EPICODE

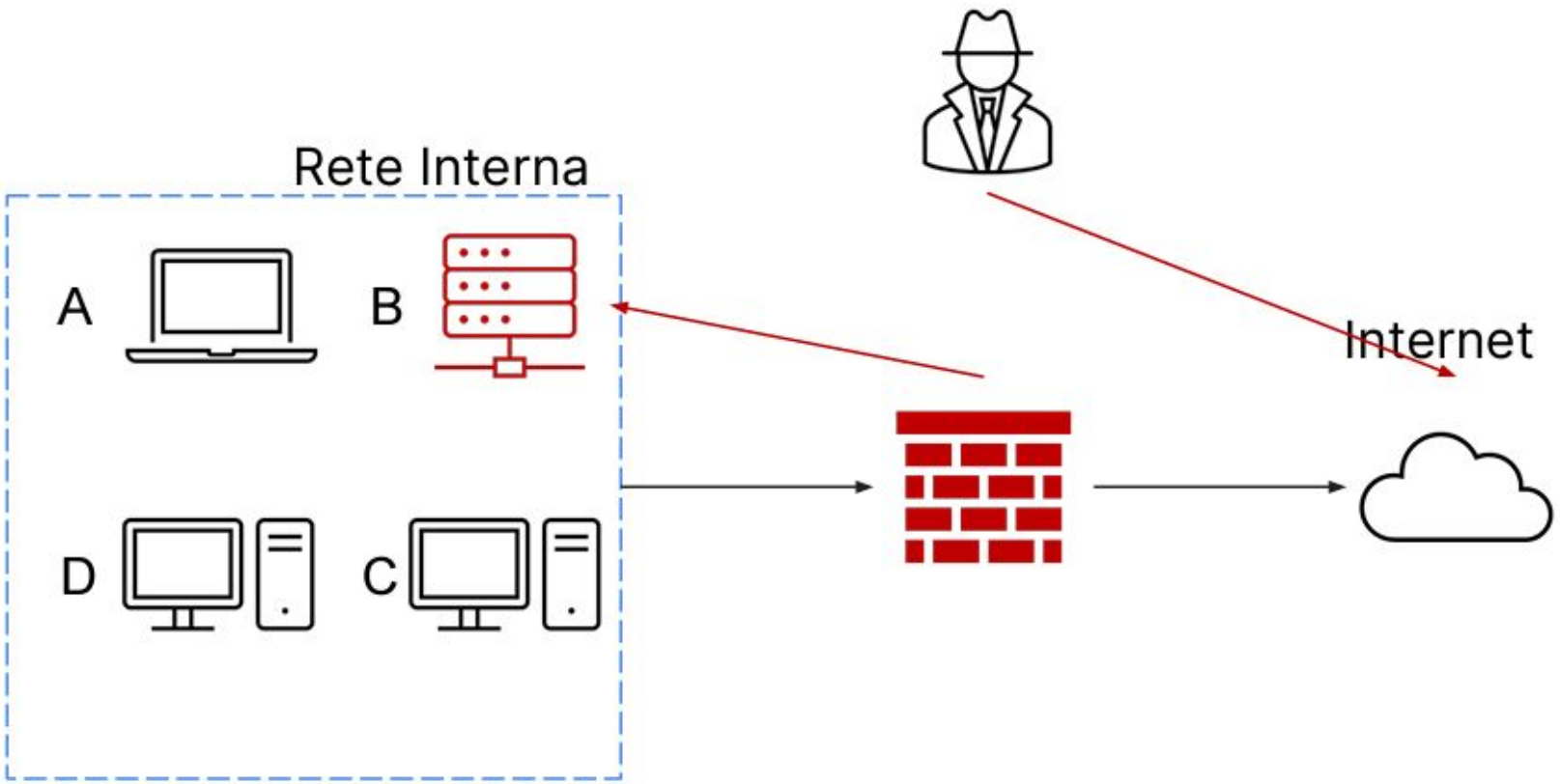
Progetto Alessandro Moscetti 08/11

Introduzione

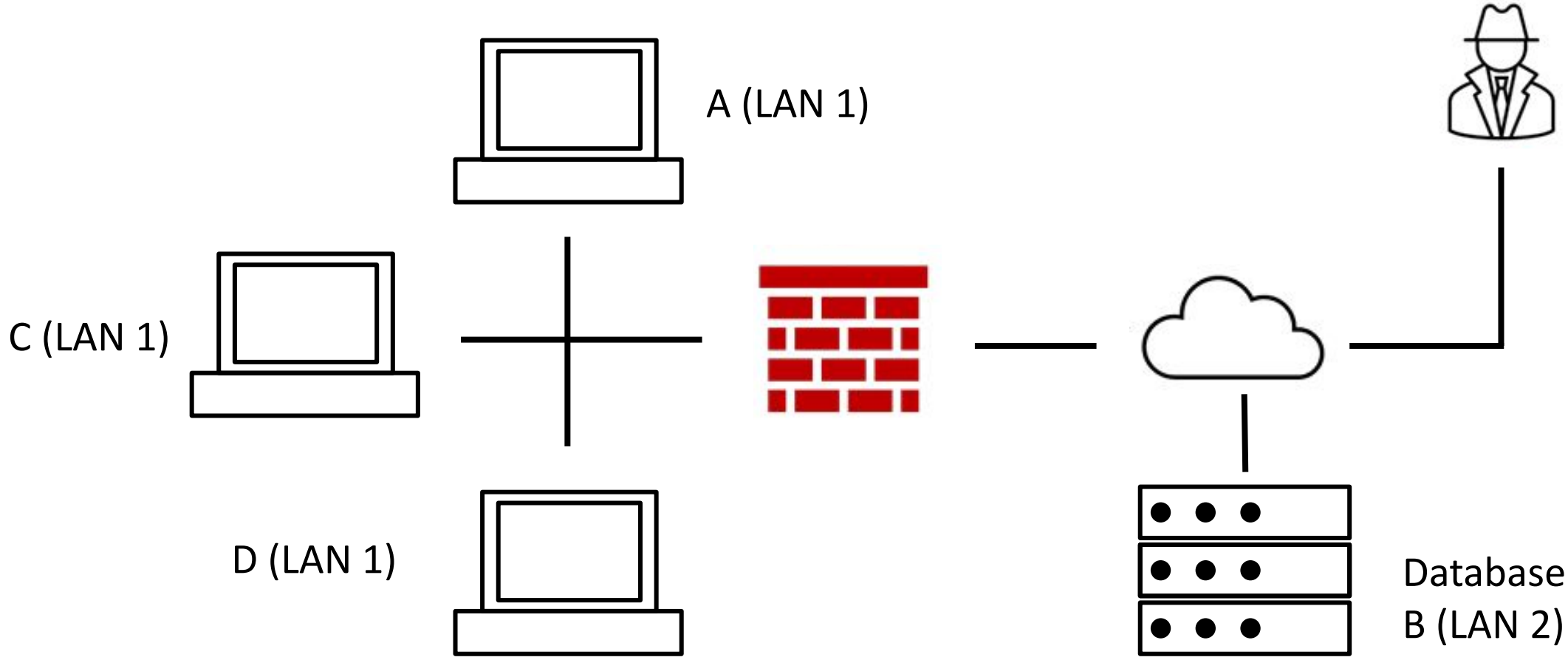
Nell’esercizio di oggi ci veniva richiesto di rispondere ai seguenti quesiti riguardanti il **database B**:

- Mostrare le tecniche di: I) Isolamento
  II) Rimozione del sistema B infetto
- Spiegare la differenza tra Purge e Destroy per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Rete



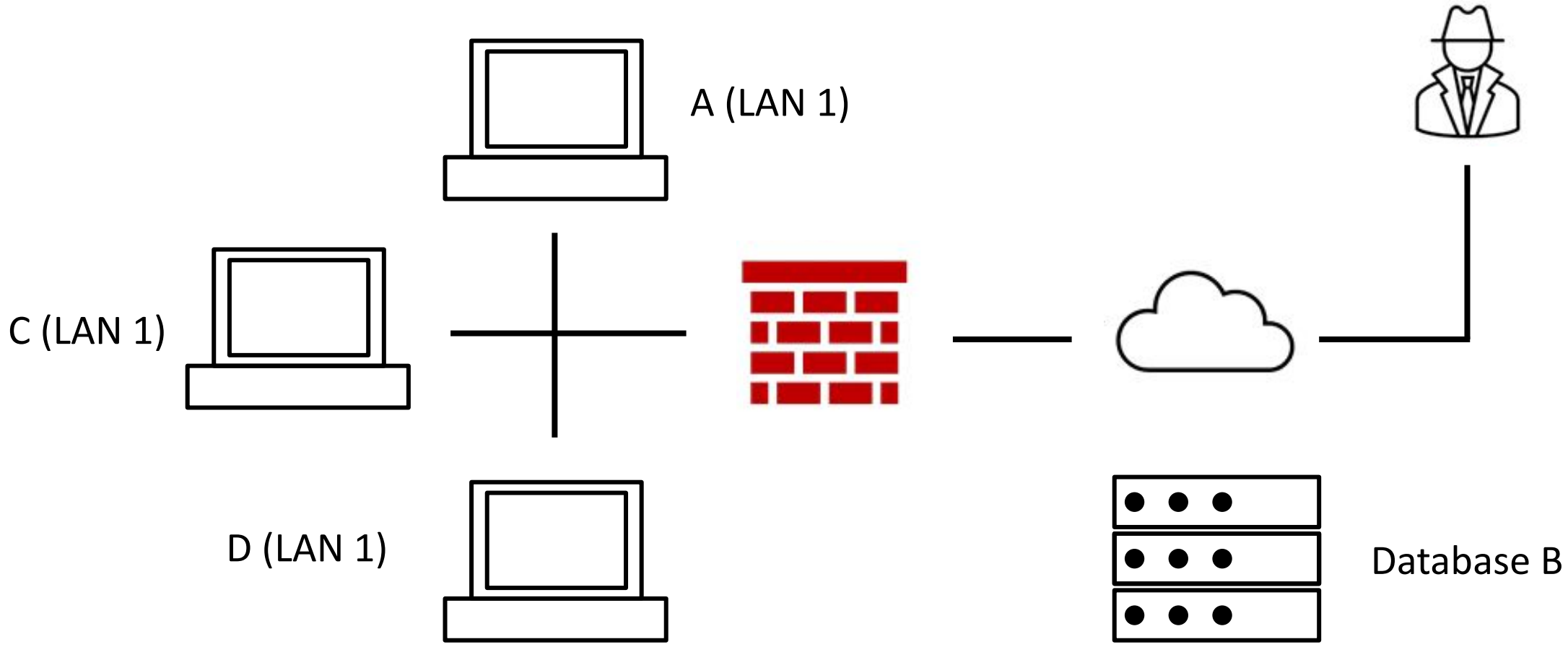
Isolamento



Spiegazione isolamento

Per andare ad isolare il dispositivo infetto siamo andati a suddividere la rete tramite LAN, così facendo possiamo evitare che la minaccia si possa muovere e moltiplicare nella nostra rete.
Nel caso dell'isolamento il dispositivo infetto verrà separato dalla nostra rete primaria ma resterà in comunicazione con Internet.

Rimozione



Spiegazione rimozione

In questo caso il sistema infetto verrà rimosso dalla rete senza nessuna comunicazione, anche internet.
Questa soluzione si adotta quando la l'isolamento non è abbastanza rispetto alla minaccia.

Differenza tra purge e destroy

Sono entrambe opzioni per gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso.
Purge si riferisce alla rimozione dei dati presenti nel disco che avviene, oltre che con un approccio logico (read and write, factory reset), con un approccio fisico come utilizzo di forti magneti per rendere ancor più inaccessibili i dati presenti.
Per **Destroy** si intende , oltre all'approccio logico e fisico precedente, a tecniche più nette per rendere ancora di più inaccessibili i dati come trapanare il disco, polverizzazione in laboratorio, ecc.
In questi casi i dischi non sarebbero riutilizzabili ma andranno sostituiti.

Grazie per l’attenzione.