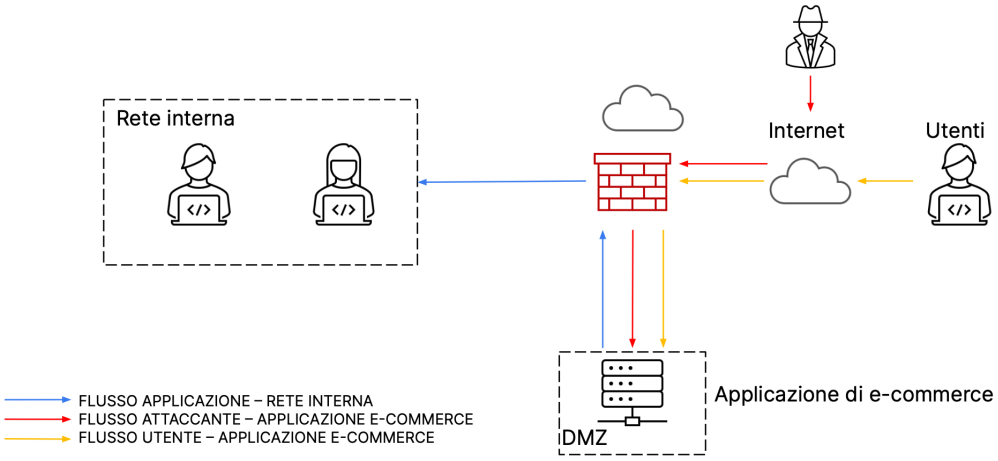
ESERCIZIO SETTIMANA 9

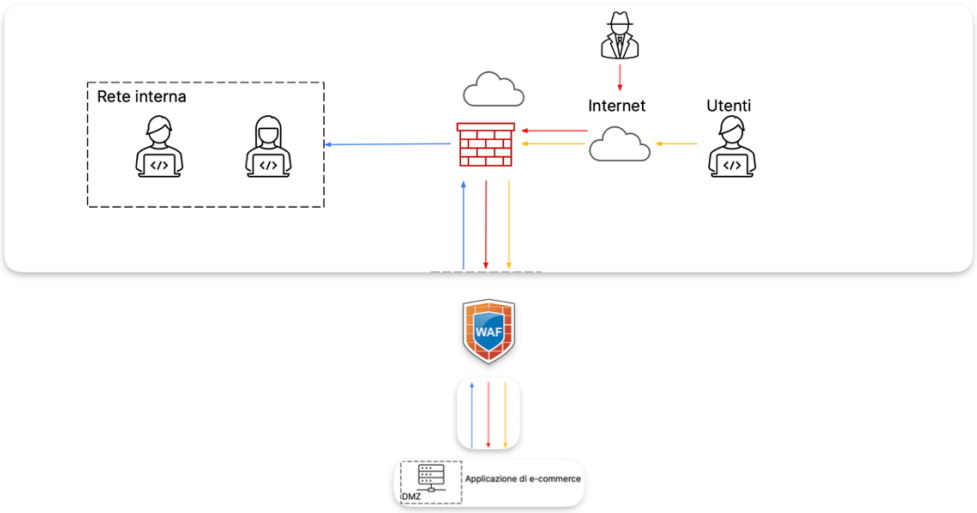
APPLICAZIONE DI E-COMMERCE

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.

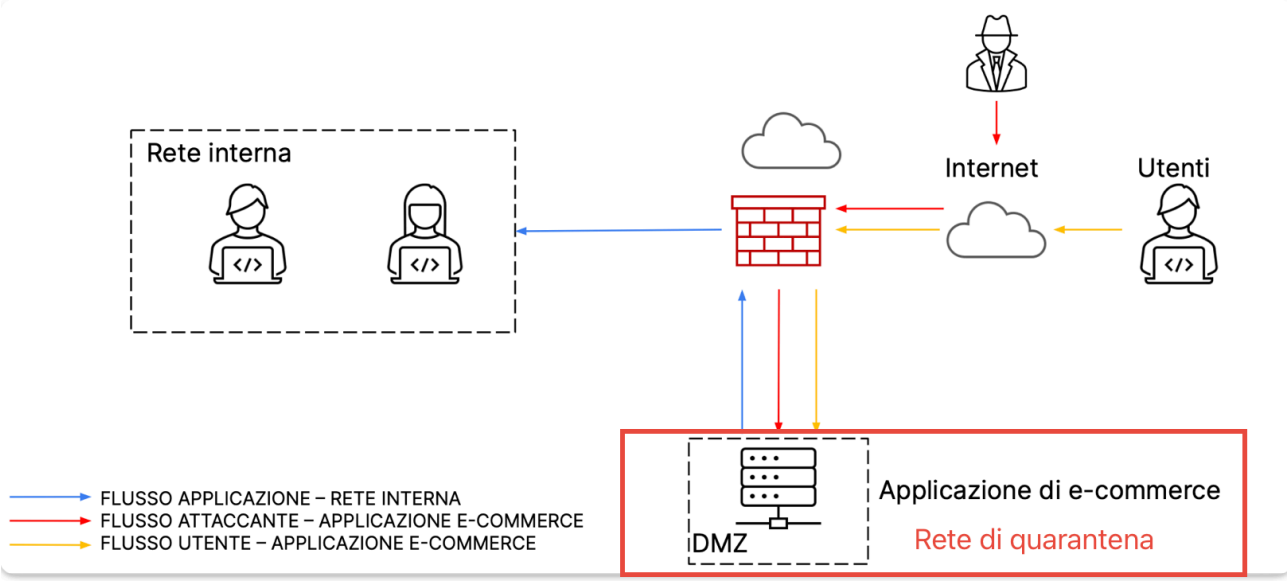


1-Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web
da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
Modificate la figura in modo da evidenziare le implementazioni



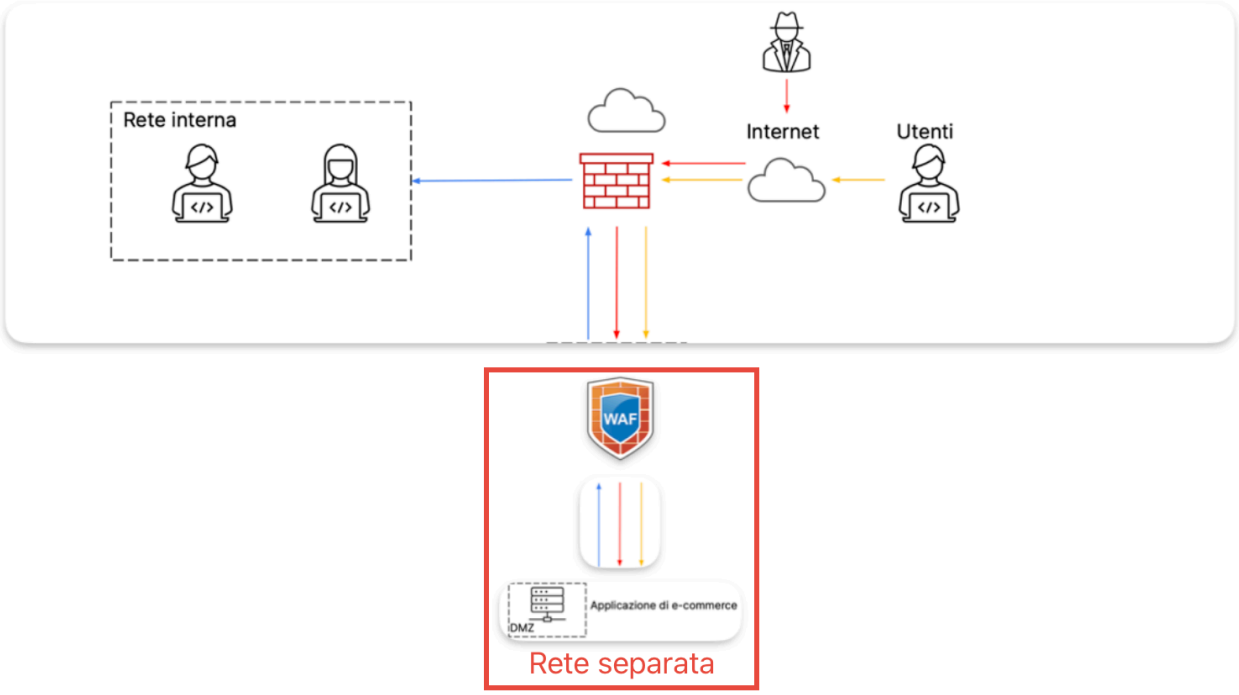
Come azione preventiva possiamo implementare un WAF (web application firewall)
Dei dispositivi di sicurezza dedicati per proteggere le applicazioni web da attacchi quali SQLi e XSS

3 -Response: l'applicazione Web viene infettata da un malware.
La vostra priorità è che il malware non si propaghi sulla vostre rete, ma è altrettanto importante non divulgare informazioni sensibili verso Internet.
Modificate la figura in slide 2 con la soluzione proposta.



In una casistica di questo genere lo scopo principale è quello di isolare e contenere l'incidente.
Una soluzione efficace è la segmentazione di rete
In questo caso la segmentazione avviene creando quella che viene chiamata rete di quarantena in questo modo eviteremo che il malware si propaghi sulla nostra rete interna.
Nei casi più gravi si procede all'isolamento della rete sia internet che interna.

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

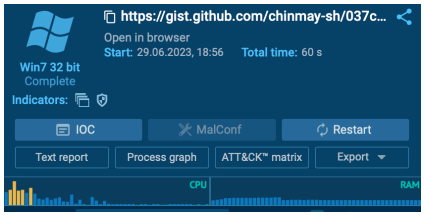


5 -Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza

Per una modifica più aggressiva dell'infrastruttura possiamo procedere all'implementazione di nuovi sistemi oltre quelli mostrati in figura come:
IDS/IPS : per identificare ed eventualmente bloccare intrusioni
SISTEMI DI BACKUP: sistemi come NAS o cloud per il salvataggio dei dati in caso di perdita o compromissione
APC: sistema di alimentazione ausiliario in caso di interruzioni elettriche
MODEM FAILOVER: modem con tecnologia failover per un costante mantenimento della disponibilità di rete internet
NAC: per il controllo degli accessi
SIEM e SOAR: per il salvataggio il monitoraggio e risposte agli eventi

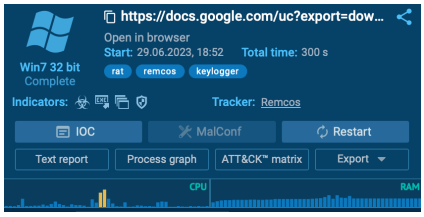
2 -Analisi attacco:

Linklosco1



Analizzando il link possiamo notare che questo fa riferimento ad uno script powershell che permette di cambiare le impostazioni DNS
Ma dall'analisi di any run vediamo che questo script va a leggere e modificare chiavi del registro di sistema dove sono contenute informazioni importanti come le zone di affidabilità dei siti web usando powershell per operare con l'account locale.

Linklosco2



Dall'analisi del secondo link possiamo notare come quello che dovrebbe essere un documento pdf in realtà nasconda un eseguibile .exe in un archivio che va a creare un file con il nome simile al file system
Dopo averlo scaricato viene eseguito il compilatore C avviando CMD.exe per l'esecuzione di comandi tramite riga per usare il task scheduler per eseguire altre applicazioni