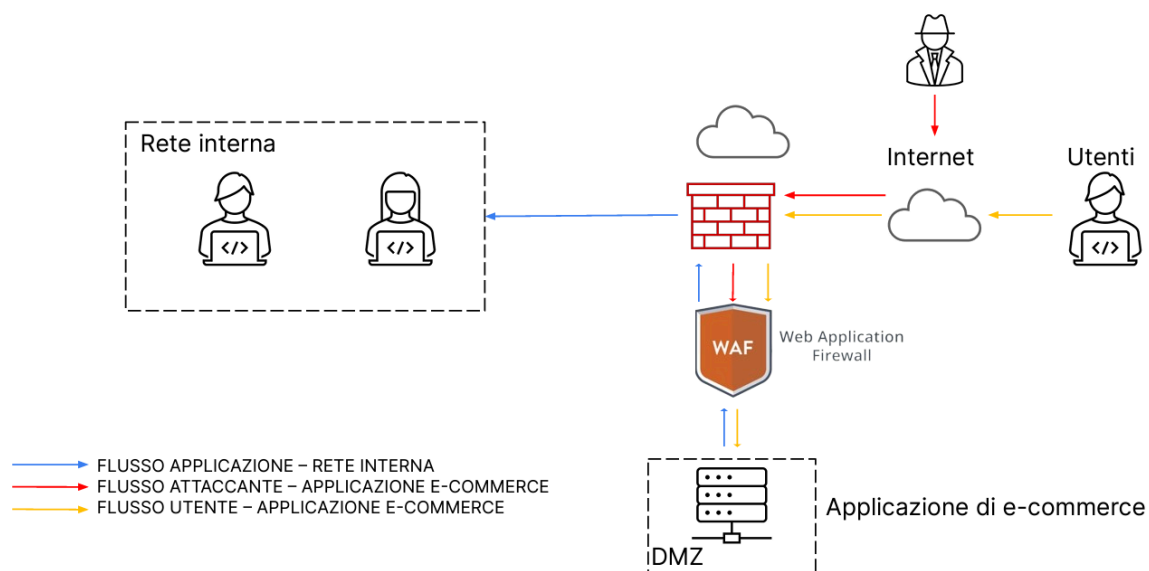



Benchmark di fine modulo 5 - Security Operation & Threat Intelligence

Quesito 1 :Esistono diverse azioni preventive che possono essere adottate per ridurre il rischio di attacchi XSS (Cross-Site Scripting) o SQLi (SQL Injection). È fondamentale intervenire sia sul lato del codice che sull'infrastruttura di sicurezza.

Dal punto di vista dello sviluppo software, è essenziale adottare pratiche di programmazione sicura. Tra le tecniche più efficaci vi sono le "Parameterized Queries" e la "Input Validation". Le "Parameterized Queries" consentono di separare i comandi SQL dai dati utente, riducendo drasticamente il rischio di SQL Injection. L'Input Validation, invece, consiste nella verifica e nel filtro degli input forniti dagli utenti per garantire che siano conformi alle aspettative e non contengano codice dannoso.

Un'altra misura preventiva di fondamentale importanza è l'utilizzo di un WAF (Web Application Firewall) in aggiunta al tradizionale firewall di rete. Mentre un firewall tradizionale si concentra principalmente sul controllo del flusso generale del traffico di rete, un WAF è progettato specificamente per proteggere le applicazioni web. Analizza e filtra il traffico HTTP/HTTPS, individuando e bloccando le minacce specifiche rivolte alle applicazioni web, come gli attacchi XSS e SQLi.



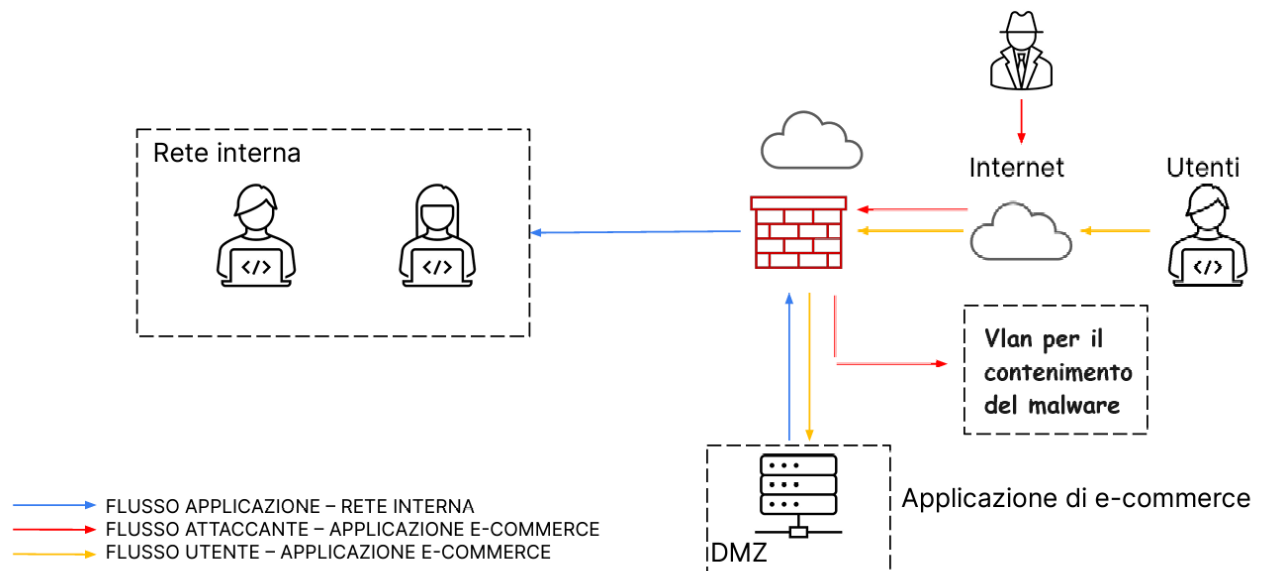


Non va trascurata l'importanza di condurre sessioni periodiche di penetration test. Queste attività consentono di individuare e risolvere eventuali vulnerabilità presenti nel sistema, spesso dovute a sistemi non aggiornati o a configurazioni non corrette. Il penetration testing fornisce una valutazione realistica della sicurezza del sistema, consentendo di apportare miglioramenti e aggiornamenti necessari per garantire una protezione efficace contro le minacce informatiche.

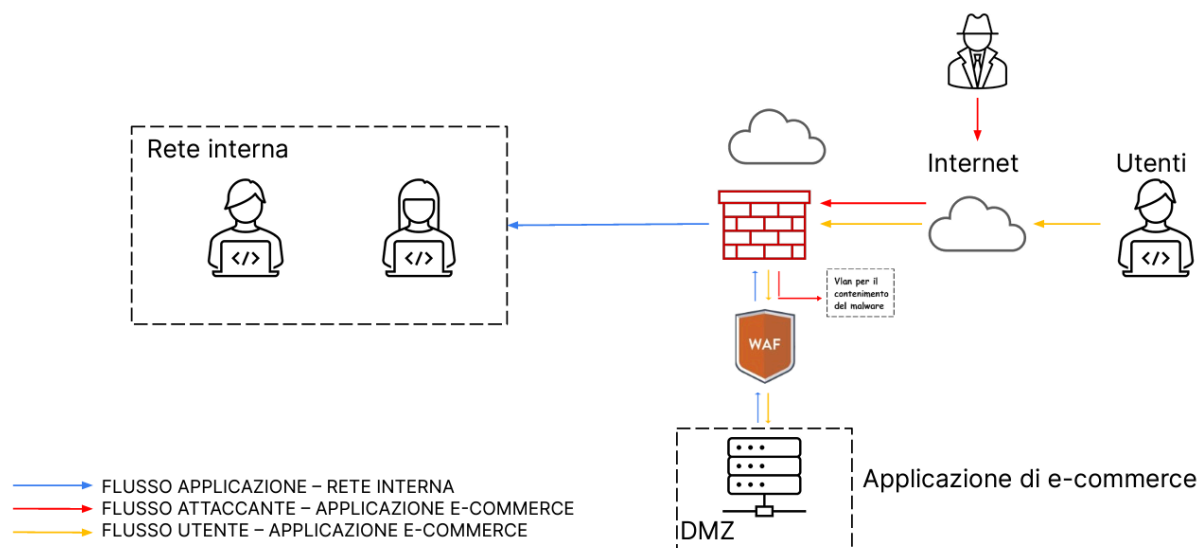
Quesito 2 : Supponendo che gli utenti spendono in media 1500€ al minuto nel nostro portale e che in questo caso l'attacco ddos causa un disservizio di 10 minuti, possiamo calcolare il costo per l'azienda per ogni singolo evento, noto come SLE (Single Loss Expectancy). Quindi, $SLE = 1500\text{€}/\text{min} \times 10 \text{ min} = 15000\text{€}$. Tra le misure preventive sicuramente più facili da implementare per tamponare (o risolvere completamente) il rischio di subire grosse perdite a causa di un attacco DDOS vi è sicuramente l'utilizzo di servizi dedicati quale ad esempio cloudflare. Un'altra soluzione molto interessante viene offerta da cisco secure. Tra i loro vari servizi spicca il loro sistema hybrid. Oltre ad offrire una protezione per gli attacchi ddos unisce il classico datacenter on-premise ad una soluzione cloud, assicurando così la continuità del servizio. E' chiaro però che soluzioni simili hanno costi non indifferenti che devono necessariamente essere valutati prima della loro implementazione.

Quesito numero 3:

Nel caso in cui la web app venga infettata da un malware e non sia fattibile l'isolamento fisico del server attaccato, è possibile adottare la tecnica di segmentazione della rete per confinare il malware in una sottorete dedicata, permettendo di studiare successivamente il comportamento in un ambiente sicuro. A tal fine, si può creare una VLAN che isoli il malware, consentendo contemporaneamente il ripristino dei servizi danneggiati. Questo approccio non solo limita i danni causati dal malware, ma permette anche il mantenimento dei servizi operativi.

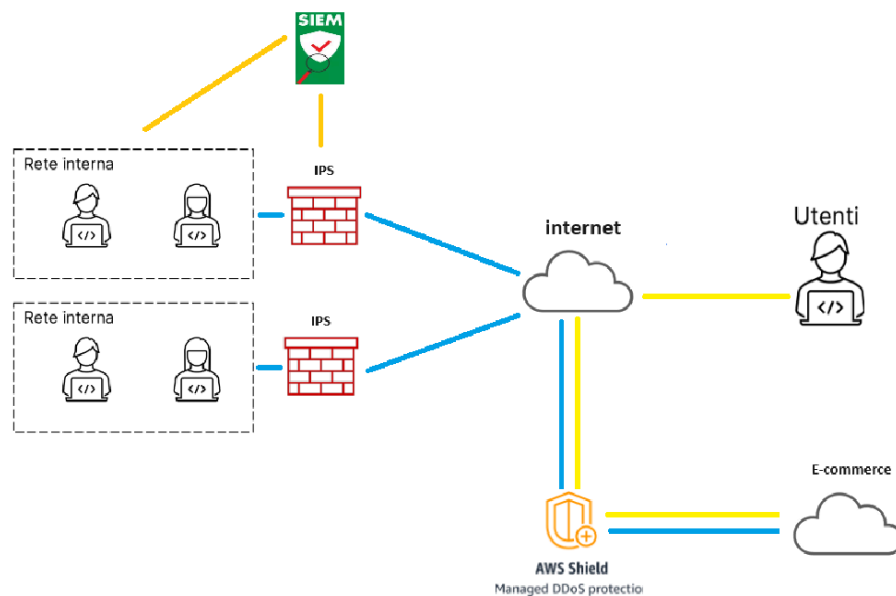


Quesito 4 : Unendo dunque le due soluzioni otteniamo una rete interna segmentata e i servizi della web app “protetti” da un WAF



Quesito 5:

La segmentazione della rete rappresenta uno dei pilastri fondamentali per garantire la sicurezza informatica di un'organizzazione. Segmentando la rete in sottoreti separate, limitiamo la diffusione di eventuali minacce o compromissioni. Questo è essenziale perché, in caso di violazione di sicurezza, limitare l'accesso del malintenzionato ad altre parti della rete può ridurre notevolmente i danni e facilitare il contenimento e il ripristino.



Volendo sfruttare per i servizi AWS i backup verranno effettuati sul cloud. lo stesso avverrà per i db della compagnia. Sulla rete sarà presente un SIEM in modo da raccogliere in un unico

ambiente i log generati da applicazioni e sistemi di rete.



La soluzione cloud-based di amazon ci permetterà hostare la web app su i loro server potendo così sfruttare aws shield per difendere il servizio da eventuali attacchi ddos con una soluzione non eccessivamente costosa ma sicuramente performante. In oltre amazon presenta una ottima soluzione per la continuità del servizio in caso di disastro, assicurando dei down-time relativamente bassi