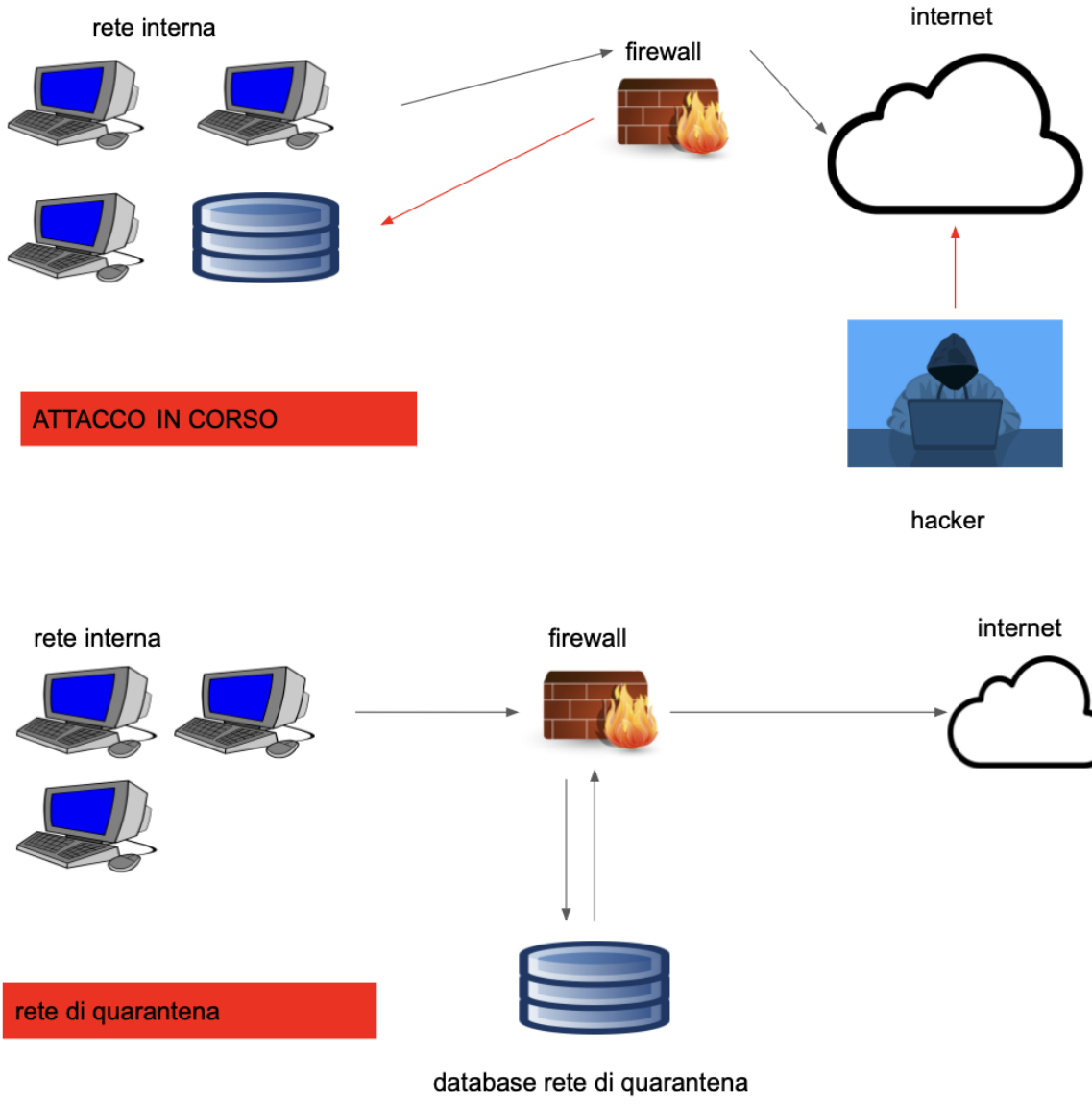
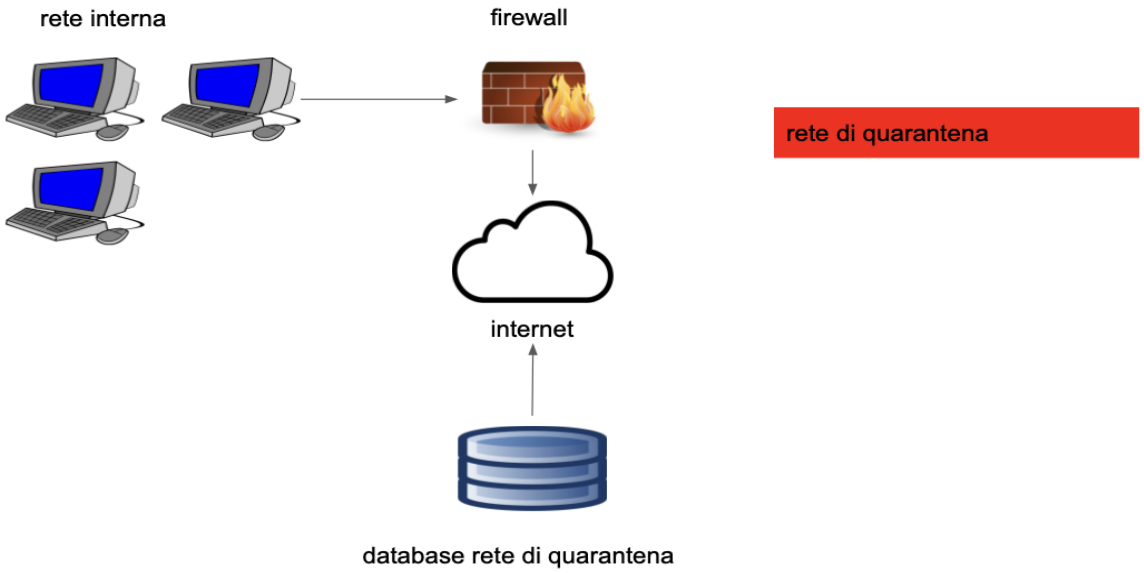
Incident response

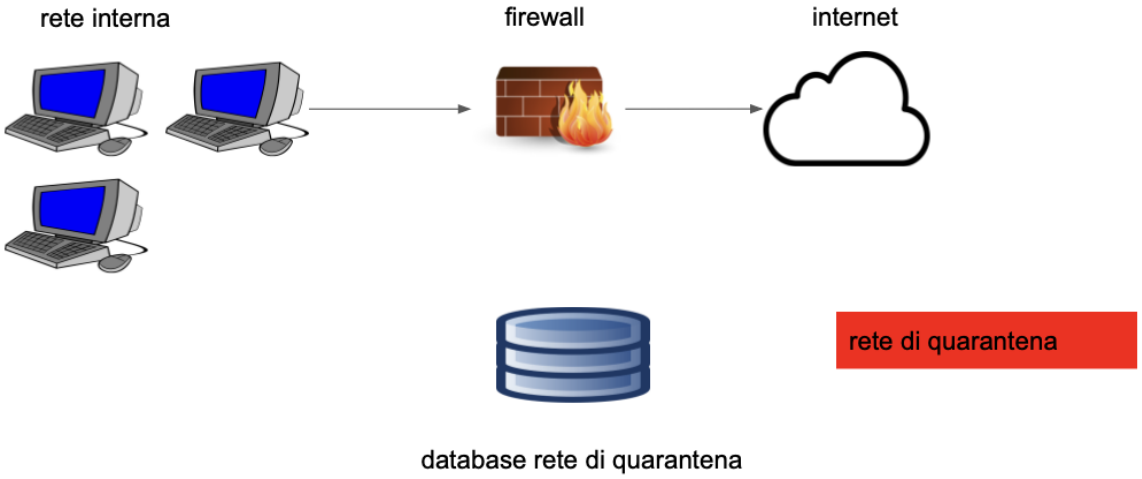
In figura il **database** con diversi dischi per lo storage è stato compromesso da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. l'attacco è ancora in corso e l'esercizio chiede di mostrare le tecniche di **isolamento** e **rimozione** del sistema infetto.

Spiega le differenze tra **Purge**, **Destroy** e **Clear**





Ci sono casi in cui l'isolamento non è abbastanza, in questo caso si procede con la rimozione del sistema dalla rete interna e da internet



Clear → Cancellazione o eliminazione dei dati in modo che non siano più visibili o accessibili agli utenti
Non implica l'eliminazione irreversibile dei dati
Purge → Si riferisce all'eliminazione completa dei dati in modo da renderli irrecuperabili. (eliminazione, sovrascrizione)
Destroy → Va oltre l'eliminazione e comporta la distruzione fisica degli oggetti stessi come ad esempio un disco rigido
La distruzione è irreversibile non rendendo possibile il recupero dei dati e il ripristino degli oggetti distrutti