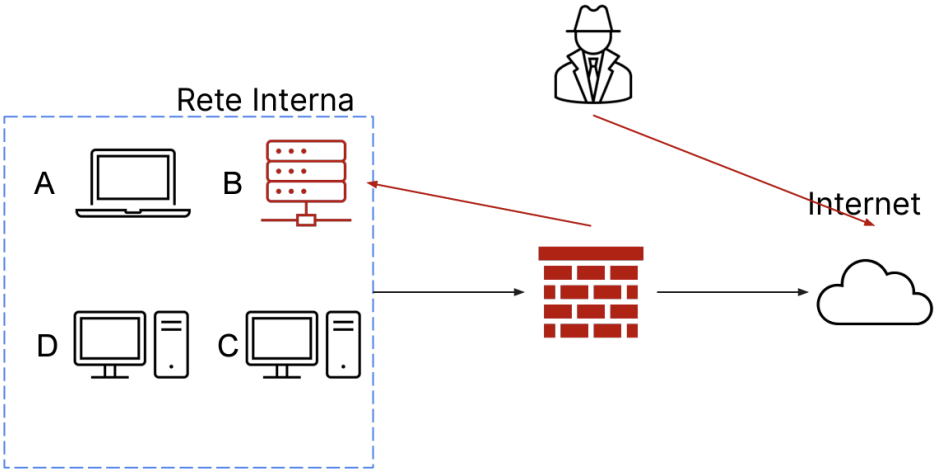
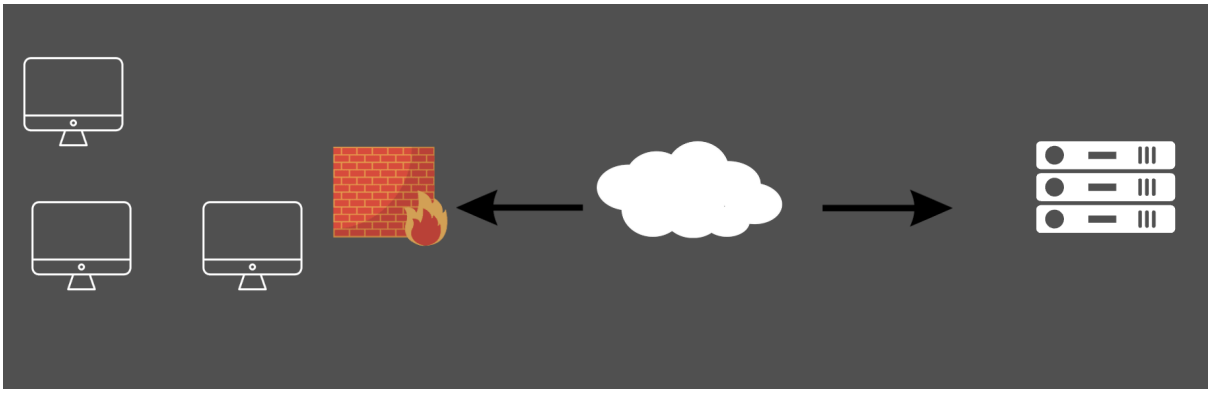
S9 L4



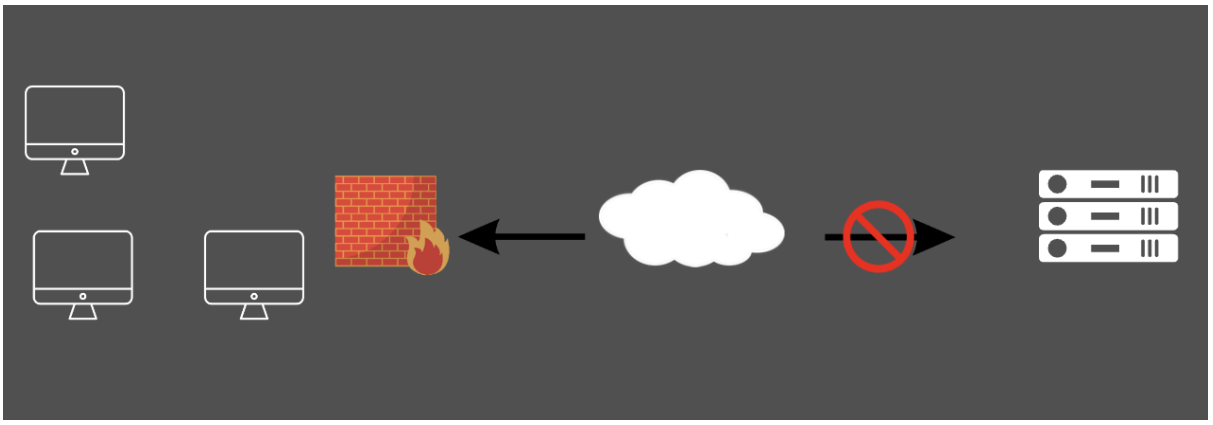
Traccia:
Con riferimento alla figura , il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.
L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai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

I) Isolamento



Possiamo notare dall'immagine che il database è sempre collegato a Internet per continuare a lavorare ma è stato per l'appunto isolato dalla LAN interna.

II) Rimozione



Il sistema è stato completamente rimosso da qualsiasi rete.

La differenza principale tra **Purge** e **Destroy** è che:
con **Purge** si intendo degli interventi fisici mirati a rendere inaccessibili dati presenti sull'hard disk, attraverso l'utilizzo di magneti specifici per esempio. Le componenti fisiche restano intatte e riutilizzabili.
Destroy, come si evince dalla parola, consiste nella disintegrazione e polverizzazione dei componenti fisici attraverso l'uso di alte temperature, rendendo i dispositivi definitivamente inutilizzabili.