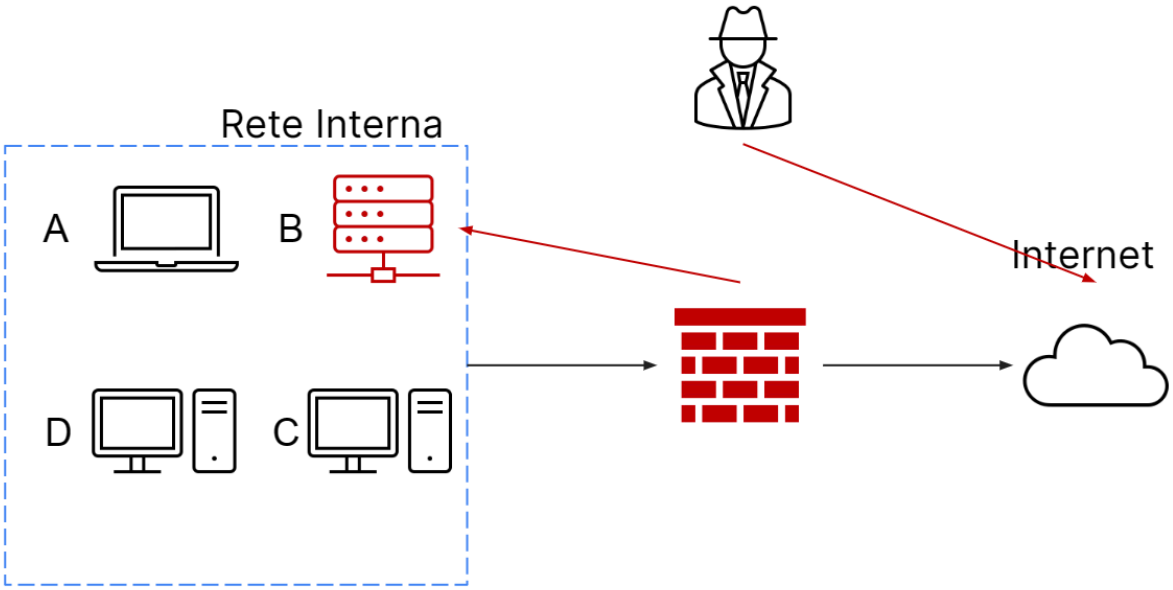
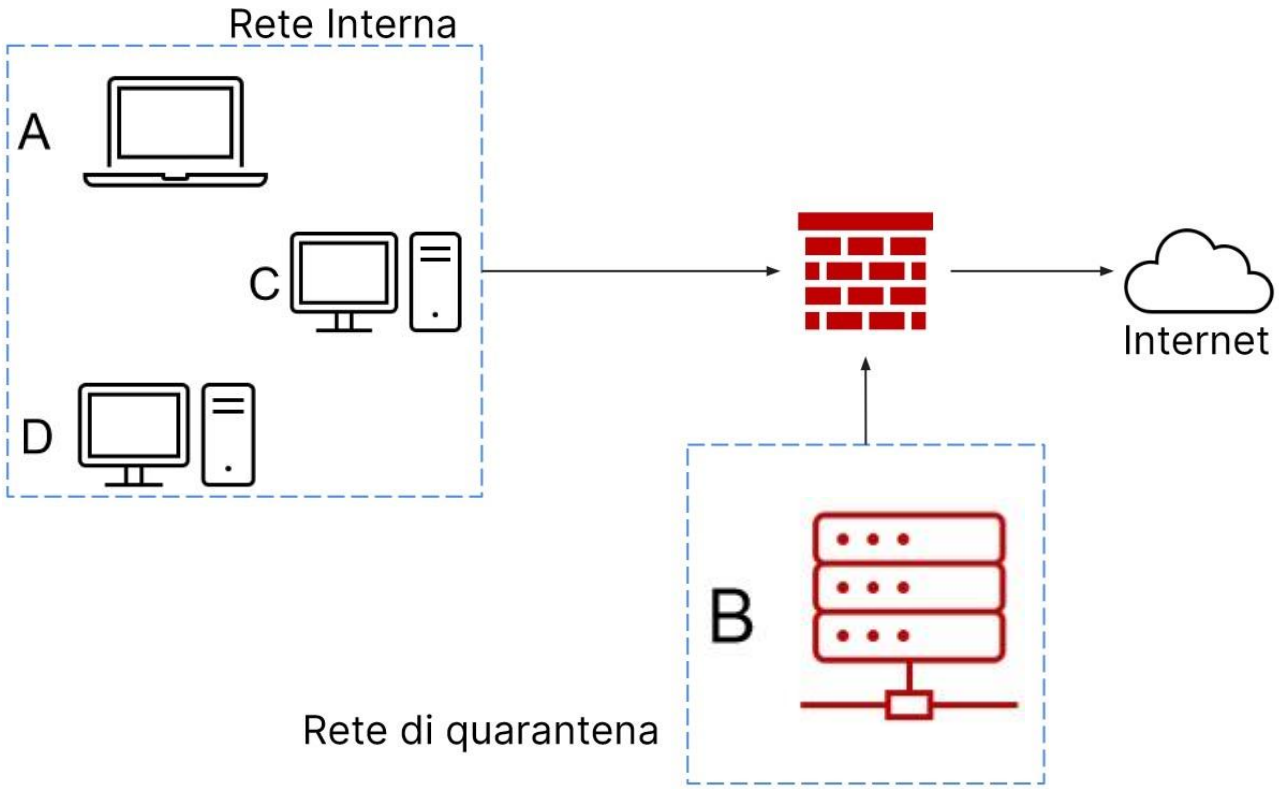
Incident Response



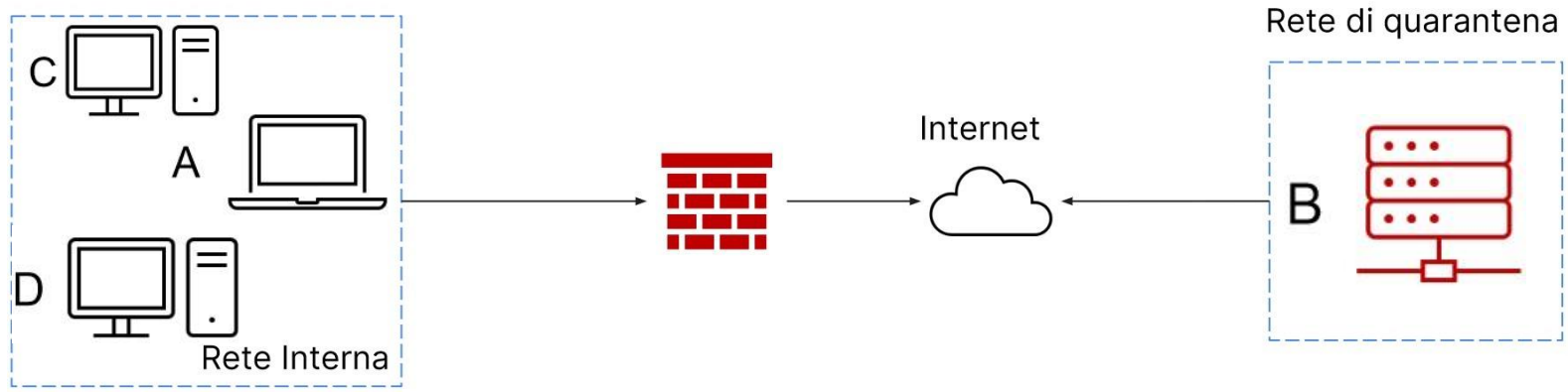
Nel caso che ci viene mostrato nell'immagine dovremmo rispondere a questo attacco, per prima cosa procederemo all'isolamento.

Ci sono diversi modi per staccare la rete infetta da quella principale.

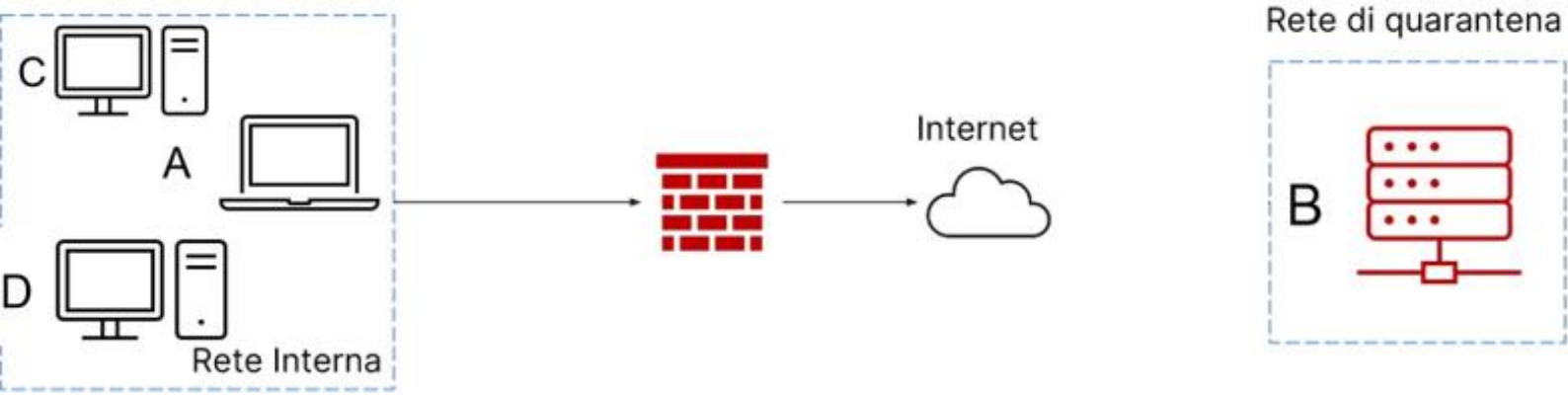
- Possiamo configurare una rete ad HOC, creando una "Rete di Quarantena" in maniera che la stessa rete infetta sia distaccata dalle altre reti così che non possa contagiare gli altri dispositivi.



- Se c’è bisogno di un contenimento maggiore possiamo creare un completo isolamento della rete infetta dal sistema, così che si possa aumentare il contenimento dell’infezione. Come si può notare l’attaccante ha ancora accesso al sistema infetto tramite internet.



- L’ultima tecncia, dove l’isolamento non è ancora bastato, in questo passeremmo direttamente alla rimozione del sistema dalla rete. Dove non ci sarà più nessun accesso.



La differenza tra Purge e Destroy è che nel primo caso vengono utilizzate, oltre che approcci soft, anche tecniche di rimozioni fisiche come nei magneti molto forti per rendere inaccessibili le informazioni mentre nel secondo caso vengono utilizzati anche metodi di laboratorio come: disintegrazione, polverizzazione dei media ad alte temperature.