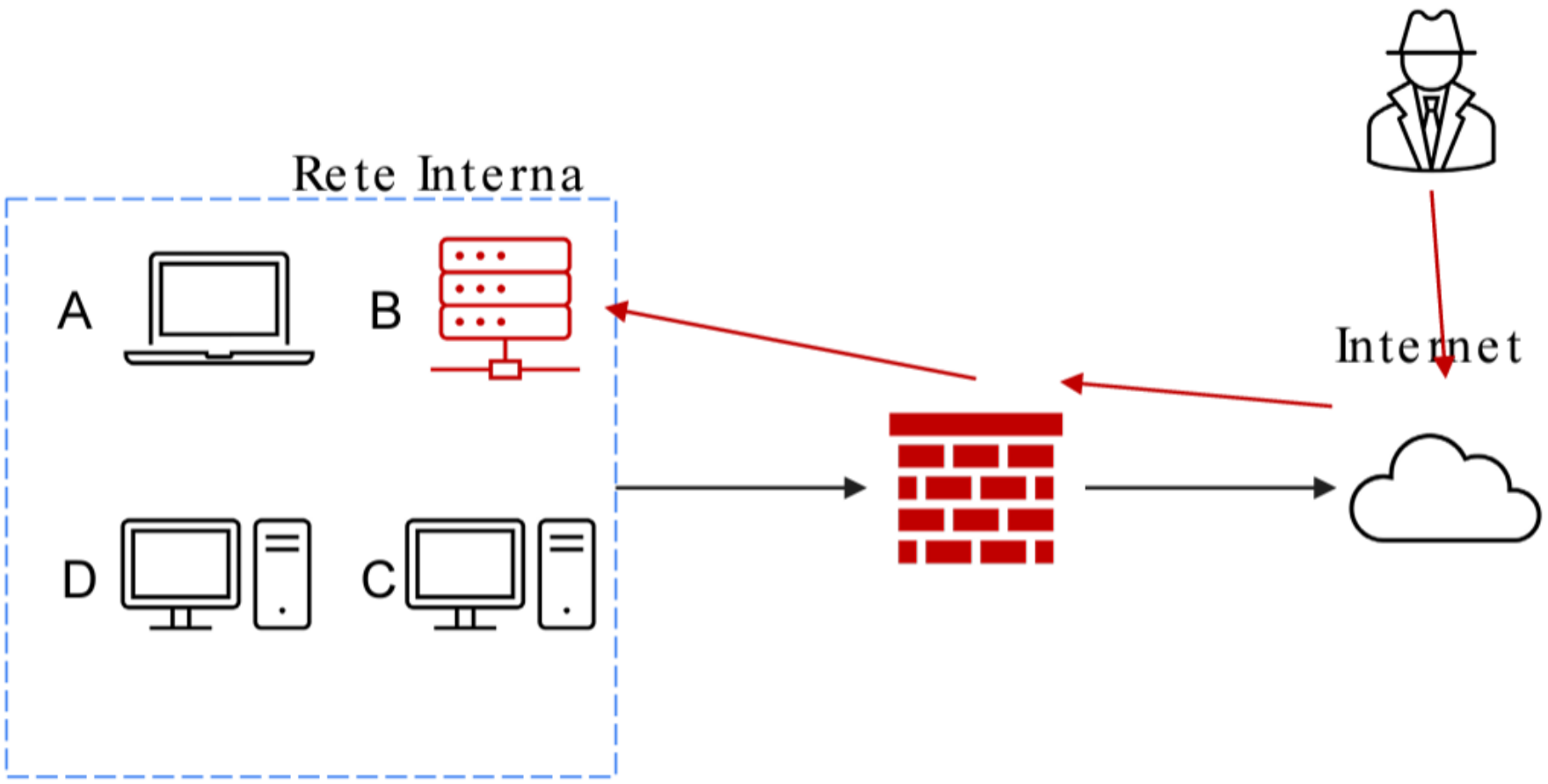
S9-L4

Rete della traccia:



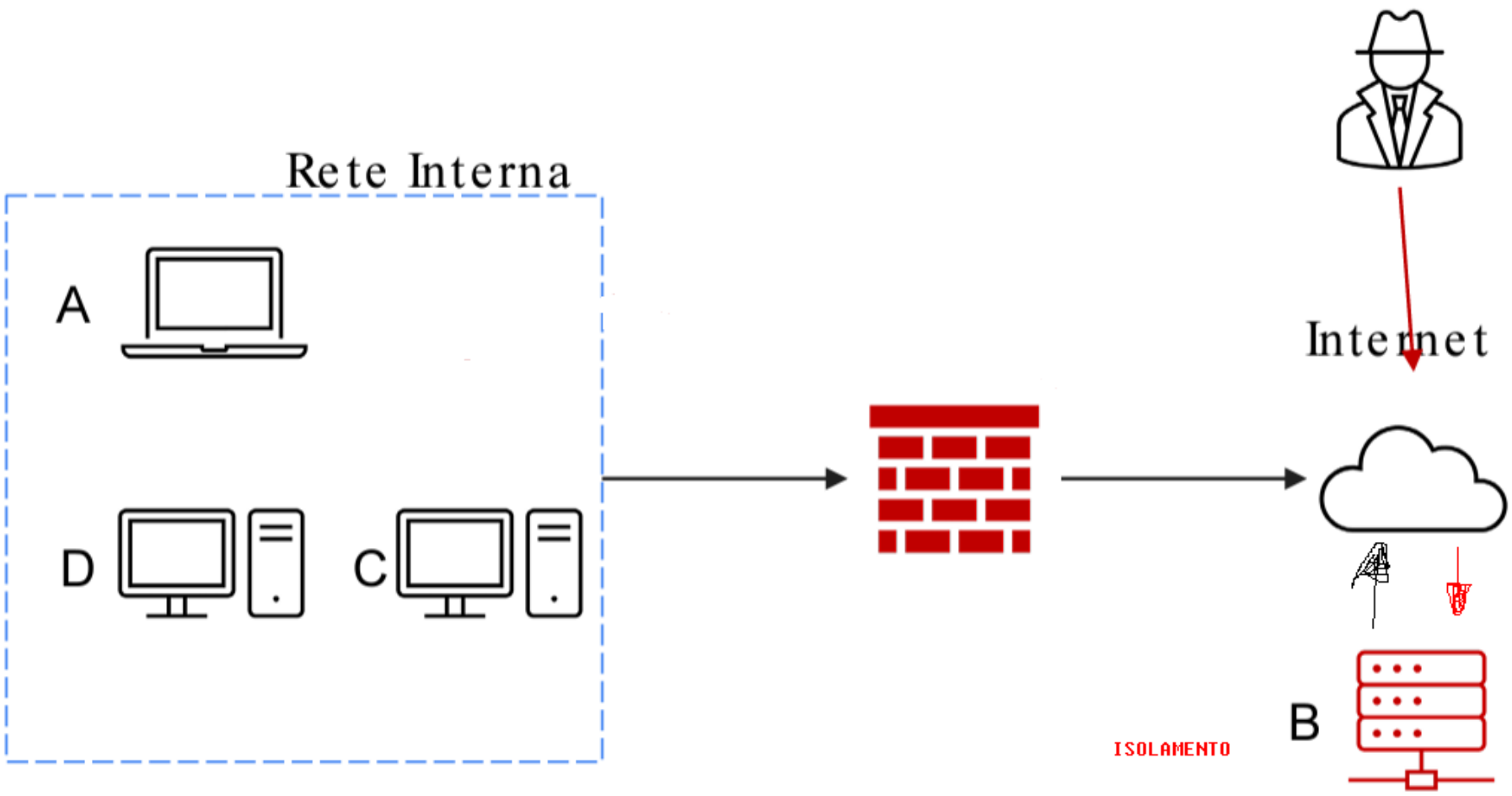
Rischio principale: pivoting.

1. Isolamento del Sistema Infetto

Nell'immagine sotto possiamo vedere come abbiamo modificato l'immagine della rete iniziale.

Isoliamo il sistema infetto restringendo l'accesso dell'attaccante alla rete interna.
Tuttavia il sistema infetto sarà ancora accessibile dall'attaccante via internet

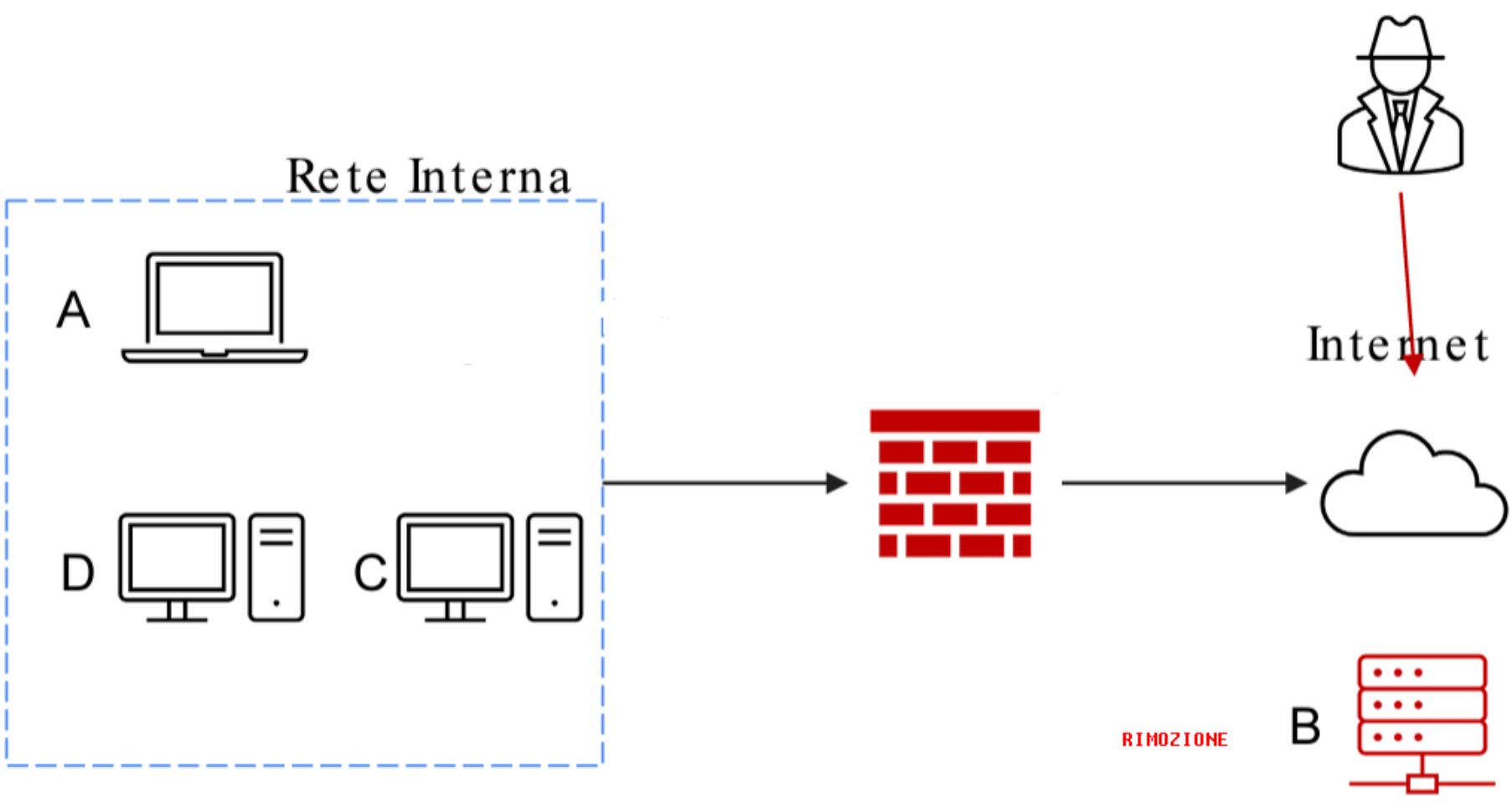
Analizziamo il flusso tramite le frecce, il percorso dell'hacker sarà in rosso.



2. Rimozione del Sistema Infetto

Rimuoviamolo totalmente per evitare che dati possano entrare ed uscire.

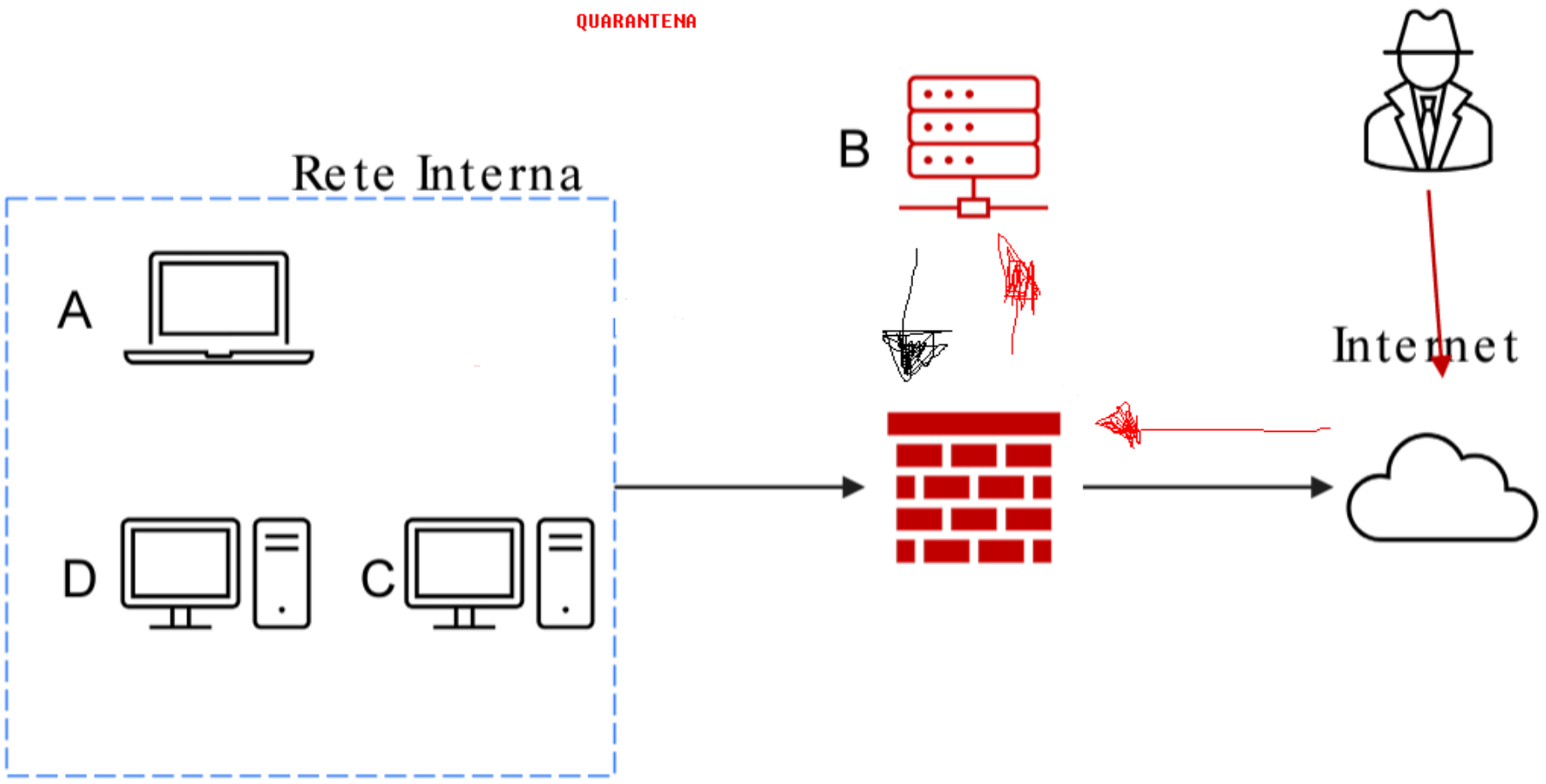
La tecnica di rimozione elimina il sistema dalla rete rendendolo inaccessibile.
Restringe l'accesso alla rete interna da parte dell'attaccante che non avrà nemmeno più accesso al sistema infetto.



3. Quarantena del sistema

Andiamo ad inserire il device colpito in una differente subnet. Questa metodica è molto rapida ma presenta comunque dei rischi.

Osserviamo il flusso graficamente :



Rischio: L’attaccante potrebbe modificare la tabella di routing ed, attaccato l’utente, potrebbe redirigere il traffico verso l’intranet.

---

4. Differenze tra Purge, Destroy e Clear

Sono tutti metodi finalizzati ad eliminare i dati sensibili dai dischi prima dello smaltimento.

- **Clear (pulizia)**: rende i dati meno accessibili cancellando le directory e i file e sovrascrivendo l'area del disco con dati casuali o uno schema di cancellazione.
  Tuttavia, i dati possono essere recuperati con tecniche avanzate di recupero.
  Questa tecnica è adeguata quando il livello di minaccia è relativamente basso.
- **Purge (purificazione)**: va oltre il semplice "clear", rendendo i dati illeggibili e irrecuperabili anche con strumenti avanzati.
  Questo può essere fatto tramite metodi come la sovrascrittura multipla con dati casuali o la smagnetizzazione (degaussing) del disco.
- **Destroy (distruzione)**: è il metodo più sicuro e consiste nella distruzione fisica del supporto di memorizzazione. Questo può essere fatto triturando il disco, fondendolo o smagnetizzandolo in modo irreversibile. La distruzione garantisce che i dati non possano essere recuperati in alcun modo.