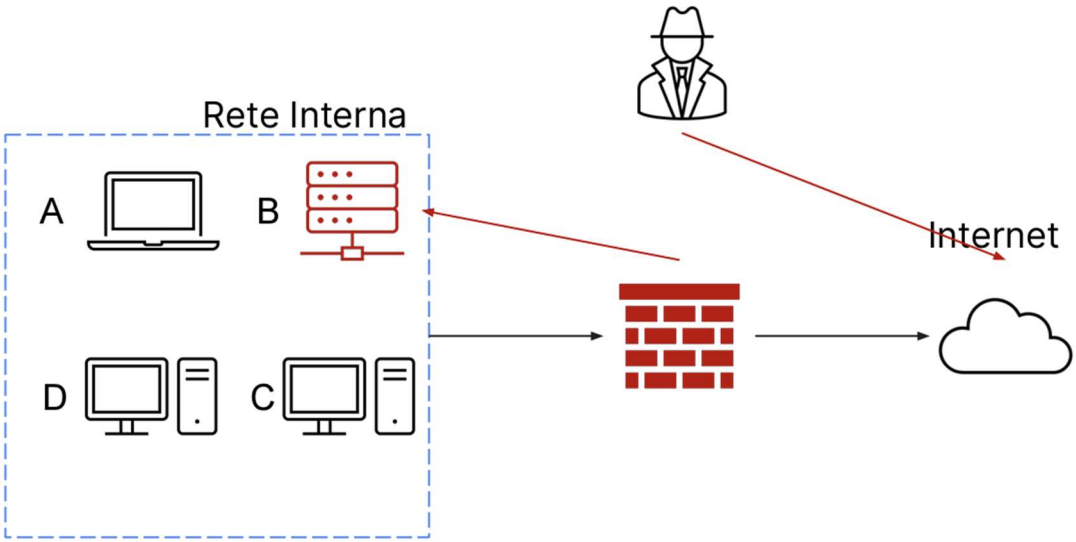
Esercizio S9-L4

L’esercizio richiede di mostrare le tecniche di: Isolamento e rimozione del sistema B infetto.



L’isolamento consiste nella completa disconnessione del dispositivo infetto dalla rete (aziendale) il quale però avrà comunque accesso a internet. Quindi prendendo in caso l’esempio nel disegno, il dispositivo andrà spostato fuori dal firewall e connesso direttamente ad internet.

Se ciò non dovesse bastare si parlerebbe di rimozione del dispositivo, ossia verranno staccati i cavi che permettono l’accesso a internet lasciando di fatto il dispositivo completamente isolato.

La differenza tra Purge e Destroy si basa sul metodo di eliminazione dei file al suo interno. Entrambi e metodi sono usati per raggiungere il risultato ma in modo diversi: il primo si basa sulla cancellazione “sicura”, a livello software dei dati all’interno dell’hdd, sovrascrivendoli il più possibile senza distruggere la copia fisica, il secondo invece è basato interamente sulla distruzione del dispositivo hardware, rendendolo inutilizzabile.