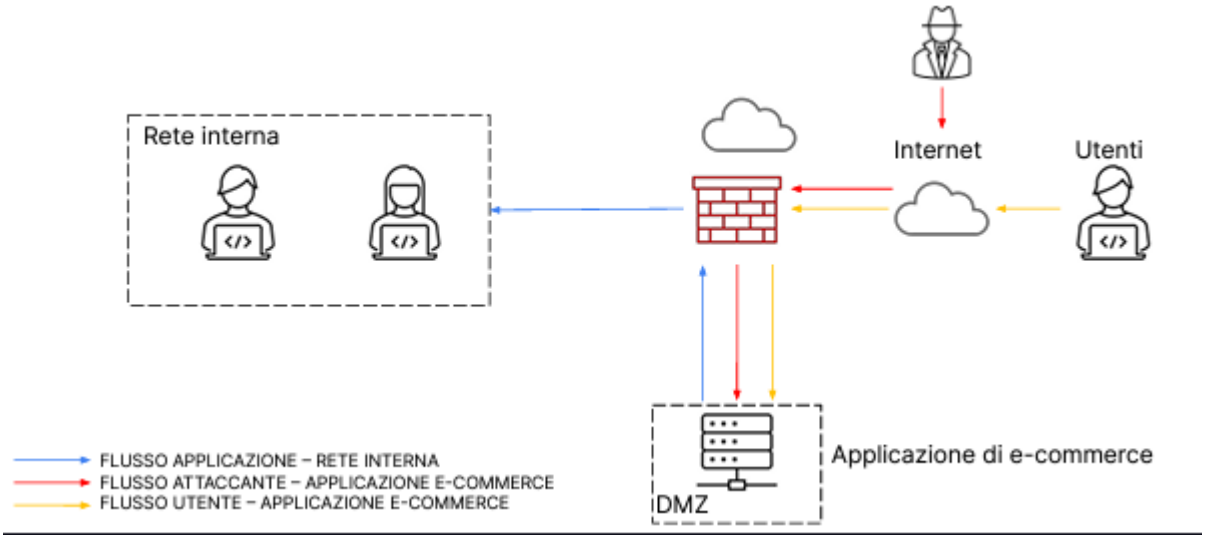
Test Modulo 5



1. Azioni Preventive

Fondamentali per la gestione e prevenzione delle minacce alla sicurezza informatica

sono le best practice tra cui troviamo:

-Penetration Test

-Threat Analysis

Oltre ad utilizzare queste ultime toccherà fare delle ulteriori implementazioni per rendere la rete

ancora più sicura.

Tra queste troviamo:

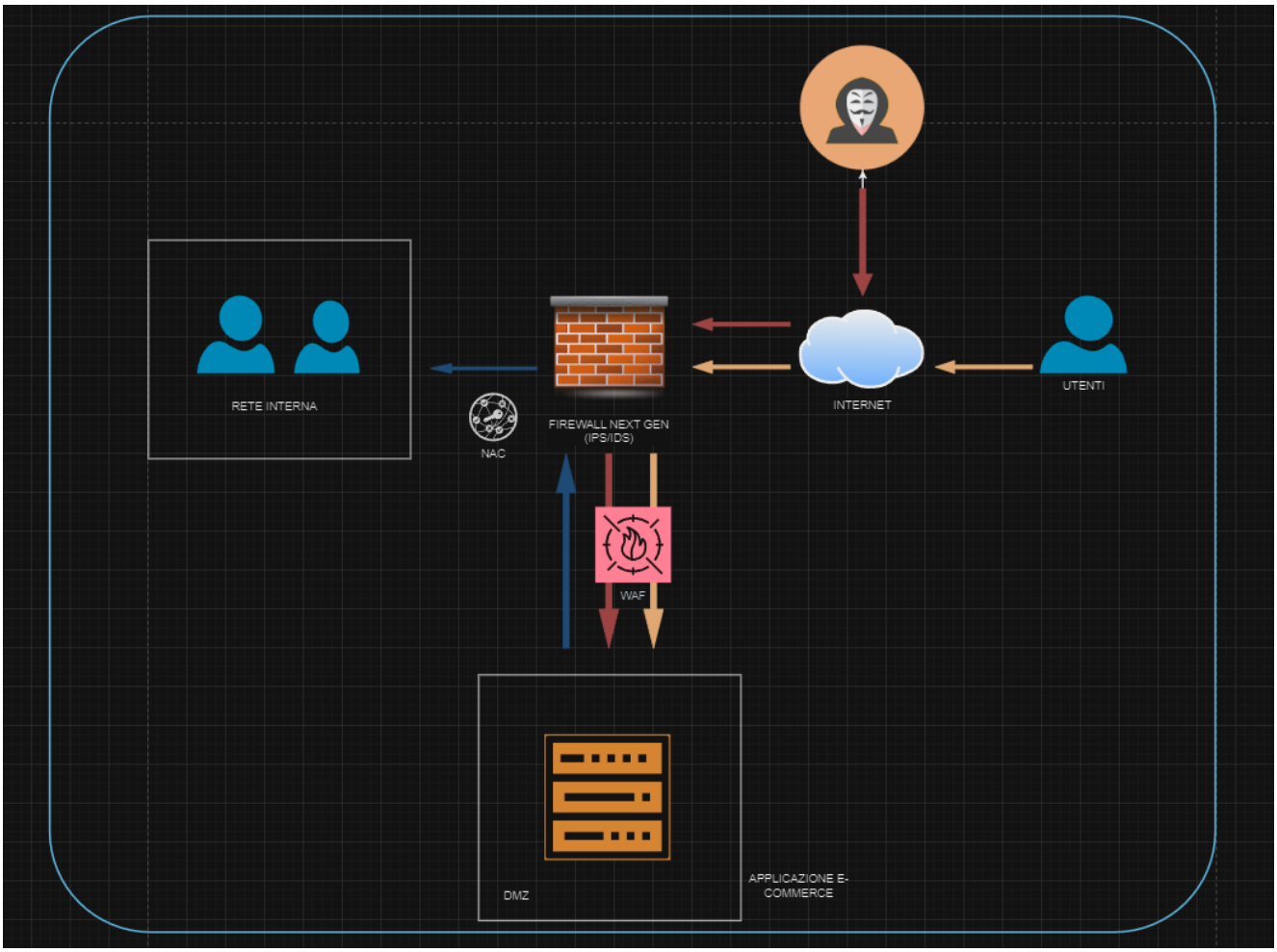
-Implementazione di query per interagire con il db e prevenire delle SQL injection.

-Validazione di dati in entrata per rifiutare qualsiasi input che contiene markup o script non consentiti per prevenire XSS

-Utilizzo di un WAF (Web App Firewall) per filtrare e monitorare il traffico HTTP/HTTPS in ingresso; codificazione dell'output per prevenzione script non autorizzati per gli utenti

-Cambio in un Firewall Next Gen contenente di base IPS/IDS

-Utilizzo di un NAC per limitare l'accesso alla rete e per assicurare che solo dispositivi autorizzati e conformi alle politiche di sicurezza possano connettersi e accedere alle risorse di rete.



2.Impatti sul business

Nel caso di un attacco di tipo DDoS dall'esterno

che non rende l'applicazione raggiungibile per 10 min, considerando che in media ogni min gli utenti spendono 1500€, si

avrà una perdita di 15.000€.

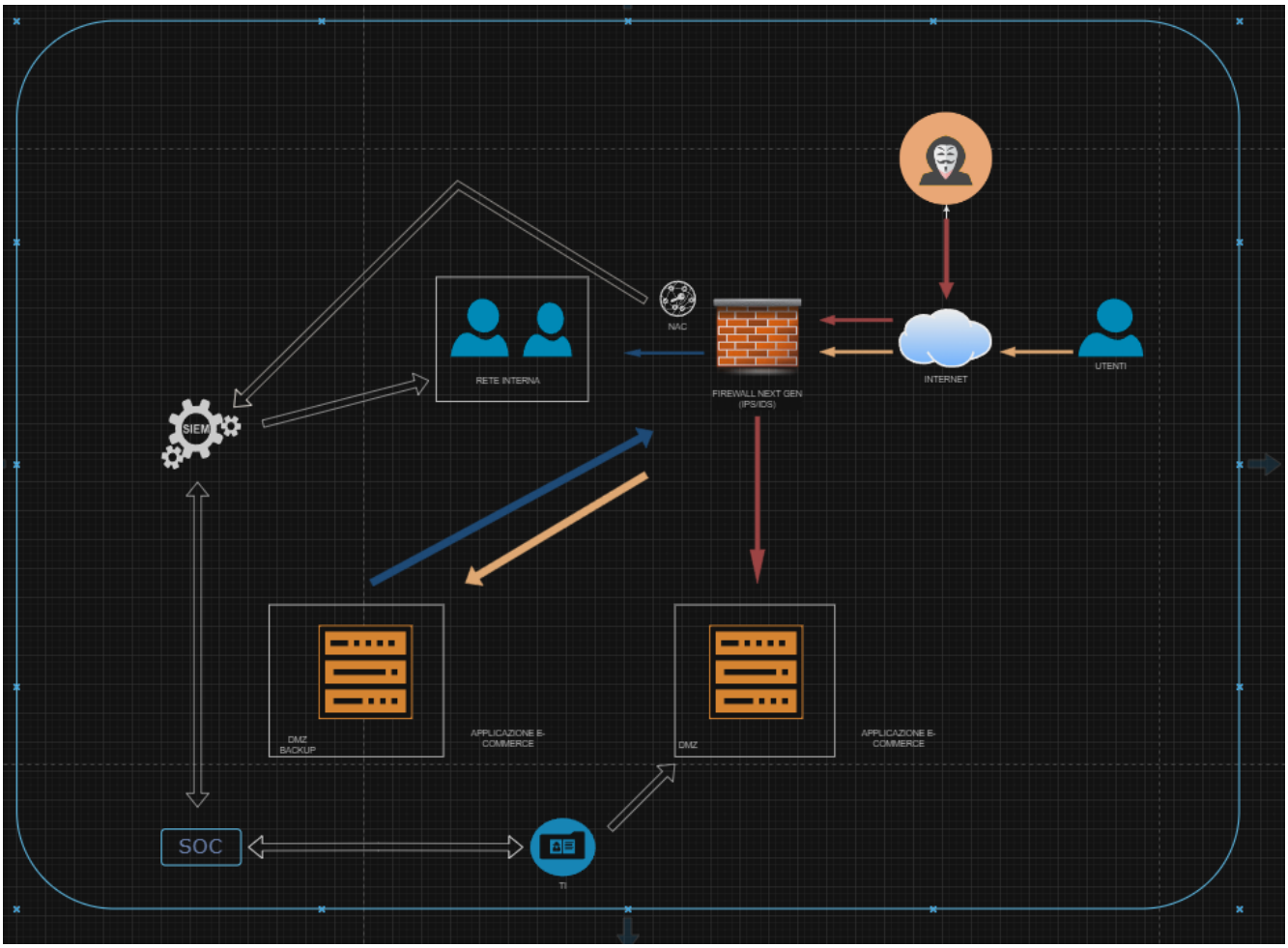
Delle implementazioni da fare per poter prevenire questi tipi di attacchi potrebbero essere:

-Servizio di mitigazione attacchi DDoS per ridurre il tempo di inattività dovuto ad attacchi DDoS,eventualmente utilizzare sistemi failover per reindirizzare il traffico verso un server alternativo per mantenere il servizio On

-Utilizzo di piattaforme Cloud con mitigazione DDoS integrato.

In base alla frequenza che si può avere di attacchi di questo tipo possiamo decidere se può valerne la pena, in termini economici, fare o meno delle implementazioni.

3.Response



Nel caso invece di attacco malware dall'esterno, la prima cosa è isolare il server DMZ e spostarsi su un server backup ed analizzare il comportamento dell'attaccante , per poi poter implementare ulteriori misure correttive al fine di prevenire futuri attacchi.

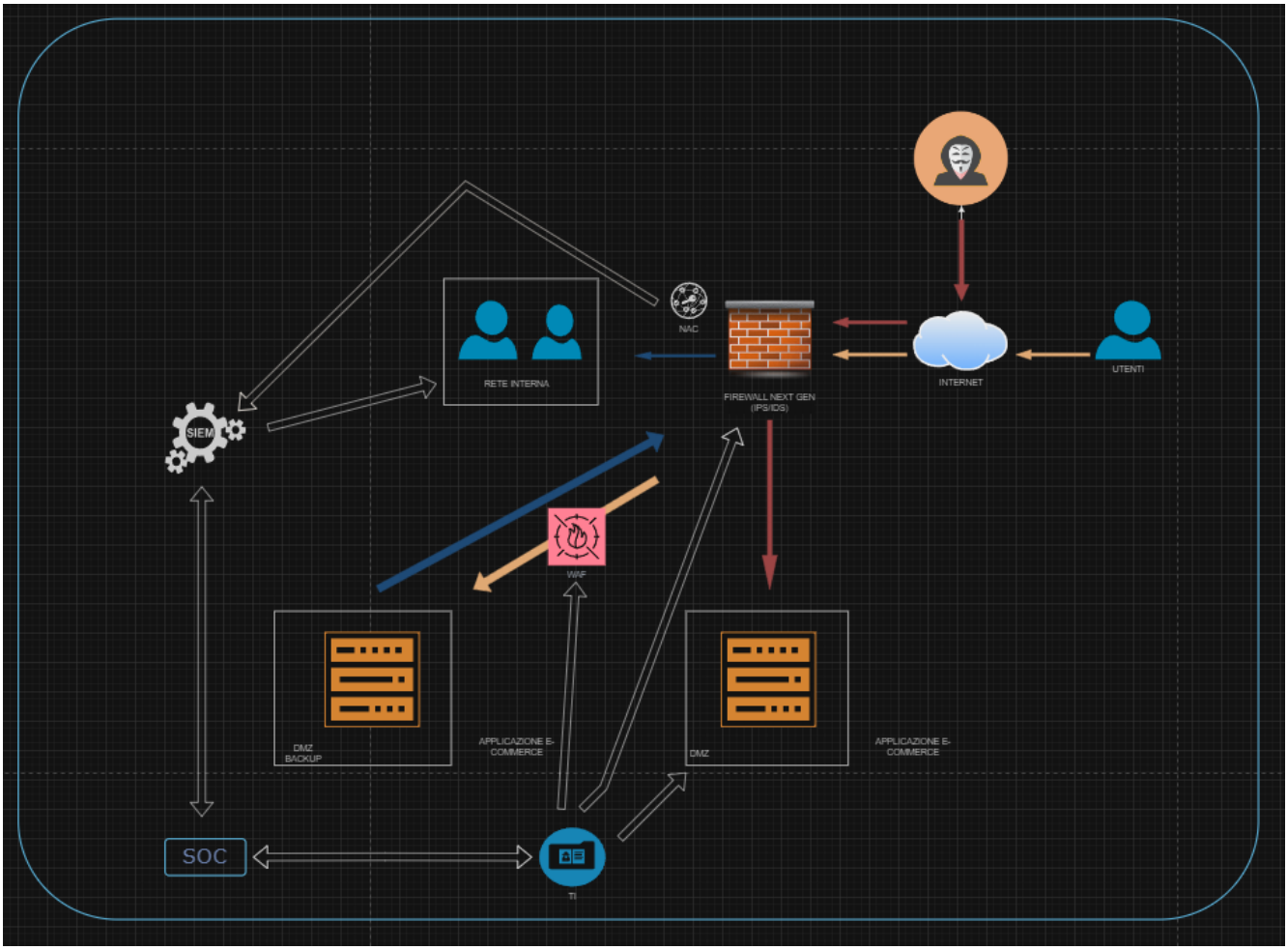
Per fare ciò utilizzeremo:

-Unità di Threat Intelligence

-Soc Security Operation Center

-SIEM Security Information and Event Management

4. Soluzione complete (unione punto 1 e 3)



5. Modifiche più aggressive infrastrutturali

Al fine di avere il massimo della sicurezza informatica verranno inseriti nell'infrastruttura aziendale:

-Unità di Threat Intelligence che avrà il compito di monitorare costantemente fonti di informazioni esterne ed interne, analizzare i dati raccolti per identificare indicatori di intromissione (IOC);

produrre report su minacce informatiche con tattiche e procedure da utilizzare sulle vulnerabilità; distribuzione delle informazioni agli stakeholder interni.

-Soc Security Operation Center per monitoraggio, analisi e risposta degli eventi di sicurezza informatica

-SIEM Security Information and Event Management, piattaforma per la raccolta,analizzare e correlare dati provenienti dall'interno dell'azienda

-Utilizzo di un Firewall di next generation con all'interno implementate delle difese da XSS,SQL inj e anti DDoS

-NAC per il controllo degli accessi di rete

- Utilizzo di Failover cluster in caso di attacco DDoS o interruzione del servizio sul server