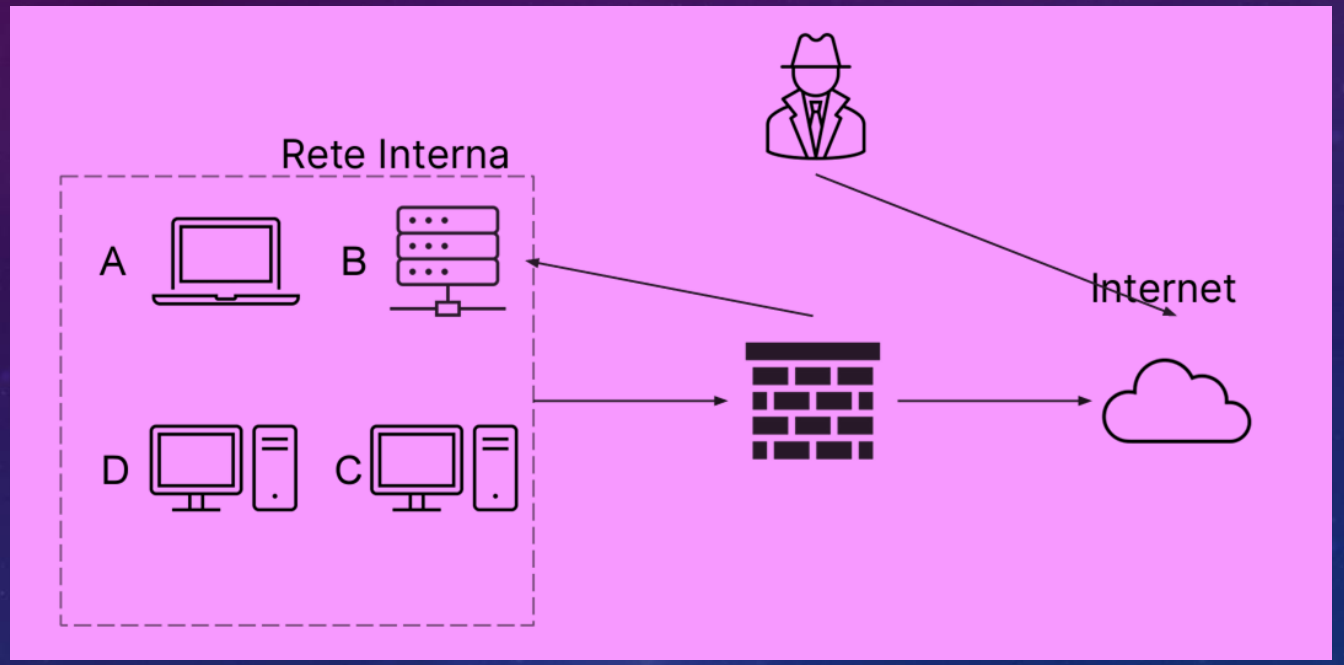
INCIDENT RESPONSE

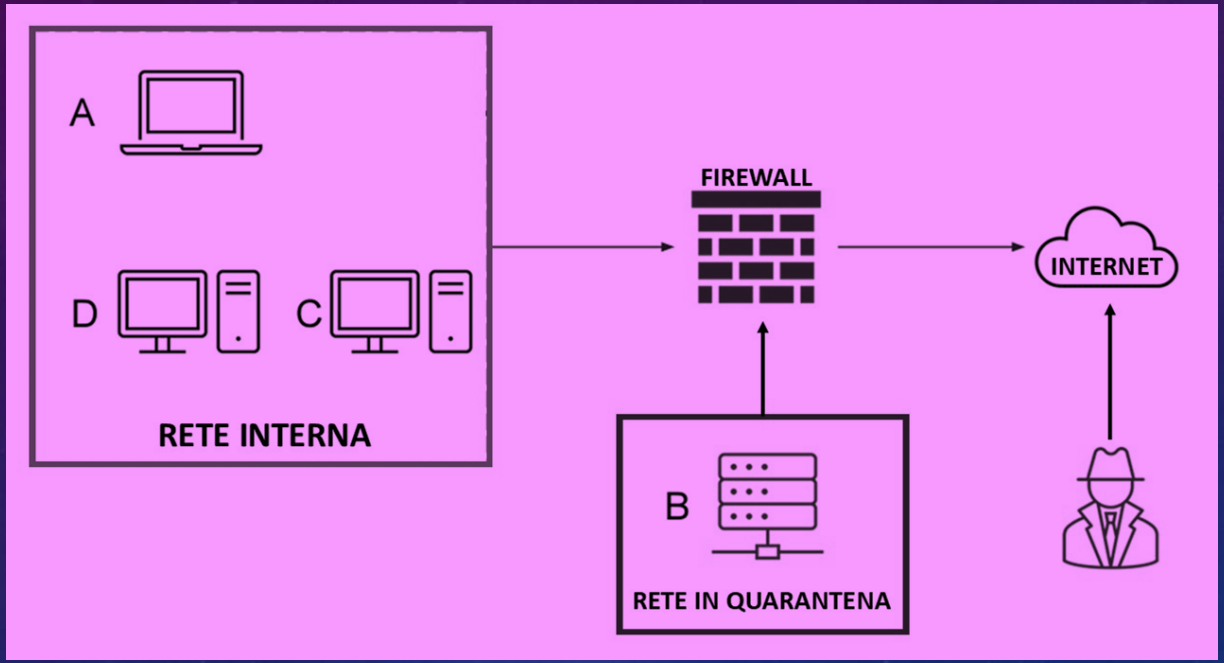
ESERCIZIO S9/L4

Il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante, che è riuscito a bucare la rete ed accedere al sistema tramite internet.
L'attacco è attualmente in corso.



- Per completare l'esercizio di oggi, andiamo a mostrate le tecniche di: Isolamento e di Rimozione del sistema B infetto
- Vediamo la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

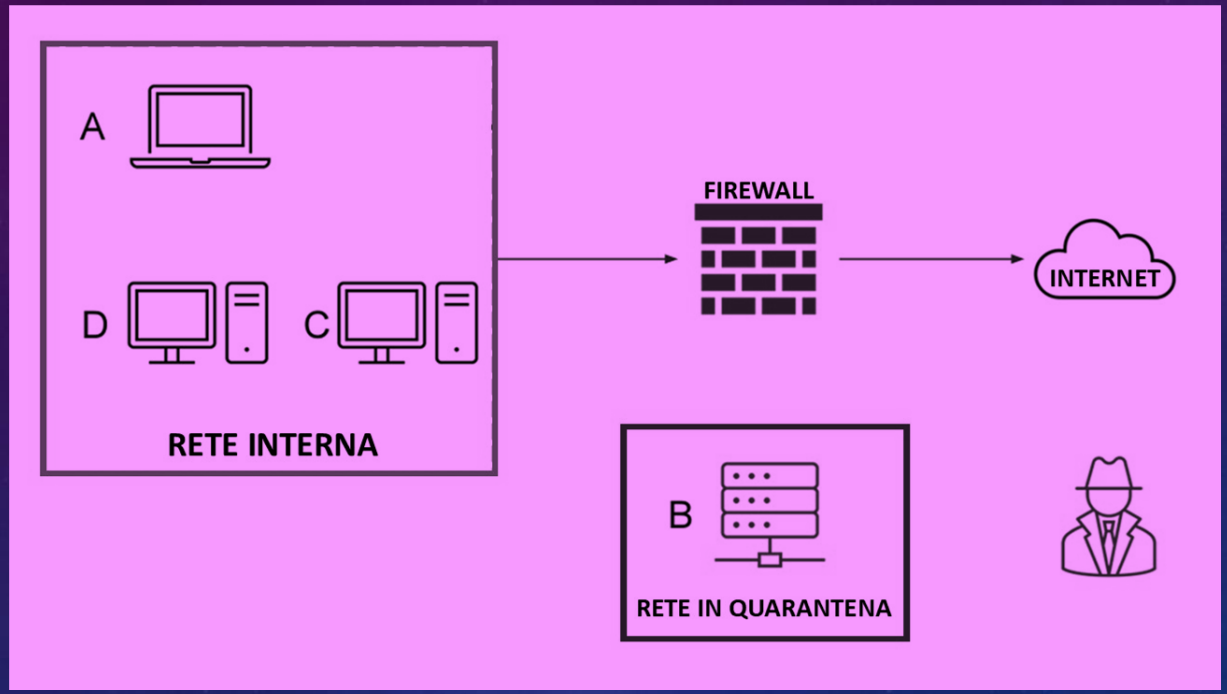
ISOLAMENTO DEL SISTEMA INFETTO «B»



L’isolamento permette di isolare un sistema infetto limitando l’accesso alla rete interna.

Il sistema però sarà ancora accessibile via internet.

RIMOZIONE DEL SISTEMA INFETTO «B»



La rimozione permette di eliminare completamente il sistema dalla rete,
rendendolo inaccessibile sia dalla rete interna che da internet.
In questo modo l'attaccante non avrà nemmeno l'accesso al sistema infetto.

DIFFERENZA TRA PURGE E DESTROY

- Purge impiega sia metodi logici che fisici per eliminare definitivamente i dati da un dispositivo di archiviazione, senza distruggere l'hardware. Le tecniche fisiche utilizzate non danneggiano l'hardware ma garantiscono l'irrecuperabilità dei dati.

- Destroy, invece, utilizza tecniche fisiche molto aggressive per rendere i dati inaccessibili, arrivando anche alla distruzione dell'hardware stesso. Questo metodo è preferito per eliminare definitivamente un dispositivo non più utilizzabile, anche se comporta costi più elevati.