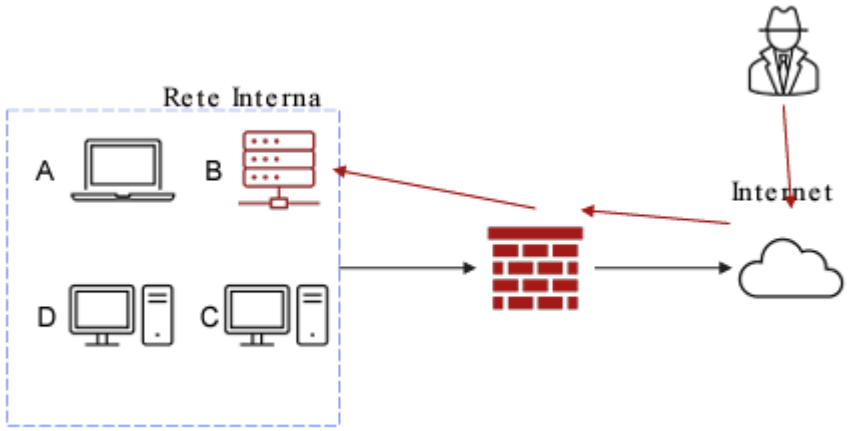
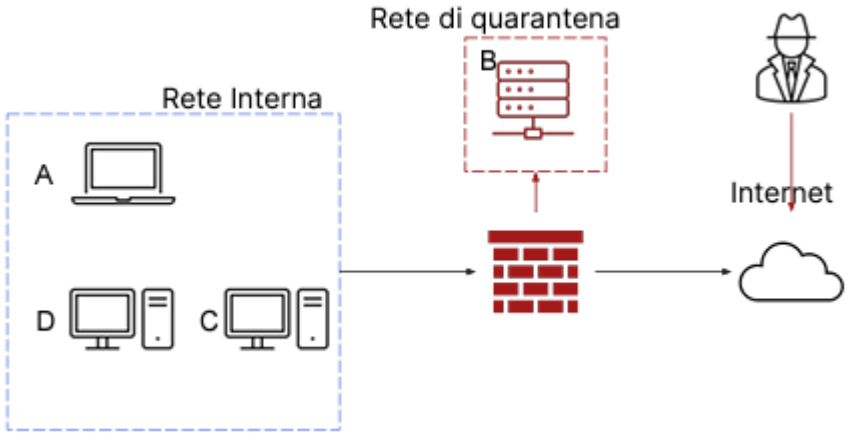
Con riferimento alla figura in slide 4, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L'attacco è attualmente in corso e siete parte del team di CSIRT.



La tecnica di isolamento consente di confinare un sistema compromesso, limitando l'accesso dell'attaccante alla rete interna. Tuttavia, il sistema infetto rimarrà comunque accessibile all'attaccante attraverso Internet.



La tecnica di rimozione prevede l'eliminazione totale del sistema dalla rete, rendendolo inaccessibile sia dalla rete interna che da Internet. Questo metodo impedisce all'attaccante di accedere al sistema compromesso e limita ulteriormente il suo accesso alla rete interna.

Purge: Questa metodologia prevede l'adozione di misure sia logiche che fisiche per la rimozione definitiva dei dati da un disco o dispositivo di storage. Le tecniche fisiche impiegate non sono invasive e non comportano la distruzione dell'hardware.

Destroy: Questa tecnica impiega metodi fisici altamente invasivi per rendere inaccessibili i dati su un disco o dispositivo di storage. Alcuni dei metodi utilizzati comportano la distruzione completa dell'hardware, rendendo impossibile il recupero sia del dispositivo che delle informazioni in esso contenute. È la soluzione preferita quando si desidera smaltire un disco che non sarà più riutilizzato, ma è anche la più costosa.