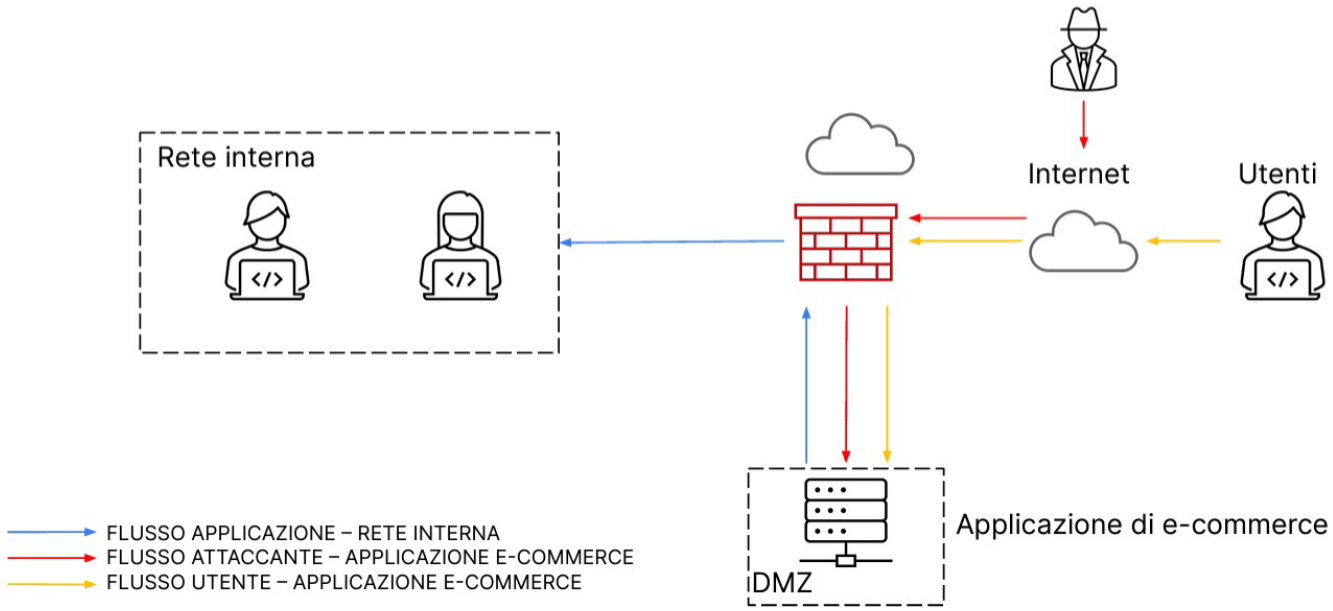
PROGETTO

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)**



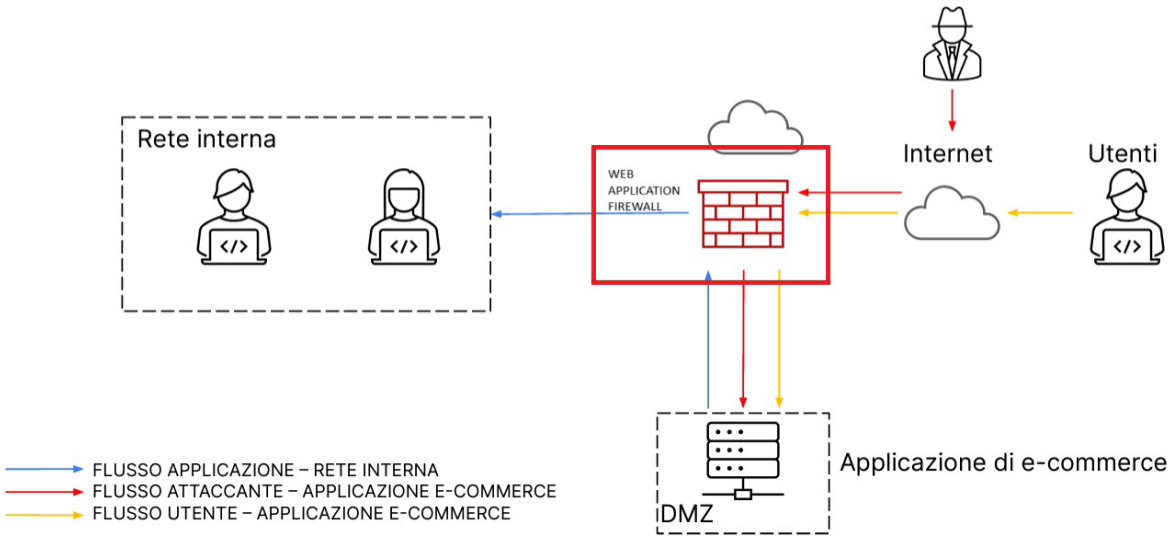
Esecuzione:

1. **Azioni preventive**

Soluzione 1

Per difendere l'attività da una potenziale minaccia SQL Injection oppure XSS, la soluzione ideale per potersi proteggere da un tipo di attacco come questo potrebbe essere la sanitizzazione dell'applicazione stessa, quindi agendo direttamente sul sito e-commerce. Di fatto la soluzione sarebbe agire sul **codice sorgente in modo statico** da parte degli utenti della rete interna dell'applicazione ed inserendo degli opportuni controlli sui campi in modo tale da controllare l'input utente. Un'altra opzione per poter migliorare sempre l'Applicazione e-commerce dal lato codice è con la tecnica di **Reverse Engineering** così da ricercare punti vulnerabili in base all'output che esso genera, di fatto controllando la presenza di controlli o meno e se vi sono punti vulnerabili che permettano ad un utente malevolo di verificarne il database.

Soluzione 2



Un'altra soluzione che implementerei è quella di potenziare il Firewall presente nella rete, configurando le policy della parte di controllo **Web Application.** Tale difesa permette di prevenire altri attacchi SQL Injection e XSS. Se tale configurazione non è presente nella macchina già presente, la si può sostituire o aggiungere fra la rete DMZ ed il firewall già presente.

2. Impatti sul business

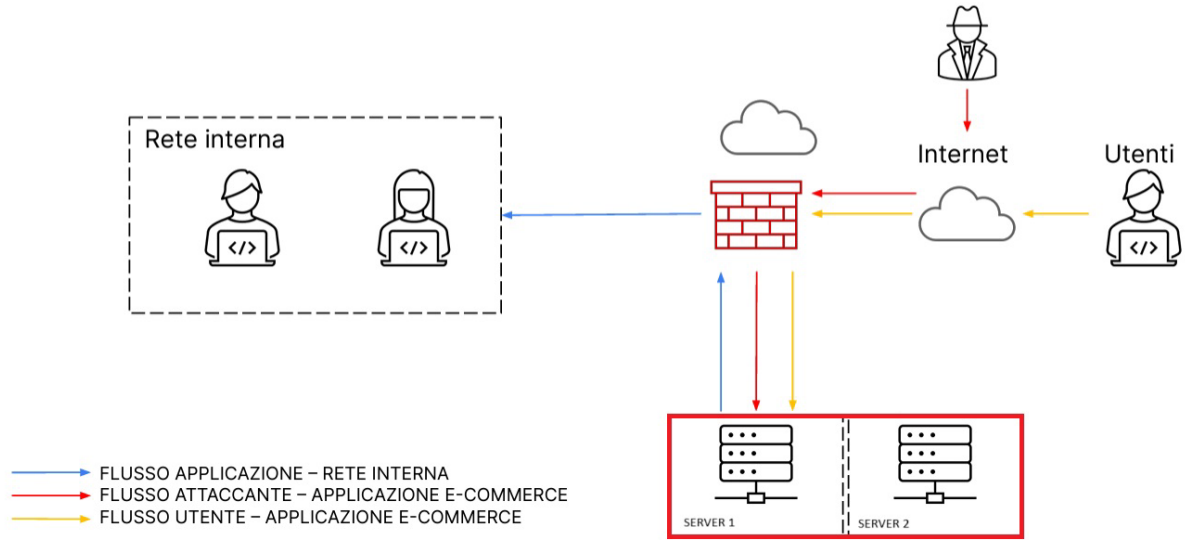
L'applicazione Web subisce un attacco di tipo DDoS dall'esterno, ciò comporta un disservizio dell'applicazione di **10 minuti**.

Di media nel sito un utente spende **1.500€/min.**

In una casistica del genere, con la rete così strutturata, si perderebbe quanto segue:

1.500€/min x **10 minuti = 15.000€**

E' possibile implementare soluzioni per poter ridurre i danni generati da una tipologia di attacco come questo. Una di queste è la creazione di una nuova macchina che sia sincronizzata con il server già esistente, creando un **Server Cluster.**



Così facendo, se si verificasse un nuovo attacco DDoS, che manda fuori servizio il Server 1, il Server 2 entrerebbe in gioco dando continuità di servizio. Ponendo che il tempo di scambio sia di 2 minuti, la perdita della compagnia si ridurrebbe a quanto segue (si fa presente che il calcolo è indicativo in quanto non è detto che un utente spenda sempre quell'importo all'interno dell'applicazione E-commerce):

1.500€/min x **2 minuti = 3.000€**

Un'altra possibile azione preventiva in un caso del genere sarebbe l'utilizzo di un Firewall IPS/IDS che monitora, rileva ed esegue azioni nel caso si verifichi un'attività "sospetta" nella rete e ne scongiura il verificarsi del danno effettivo dell'attacco DDoS.

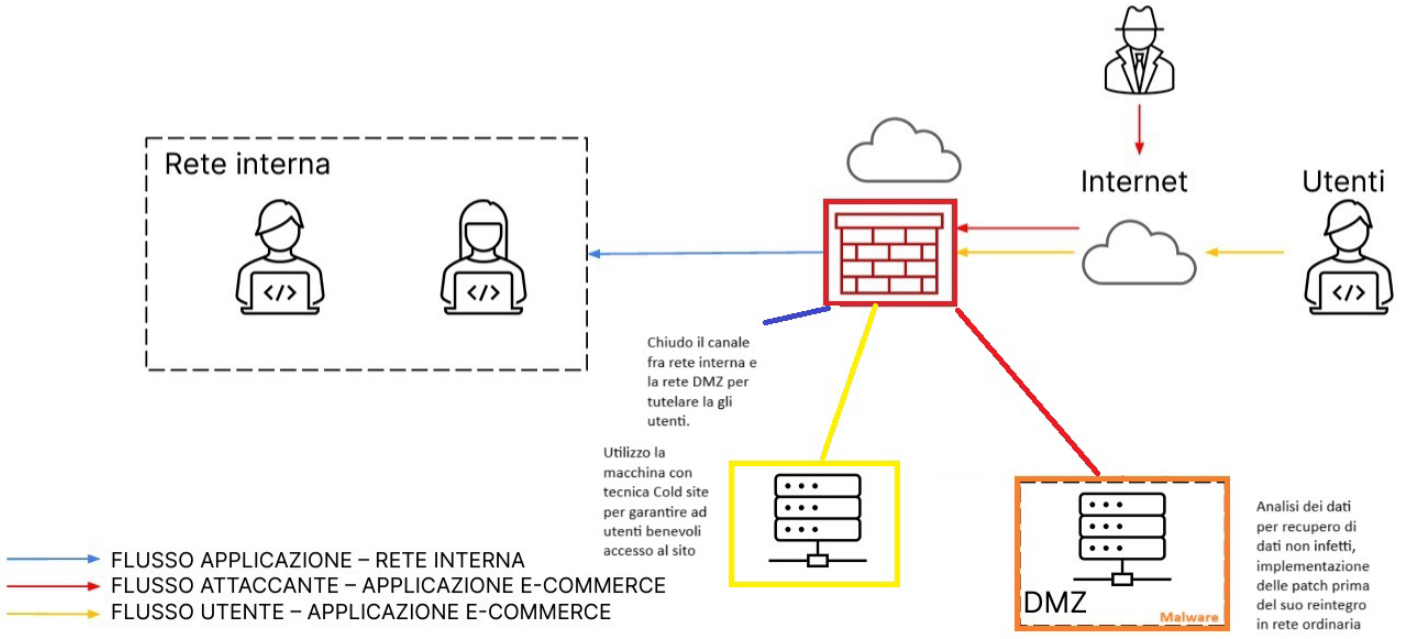
Ipoteticamente, potrebbe essere posizionato insieme al firewall già esistente oppure integrato con delle policy specifiche quall'ora la macchina firewall già esistente le supportasse.

3. Response

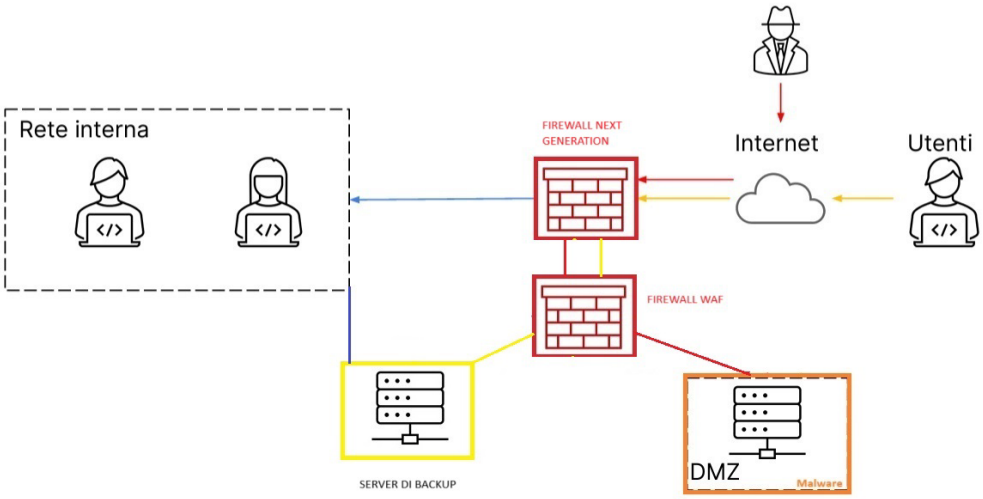
L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

Per proteggere la rete interna da una intrusione da parte dell'attaccante che ha già agito nell'applicazione E-commerce, utilizzerei il seguente approccio:

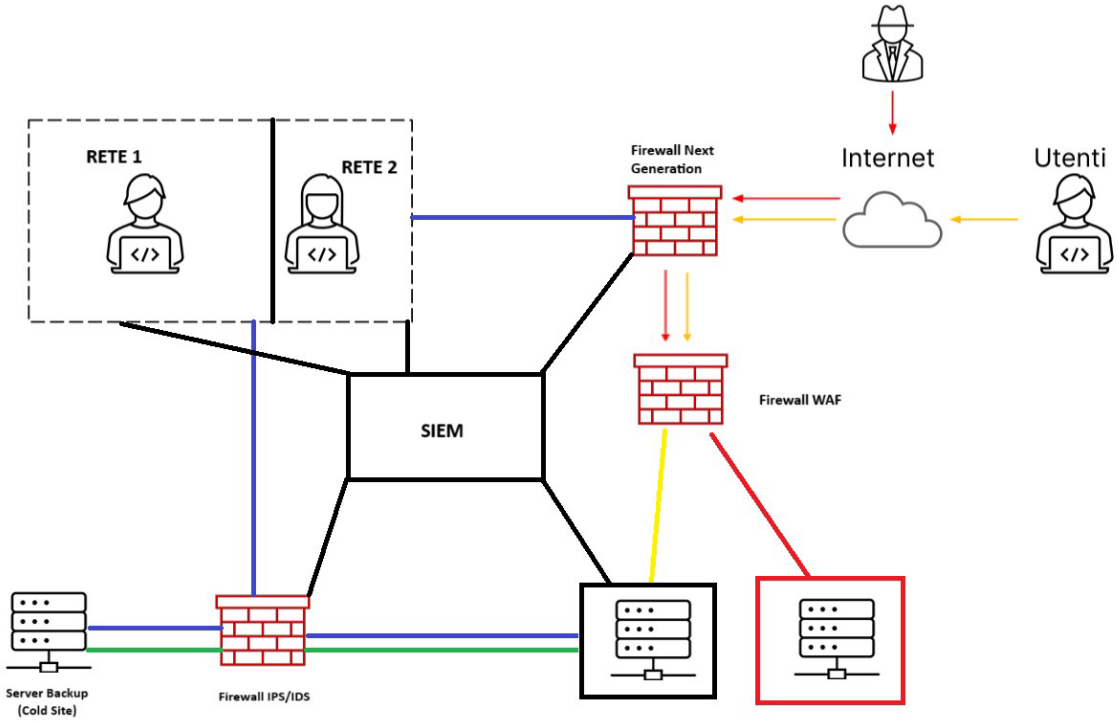
1. **Chiuderei il canale** di comunicazione fra la rete interna e l'applicazione utilizzando il firewall.
2. **Isolare** la macchina in una rete differente e creandone una nuova contenente un server di backup. Potrebbe essere una macchina interamente identica a quella già esistenze che contiene un full backup del primario.
3. **Revisione delle politiche del firewall** che ne impedisca l'accesso alla nuova macchina e ne potenzi i controlli utilizzando anche firewall con tecnologia Next Generation Firewall. Tale macchina sarebbe opportuno inserirla in sostituzione di quella esistente. Un controllo più approfondito dei pacchetti (di fatto è una verifica del pacchetto su tutti i livelli della pila ISO/OSI) evita che altri malware futuri entrino nel sistema.
4. **Controlli sulla macchina infetta per verificare se vi sono dati recuperabili**. Effettuando aggiornamenti con delle **patch di sicurezza** al fine di migliorare anche la sicurezza stessa della macchina. Indagare sulla macchina per verificarne i dati compromessi e quelli "salvabili". Eliminare il malware una volta identificato. Soltanto quando la macchina è pienamente ripristinata, valutarne il reintegro in servizio.



4.Soluzione completa.



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



Una ulteriore modifica molto più aggresiva è con l'aggiunta dei seguenti dispositivi per il controllo e riparo di tutta l'infrastruttura come segue:

- **Firewall Next Generation**: per il blocco di pacchetti che trasportano file infetti eseguendo un controllo completo (tutti i livelli pila ISO/OSI).
- **Firewall WAF separato**: Inserito fra Firewall NG e i server dell'applicazione E-Commerce, per una prevenzione di attacchi SQL Injection e XSS.

- **La creazione di due Server con formula cluster**. Se il primario (Riquadro rosso) dovesse andare in down per attacco DDoS o per un attacco malware viene isolato dalla rete e reso accessibile solo all'attaccante. Mentre il Secondo Server (riquadro nero) viene utilizzato per connettere gli utenti ordinaroi.
- Per una maggiore tutela, aggiungo un **Firewall IPS/IDS** che tiene in comunicazione rete interna e il server di Backup in Cold site, meno dispendioso per il mantenimento ma più sicuro se programmato un backup periodico. Il backup da effettuare sulla base del Secondo Server (riquadro nero).
- Il collegamento fra secondo server (riquadro nero) e la rete interna passa per firewall IPS/IDS cosi da prevenire e bloccare una potenziale scansione da parte di un attaccante (esempio controllo nmap o simili).
- Firewall Next Generation, Server Secondario, Firewall IPS/IDS e Rete interna sono tutte controllate dal **SIEM** al fine di avere file di log collector per verificarne che non vi siano accessi illeciti o compromissione delle misure di sicurezza da parte di qualsiasi minaccia "avversaria" o potenzialmente "interna". Questo per rinforzare il concetto di **riservatezza** del dato secondo la **CIA**
- Inoltre tutte le macchine contenenti il l'applicativo E-commerce devono utilizzare una tecnologia **RAID – 5** fra i loro dischi interni.
- Separazione della rete interne in due reti distinte: la **Rete 1** ha possibilità di accedere alla web application da un canale preferenziali come indicato nel punto precedente, ma non può avere accesso alla rete internet. Contrariamente la **Rete 2** non potrà in alcun modo accedere ai server di backup e al Server secondario del cluster (Riquadro nero), ma potrà accedere alla rete internet esterna tramite il Firewall Next Gen. Tutti gli accessi log vengono controllati nel **SIEM.** Le due reti non sono comunicanti fra di loro.