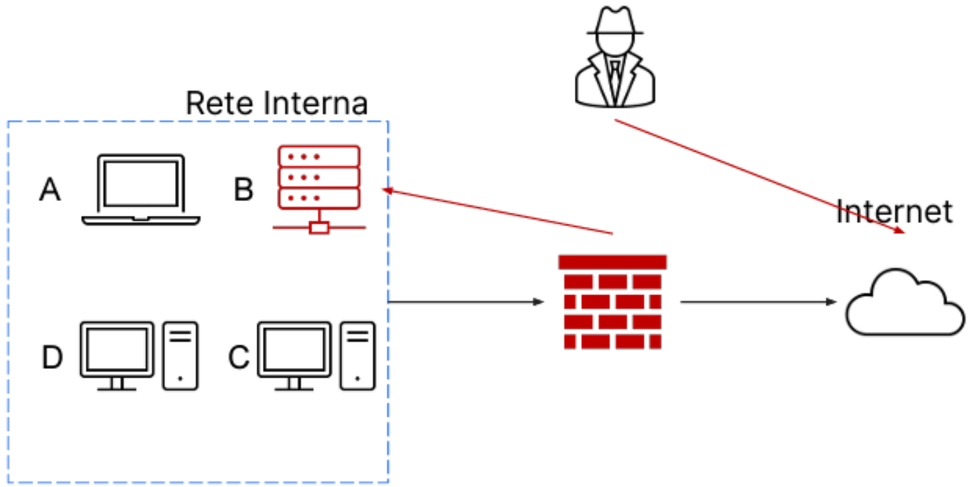
S9/L4 TRACCIA

Con riferimento alla figura sotto, 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.
Rispondere ai seguenti quesiti. Mostrate le tecniche di:

I) Isolamento
II) Rimozione del sistema B infetto

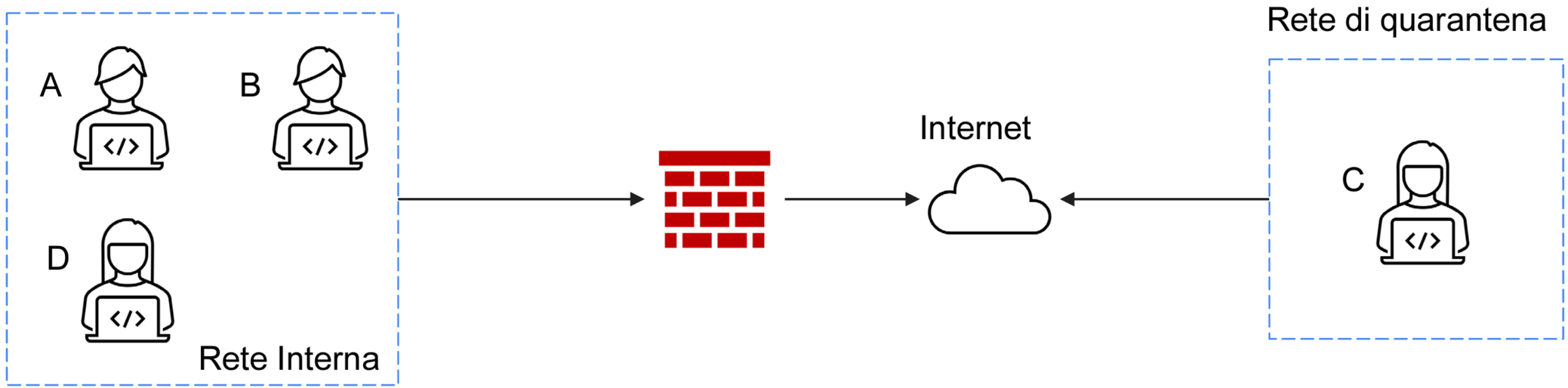
Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



ISOLAMENTO

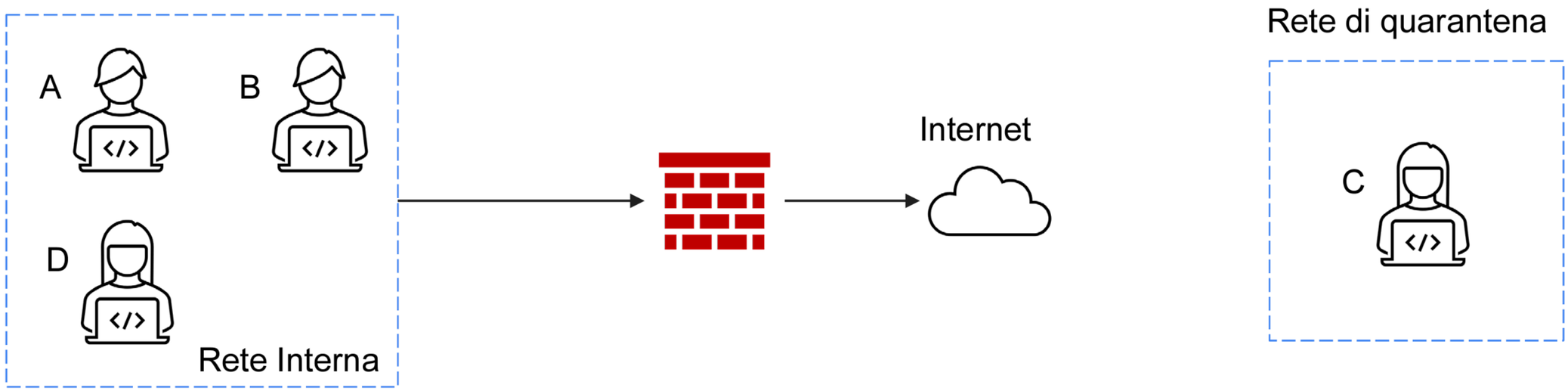
Quando è necessario un contenimento maggiore dei danni da parte di un attacco, si utilizza la tecnica dell'isolamento, mostrato nella figura di seguito. L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.Notare che in questo scenario l'attaccante ha ancora accesso al sistema C tramite internet.

Perchè isolarlo e non staccarlo completamente ? Si attua questa pratica di isolamento per continuare a tenere traccia delle azioni da parte dell'attaccante, non "staccandolo" completamente dalla rete lui stesso crederà di essere ancora dentro permettendoci così tempo di manovra per capire cosa effettivamente volesse attaccare.



RIMOZIONE

Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet. In quest'ultimo scenario, l'attaccante non avrà né accesso alla rete interna né tanto meno alla macchina infettata.”



PURGE - DESTROY

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

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 maggior sforzo in termini economici.