Report incident response

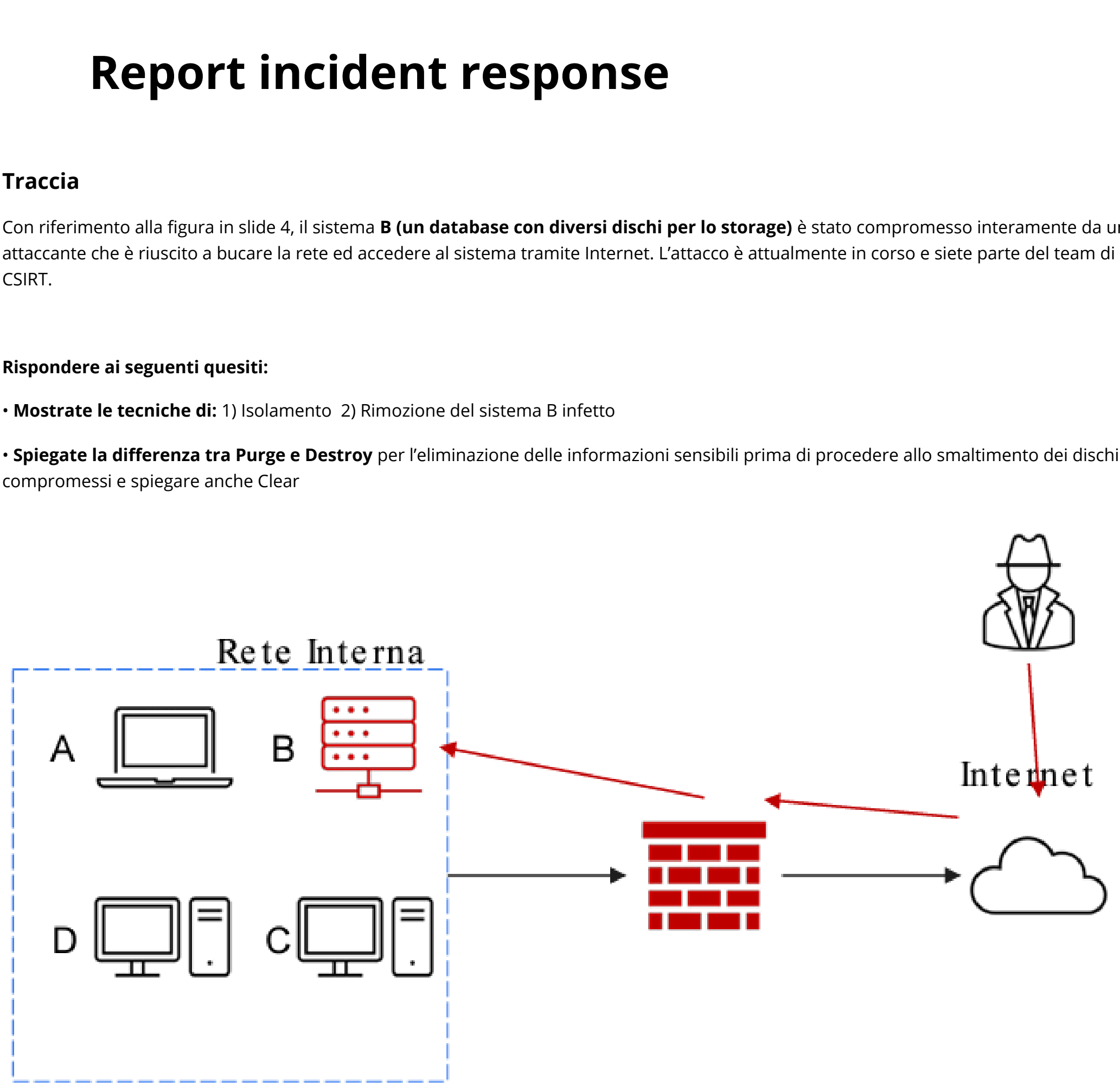
Traccia

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:** 1) Isolamento 2) 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 e spiegare anche Clear

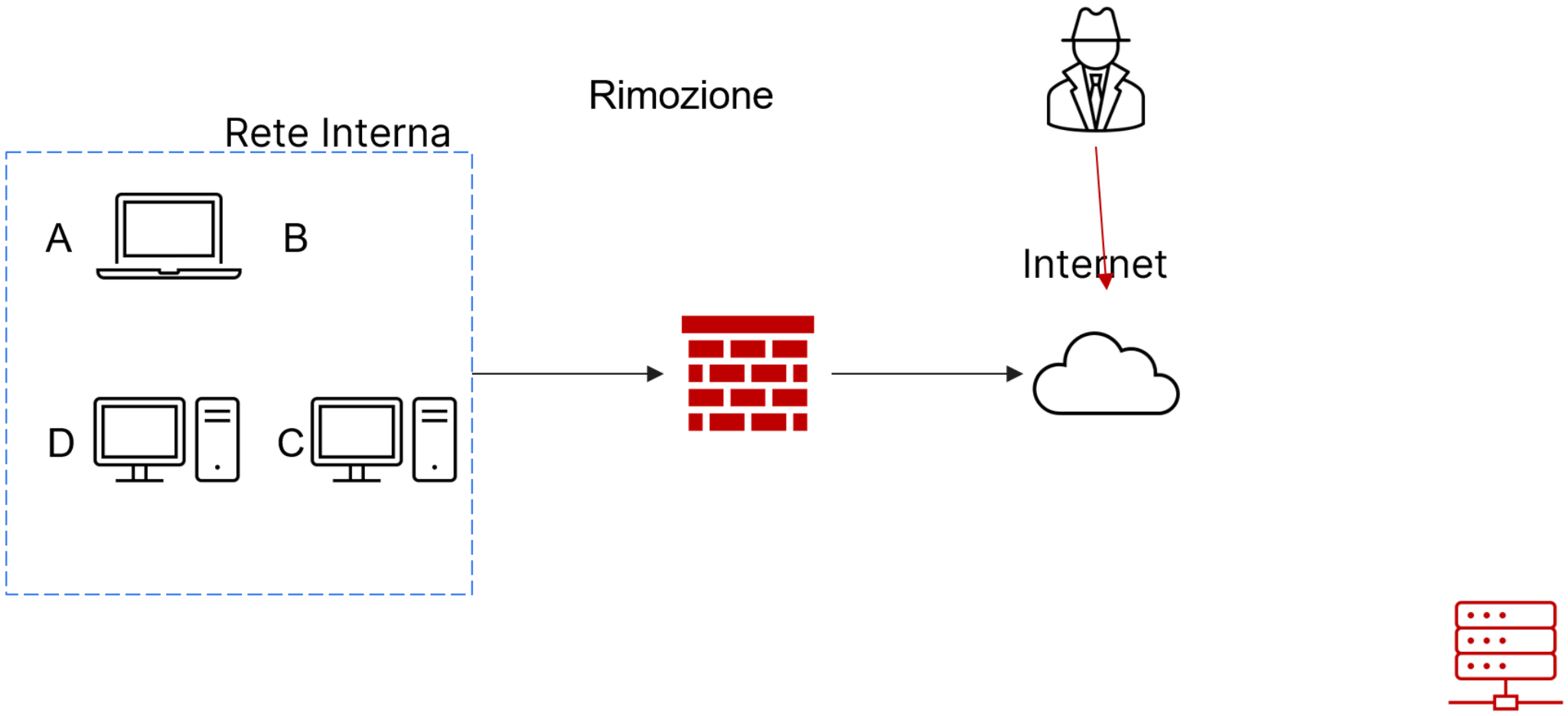


Risoluzione esercizio

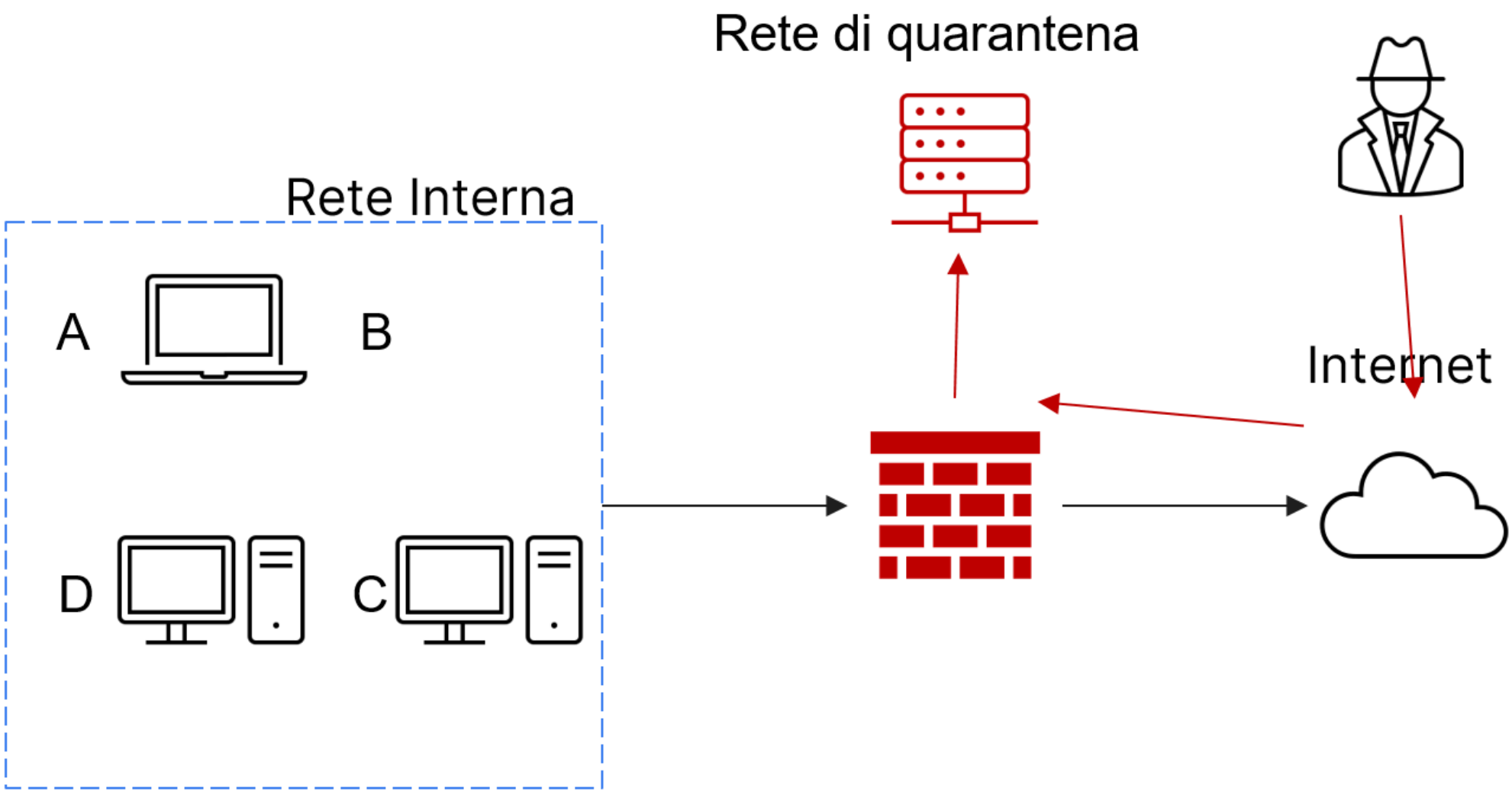
Tecniche di isolamento

L'isolamento è una tecnica utilizzata per limitare i danni e prevenire ulteriori compromissioni del sistema durante un attacco in corso. Ecco alcune tecniche di isolamento:

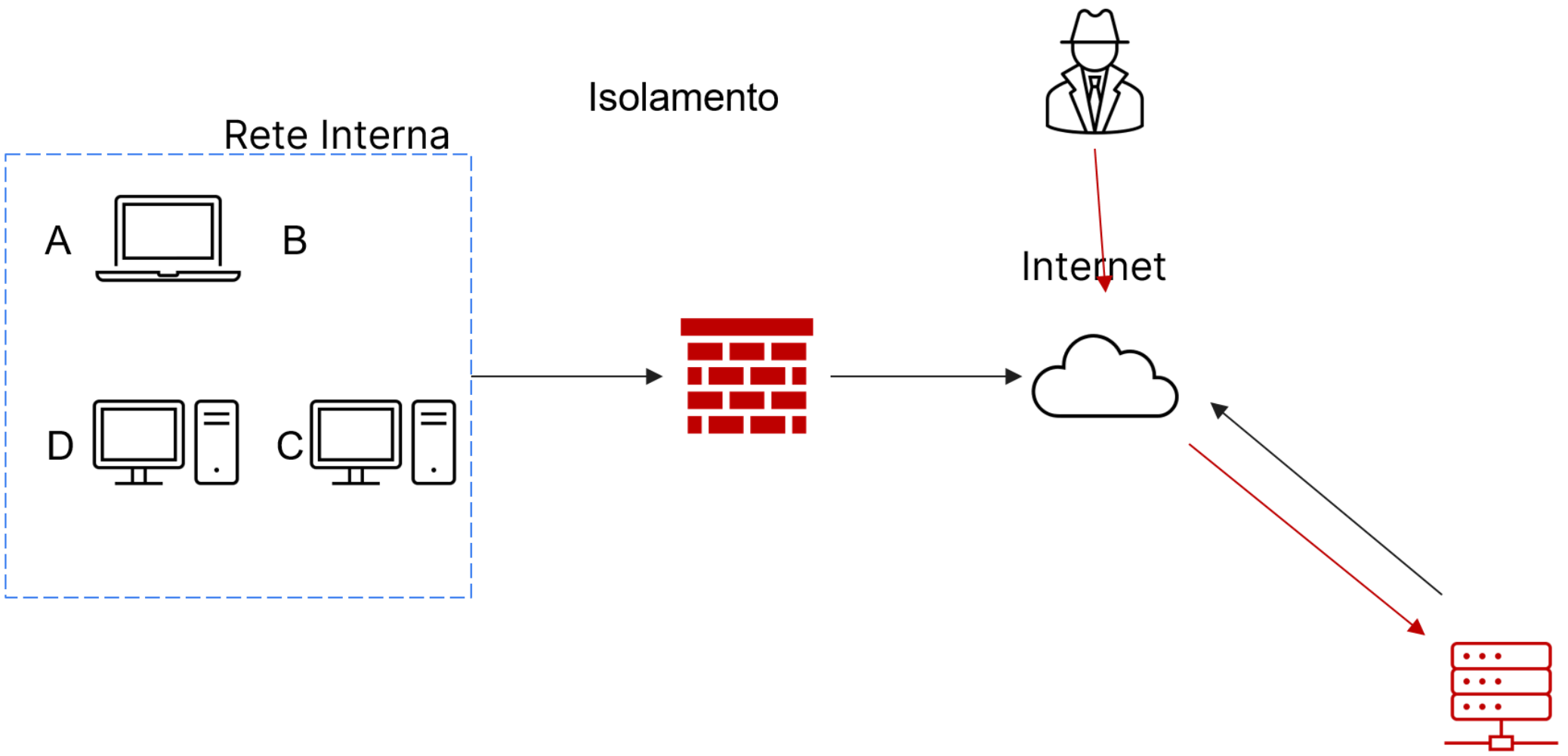
- **Disconnessione dalla Rete:**
  - scollegare fisicamente i cavi di rete o disabilitare le interfacce di rete per interrompere immediatamente l'accesso dell'attaccante.
  - questa azione previene ulteriori comandi da parte dell'attaccante e limita la possibilità di esfiltrazione di dati.



- **Isolamento Logico:**
  - utilizzare firewall o sistemi di prevenzione delle intrusioni (IPS) per bloccare il traffico verso e da il sistema B.
  - questo metodo è meno drastico della disconnessione fisica ma può essere efficace se configurato correttamente.



- **Creazione di una VLAN Isolata:**
  - spostare il sistema compromesso in una VLAN dedicata e isolata per monitorare il traffico e impedire ulteriori movimenti laterali all'interno della rete.



Rimozione del Sistema B Infetto

La rimozione del sistema infetto è una fase critica che deve essere eseguita con attenzione per evitare ulteriori danni e preservare le prove per analisi future.

- **Documentazione:**
  - prima di rimuovere il sistema, documentare tutte le attività e raccogliere i log di sistema, le configurazioni di rete e altre informazioni rilevanti per l'analisi post-incidente.

- **Rimozione:**
  - rimozione del dispositivo attraverso lo scollegamento dei cavi di rete o della disabilitazione delle interfacce di rete per impedire l’accesso all’attaccante.

- **Backup di Emergenza:**
  - creare un backup completo del sistema infetto per preservare le prove digitali che potrebbero essere cruciali per l'analisi forense.

- **Ricostruzione del Sistema:**
  - utilizzare immagini di backup precedenti non compromesse per ripristinare il sistema su hardware pulito.
  - applicare tutte le patch di sicurezza e configurare correttamente i controlli di accesso prima di rimettere il sistema in produzione.

Differenza tra Purge e Destroy

- **Purge (Pulizia):**
  - il processo di purgazione (**purge**) comporta l'eliminazione delle informazioni sensibili in modo tale che non possano essere recuperate con tecniche di recupero di dati standard. Questo può includere la sovrascrittura dei dati con informazioni casuali più volte. È spesso utilizzato quando i supporti di memorizzazione devono essere riutilizzati.

- **Destroy (Distruzione):**
  - la distruzione implica l'eliminazione fisica del supporto di memorizzazione, rendendo impossibile qualsiasi recupero dei dati. Questo può includere la frantumazione dei dischi, la demagnetizzazione (**degaussing**) o l'incenerimento. È utilizzato quando i supporti

devono essere definitivamente smaltiti e non si intende riutilizzarli.

- **Clear (Pulizia di base):**
  - il **clearing** è un metodo meno rigoroso rispetto al **purge**, che comporta la rimozione dei dati in modo che non possano essere recuperati da utenti non autorizzati con strumenti software standard, ma potrebbe non proteggere i dati contro attacchi avanzati di recupero. Un esempio è la semplice formattazione di un disco o la cancellazione dei file.