

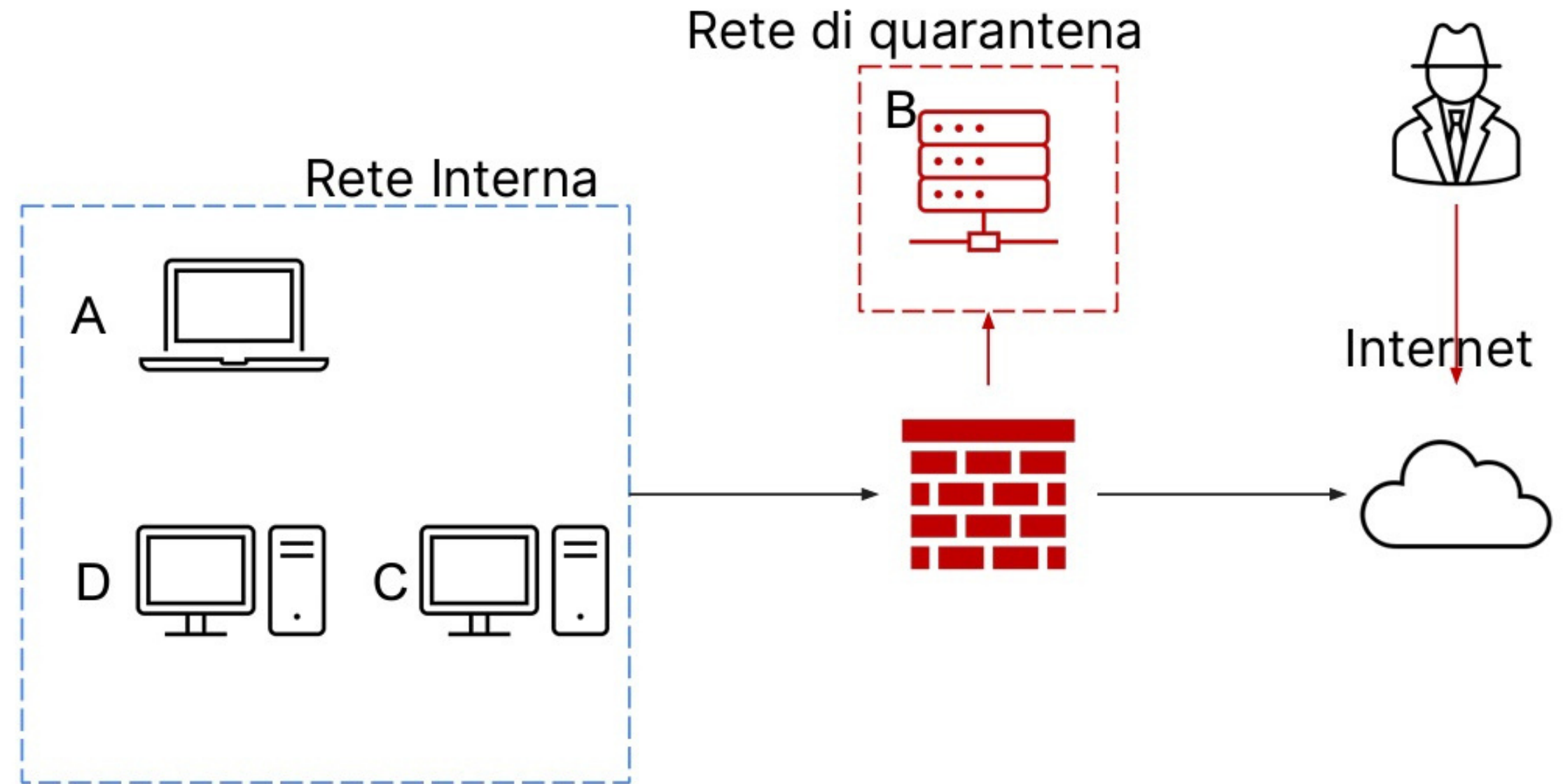


S9L4

Soluzione - **ISOLAMENTO**

- Mostrate le tecniche di: I) **Isolamento** II) Rimozione del sistema **B infetto**

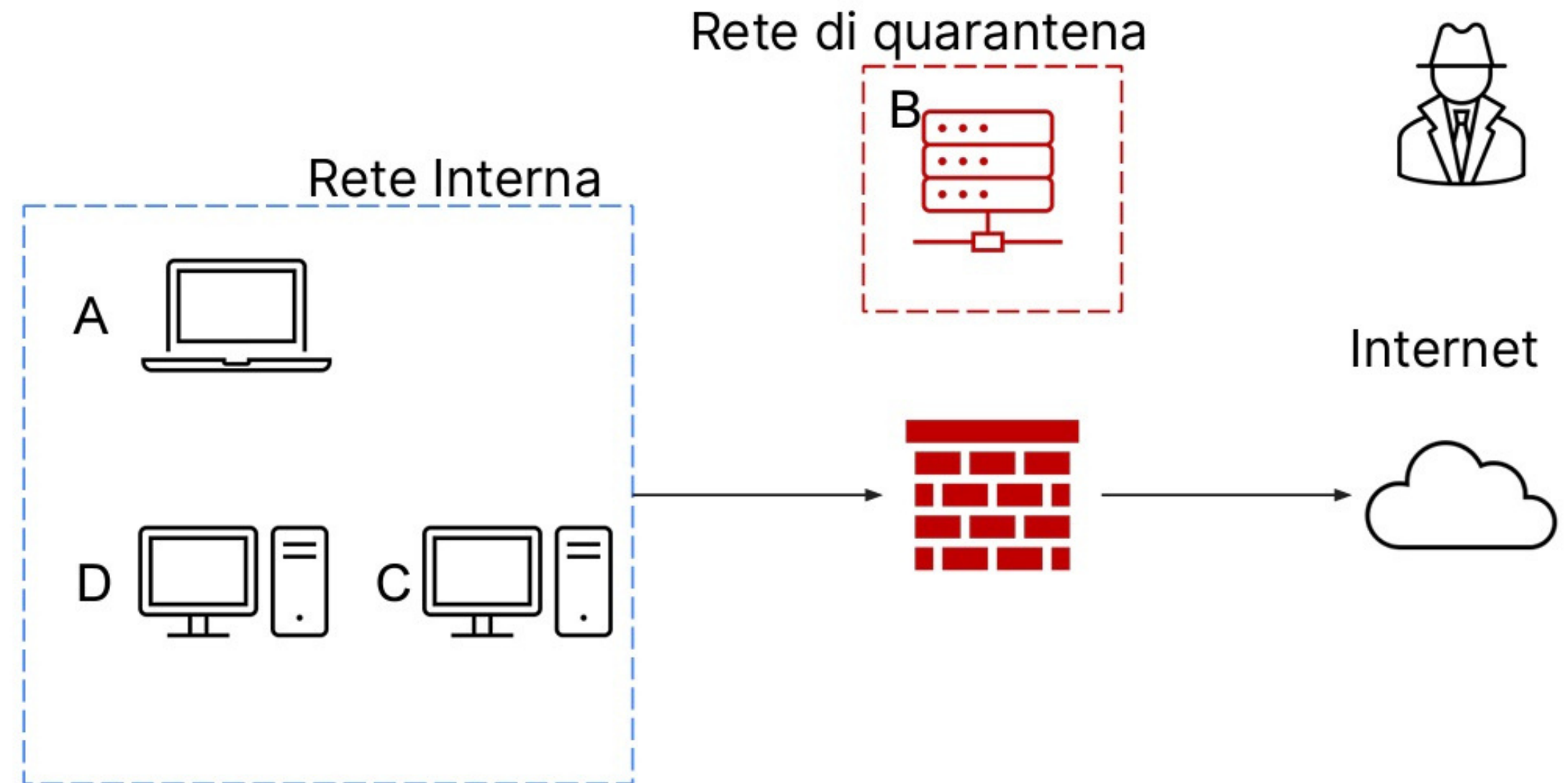
La tecnica di isolamento permette di isolare un sistema infetto restringendo l'accesso dell'attaccante alla rete interna. **Tuttavia il sistema infetto sarà ancora accessibile dall'attaccante via internet**



Soluzione - **RIMOZIONE**

- Mostrate le tecniche di: I) Isolamento II) **Rimozione** del sistema **B infetto**

La tecnica di Rimozione elimina completamente il sistema dalla rete, di fatto rendendolo inaccessibile sia da rete interna che da internet. **Questo approccio restringe l'accesso alla rete interna da parte dell'attaccante che non avrà nemmeno più accesso al sistema infetto.**



Soluzione - **PURGE**

- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Purge: per quest'approccio si adottano sia misure logiche che misure fisiche per l'eliminazione permanente dei dati su un disco / dispositivo di storage. Le tecniche fisiche utilizzate tuttavia non sono invasive, e non implicano la distruzione dell'hardware

Soluzione - **DESTROY**

- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Destroy: utilizza tecniche fisiche molto invasive per rendere inaccessibili i dati su un disco / dispositivo di storage. Alcune delle tecniche prevedono la distruzione a livello di hardware di fatto rendendo non recuperabile l'hardware e le relative informazioni salvate su di esso. È il metodo preferito quando si vuole smaltire un disco non riutilizzabile, ma è anche quello che costa di più.