

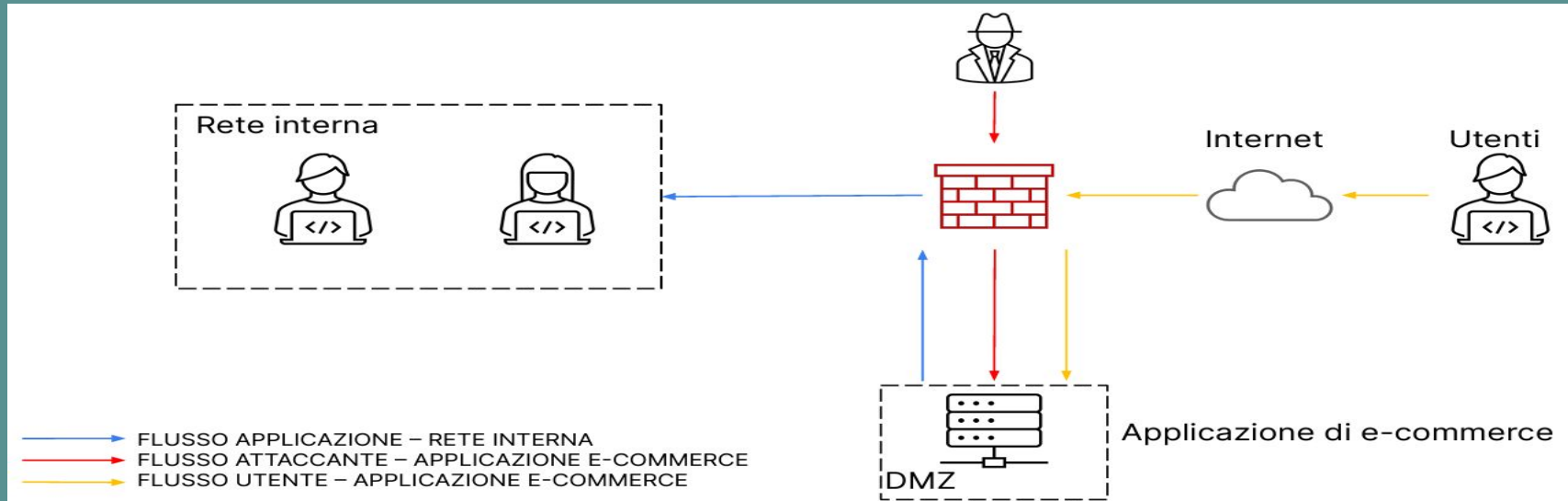
S9/L5 Epicode Cybersecurity

Analisi dei log

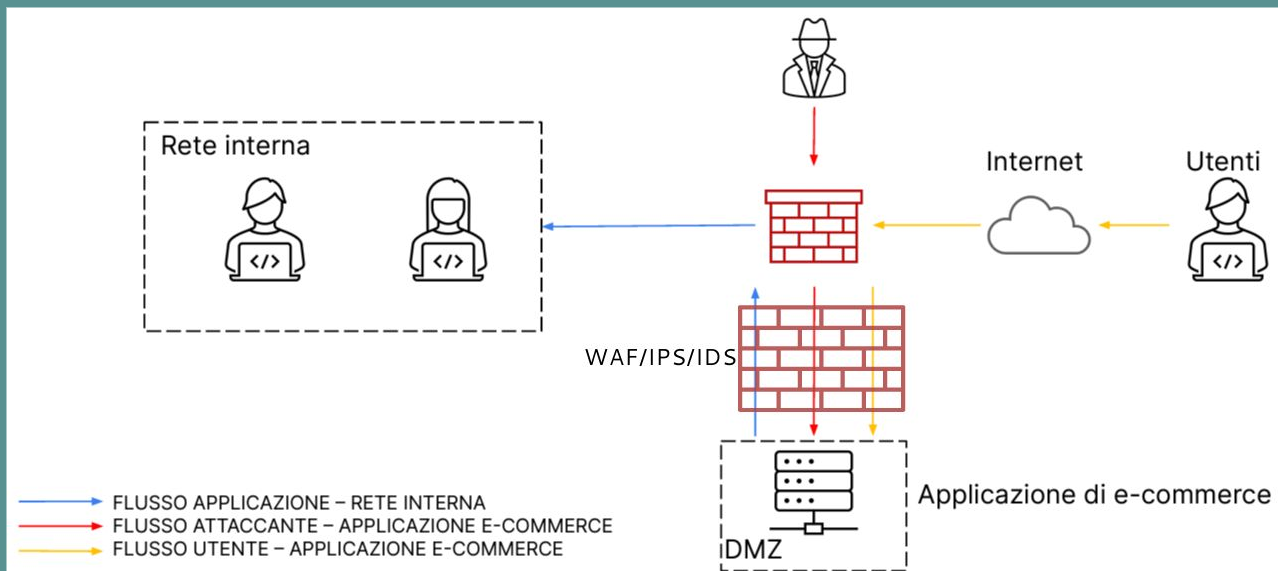


● Introduzione	3
● Azioni preventive	4
● Valutazione impatto su business	6
● Incident response	7


Nell'esercizio di oggi ci viene chiesto di compiere azioni preventive, valutare gli impatti sul business ed effettuare un incident response avendo come schema di base questa architettura di rete.



La prima parte dell'esercizio ci richiede di implementare delle azioni preventive per difendere la Web application da attacchi SQLi o XSS. L'azione più efficace da compiere sarebbe quella di aggiungere un **Web Application Firewall (WAF)**, un firewall appositamente dedicato alle applicazioni web che fa in modo di bloccare tentativi di attacchi in entrata come quelli da noi ipotizzati, tra la rete internet e l'applicazione di e-commerce. Come possiamo vedere nell'immagine della slide precedente, la DMZ presente nella rete e-commerce porta un flusso alla rete interna, quindi proteggere la prima serve anche a proteggere la seconda. Un'altra utile implementazione sarebbe quella di un **IDS/IPS**, ovvero un sistema che sia in grado di rilevare l'intrusione e lo segnali (IDS) o prenda direttamente delle contromisure (IPS).



Il secondo quesito che ci viene posto è una valutazione degli impatti sul business. Nel caso in analisi sappiamo che la web application subisce un attacco Ddos che la rende irraggiungibile per **10 minuti** e che, ogni minuto, su di essa vengono spesi **1.500 €**. Per valutare l'impatto, quindi, basterà moltiplicare i 1.500 € persi ogni minuto per i 10 minuti di inattività: $1.500 * 10 = 15.000$. Così sappiamo quindi che il nostro business, in questi 10 minuti di inattività, ha perso **15.000 €**.



Il terzo quesito posto ci chiede di applicare un incident response; la nostra web application è stata infettata da un malware e dobbiamo evitare che esso si propaghi alla rete interna senza la necessità di rimuovere l'accesso all'attaccante sulla macchina infetta.

Il metodo più efficace da utilizzare in questo caso è l'**isolamento**, ovvero la macchina infetta verrà totalmente disconnessa dalla rete interna ma manterrà l'accesso ad internet.