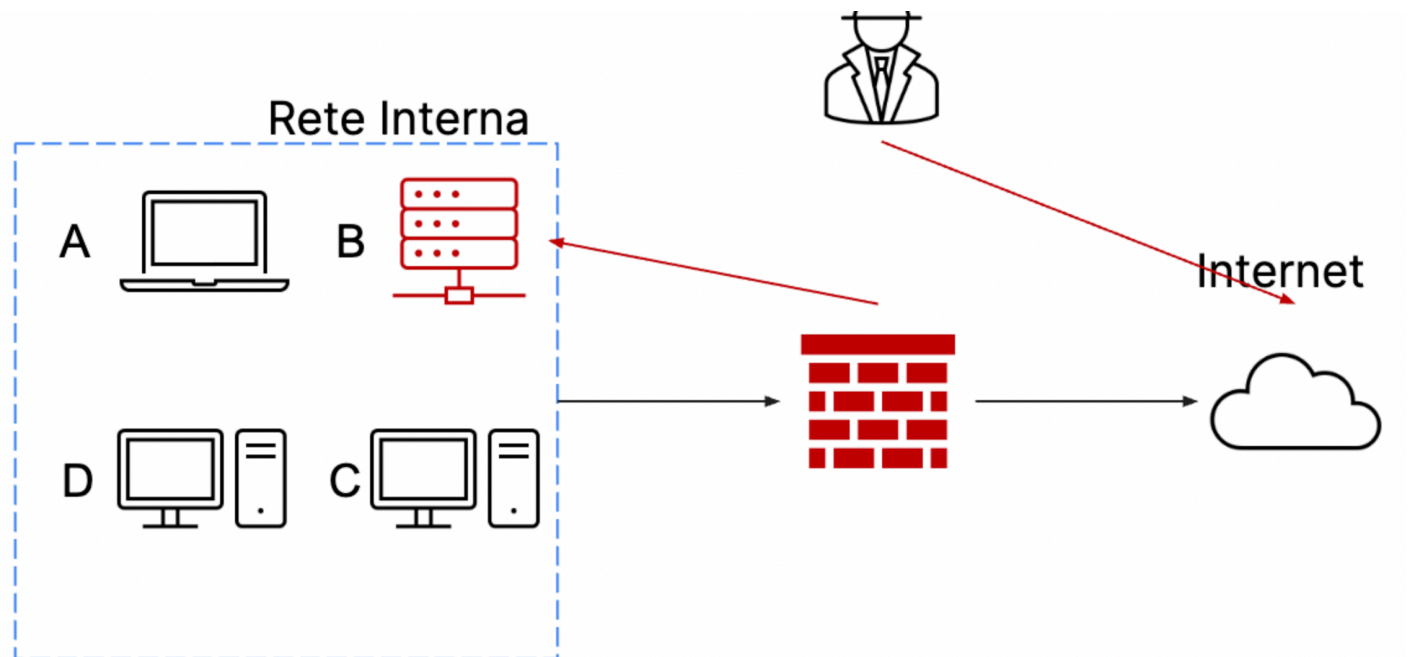
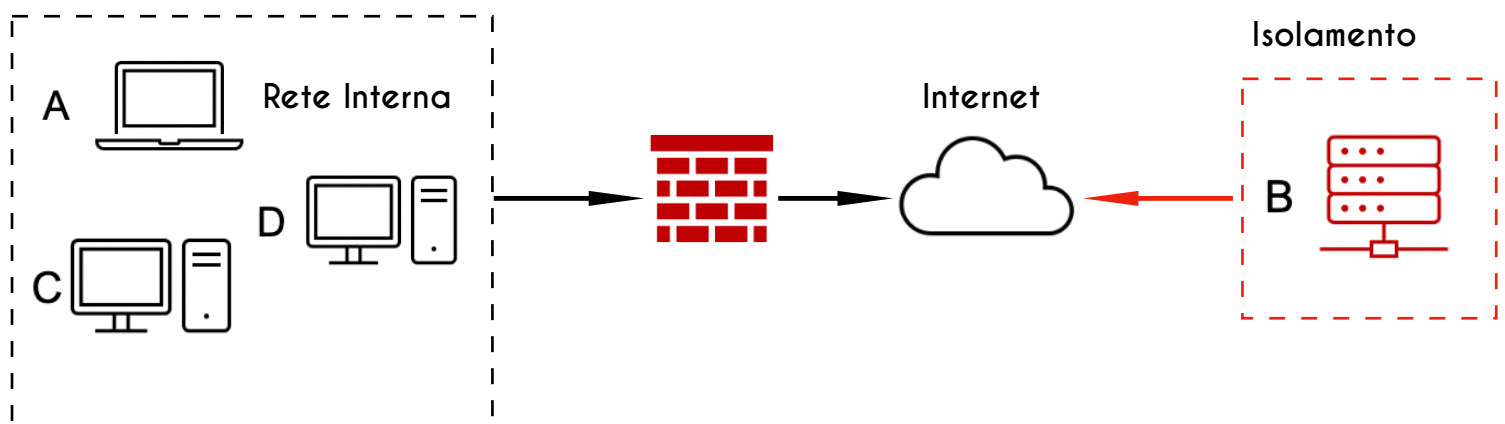


Esercizio G4

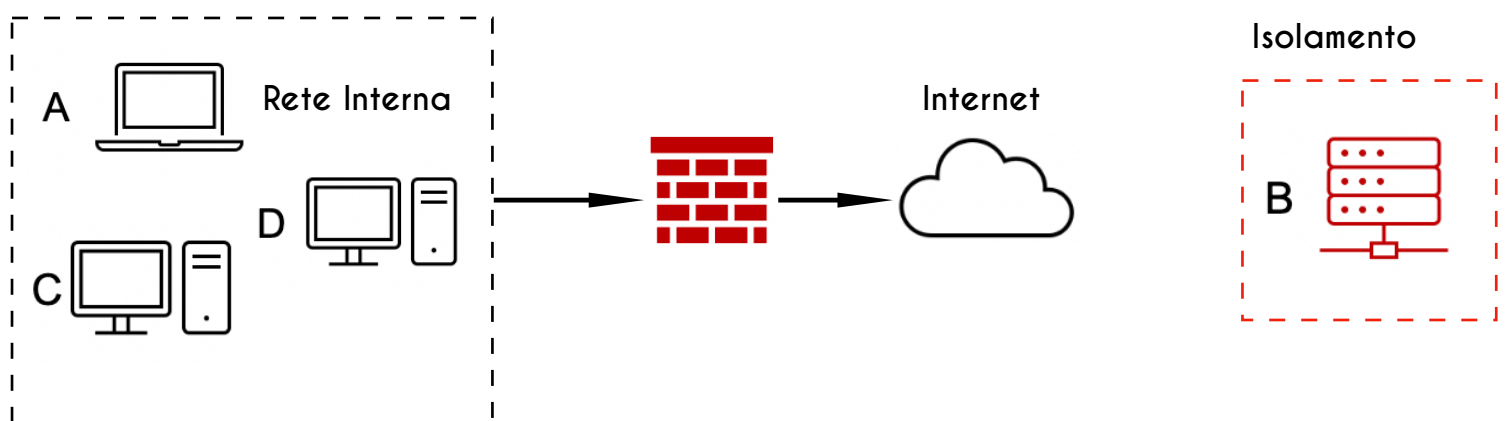
Database compromesso interamente da un attacco che è riuscito a bucare la rete ed accedere al sistema tramite internet.



Con questo isolamento andiamo a disconnettere il database compromesso dalla nostra rete interna.



Dato che questo non è sufficiente, andiamo a isolare completamente il database. Rimuovendo l'accesso anche da internet, così da bloccare/fermare l'attacco.



A questo punto si vanno a rimuovere eventuali malware o backdoor che ci possono essere.

Destroy: rende i dati inaccessibili perché vengono usati metodi di distruzione fisica.

Purge: Viene usato per lo più, per eliminare i contenuti a livello logico.