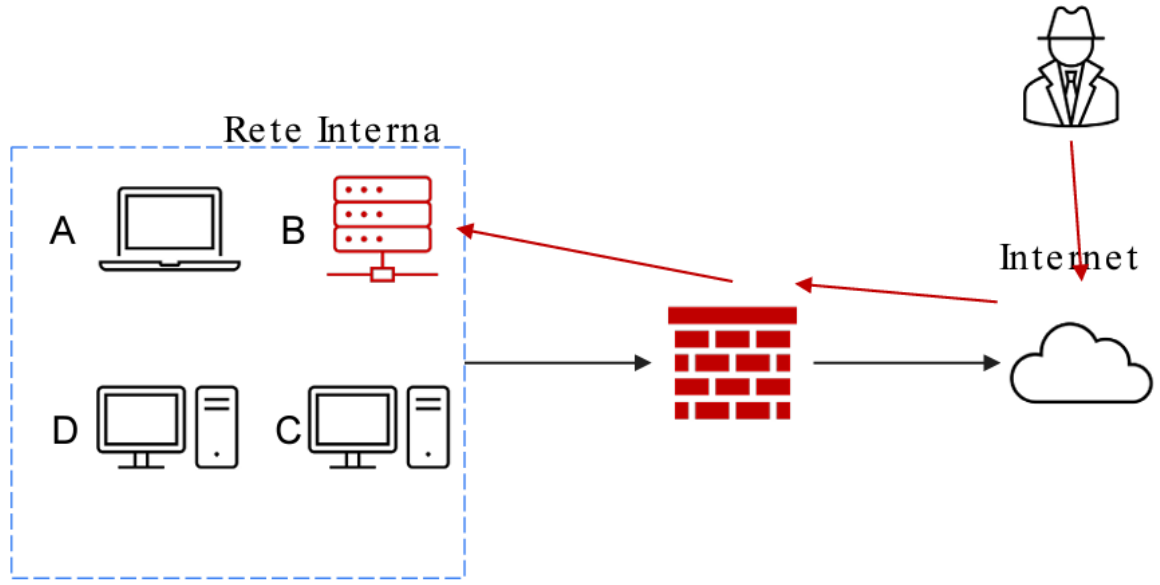
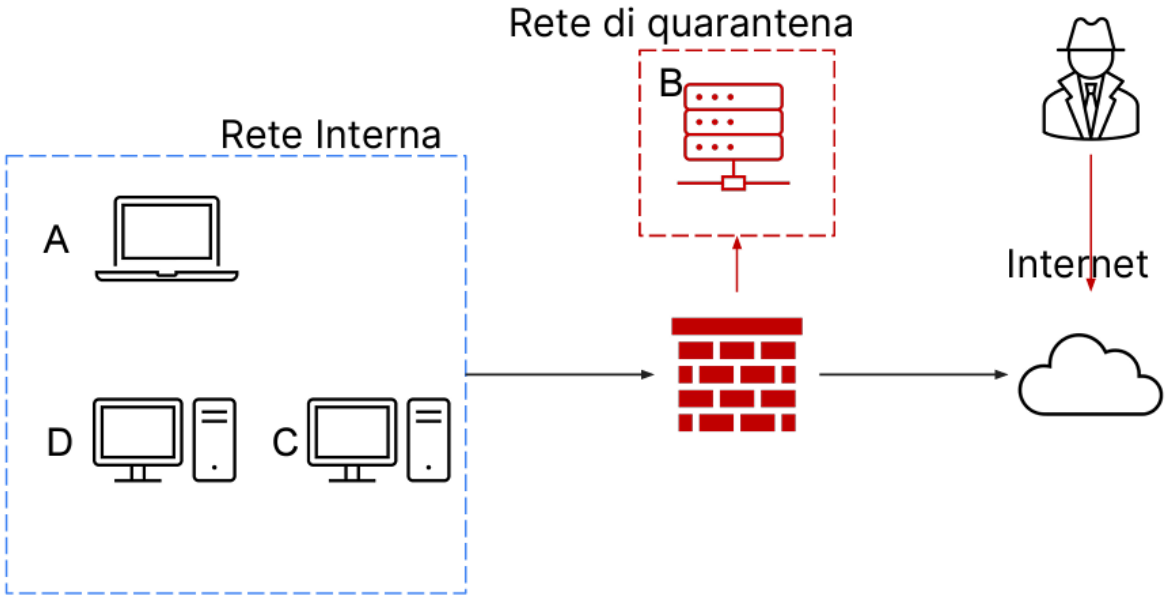
Con riferimento alla figura, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.



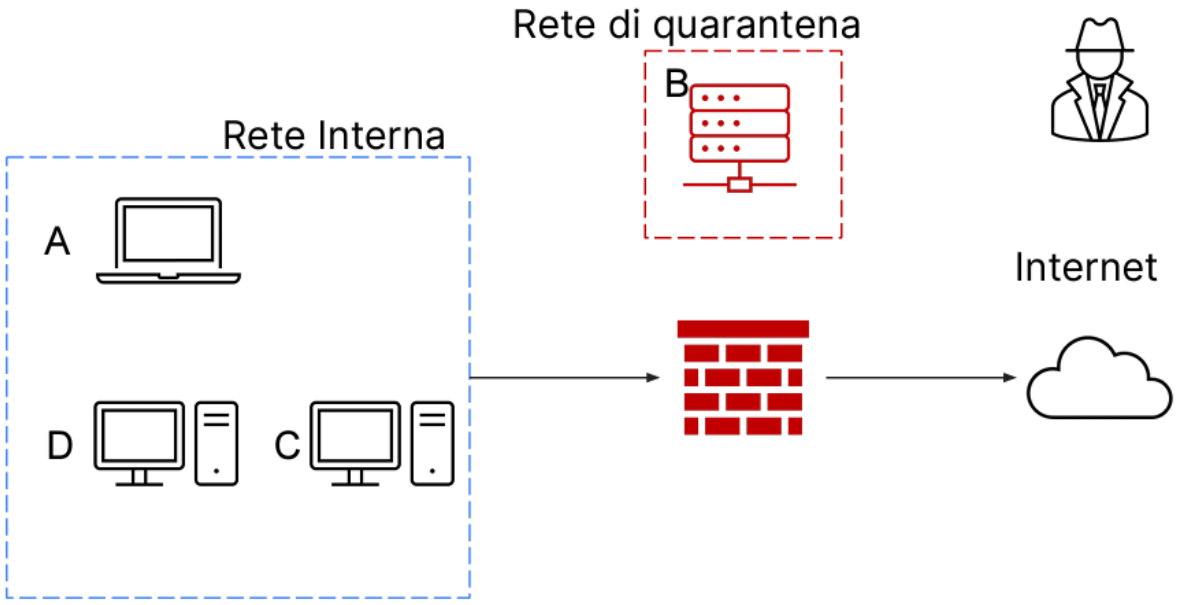
TECNICA DI ISOLAMENTO

La tecnica di isolamento permette di isolare un sistema infetto restringendo l'accesso dell'attaccante alla rete interna. Tuttavia, il sistema infetto sarà ancora accessibile dall'attaccante via internet



TECNICA DI RIMOZIONE

La tecnica di Rimozione elimina completamente il sistema dalla rete, di fatto rendendolo inaccessibile sia da rete interna che da internet. Questo approccio restringe l'accesso alla rete interna da parte dell'attaccante che non avrà nemmeno più accesso al sistema infetto.



Generalmente, possiamo individuare tre opzioni per la gestione dei media contenenti informazioni sensibili:

• Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempiounapproccioditiporeadandwritedoveilcontenutovienesovrascrittopiùe più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale;

• Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi;

• Destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.