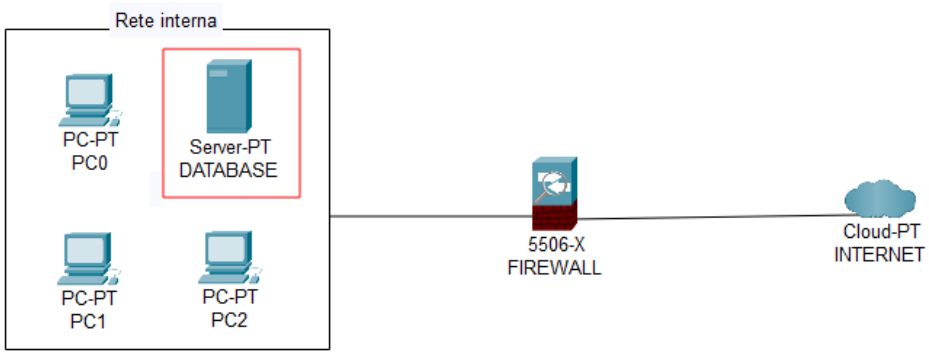
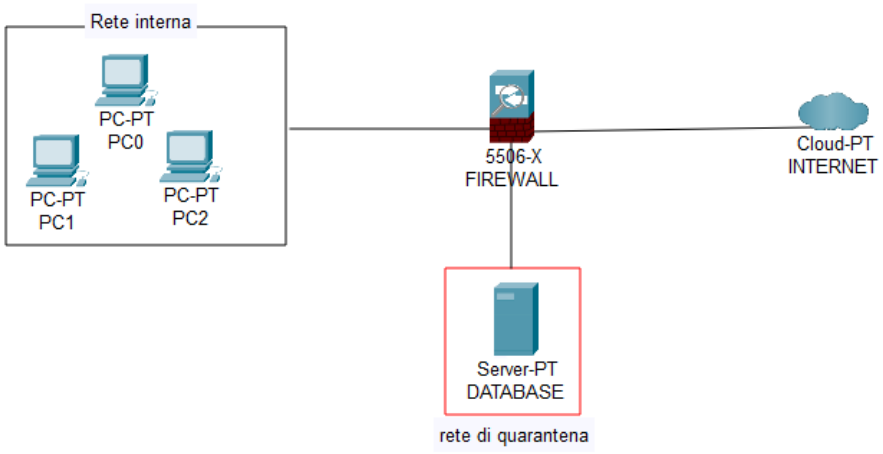
Incident response

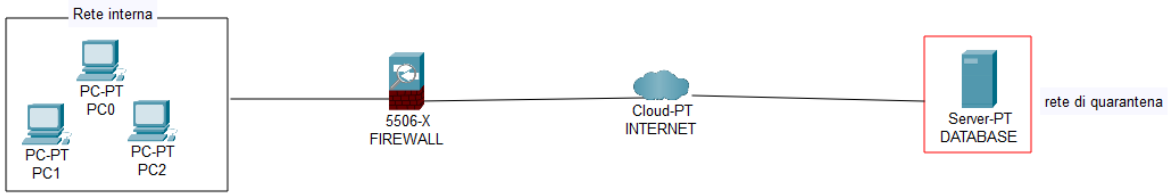
In figura, il sistema B (database con diversi dischi per lo storage) è stato compromesso da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attaccante è ancora in corso e l'esercizio chiede di mostrare le tecniche di **Isolamento** e **rimozione** del sistema infetto. Spiegare la differenza tra **Purge**, **Destroy** e **Clear.**



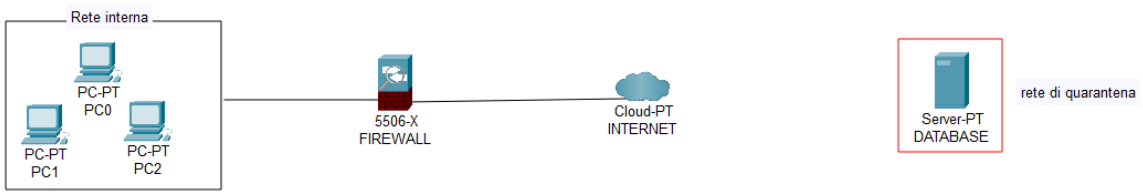
La segmentazione permette di separare il sistema dagli altri computer sulla rete, creando una rete ad hoc, che viene chiamata <<rete di quarantena>>.



Sebbene la segmentazione riesca a limitare la riproduzione del malware e l'accesso al resto della rete da parte dell'attaccante, spesso non è sufficiente per chiudere la fase di contenimento. In questo caso si utilizza la tecnica di isolamento.



Ci sono casi in cui l'isolamento non è abbastanza, si procede con la completa rimozione del sistema dalla reta sia interna che internet.



Ci sono tre opzioni per la gestione dei media contenenti informazioni sensibili:

clear: il dispositivo viene completamente ripulito con tecniche logiche. Si può effettuare un reset di fabbrica oppure la sovrascrittura del dispositivo, più volte per riportare il dispositivo nello stato iniziale.

Purge: oltre all'approccio logico, si usano anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere l'informazione inaccessibile su determinati dispositivi.

Destroy: con questa tecnica avviene una vera e proprio distruzione del dispositivo, utilizzando tecniche di laboratorio come disintegrazione, polverizzazione ad alte temperature o trapanazione.