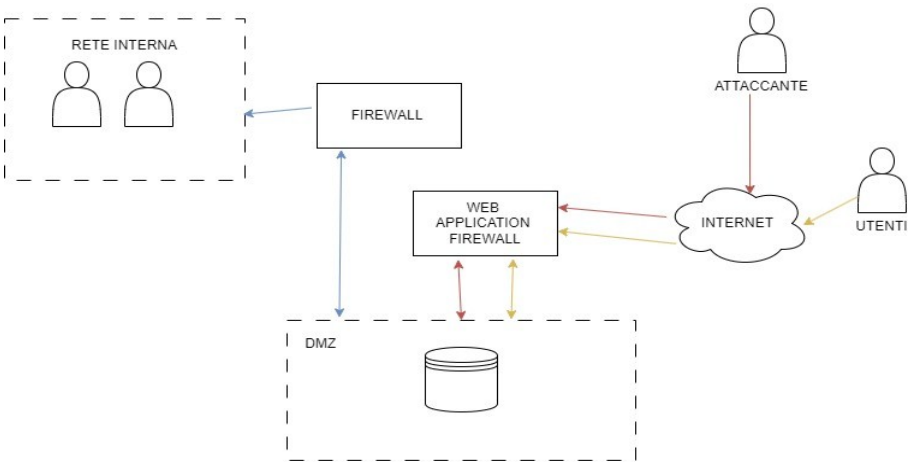
3. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura con la soluzione proposta.

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)

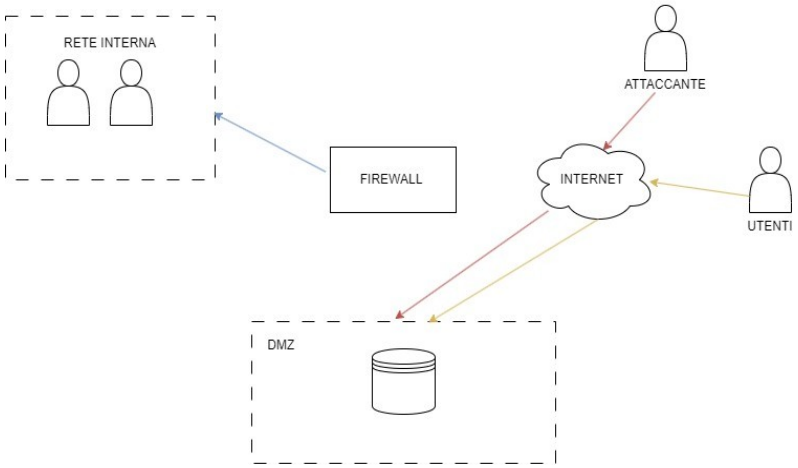
1 AZIONI PREVENTIVE

Attacchi ad applicazioni web di tipo SQLi o XSS vengono prevenuti a livello di programmazione, inserendo filtri agli eventuali input permessi all'utente in modo tale che si possa controllare il tipo di dati che vengono inseriti. Un'ulteriore prevenzione puo' essere quella di aggiungere un **WAF**(web application firewall) che si occupa specificatamente di controllare il traffico rivolto alle applicazioni web.

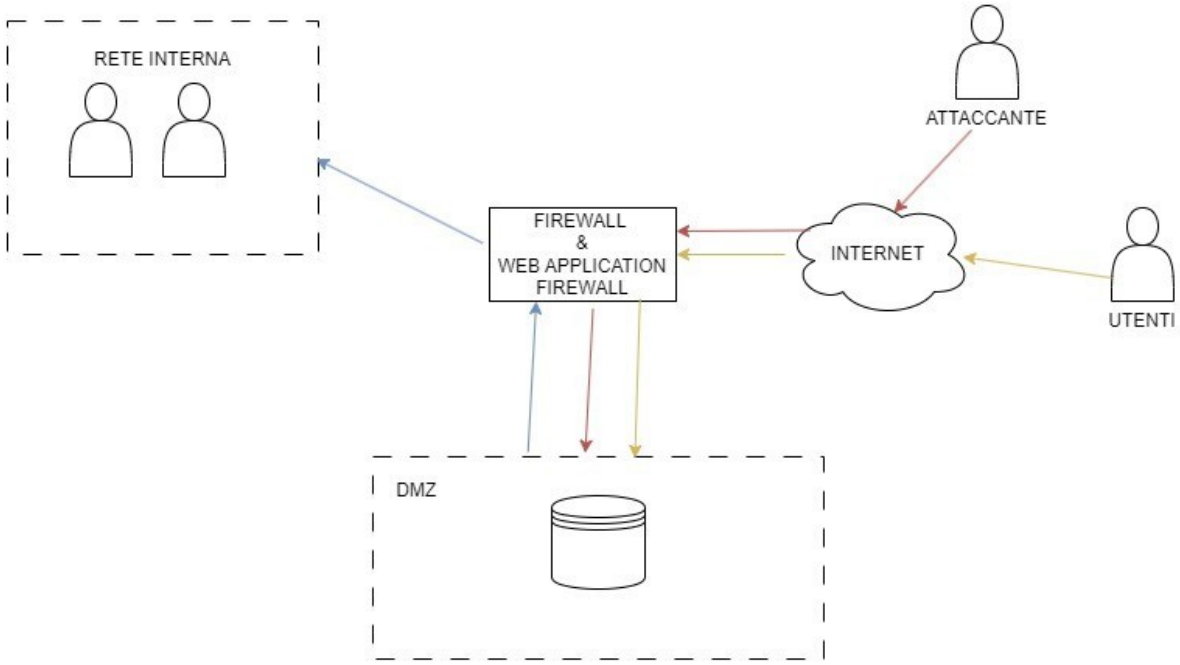


2 IMPATTI SUL BUSINESS
Se un attacco ddos non rende il servizio disponibile per 10 minuti e la media di guadagno per minuto e' di 1500€ allora la perdita dell'azienda ammonta a 15000€.
Un'azione preventiva puo' essere quella di creare un cluster di server che permetta il **failover**, lo switch automatico ad un sistema secondario funzionante in caso di interruzione del sistema primario; questi server sono sincronizzati tra loro e svolgono lo stesso ruolo.

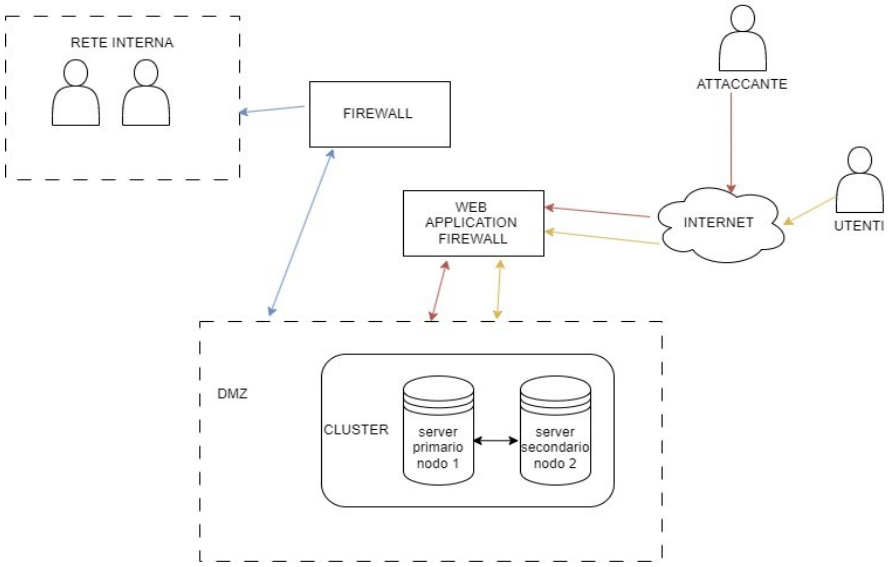
3 RESPONSE
La tecnica necessaria ad evitare che il server infetto possa comunicare con la rete interna ma lasciandogli la connessione a internet si chiama **isolamento**.



4 SOLUZIONE COMPLETA



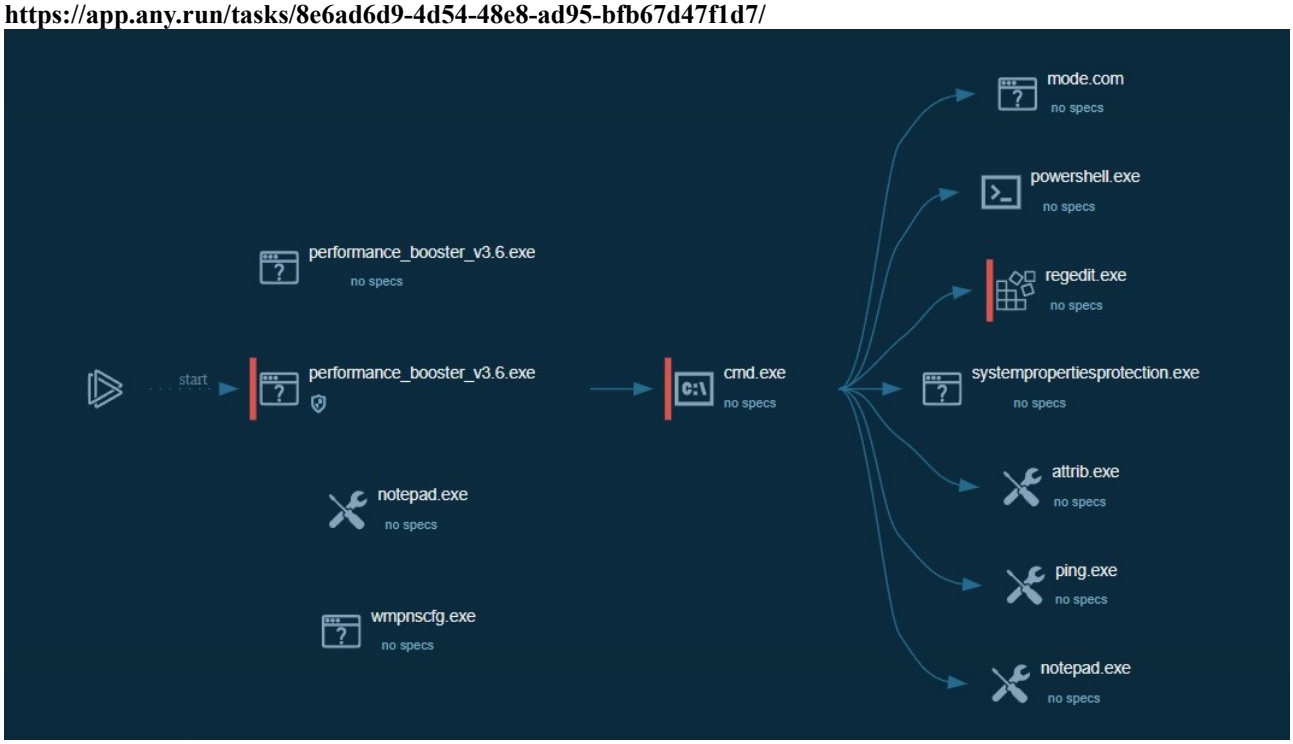
5 MODIFICA PIU' AGGRESSIVA DELL'INFRASTRUTTURA



Si aggiunger un cluster costituito da almeno 2 server che lavorano in sincrono per permettere il failover in caso di attacco del primario

Bonus: **Analizzare le seguenti segnalazioni caricate su anyrune fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:**

https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/



Questa segnalazione riguarda un file eseguibile di nome PERFORMANCE_BOOSTER_v3.6.exe; eseguendolo, viene aperta una sessione sul cmd tramite un file .bat e allo stesso tempo una powershell a cui vengono modificati i permessi di scrittura per eseguire anche degli script(unrestricted) che cerca nell'editor del registro informazioni: impostazioni internet, software installati, percorsi di installazione di outlook, se il .NET e' installato e la cronologia delle recenti connessioni da remoto (RDP remote desktop protocol).
In soldoni, facendo partire il programma si avvia una finestra di command con una lista di azioni da eseguire da parte dell'utente al fine di aumentare le performance della macchina ma nel frattempo gli vengono presumibilmente sottratte informazioni della macchina dal registro di sistema.
Potrebbe essere un trojan di information gahering.

https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

questa segnalazione invece riguarda l'aggiornamento di microsoft edge tramite una pagina internet di microsoft; ovviamente i privilegi di questo aggiornamento potrebbero destare allarme ma, visto che e' microsoft stessa l'artefice, non c'e' da preoccuparsi. Il link della pagina web non sembra manomesso e gli eseguibili sembrano legittimi.