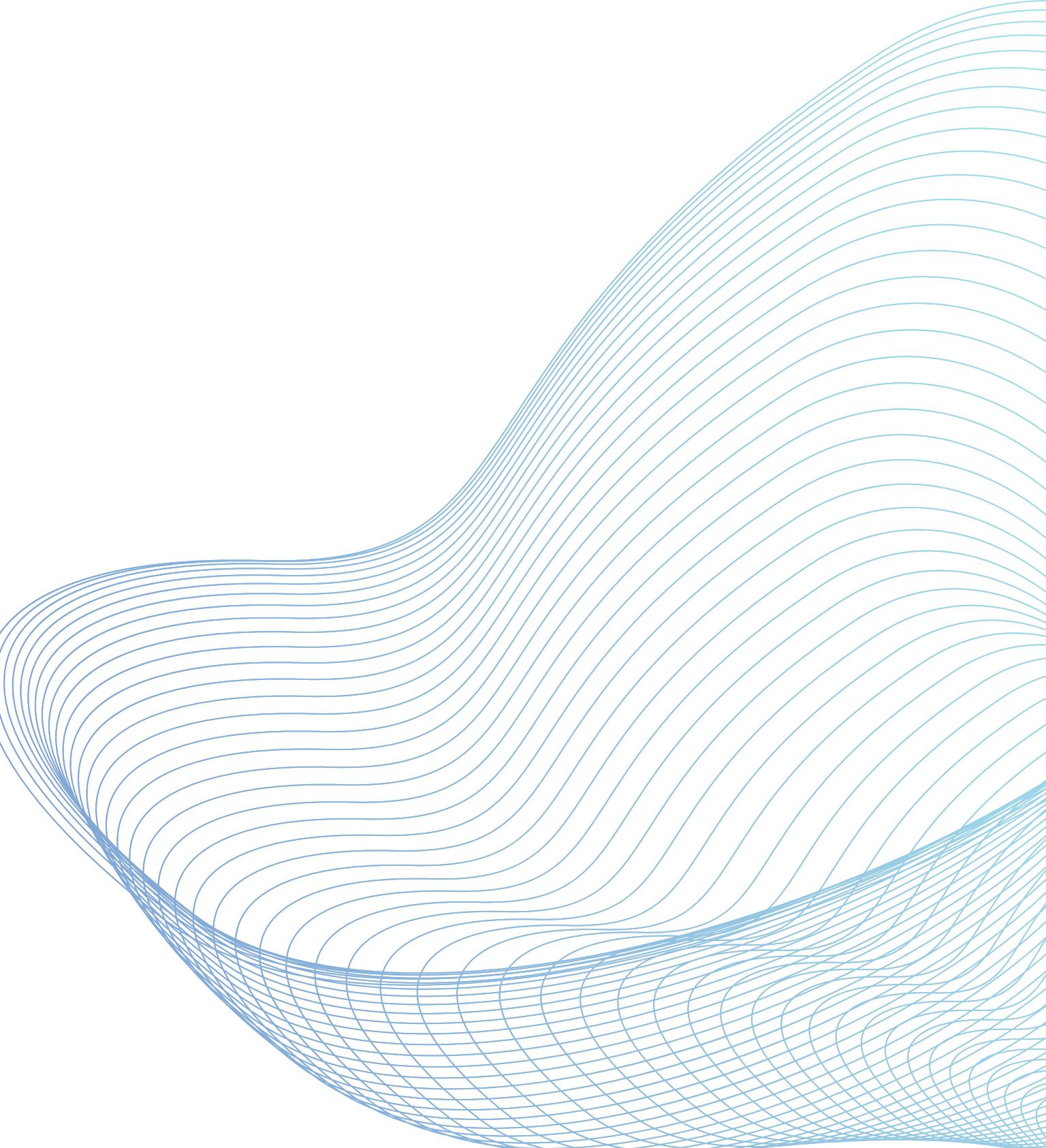


CONSEGNA

S9/L4

di Giuseppe Lupoi



INDICE

3 - Traccia

4 - Slide della pratica

5 - 1° Tecnica - Isolamento

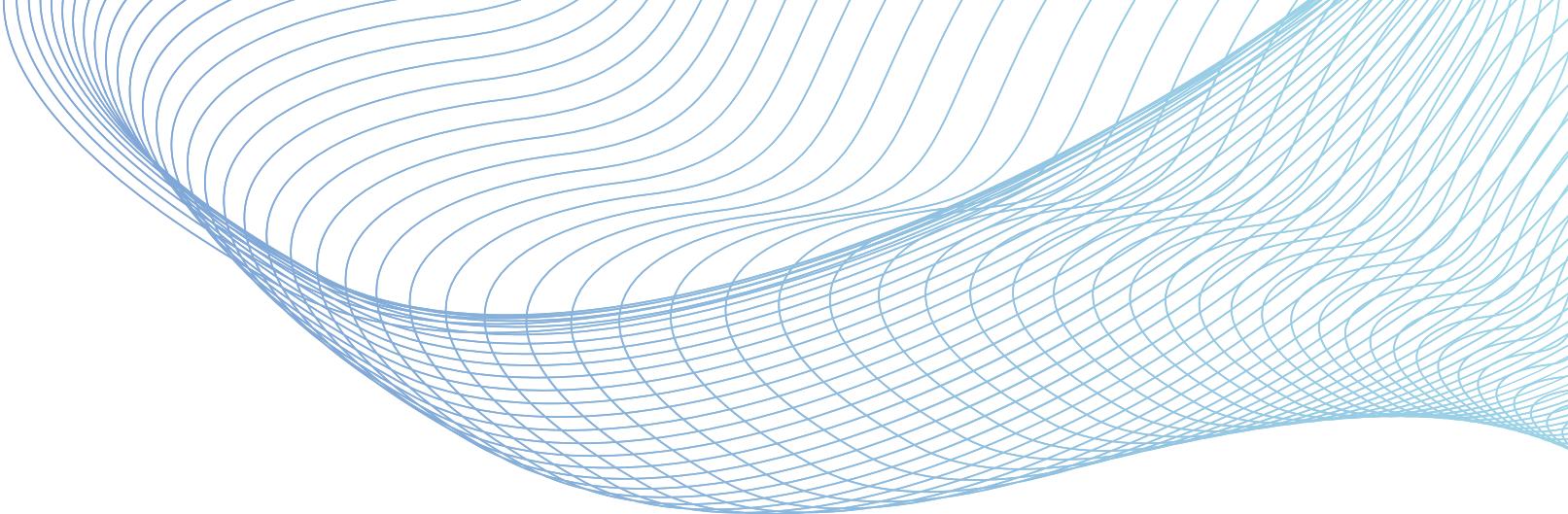
6 - Schema di rete con Isolamento

7 - 2° Tecnica - Rimozione

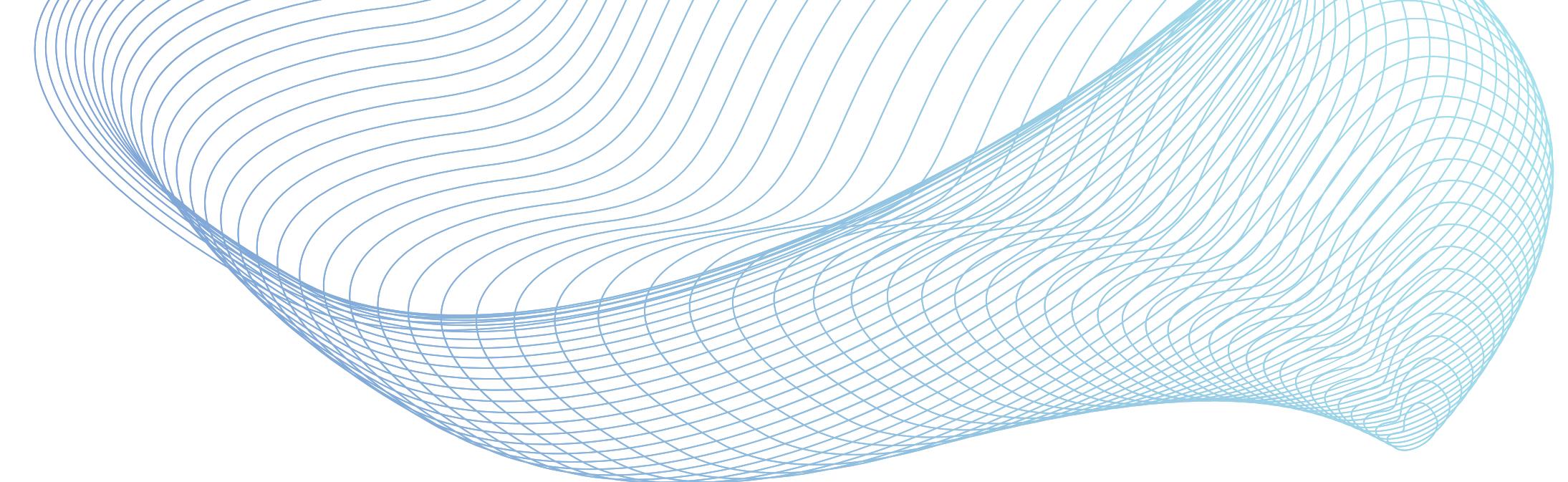
8 - Schema di rete con Rimozione

9 - Metodo Purge

10 - Metodo Destroy

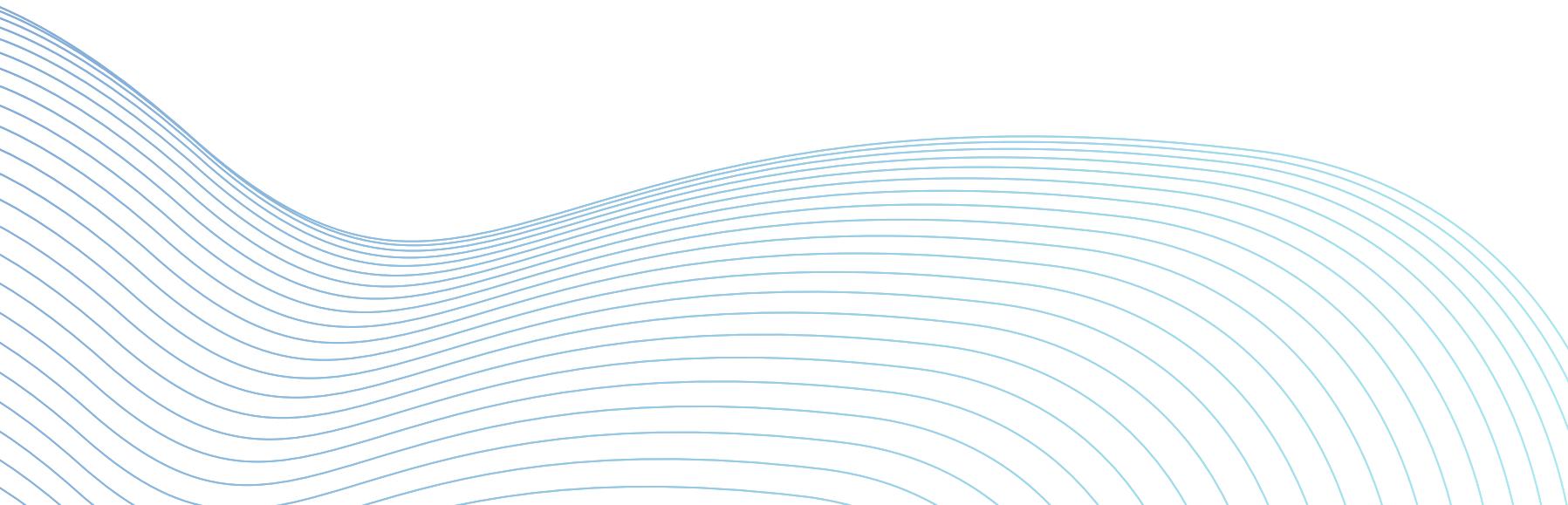


TRACCIA

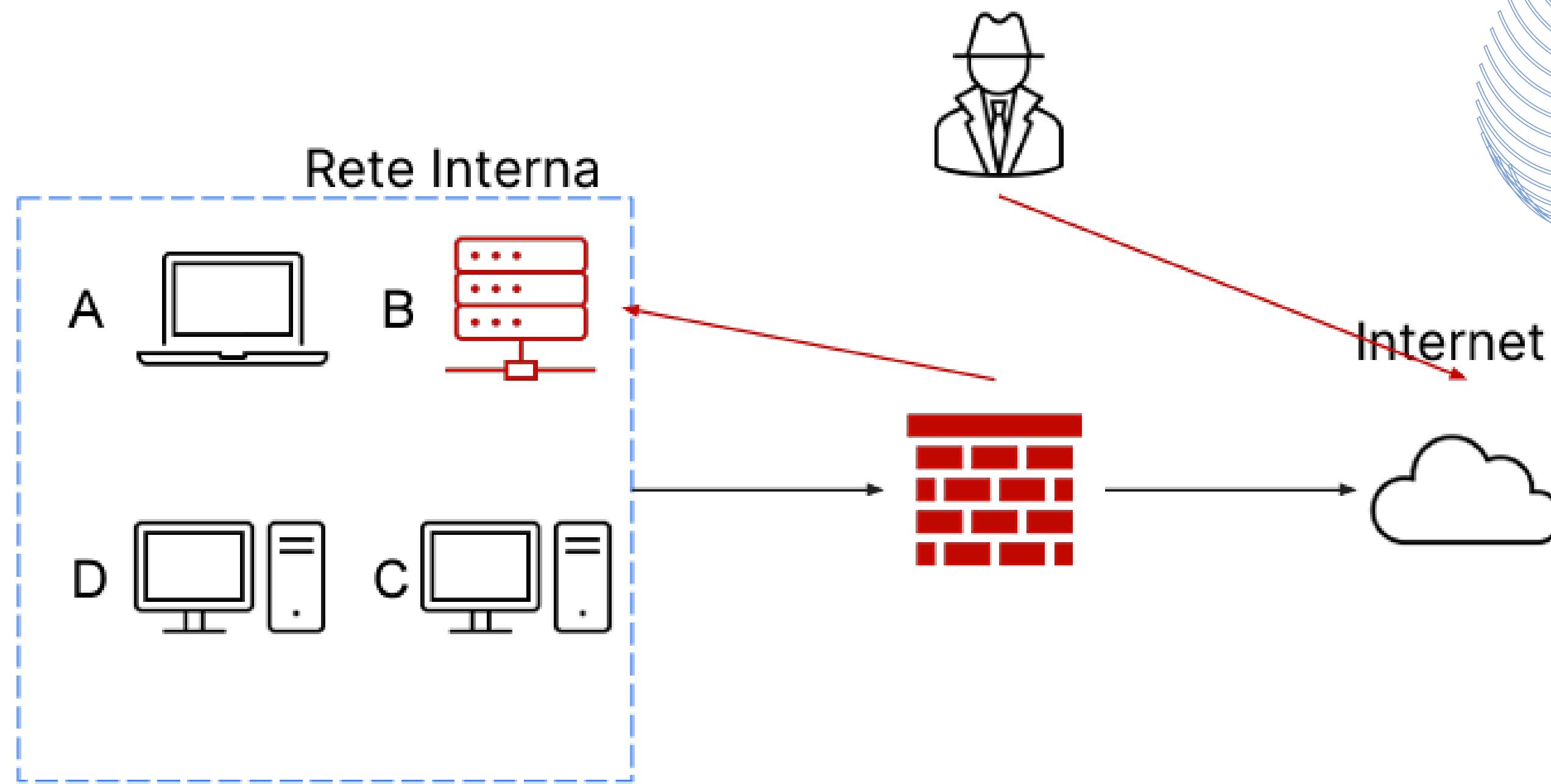


Con riferimento alla figura in slide 4, il sistema **B** (**un database con diversi dischi per lo storage**) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.
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
- 

Riporto la figura menzionata in precedenza della slide 4 nella pratica di oggi.



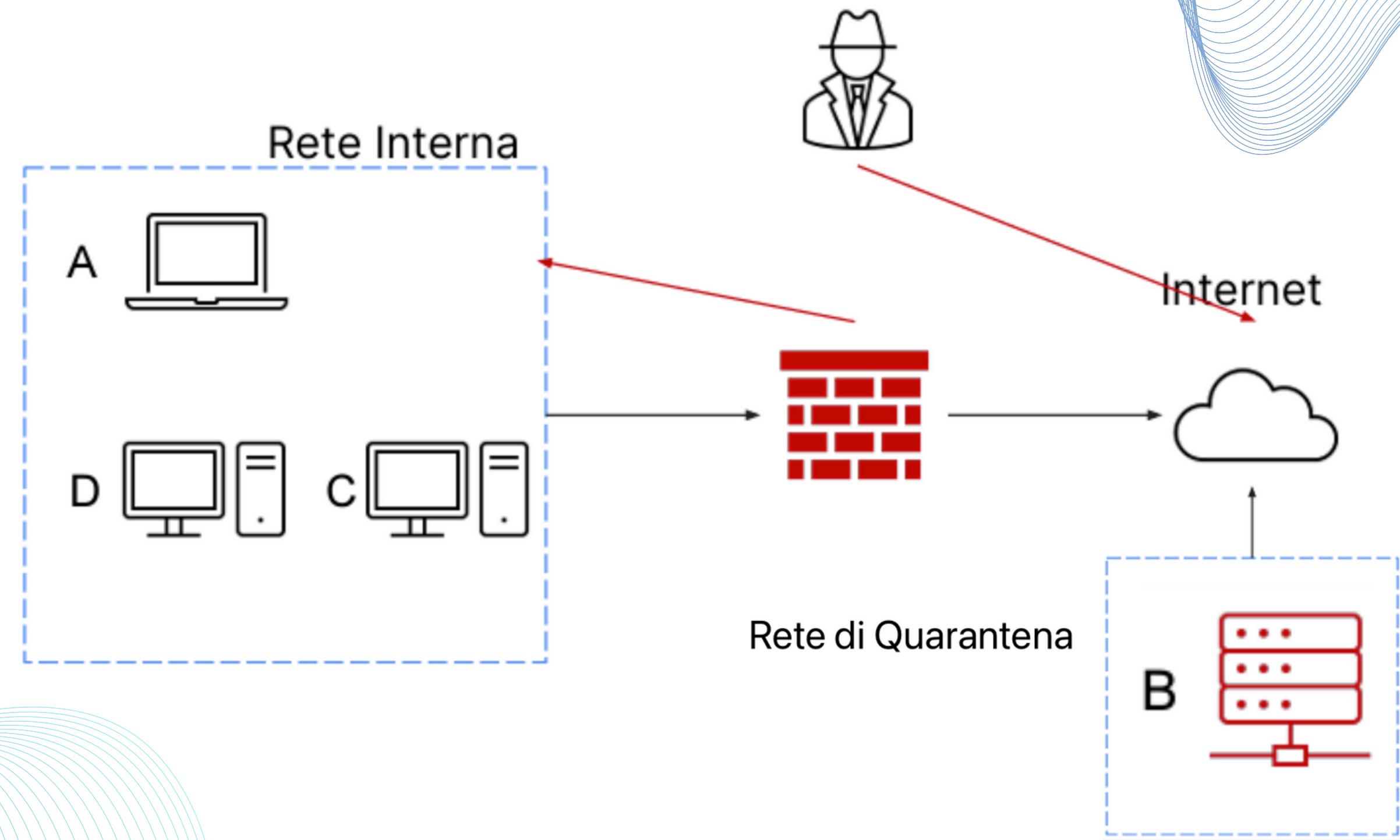
I TECNICA: ISOLAMENTO

Andremo oggi a vedere le due principali tecniche utilizzate per far fronte a quella che è la riduzione dell'impatto causato da un evento / incidente.

Partendo dalla tecnica dell'**Isolamento**, infatti una volta riconosciuto un attacco o incidente sarà il primo tentativo da fare per sanitizzare il sistema o dispositivo attaccato.

Immaginiamo dunque uno scenario dove in una rete di computer aziendali uno tra tutti è stato colpito da un virus, si provvederà quindi a mettere il computer infetto in quella che possiamo chiamare "**rete di quarantena**" quanto prima per evitare che appunto il virus si estenda poi sulle altre macchine della stessa rete per causare danni maggiori, consentendo quindi ancora l'accesso ad internet all'attaccante dalla macchina infetta ma buttandolo fuori dalla rete interna.

Ricordando lo scenario visto nella pagina precedente espongo un possibile schema di rete modificando l'immagine della pratica in slide n°4.



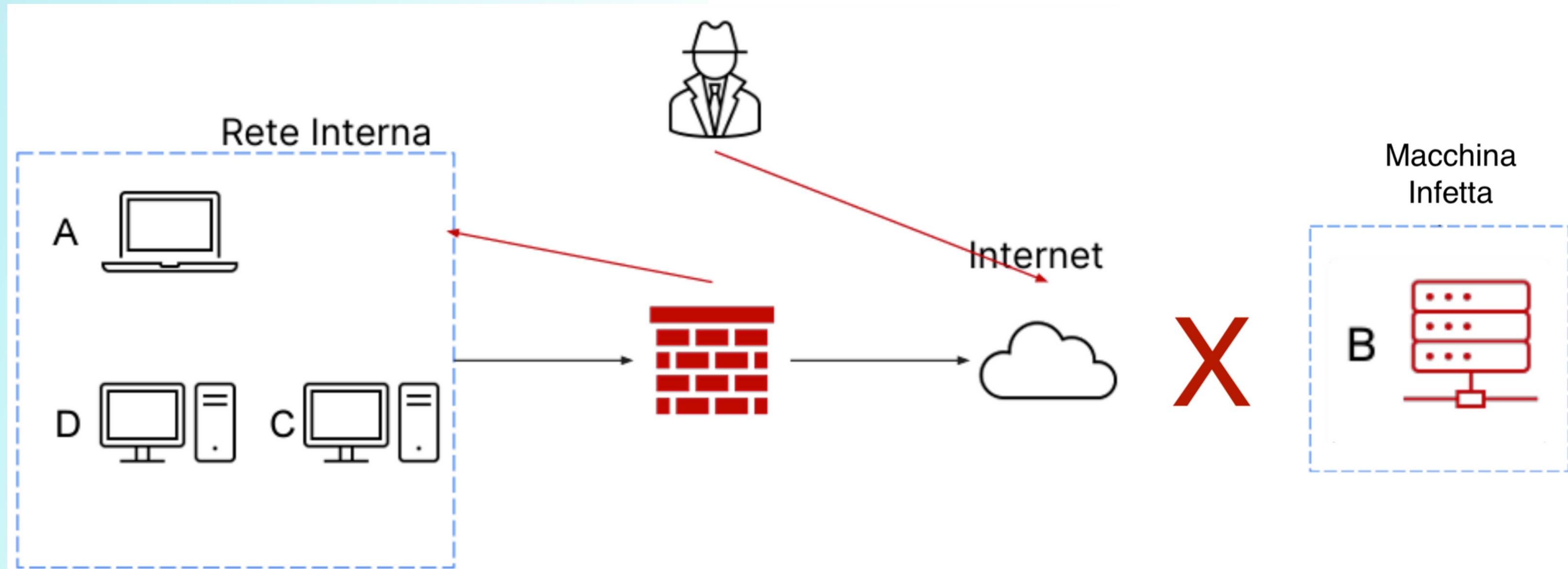
II TECNICA: RIMOZIONE

Se anche dopo aver apportato la tecnica dell'Isolamento vista in precedenza il dispositivo continua ad esporre problematiche si può passare alla tecnica della **Rimozione**.

Questa tecnica consiste a differenza della prima nel rimuovere completamente la macchina da tutte le reti a cui era connessa in precedenza, sia sulla rete internet che sulla rete interna aziendale in questo caso.

In quest'ultimo scenario che vedremo l'attaccante sarà così completamente isolato non avendo più accesso ne alla macchina infetta ne alla rete interna.

Ripreendo nuovamente la slide della pratica, modificandola questa volta per esporre un esempio di **Rimozione** del dispositivo.



GESTIONE O PULIZIA DI UNO STORAGE: PURGE

Solo dopo aver eliminato o per lo meno ridotto il tentativo di attacco sulle nostre macchine sarà necessario sanitizzare il sistema, ovvero parte di tutte quelle procedure che “puliscono” un disco o uno storage che è stato compromesso in precedenza accertandosi per prima cosa che i contenuti sensibili contenuti in esso non siano più presenti o accessibili.

Tra le varie tecniche viste oggi affrontiamo quella del **Purge**, dove appunto si andrà a fare una pulizia logica di tutti i dati presenti riportando il disco al suo stato iniziale, simile alla tecnica Clear ma con aggiunta di atti fisici come l'utilizzo di forti magneti per rendere le informazioni contenute impossibili da leggere.

GESTIONE O PULIZIA DI UNO STORAGE: DESTROY

Quello del **Destroy** invece è sicuramente il metodo più diretto per liberarsi completamente del dispositivo infetto e di tutti i dati al suo interno, come ultima spiaggia in caso i metodi visti prima non sortiscano alcun effetto.

Nel termine stesso della parola la macchina verrà effettivamente distrutta per evitare appunto che contenuti sensibili al suo interno vengano compromessi o rubati, in questo caso si utilizzano tecniche di laboratorio come la disintegrazione o la polverizzazione dei dispositivi ad alte temperature.

Sebbene questo metodo sia sicuramente il più efficace per risolvere il problema come contro l'azienda in questione affronterà delle elevate spese finanziarie per procedere in questo senso.