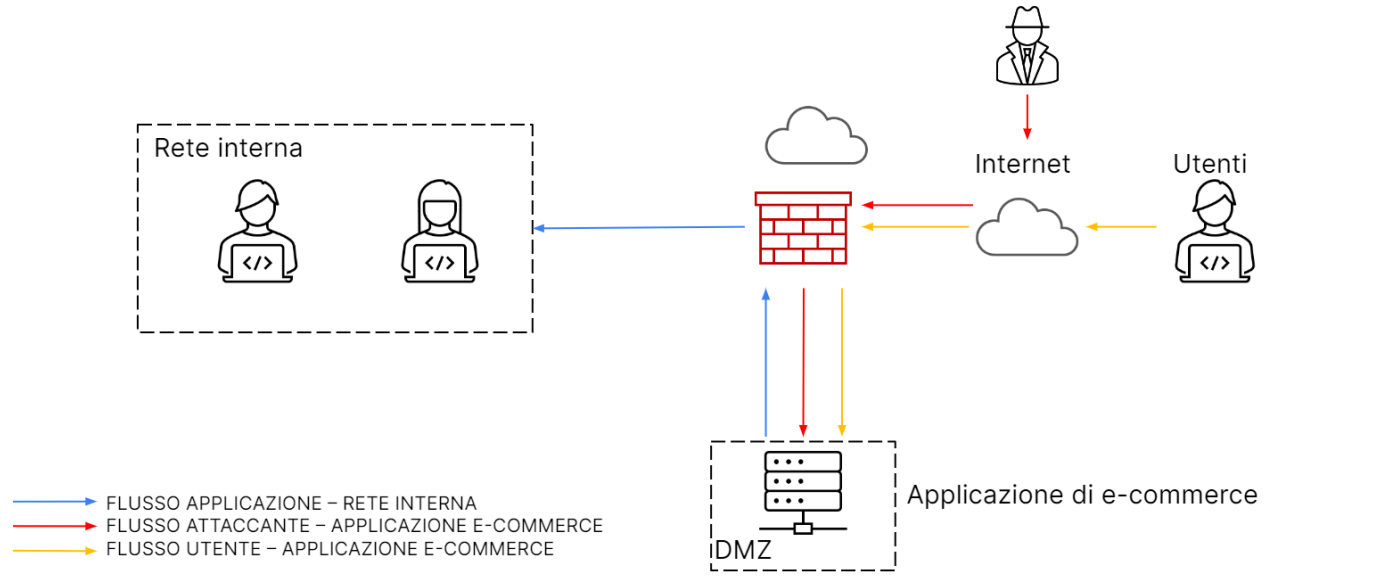
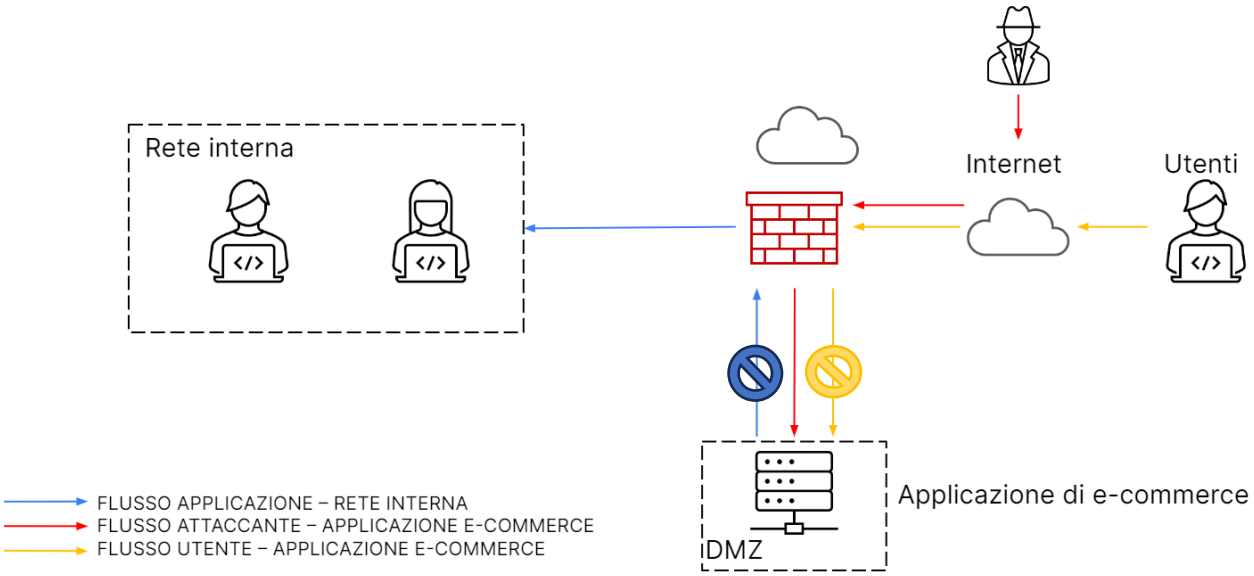


1 Immaginando una rete come quella nella figura sopra le azioni preventive che possiamo attuare per ridurre il rischio di attacchi XSS e SQLi sono innanzitutto settare correttamente le regole del firewall per evitare che dalla DMZ si possa liberamente accedere alla rete interna e segmentare la rete suddividendola in più subnet attraverso l'aggiunta di un Firewall che consenta di separare una subnet all'altra, questo ci permetterà di migliorare la sicurezza evitando la propagazione di attacchi all'interno della rete e permetterà un miglior controllo degli accessi per garantire che gli utenti accedano solo alle risorse a cui hanno effettivamente diritto. Inoltre tra le altre azioni preventive possiamo: mantenere costantemente aggiornati i componenti dell'applicazione, inclusi i framework, le librerie e il software del server così che le nuove patch di sicurezza siano sempre installate; implementare una Content Security Policy per mitigare gli attacchi XSS; limitare i privilegi del database in modo che l'applicazione web abbia solo le autorizzazioni necessarie per svolgere le sue funzioni ed evitare di utilizzare account con privilegi elevati per l'applicazione.

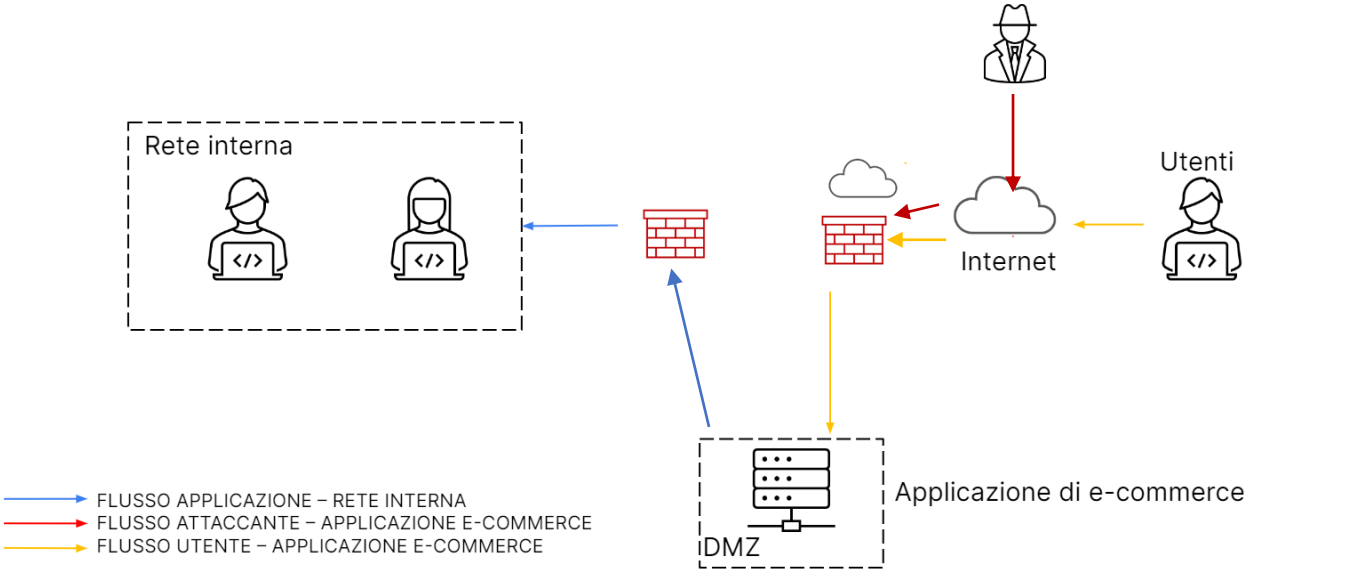
2 Se l'app web subisce un attacco di tipo DDoS che rende il sito non raggiungibile per 10min. avremo un danno economico di circa 15.000 euro (sapendo che in media gli utenti ne spendono 1.500 al min.). Per ridurre il rischio di questo tipo di attacco si possono implementare sistemi di monitoraggio del traffico di rete per identificare rapidamente un attacco DDoS in corso, possiamo imporre limiti sul numero di richieste che possono essere effettuate da un singolo indirizzo IP in un breve periodo di tempo ed utilizzare firewall e strumenti di filtraggio del traffico per bloccare il traffico sospetto.
Dobbiamo progettare l'architettura della rete e dei servizi in modo che siano resilienti agli attacchi DDoS ad esempio distribuendo i servizi e i server su più data center o posizioni geografiche; utilizzando sistemi di bilanciamento del carico per distribuire in modo uniforme il traffico tra i server, questo riduce la probabilità che un server venga sovraccaricato da un attacco DDoS; possiamo considerare l'acquisto di un hardware specifico per la protezione DDoS, come dispositivi di mitigazione DDoS e l'utilizzo di servizi di mitigazione DDoS forniti da terze parti. Infine dobbiamo assicurarci che il servizio DNS sia resiliente e in grado di gestire un aumento del traffico.

3 Se l'app viene infettata da un malware e la priorità è che non si propaghi sulla rete piuttosto che rimuovere l'accesso dell'attaccante alla macchina infettata quello che dobbiamo fare è isolare la macchina; possiamo farlo disconnettendo fisicamente il sistema dalla rete o configurando il firewall per bloccare il traffico dal sistema infetto; inoltre negheremo l'accesso ad altri utenti per evitare che possano subire attacchi (XSS persistente), quindi anche se

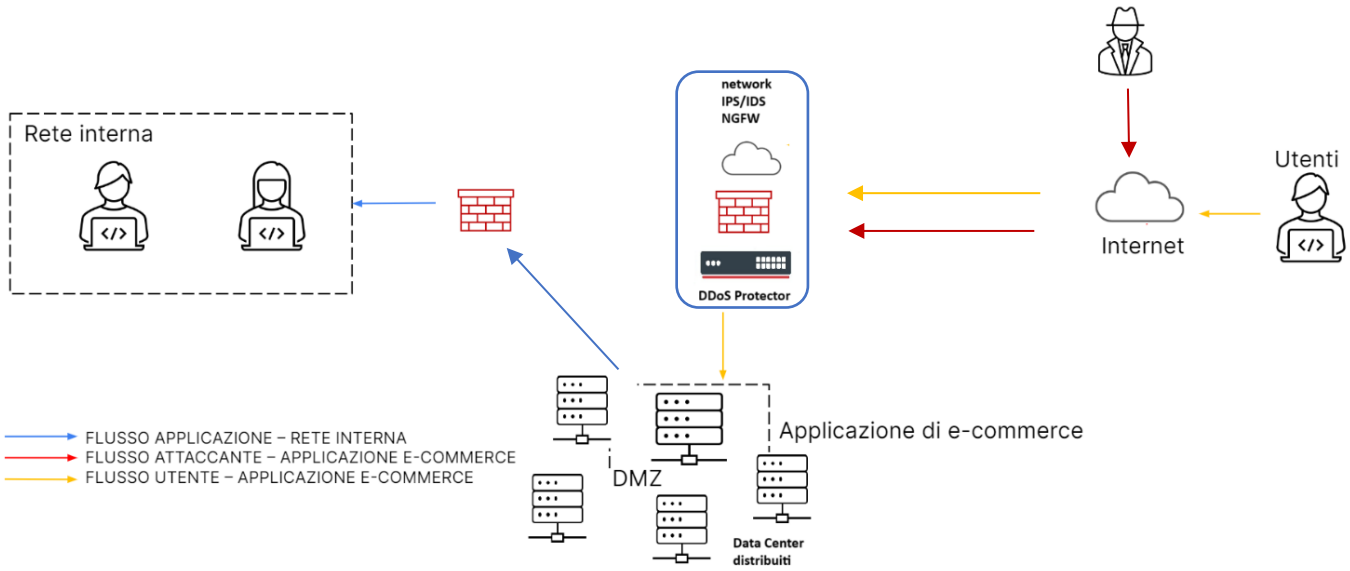
il malintenzionato riuscisse a connettersi alla web app non potrebbe infettare il resto della rete essendo stata isolata.



4 Nella Soluzione completa abbiamo due firewall in modo da segmentare la reta inoltre un eventuale attaccante che dovesse riuscire a superare il primo firewall per accedere al server DMZ troverebbe un secondo firewall per accedere alla rete interna che settato correttamente blocca le connessioni indesiderate.



5 Vediamo infine quello che potrebbe essere una modifica della rete con l’aggiunta di un hardware DDoS protector, di un ulteriore firewall che segmenti la rete e che preveda la distribuzione dei servizi e dei server su più data center.


Rete interna
network
IPS/IDS
NGFW
DDoS Protector
Internet
Utenti
Applicazione di e-commerce
DMZ
Data Center
distribuiti
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE