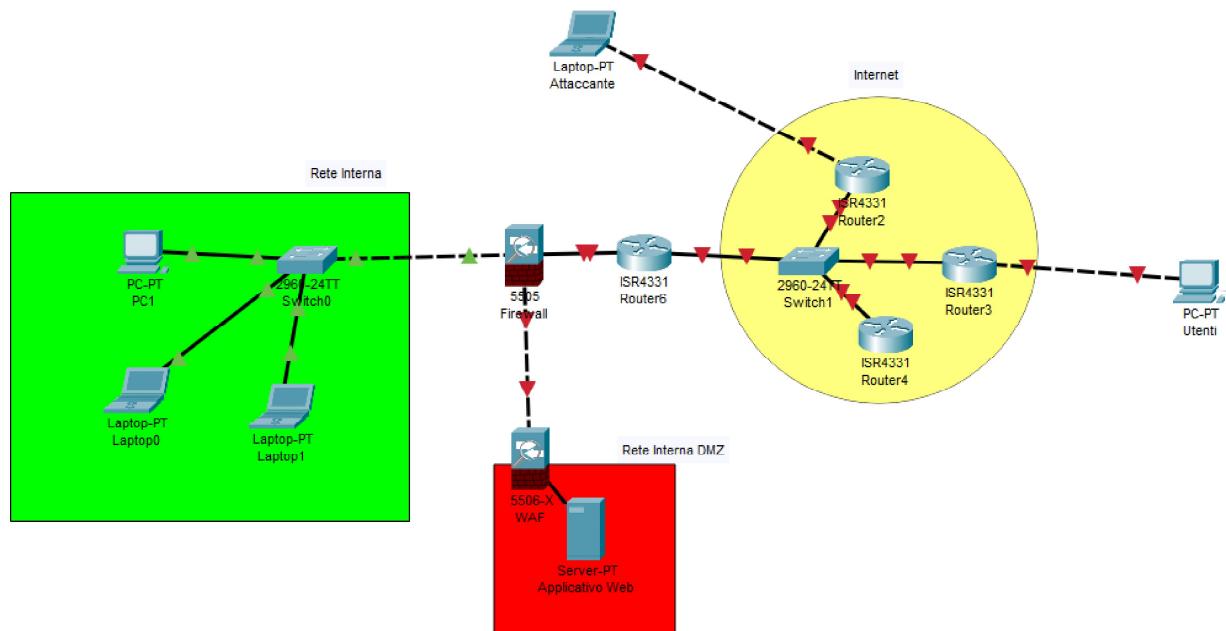


Risoluzione:

Azioni preventive

Per difendere l'applicazione Web da attacchi di tipo SQLi e XSS, si possono implementare le seguenti azioni preventive:

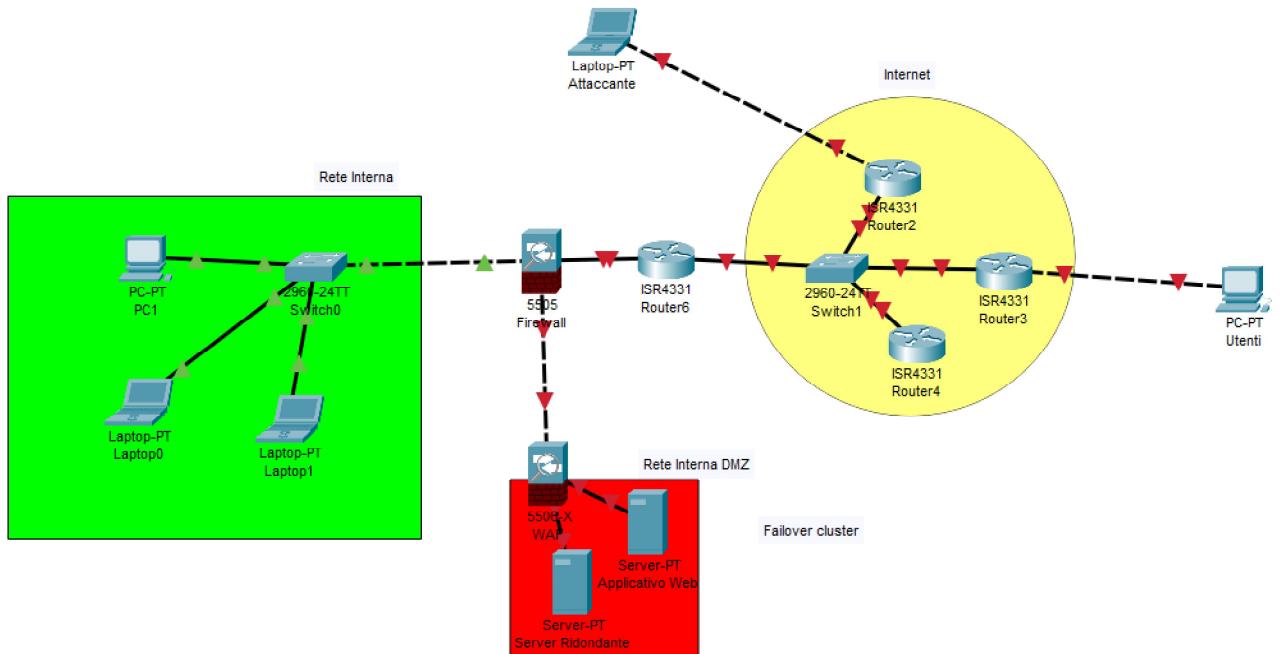
- ❖ Validazione dei dati in input: tutti i dati inseriti dall'utente devono essere validati, filtrati e sanificati, in modo da evitare l'inserimento di stringhe malevoli.
- ❖ Utilizzo di parametri preparati per le query SQL: l'applicazione dovrebbe utilizzare parametri preparati per le query SQL invece di concatenare i valori direttamente nelle query, in modo da prevenire attacchi di tipo SQLi.
- ❖ CSRF: i token CSRF (Cross-Site Request Forgery) vengono utilizzati per evitare che un attaccante possa sfruttare la sessione di un utente per eseguire azioni malevoli.
- ❖ Inserimento di un apposito WAF prima del server per gestire meglio eventuali attacchi



Impatti sul business

In caso di attacco Ddos, considerando in media una spesa media al minuto di 1.500 €, un downtime di 10 minuti causerebbe una perdita di circa 15.000€

Per ridurre l'impatto si potrebbe inserire nel architettura un ulteriore server (ridondanza) da attivare nel caso il primo venga attaccato, così da garantire la business continuity e quindi limitare il danno.



Response

Isolare immediatamente la macchina infetta: è importante limitare l'accesso della macchina infetta alla rete interna per prevenire la propagazione del malware.

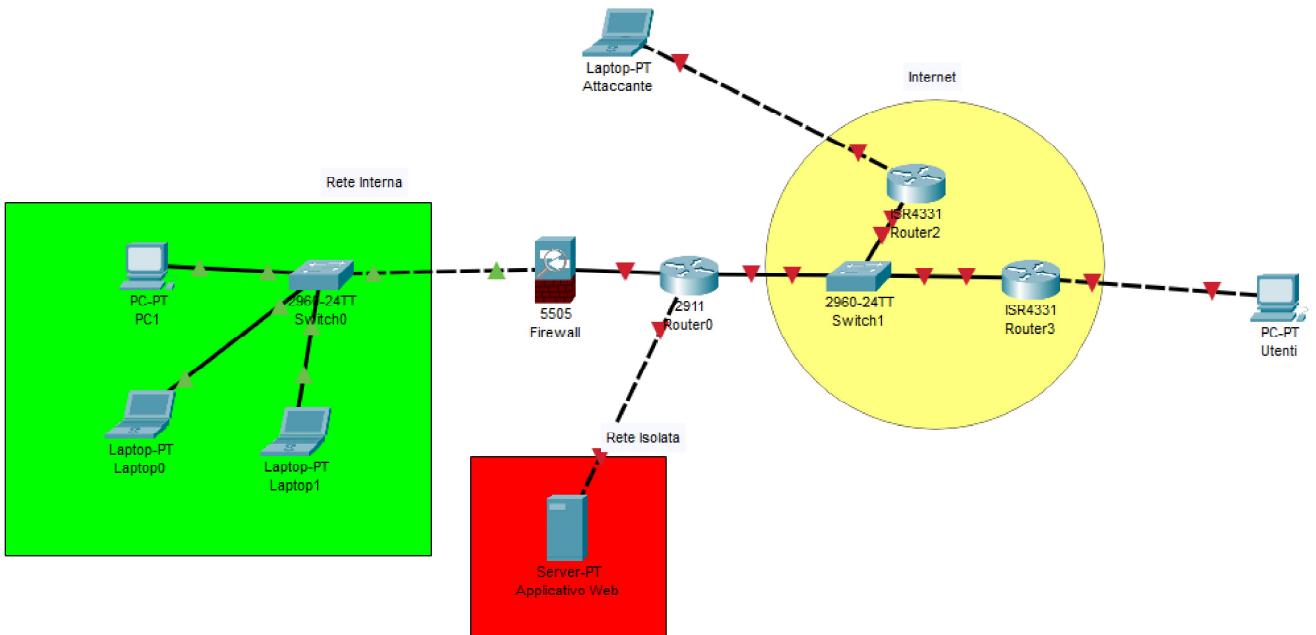
In questo caso, potrebbe essere necessario limitare l'accesso solo alla rete DMZ, impedendo l'accesso ad altre parti della rete interna.

Potremmo non voler rimuovere la connessione remota al attaccante per poter studiare le sue mosse.

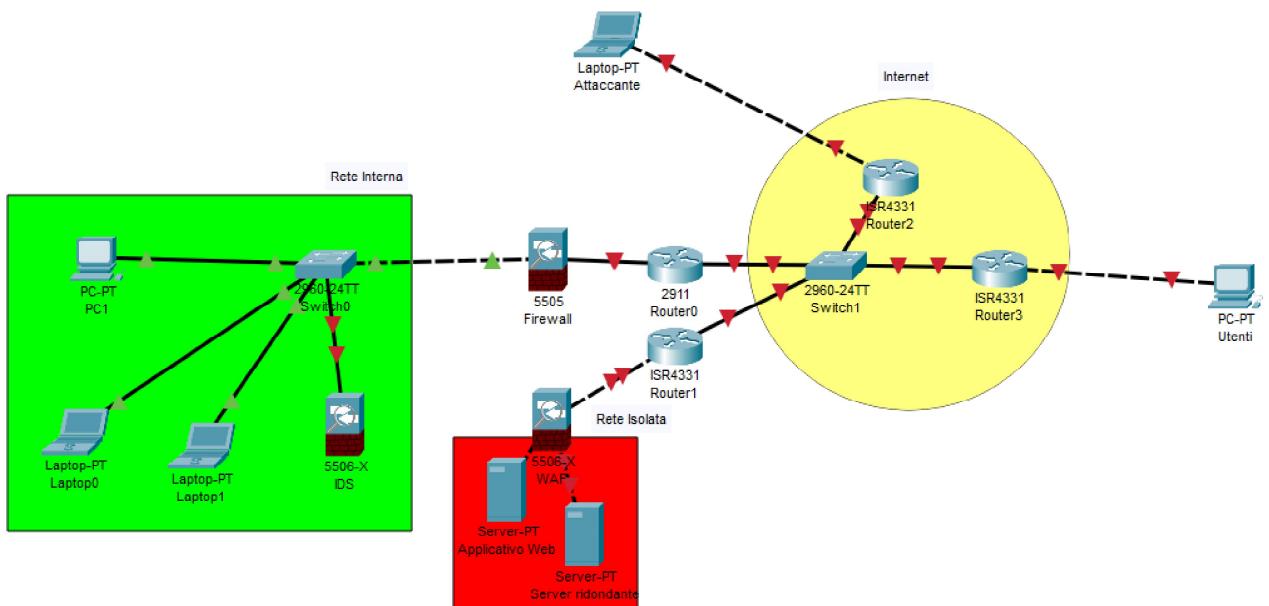
Analisi del malware: una volta isolata la macchina infetta, si dovrebbe procedere all'analisi del malware per capire come è entrato e quali sono i danni che ha causato. Questo aiuterà a prendere decisioni informate su come procedere.

Rimozione del malware: una volta che il malware è stato analizzato, viene rimosso dalla macchina infettata.

Pulizia e ripristino: infine, sarà necessario procedere alla pulizia della macchina infetta e al ripristino della sua configurazione precedente per evitare ulteriori danni.



Architettura di rete alternativa



L'architettura in questo caso proposta, isolerebbe la rete del applicativo web da quella interna in modo da non comprometterla in caso di attacco, si usa poi un altro provider per la rete del Server web.

Viene aggiunto poi un IDS alla rete interna per aumentarne la sicurezza.

Inoltre integra le soluzioni precedentemente proposte.