1. Azioni preventive per SQLi e XSS

Per proteggere l'applicazione web da attacchi di **SQL Injection (SQLi)** e **Cross-Site Scripting (XSS)**, è possibile implementare le seguenti misure preventive:

- **Prevenzione contro SQLi**:
    - **Query parametrizzate (Prepared Statements)**: Utilizzare query SQL parametrizzate per evitare che l'input dell'utente interagisca direttamente con i comandi SQL. Questo impedisce l'esecuzione di codice SQL malevolo.
    - **Validazione degli input**: Implementare una rigorosa validazione degli input per rifiutare qualsiasi sintassi sospetta che potrebbe essere usata per un attacco SQLi.
    - **ORM (Object-Relational Mapping)**: Usare ORM per astrarre le interazioni col database, minimizzando l'esposizione a SQL grezzo.
- **Prevenzione contro XSS**:
    - **Sanitizzazione dell'input**: Pulire gli input dell'utente rimuovendo o codificando i caratteri HTML speciali che possono essere utilizzati per inserire codice JavaScript non sicuro.
    - **Content Security Policy (CSP)**: Implementare una politica di sicurezza dei contenuti che impedisca l'esecuzione di script non autorizzati.
    - **Sanitizzazione dell'output**: Quando i dati inseriti dall'utente vengono visualizzati sul sito web, devono essere correttamente trattati per rimuovere o codificare i caratteri speciali, al fine di prevenire l'esecuzione di codice dannoso (XSS).

Modifica dell'architettura:

- Aggiungere firewall applicativi (Web Application Firewall, WAF) per monitorare e filtrare il traffico HTTP sospetto.
- Implementare servizi di logging e monitoring in tempo reale per rilevare attacchi in corso in cloud.

  Vantaggi in cloud:

- **Ridondanza e scalabilità**: I sistemi esterni offrono ridondanza e scalabilità. Non devi preoccuparti di gestire direttamente i server di logging.
- **Accesso da remoto**: I team di sicurezza possono accedere ai log e ai dati da qualsiasi parte del mondo senza dover accedere alla rete interna.

2. Impatti sul business: Attacco DDoS

Se l'applicazione subisce un attacco **DDoS** e diventa irraggiungibile per 10 minuti, l'impatto finanziario sarebbe:

- **Calcolo dell'impatto**:
    - Perdita per minuto = 1.500 €
    - Durata del downtime = 10 minuti
    - Impatto totale: 1.500 € x 10 = **15.000 € di perdita totale**

Azioni preventive:

- Implementare un **WAF (Web Application Firewall)** con capacità di mitigazione DDoS.
- Utilizzare un **servizio di distribuzione del traffico (CDN)** per gestire il carico e bloccare tentativi di sovraccarico.

3. Response: Malware sull'applicazione Web

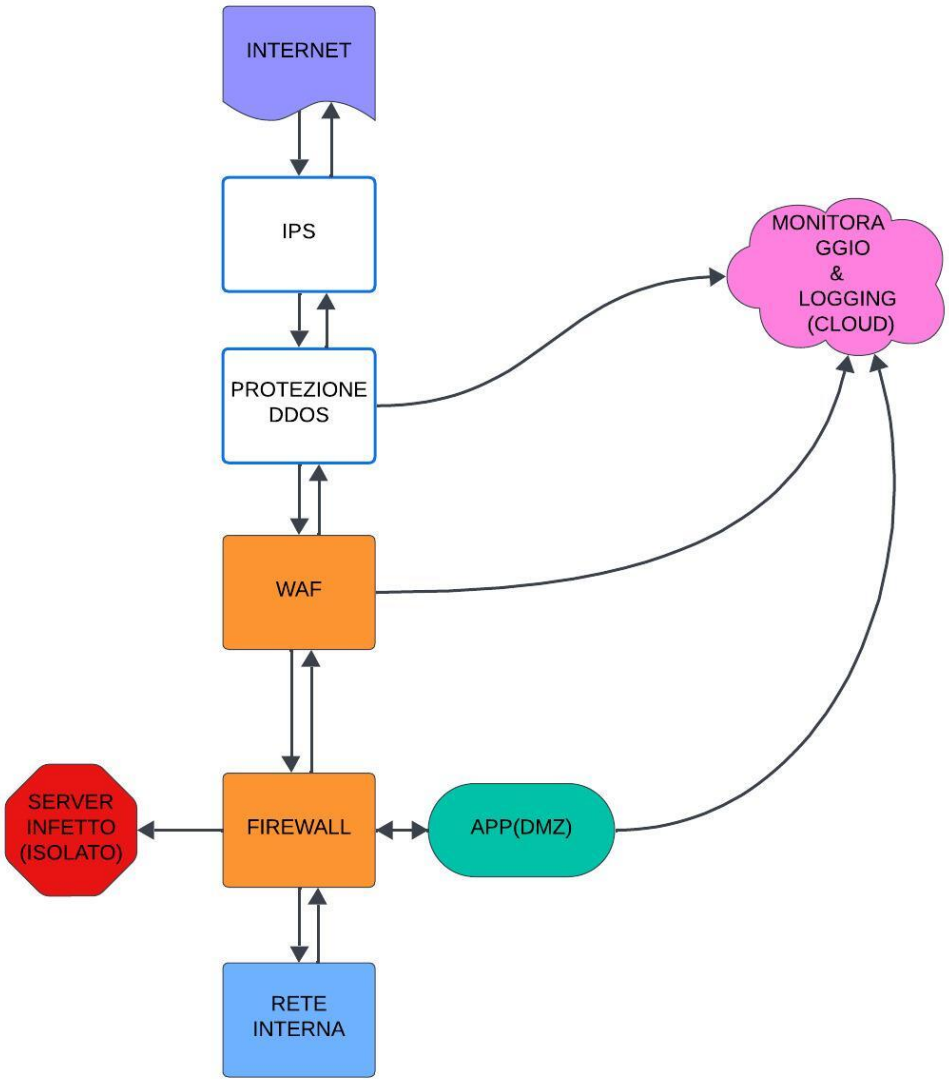
Se l'applicazione viene infettata da un malware e la priorità è evitare la propagazione, senza però rimuovere l'accesso dell'attaccante, le azioni consigliate sono:

- **Isolamento del server infetto**: Configurare le regole del firewall per isolare il server compromesso dal resto della rete interna.
- **Segmentazione della rete**: Utilizzare VLAN o firewall interni per separare le reti e limitare la propagazione del malware.
- **Monitoraggio continuo**: Continuare a monitorare l'attività dell'attaccante per capire meglio le sue intenzioni e tattiche.
- Configurare un **Intrusion Prevention System (IPS)** per rilevare e fermare comportamenti anomali.

4. Soluzione completa

Unire le soluzioni preventive per SQLi e XSS con quelle per la risposta al malware, modificando l'infrastruttura:

- Firewall applicativi, protezioni DDoS, regole di firewall per l'isolamento, monitoraggio in tempo reale e IPS.



5. Modifica aggressiva dell'infrastruttura

Architettura più "aggressiva" per migliorare la sicurezza:

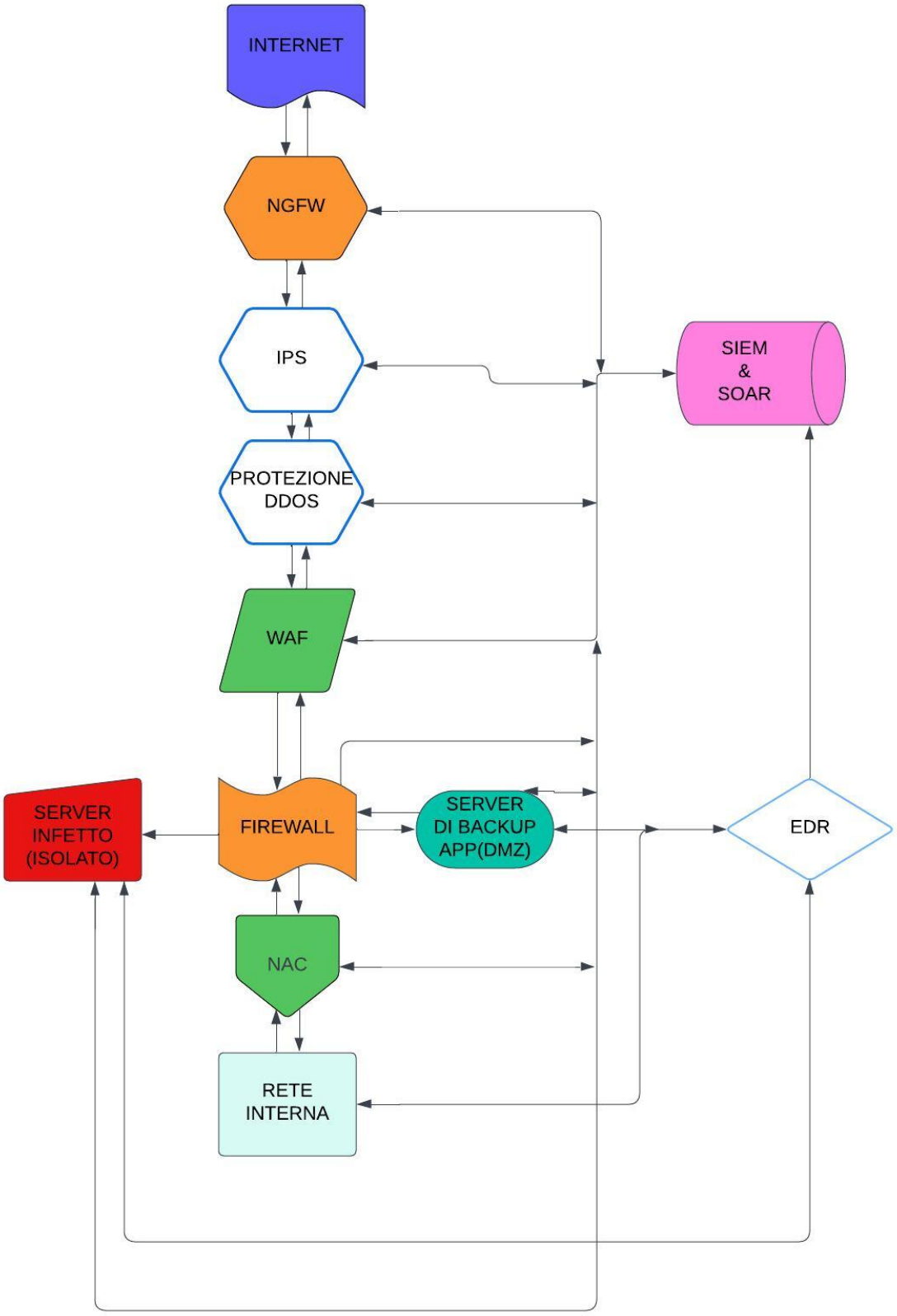
- **Intrusion Prevention System (IPS)**: Aggiungere un sistema di prevenzione delle intrusioni.
- **Disaster Recovery Plan**: Integrare procedure di disaster recovery per rispondere a downtime prolungati.
- **Backup e Ripristino**: Implementare backup regolari e testare i processi di ripristino in caso di attacco o infezione.
- **Server di backup:** implementare un server di backup di emergenza.

- **NAC:** Network Access Control è una soluzione che controlla l'accesso alla rete aziendale in base a regole di sicurezza predefinite. Il NAC verifica l'identità e la conformità dei dispositivi (come computer, smartphone, tablet) che tentano di connettersi alla rete, permettendo l'accesso solo a quelli **autorizzati** e **conformi** alle policy di sicurezza. Se un dispositivo non soddisfa i requisiti (ad esempio, mancanza di patch di sicurezza o antivirus non aggiornato), il NAC può **limitare l'accesso** o **isolarlo** in una rete di quarantena fino a quando non viene reso sicuro.
- **NGFW**: I firewall di nuova generazione (NGFW) possono fare una deep packet inspection (DPI), analizzando il contenuto dei pacchetti a livello di dati (payload), non solo l'intestazione. **Rilevamento di malware o exploit,** questo permette di identificare e bloccare traffico che contiene **malware**, **virus**, **tentativi di exploit**, o altre minacce anche se mascherate in traffico legittimo. **Ispezione di traffico web,** Rileva e blocca contenuti web potenzialmente pericolosi o proibiti.
- **SIEM & SOAR: SIEM (Security Information and Event Management)**: Sistema che raccoglie, analizza e correla **log e eventi** di sicurezza provenienti da diverse fonti della rete (come firewall, EDR, IPS, ecc.), offrendo una **visione centralizzata** degli incidenti di sicurezza. Il SIEM aiuta a **identificare anomalie** e **rilevare minacce**, fornendo report e alert su attività sospette.

  SOAR (Security Orchestration, Automation, and Response): Strumento che automatizza le **risposte agli incidenti** di sicurezza basate sui dati raccolti dal SIEM. Il SOAR **orchestra** azioni automatiche o semi-automatiche per mitigare le minacce, come isolare un dispositivo compromesso, bloccare IP sospetti o avviare la riparazione di un sistema vulnerabile.
- **EDR :** L'EDR è una soluzione focalizzata sul monitoraggio, rilevamento e risposta alle minacce sugli **endpoint** (come laptop, server e dispositivi mobili). Rileva attività sospette come **malware**, **ransomware** o comportamenti anomali, e può rispondere **autonomamente** isolando l'endpoint o bloccando processi malevoli. Gli EDR forniscono dati dettagliati al **SIEM** per la correlazione degli eventi di sicurezza e per migliorare la protezione della rete.

  Architettura aggiornata aggressiva:

- **NGFW**
- **IPS**
- **Protezione DDoS tra Internet e l'applicazione.**
- **Firewall applicativi (WAF) tra l'utente e l'applicazione.**
- **Firewall**
- **Server di backup online**
- **Server compromesso isolato da firewall**
- **NAC**
- **SIEM & SOAR**
- **EDR**


INTERNET
NGFW
IPS
PROTEZIONE DDOS
WAF
FIREWALL
NAC
RETE INTERNA
SERVER INFETTO (ISOLATO)
SERVER DI BACKUP APP(DMZ)
SIEM & SOAR
EDR