PROGETTO

Security Operation
M5W20-D4

31 / 01 / 2025

Cybersecurity Analyst

Security Operation
Matteo Madonia

SOMMARIO

1. Traccia progetto

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1.1 **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

1.2 **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

1.3 **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.

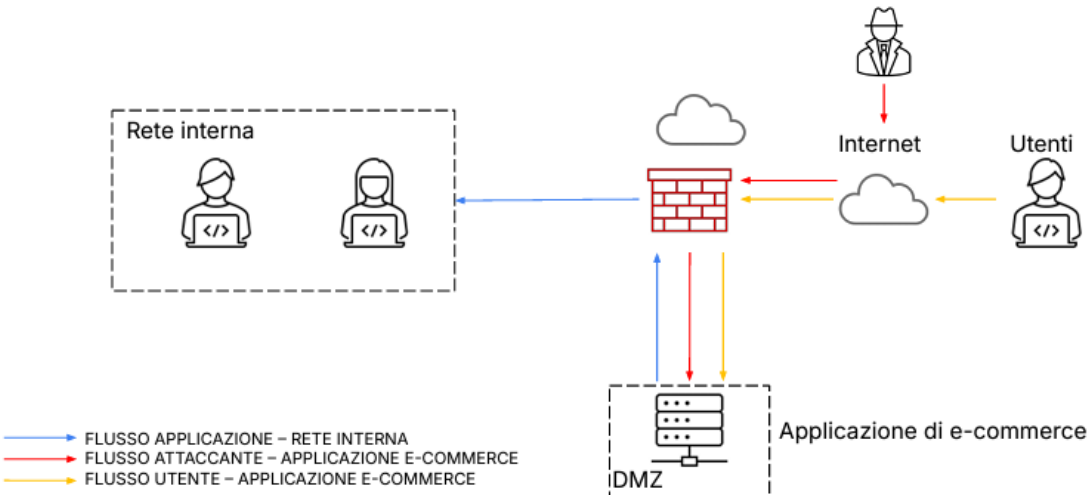
1.4 **Soluzione completa:** unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

1.5 **Modifica "più aggressiva"** dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

2. Analisi dell'architettura di rete proposta

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.



2.1 Struttura:

- Rete interna (LAN) composta da due utenti
- Firewall
- DMZ (Demilitarized Zone)
- Internet
- Utenti esterni connessi ad internet
- Attaccante

2.2 Definizione di DMZ:

La **DMZ (Demilitarized Zone)** è una sottorete isolata, separata da tutte le altre reti che funge da zona intermedia tra una rete privata (LAN) e una rete esterna (solitamente Internet). Il suo scopo principale è migliorare la sicurezza ospitando servizi pubblicamente accessibili, come server web, così come nel nostro caso per questo progetto

3. Svolgimento del progetto

3.1 Quesito 1

3.1.1 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?

3.1.2 Definizione attacco SQL Injection

L'**SQL Injection (SQLi)** è un attacco informatico che sfrutta vulnerabilità nelle applicazioni web per manipolare le query SQL inviate al database. Questo permette a un attaccante di **accedere, modificare o eliminare dati sensibili** e, in alcuni casi, ottenere il pieno controllo del sistema.

3.1.3 Definizione attacco XSS e tipologie

L'**XSS (Cross-Site Scripting)** è un attacco informatico che consente a un attaccante di iniettare codice JavaScript malevolo in una pagina web visualizzata da altri utenti. Questo può portare a:

- **Furto di sessioni e credenziali**
- **Reindirizzamenti a siti malevoli**
- **Esecuzione di azioni dannose con i privilegi dell'utente**

Esistono 3 tipologie di attacchi XSS:

- XSS Reflected (non persistente)
- XSS Persistent (è il più pericoloso in quanto "persiste" nella piattaforma web)
- XSS DOM-Based

3.1.4 Azioni preventive per la difesa della web-app

- Una prima soluzione è l'implementazione di un **Web Application Firewall (WAF)** tra l'applicazione web di e-commerce e il firewall aziendale, incrementando la sicurezza del perimetro;
- **Filtraggio di dati in ingresso** al fine di prevenire l'immissione di eventuale codice malevolo da parte di un'attaccante;
- **Implementazione delle CSP**, Content Security Policy, ovvero della policy specifiche che limitano l'esecuzione di script malevoli da parte dell'attaccante
- **Sanitizzazione e validazione dell'input**, accettando in ingresso solo caratteri specifici e complessi (questa azione preventiva riguarda soprattutto gli attacchi di tipo SQL Injection); accettazione di sole query sicure; implementazione di **sistemi NAC**
- Per quanto riguarda la prevenzione dagli attacchi XSS, è importante accertarsi della **corretta validità di scrittura della web-app**;
- **Implementazione dei SameSite Cookies e HttpOnly**
- **Implementazione della crittografia,** con l'utilizzo del protocollo di trasmissione dati HTTPS
- Implementazione di un **SOC**, Security Operation Center, potrebbe sicuramente essere utile per il controllo di tutta l'infrastruttura della rete, per filtrare tutte le informazioni in entrata e uscita, elaborandole, per rilevare, prevenire e rispondere rapidamente agli incidenti di sicurezza informatica. In caso di possibile attacco come in figura, da parte di un attaccante, sarà possibile intervenire tempestivamente e venire allertati del pericolo.

Ricordiamo di seguito gli obiettivi di un SOC:
- Rilevare e rispondere agli incidenti di sicurezza;
- Monitorare continuamente le infrastrutture IT;
- Prevenire gli attacchi informatici;
- Migliorare la postura di sicurezza dell'organizzazione.

- I possibili altri strumenti di cui un SOC potrà avvalersi per un possibile attacco esterno:
  - **SIEM** (Security Information and Event Management)
  - **IDS/IPS** (Intrusion Detection/Prevention Systems)
  - **SOAR** (Security Orchestration, Automation and Response)

3.1.5 Definizione di SIEM

SIEM (Security Information and Event Management) è uno strumento di monitoraggio continuo, che analizza i registri raccolti per evidenziare eventi o comportamenti di interesse. L'obiettivo è la raccolta centralizzata dei log e degli eventi generati da applicazioni e sistemi in rete per permettere agli analisti della sicurezza di agire in maniera tempestiva di fronte ad allarmi e incidenti di sicurezza.

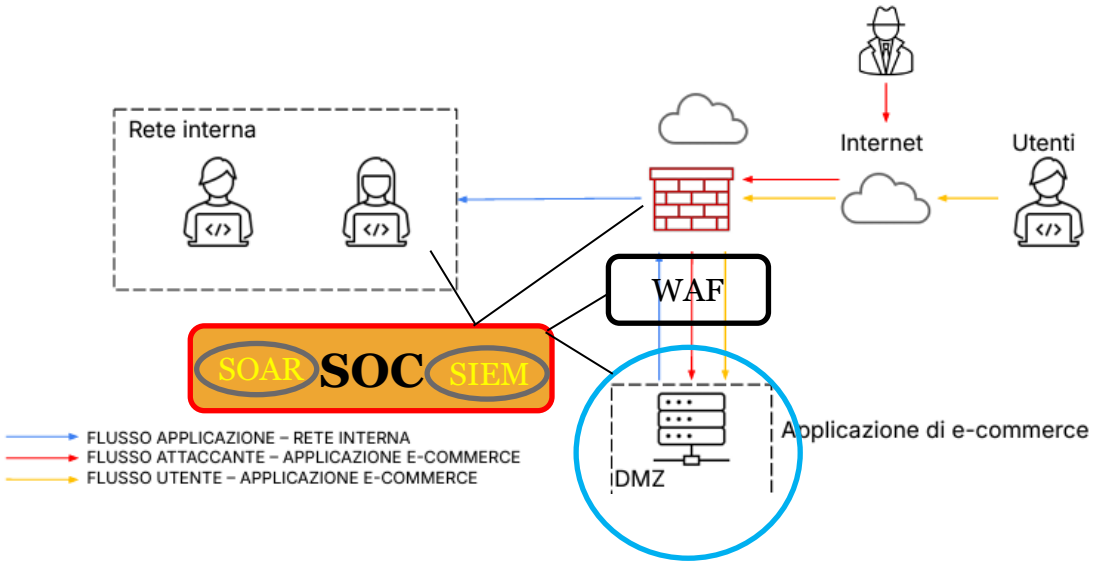
3.1.6 Definizione di SOAR

Il **SOAR** (Security Orchestration, Automation and Response) racchiude tutte le applicazioni software o i tool necessari ad un'azienda per raccogliere ed analizzare i dati correlati alla sicurezza informatica.

3.1.7 Soluzione grafica: Si ripropone di seguito l'immagine modificata come richiesto

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.



All'interno del cerchio azzurro, possiamo racchiudere tutte le soluzioni d'implementazione sopra proposte, quindi filtraggio di dati in ingresso, implementazione delle CSP, sanitizzazione e validazione

dell'input, corretto codice di scrittura della web-app e Implementazione dei SameSite Cookies e HttpOnly.

All'interno del **riquadro nero** troviamo il WAF, ovvero il Web Application Firewall, una tipologia professionale e fondamentale di Firewall necessario per tutte le web-app che risiedono su web-server.

All'interno del **riquadro rosso**, il SOC, con il SIEM e SOAR, strumenti utilizzati dal SOC per operare efficacemente

3.2 Quesito 2

3.2.1 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

Si riporta di seguito il calcolo eseguito:

BI (Business Impact) = spesa media utenti x tempo disservizio
BI (Business Impact) = € 1.500,00 x 10 minuti = € 15.000,00

3.2.2 Definizione di DDos
L'attacco Distributed Denial Of Service (DDoS), è un attacco pericoloso e altamente dannoso, in quanto arreca all'intero sistema disservizi, rallentamenti o addirittura l'impossibilità di utilizzare qualsiasi componente software e/o Hardware collegato al sistema e all'infrastruttura di rete. Rende un servizio, un server o una rete indisponibile per gli utenti legittimi, sovraccaricandolo con un'enorme quantità di traffico dannoso proveniente da più fonti distribuite. E' necessaria una rete di pc infetti (botnet), controllati da un unico dispositivo lato Hacker/Attaccante.

3.2.3 Come funziona un attacco DDoS?
Questi dispositivi infetti vengono usati per inviare un numero eccessivo di richieste a un server o a una rete target. Il sistema bersaglio si sovraccarica, rallenta o smette di funzionare, impedendo l'accesso agli utenti legittimi.

3.2.4 Mitigazioni attacco DDoS
Eventuali valutazioni per mitigare questa problematica, sicuramente possono essere correlate a quanto specificato nel quesito 1, quindi un'ottima prevenzione, si dell'infrastruttura di rete ma soprattutto rivolta ad implementare tutte quelle soluzioni atte ad una maggiore protezione della web-application e al server sul quale risiede. Per esempio:

- **Implementare un CDN (Content Delivery Network)**: Distribuisce il traffico tra più server, riducendo il rischio di sovraccarico;
- **Configurare limiti di banda e rate limiting**: Limita il numero di richieste da un singolo IP in un certo periodo di tempo.
- **Monitorare il traffico di rete**: Strumenti come Wireshark, Snort o IDS/IPS possono rilevare anomalie nel traffico.
- **Utilizzo di Firewall e filtri IP**
- **Implementazione di un WAF (Web Application Firewall)**

In questo caso, essendo l'attacco in corso, un'importante valutazione preventiva atta a mitigare questa problematica è inoltre l'esistenza di un **BCP** (**Business Continuity Plan**) di cui ogni azienda deve essere necessariamente provvista, può aiutarci a mitigare il temporaneo disservizio, garantendo, anche se in parte la continuità del business della compagnia; un **DRP** (Disaster Recovery Plan) è necessario per il ripristino, nel minor tempo possibile, del sistema;
nota bene: il tempo previsto per DRP deve essere sempre </= BCP

Predisposizione di aree definite **cold site**, **hot site** e **warm site**, che in caso di attacco esterno, permettono ad una compagnia la continuazione del business, però con metodologie differenti.
Una cold site è un ambiente di lavoro identico a quello in utilizzo dalla compagnia ma momentaneamente "spento", pronto ad essere attivato al momento della necessità (costo relativamente basso ma inefficiente dal punto di vista del pronto intervento, perché l'attivazione richiede parecchio tempo);
una hot site è un ambiente di lavoro identico a quello in utilizzo dalla compagnia, ma sempre attivo, costantemente aggiornato e pronto all'utilizzo (maggiori costi che impattano sulla compagnia ma efficienza massima che permette la continuità delle attività senza disservizi). Le worm site sono una via di mezzo tra le due sopra citate.

3.3 Quesito 3

3.3.1 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 in slide 2 con la soluzione proposta.

3.3.2 Definizione di Malware
Il **malware** (*malicious software*) è un software progettato per infiltrarsi, danneggiare o compromettere dispositivi, reti o dati senza il consenso dell'utente.

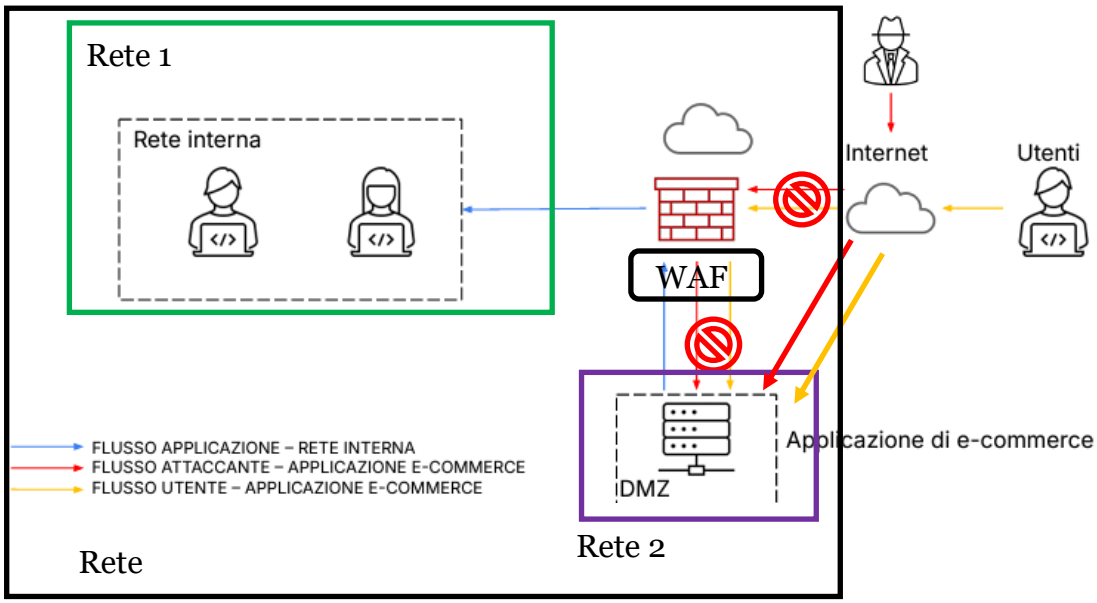
3.3.3 Tipologie di Malware

- **Virus**: Si attacca a file eseguibili e si replica quando vengono eseguiti.
- **Worm**: Si diffonde autonomamente attraverso reti senza bisogno di un host.
- **Trojan (Cavallo di Troia)**: Si maschera da software legittimo per ingannare l'utente e installare codice malevolo.
- **Ransomware**: Cripta i dati e richiede un riscatto per sbloccarli.
- **Spyware**: Monitora le attività dell'utente e raccoglie informazioni senza autorizzazione.
- **Adware**: Mostra pubblicità intrusive, talvolta con intenti dannosi.
- **Rootkit**: Nasconde la presenza di malware e garantisce accesso privilegiato agli attaccanti.
- **Keylogger**: Registra i tasti premuti dall'utente per rubare credenziali e informazioni sensibili.

3.3.4 Soluzione alla problematica
In questa panoramica di attacco, dove il malware ha infettato la web-application e quindi il server web, la soluzione è la **Segmentazione della Rete**, andando a proteggere ciò che non è stato infettato, quindi isolando la DMZ (demilitarized zone) ormai infetta, rendendola raggiungibile direttamente dall'attaccante, preservando la rete interna della compagnia; di seguito la soluzione proposta.

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.

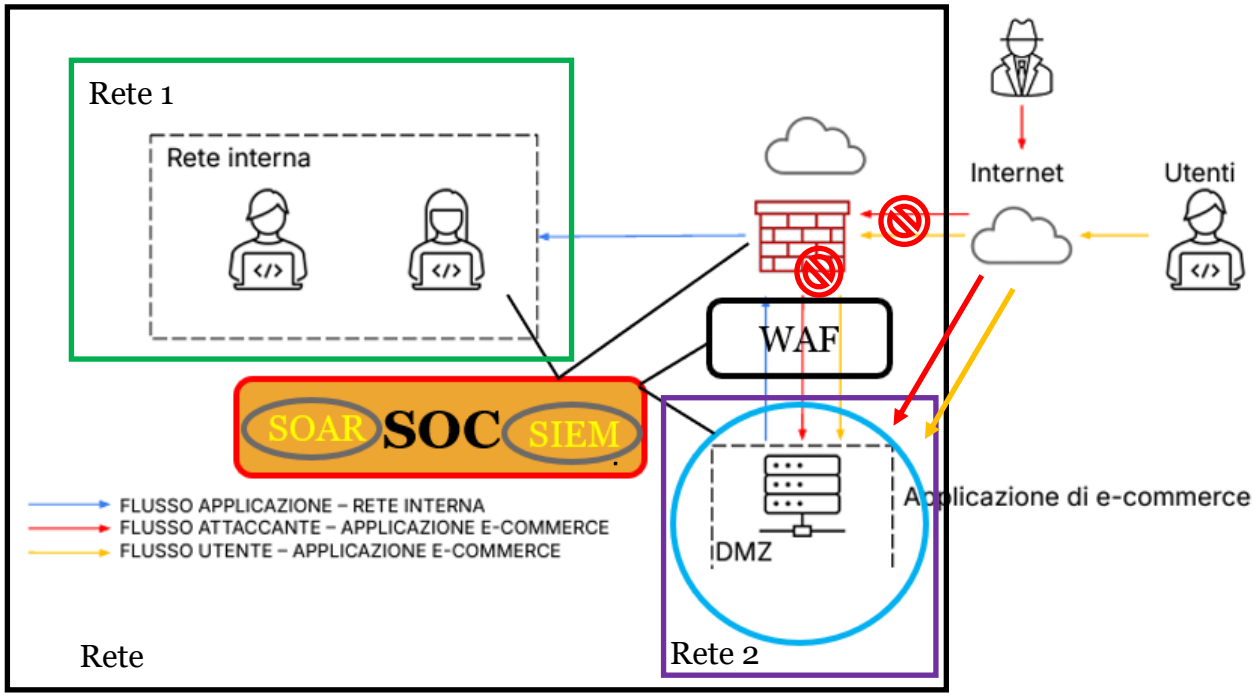


In figura, la rete è stata segmentata in due reti differenti per evitare la propagazione del malware; l'attaccante raggiungerà direttamente la piattaforma di e-commerce, ormai infetta, senza andare a compromettere alle zone del sistema; per quanto riguarda gli utenti interni, potranno comunicare direttamente con la DMZ, passando per il WAF.

3.4 Quesito 4

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

Nell'immagine sottostante sono state unite le soluzioni sopra esposte.



3.4.2 Descrizione soluzione: si descrive di seguito l'architettura di rete proposta in figura:

All'interno del **cerchio azzurro**, possiamo racchiudere tutte le soluzioni d'implementazione sopra proposte, quindi filtraggio di dati in ingresso, implementazione delle CSP, sanitizzazione e validazione dell'input, corretto codice di scrittura della web-app e Implementazione dei SameSite Cookies e HttpOnly.

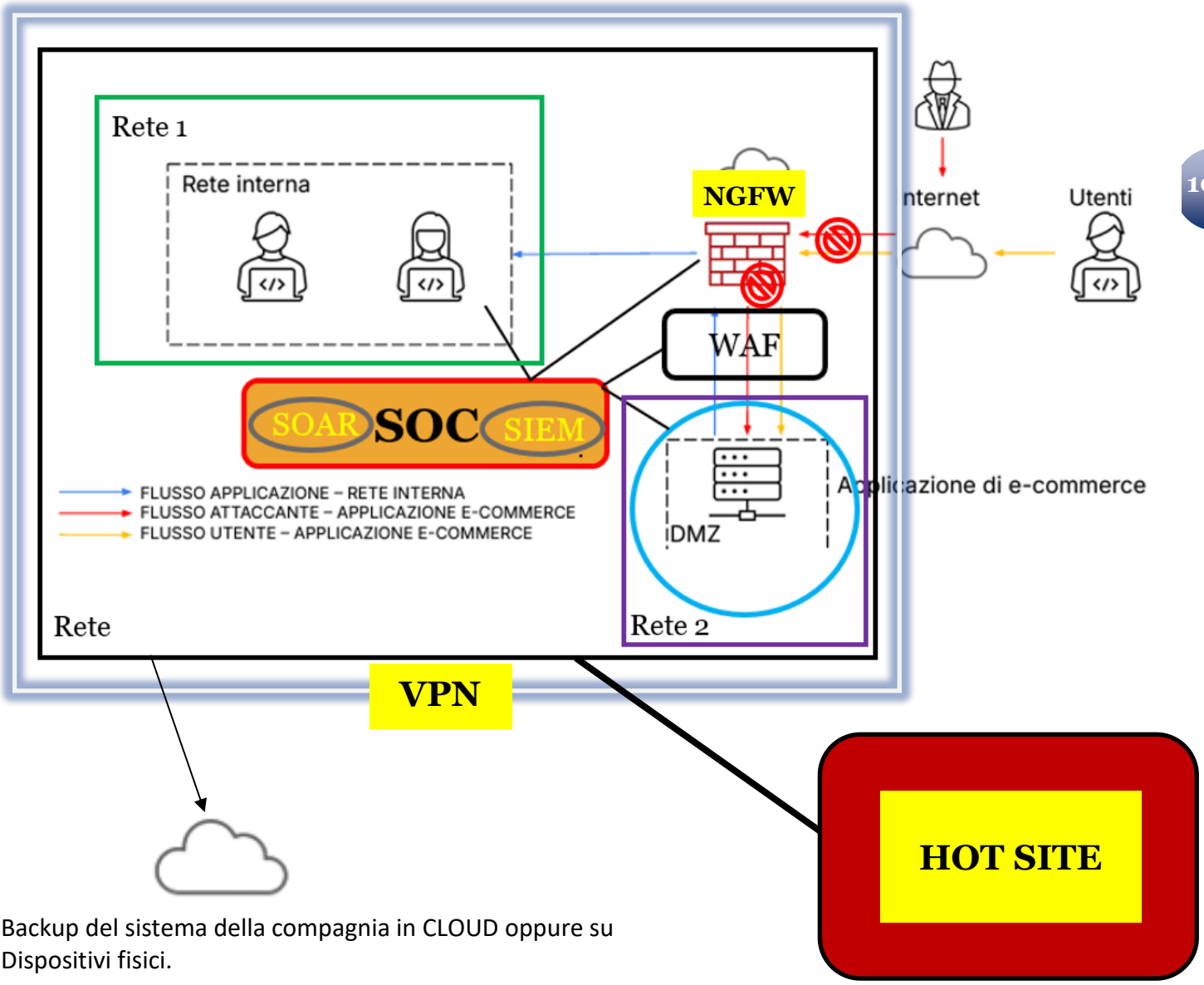
All'interno del **riquadro nero** troviamo il WAF, ovvero il Web Application Firewall, una tipologia professionale e fondamentale di Firewall necessario per tutte le web-app che risiedono su web-server.

All'interno del **riquadro rosso**, il SOC, con gli strumenti SIEM e SOAR, utilizzati per operare efficacemente

Nei riquadri **verde** e **viola** sono state individuate le due reti differenti, in seguito alla segmentazione di rete

3.5 Quesito 5

3.5.1 Modifica "più aggressiva" dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2).



Backup del sistema della compagnia in CLOUD oppure su Dispositivi fisici.

3.5.2 Descrizione soluzione: si descrive di seguito l'architettura di rete proposta in figura, con una modifica più efficace e aggressiva:

All'interno del **cerchio azzurro**, possiamo racchiudere tutte le soluzioni d'implementazione sopra proposte, quindi filtraggio di dati in ingresso, implementazione delle CSP, sanitizzazione e validazione dell'input, corretto codice di scrittura della web-app e Implementazione dei SameSite Cookies e HttpOnly.

All'interno del **riquadro nero** troviamo il WAF, ovvero il Web Application Firewall, una tipologia professionale e fondamentale di Firewall necessario per tutte le web-app che risiedono su web-server.

All'interno del **riquadro rosso**, il SOC, con gli strumenti SIEM e SOAR, utilizzati per operare efficacemente

Nei riquadri **verde** e **viola** sono state individuate le due reti differenti, in seguito alla segmentazione di rete

-> E' stata implementata sul perimetro di tutta la rete una **VPN (Virtual Private Netrwork)**, che permette il mascheramento dell'indirizzo IP verso l'esterno, quindi internet; è una tecnologia che crea una connessione sicura e crittografata tra il dispositivo dell'utente e una rete privata attraverso Internet.
Tra le funzioni principali:

- Protezione della privacy
- Anonimato online
- Accessi sicuri a risorse
- Sicurezza su reti pubbliche

-> Previsto il **backup di sistema** della compagnia in CLOUD oppure su apparecchi hardware professionali

-> Implementazione di una **Hot Site** (se economicamente possibile per la compagnia), pronta all'utilizzo in caso di attacco malware

-> Utilizzo, oltre al WAF, anche di un **NGFW (Next-Generation Firewall)** è un firewall avanzato che combina le funzionalità tradizionali di un firewall con strumenti di sicurezza avanzati, come il rilevamento delle minacce, il controllo delle applicazioni e la prevenzione delle intrusioni (IPS). Nel nostro caso viene sostituito a quello già esistente nell'architettura di rete.