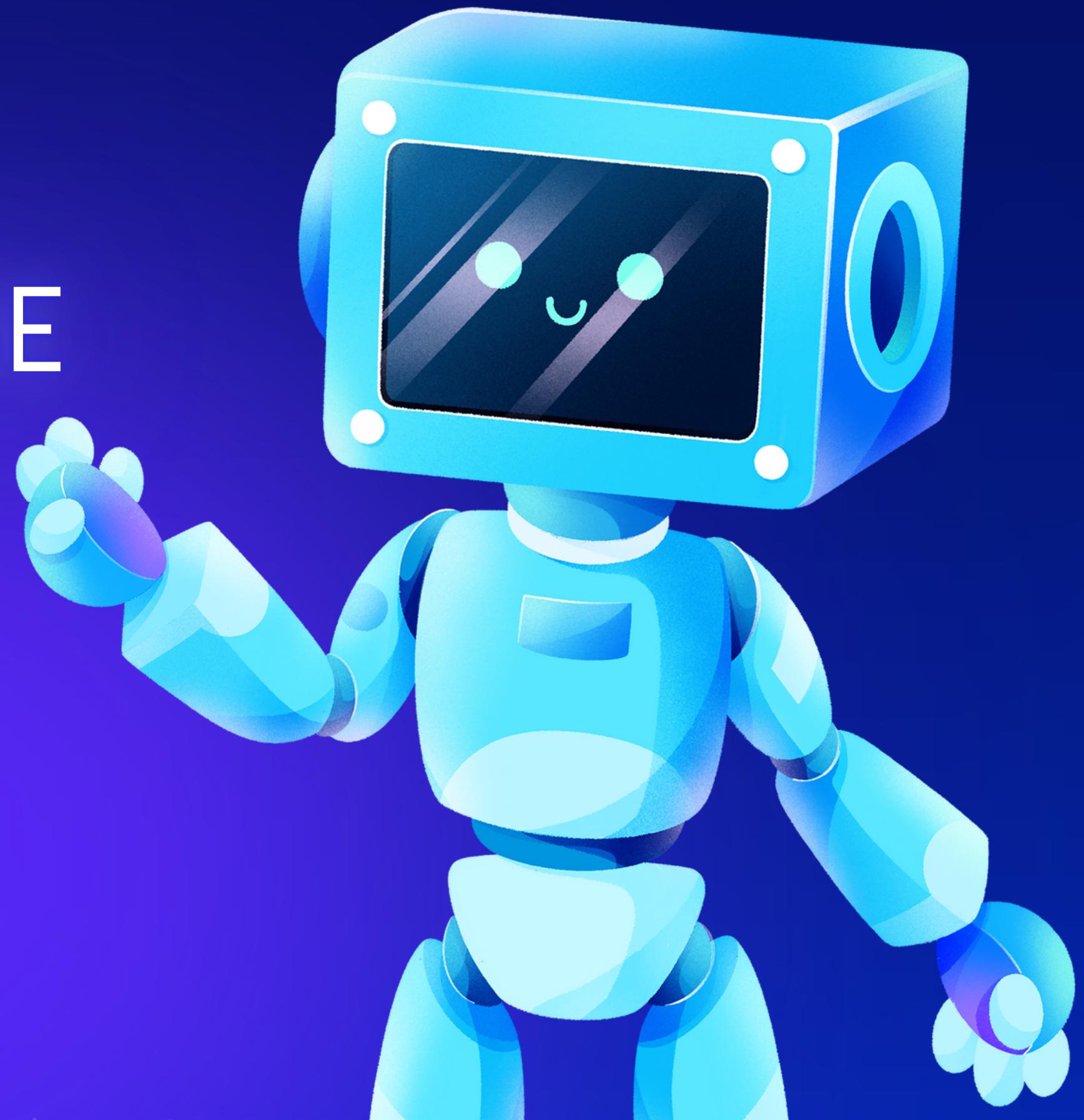


INCIDENT RESPONSE

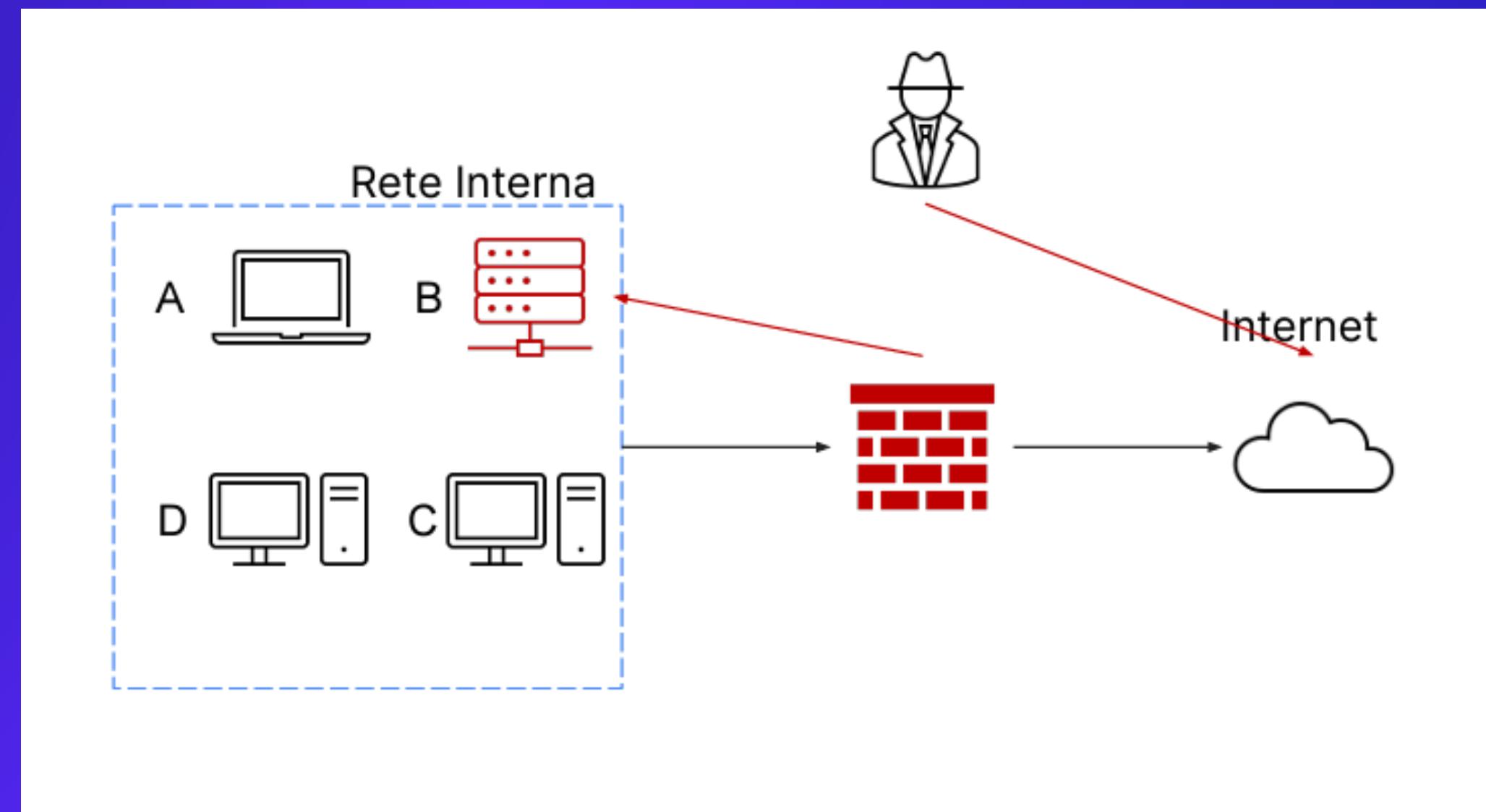
Ernesto Robles



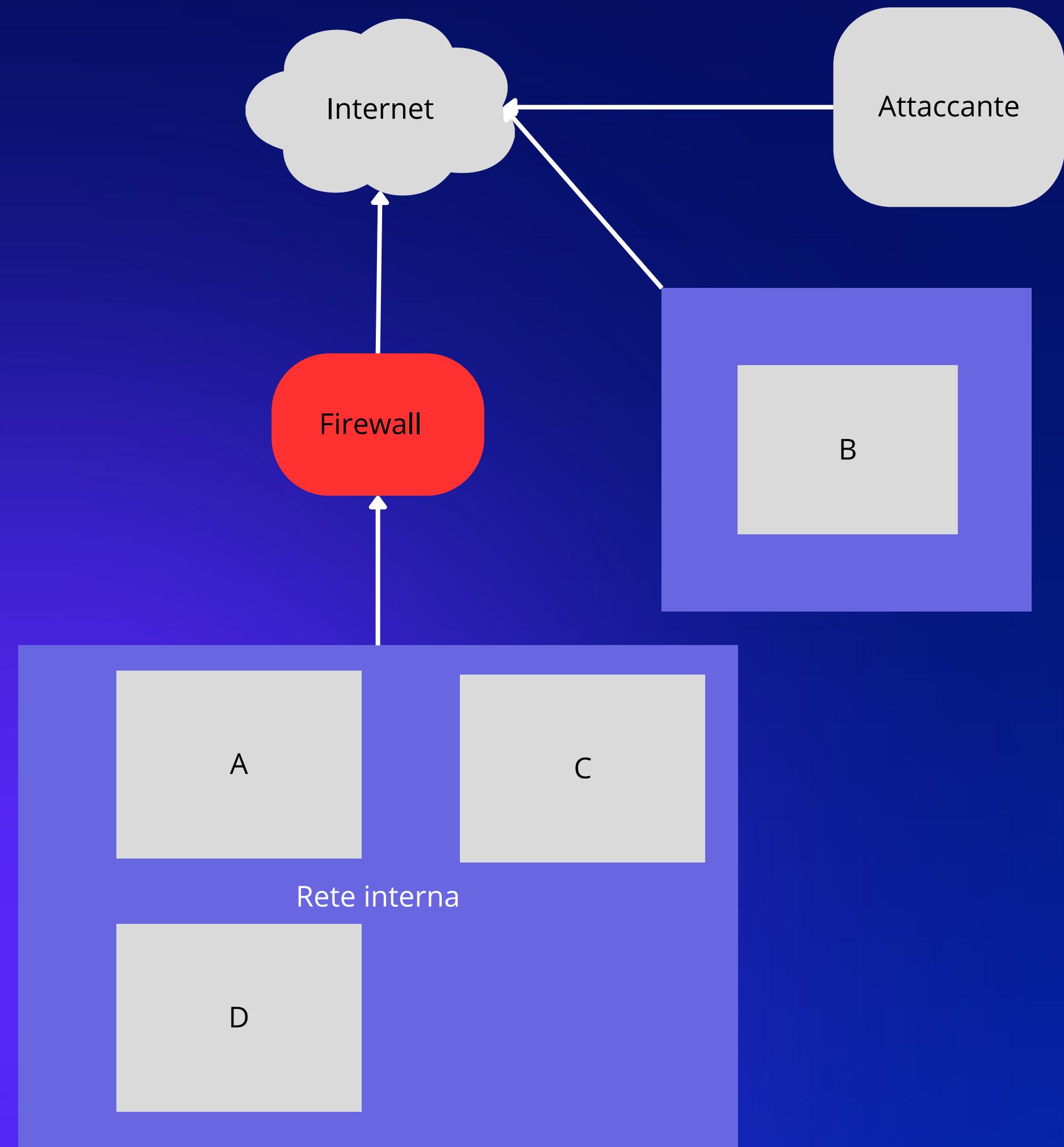


il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

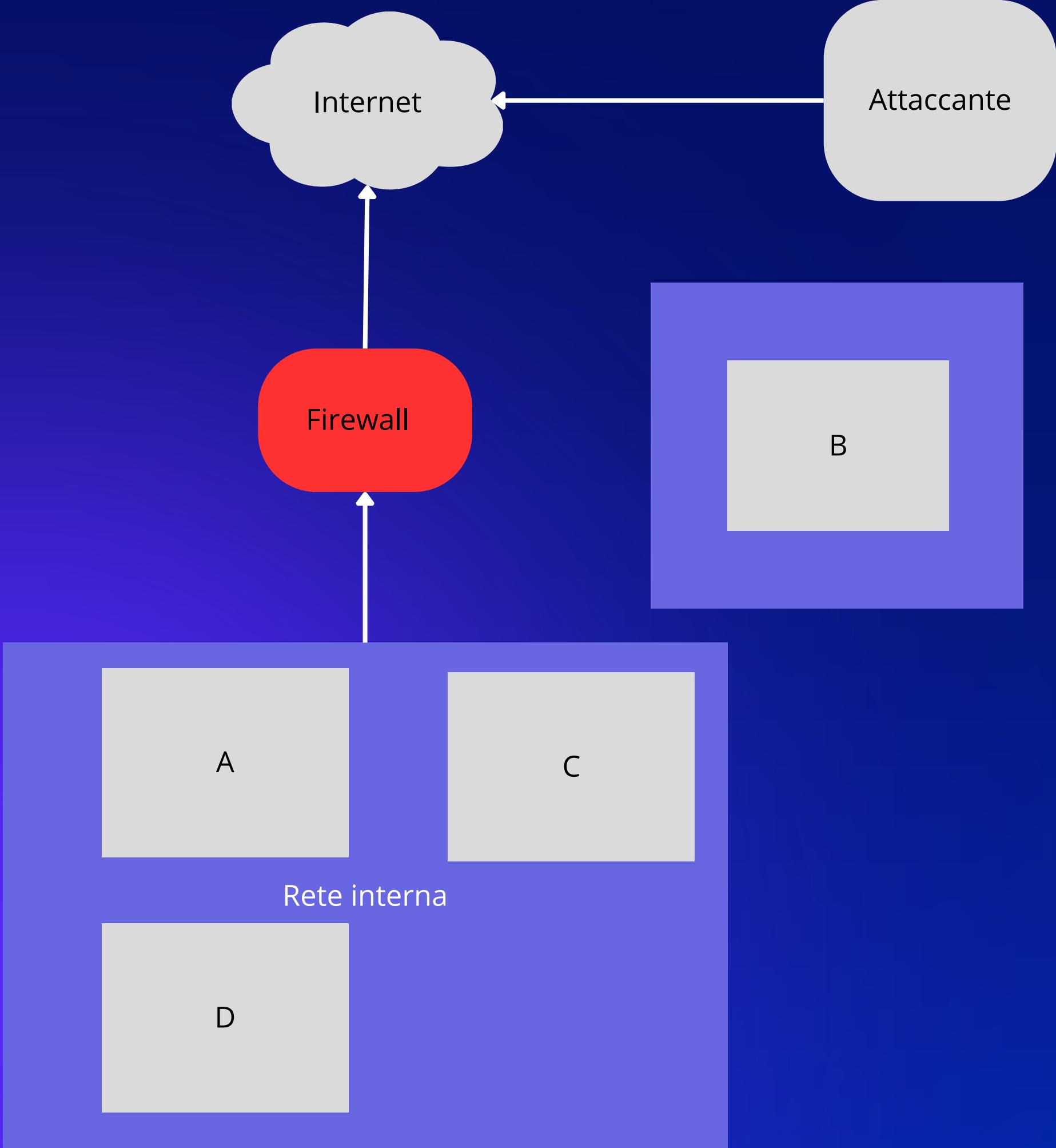
L'attacco è attualmente in corso ed essendo parte del team di CSIRT bisogna porvi una risposta.



La prima attività per contenere gli impatti è isolare il sistema rispetto al resto della rete in modo tale che il malware non si riproduca su altri nodi. Con l'uso della tecnica dell'isolamento si ottiene un contenimento maggiore, questo consiste nella completa disconnessione del sistema infetto dalla rete per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante, il quale però avrebbe ancora accesso al sistema B attraverso internet.

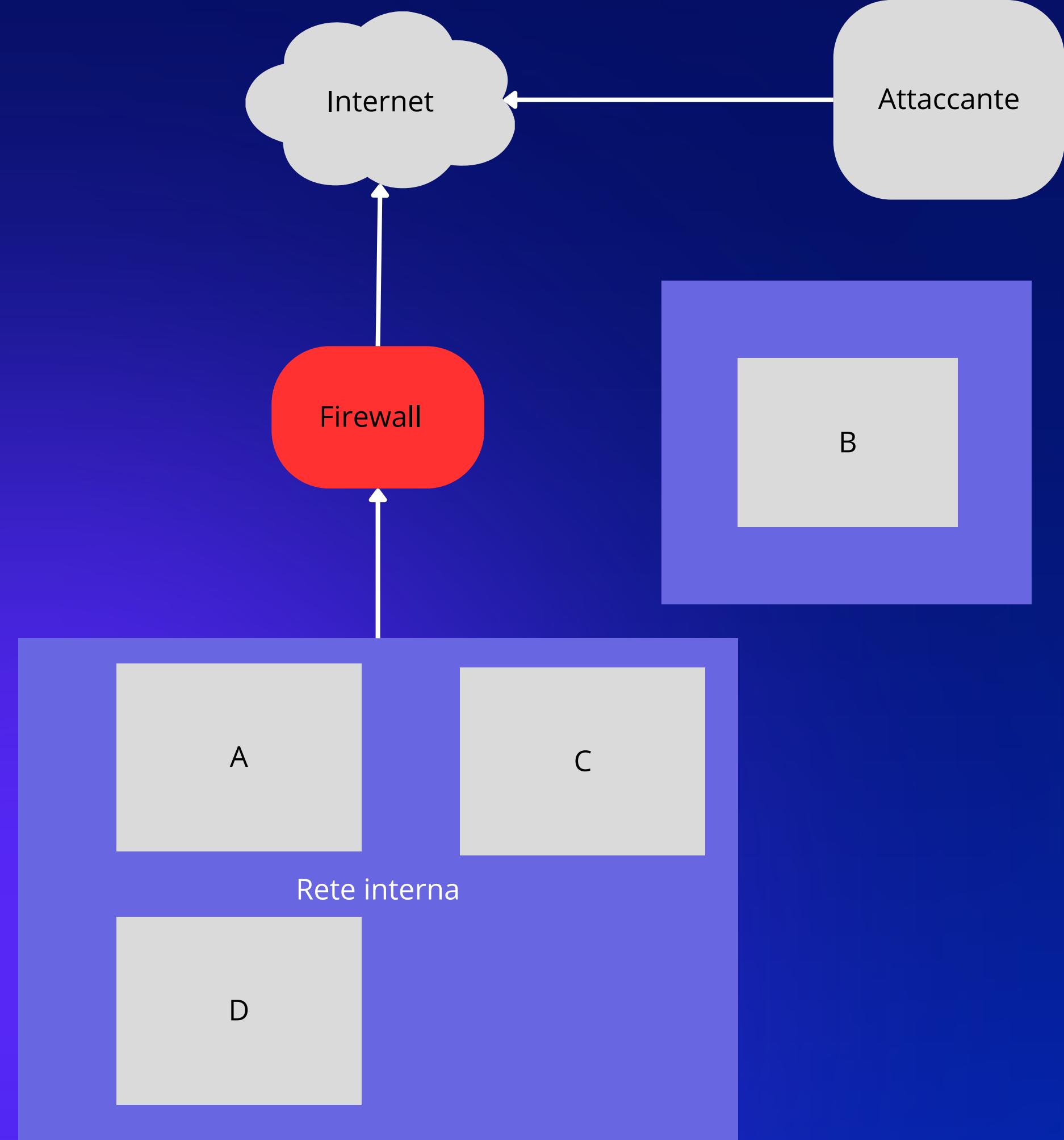


In alcuni casi l'isolamento non è ancora abbastanza perciò si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet in questo modo l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata



Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia la fase di recupero che consiste nel ristabilire la normale operatività delle applicazioni e dei servizi. Include ad esempio il recupero dei dati e delle informazioni perse, lo scopo della fase di recupero è anche quello di evitare che lo stesso attacco possa capitare nuovamente in futuro.

Per la gestione dei media contenenti informazioni sensibili possiamo seguire opzioni come Purge o Destroy.



Purge adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Destroy ha un approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.

