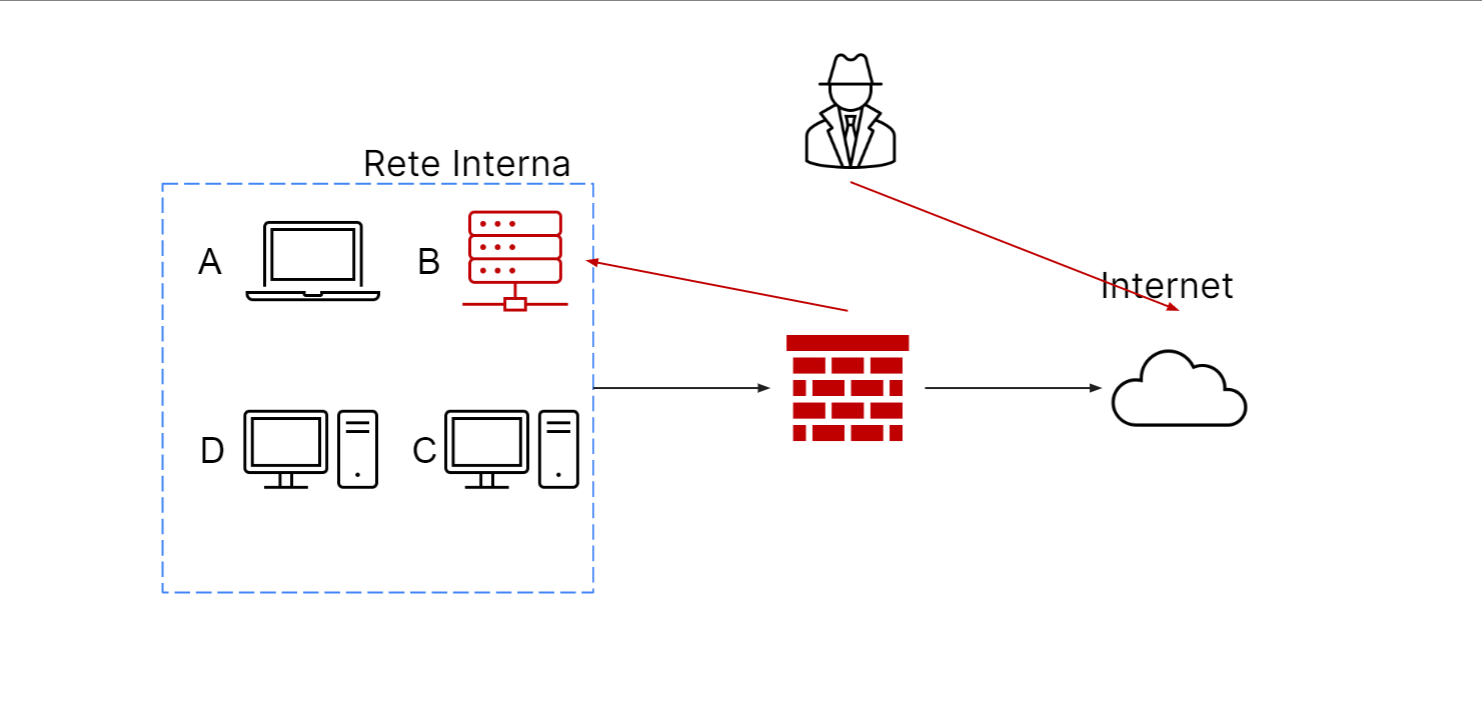
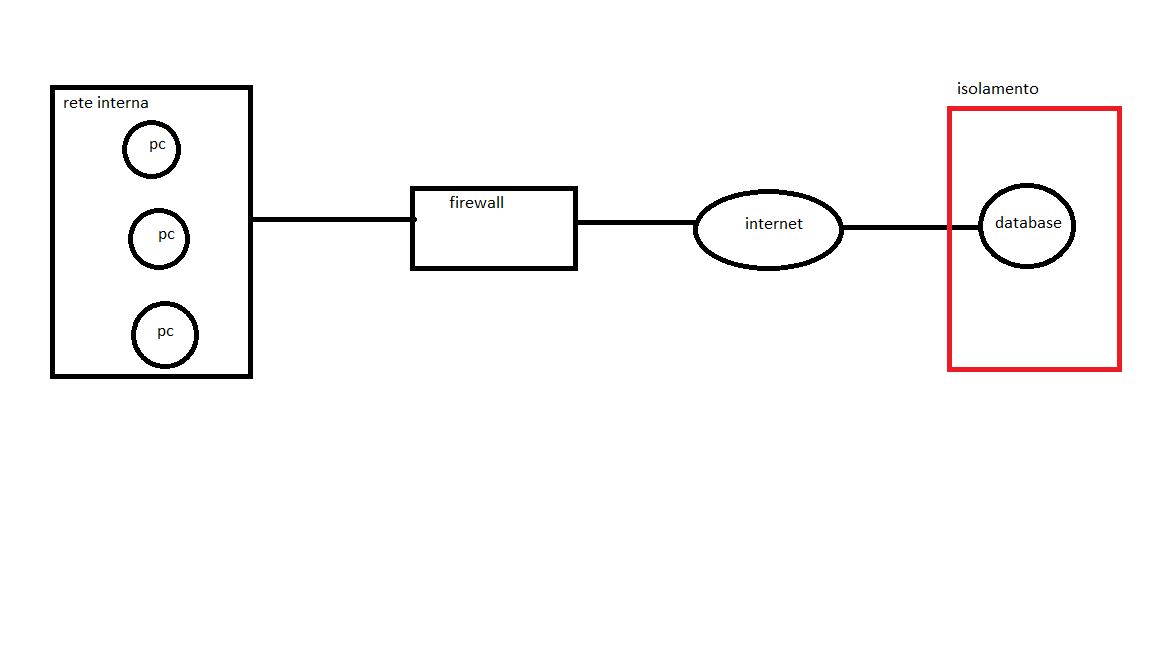
# Incident response

Data questa situazione dobbiamo usare delle tecniche per rimediare alla situazione.

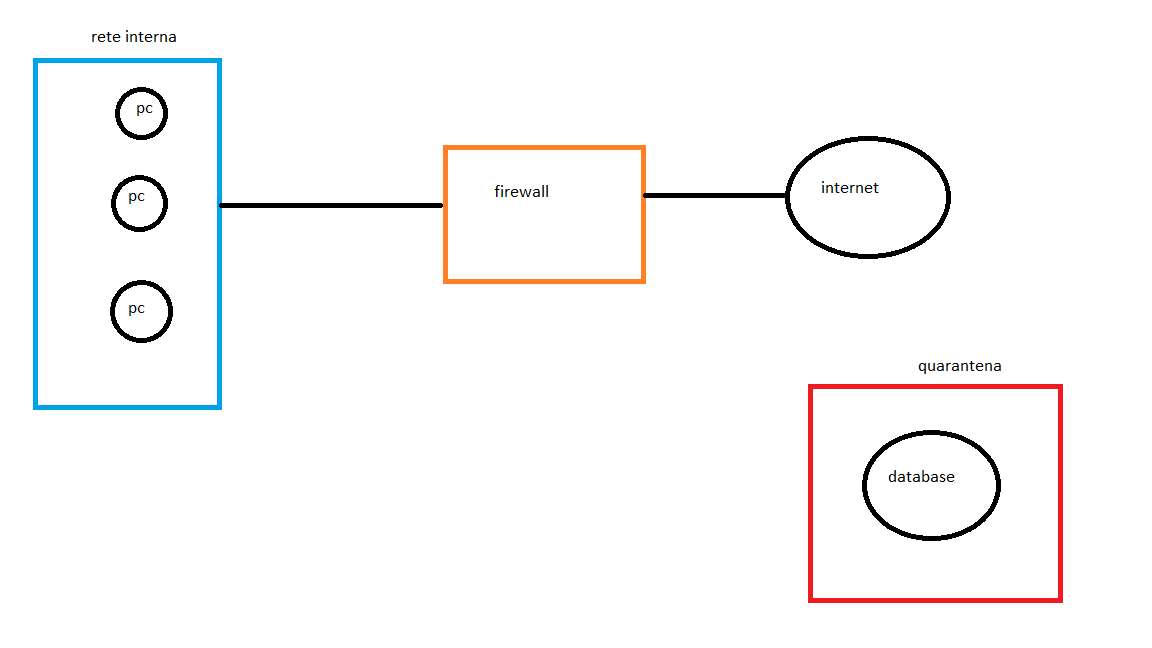


Tecnica di isolamento



La prima tecnica che si può usare è quella dell’isolamento, cioè la disconnessione del sistema infetto dalla rete interna, ma non da internet. Questa tecnica viene usata nel caso bisogni indagare sull’attaccante e scoprire informazioni su di lui.

Tecnica di rimozione



Nel caso in cui si voglia solo eliminare la minaccia si procede con la rimozione, ovvero la macchina viene rimossa sia dalla rete interna che da internet.

Rimozione informazioni

Per eliminare i dati sensibili si possono utilizzare 2 tecniche:

* **Purge** – i dati vengono eliminati oltre che in maniera logica, anche in maniera fisica mediante l’uso di magneti per rendere i dati inaccessibili.
* **Destroy** – questa tecnica è la più completa per eliminare i dati, poiché oltre alle tecniche logiche e fisiche si utilizza anche la disintegrazione e polverizzazione ad alte temperature.

Entrambe le situazioni dipendono molto dalla disponibilità economica dell’azienda, dal tempo a disposizione e dalle necessità perché a seconda di quale si usi cambiano.