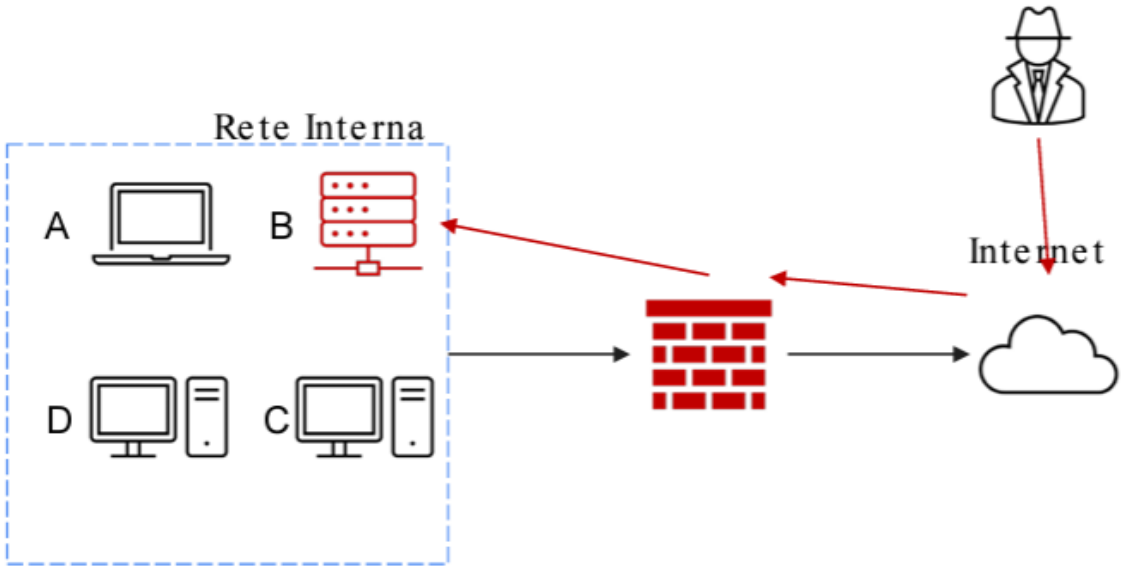
Tecniche di Isolamento

Esercizio: 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. Indicare anche Clear



Purge:

L'operazione di "purge" è utilizzata per rimuovere in modo permanente dati che non sono più necessari. Questa operazione spesso comporta non solo l'eliminazione dei dati, ma anche la liberazione delle risorse associate.

Destroy:

Si riferisce alla completa distruzione di un oggetto o risorsa in un programma, rendendolo irrecuperabile. È un termine spesso utilizzato in programmazione orientata agli oggetti per indicare la distruzione di istanze di oggetti.

Clear:

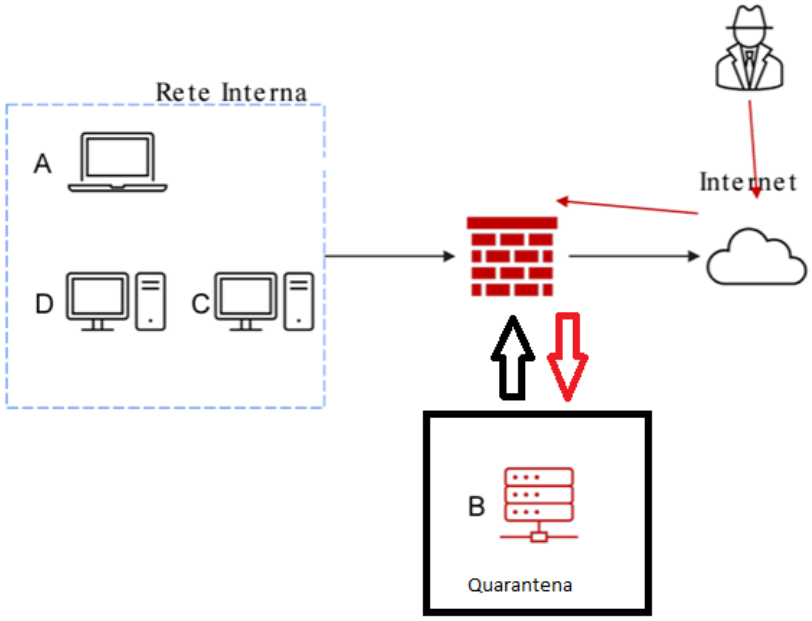
L'operazione di "clear" implica resettare o pulire il contenuto di una struttura dati o di una risorsa senza rimuoverla completamente. In pratica, i dati all'interno della struttura sono eliminati, ma la struttura stessa rimane intatta e pronta per essere riutilizzata.

In sintesi:

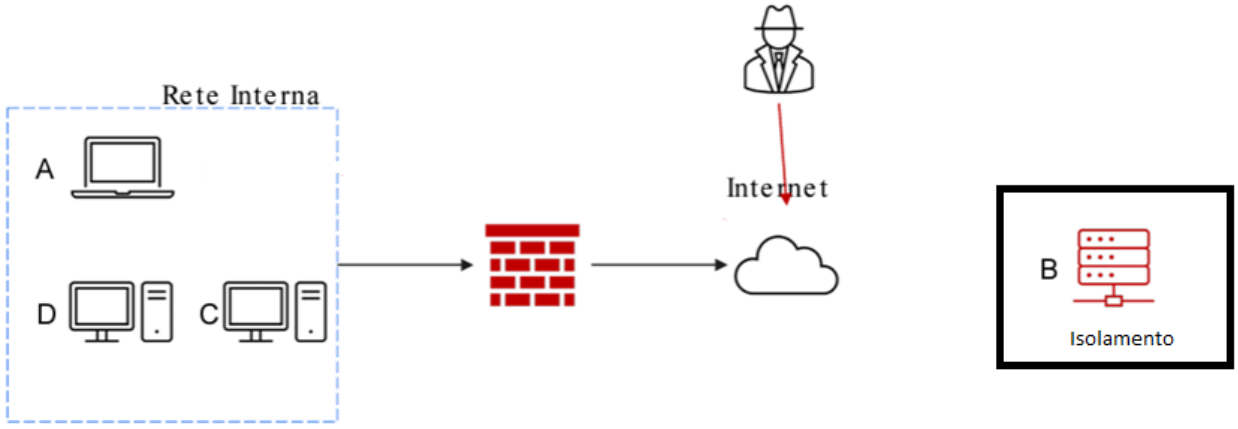
Purge: Eliminazione permanente dei dati e liberazione delle risorse.

Destroy: Distruzione completa di un oggetto o risorsa, rendendolo irrecuperabile.

Clear: Pulizia o reset dei dati all'interno di una struttura, mantenendo la struttura intatta e pronta per nuovi dati.



Quarantena



Isolamento con rimozione del sistema infetto