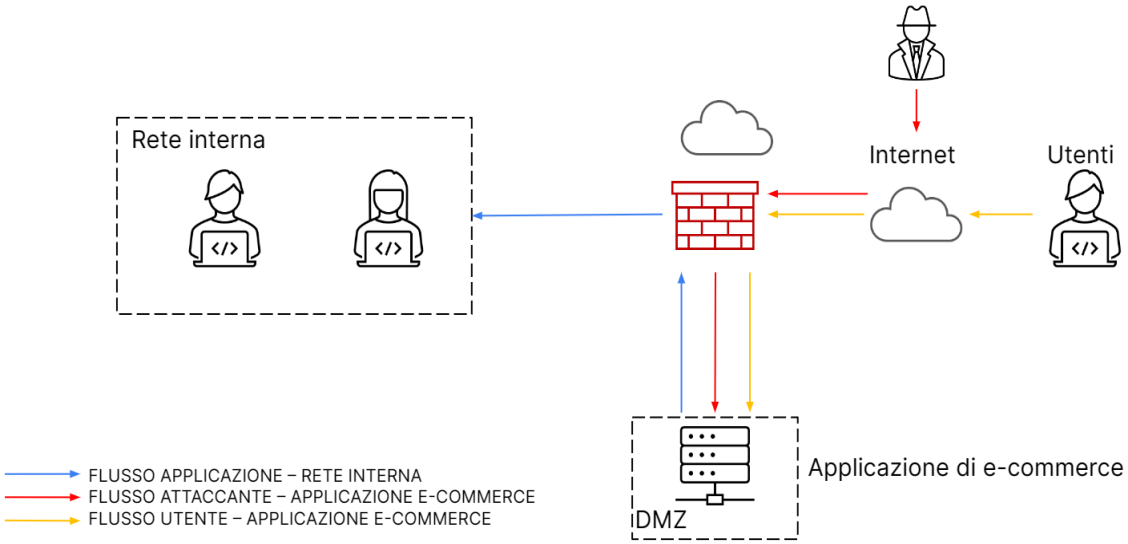
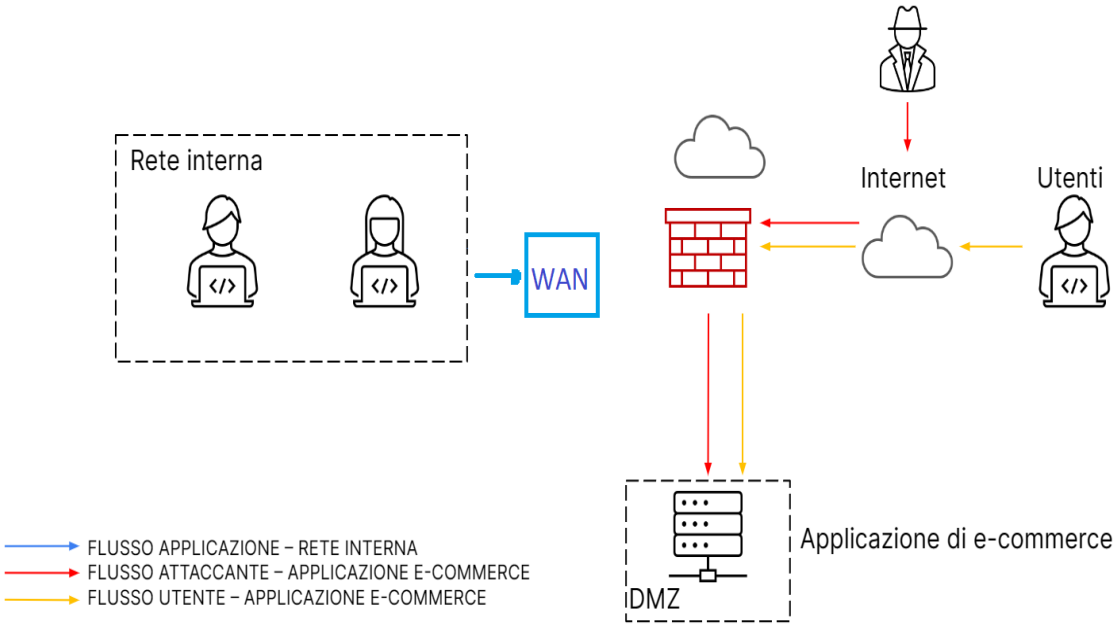
Risposta 1 e 3 esercizi



*La foto sopra fa capire quale sia il problema, la soluzione di ciò va in base al budget, adesso nella foto in basso con un budget economico di **5000 EURO** si può usare una **WAN** e isolare la rete interna, implementando ciò il malintenzionato "Hacker" non riesca ad avere accesso alla rete interna.*

Il Risultato finale nella foto in basso con il primo budget:



Per quanto riguarda l'attacco "Xss", la cosa più giusta da fare è togliere tutti i caratteri non convenzionali di input dalla web app tipo (<> script etc.) cambiando tutto con le espressioni regolari perché il codice maligno può entrare attraverso gli URL, ragion per cui se non abbiamo questa difesa alzata l'attaccante entra tranquillamente.

Invece per "Sqli" è simile ma non uguale, bisogna sanare gli input degli utenti, aggiornare sempre tutto plugins etc. Gestire bene i privilegi di SQL, ed implementare le proprie logiche in modo da renderlo più sicuro, tenendo costantemente aggiornati, il rischio si riduce di molto.

Nella foto, è stato cancellato il flusso della rete interna cosi che il malintenzionato non possa accedere alla rete interna.

Risposta 2-5 Esercizi

Secondo il calcolo delle perdite ***"sle = av * ef***

Ovvero 1500/10 = 150", la perdita

ammonta ogni 10 minuti a *150EURO*, un dato significativo per il business della Web App

Per difendersi dal "Ddos" conviene mettersi in modalità amministratore, un utente normale non può avere permessi e quindi avendo i permessi una volta fatto ciò si può mitigare l'attacco diversamente. Attraverso firewall e altre cose che l'amministratore può maneggiare come per esempio i sistemi di rilevazione.

SECONDA SOLUZIONE PIU'AGGRESSIVA

Se vogliamo una modifica più aggressiva della struttura, *possiamo cambiare il* ***router*** *se non è performante, il secondo budget sarà* ***10000EURO*** *bisogna anche usare un* ***firewall software*** *per mitigare l'attacco usando varie policy.*