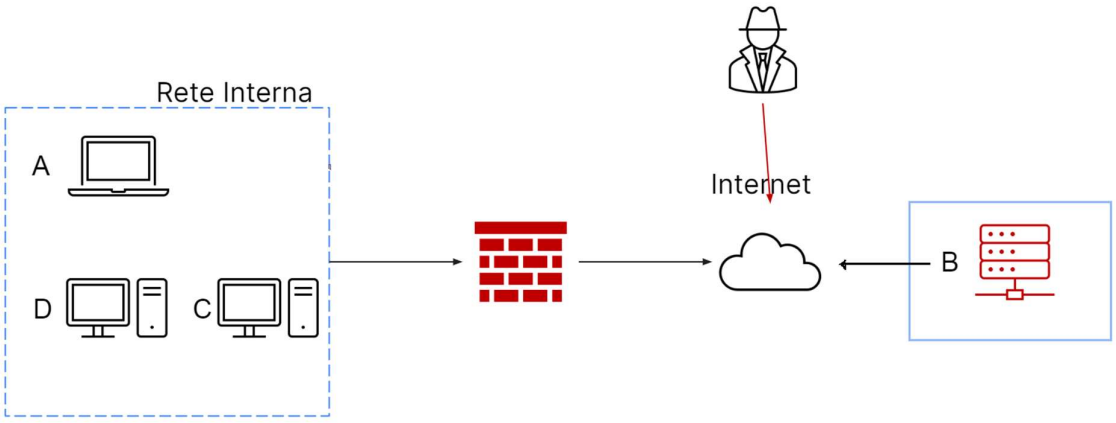
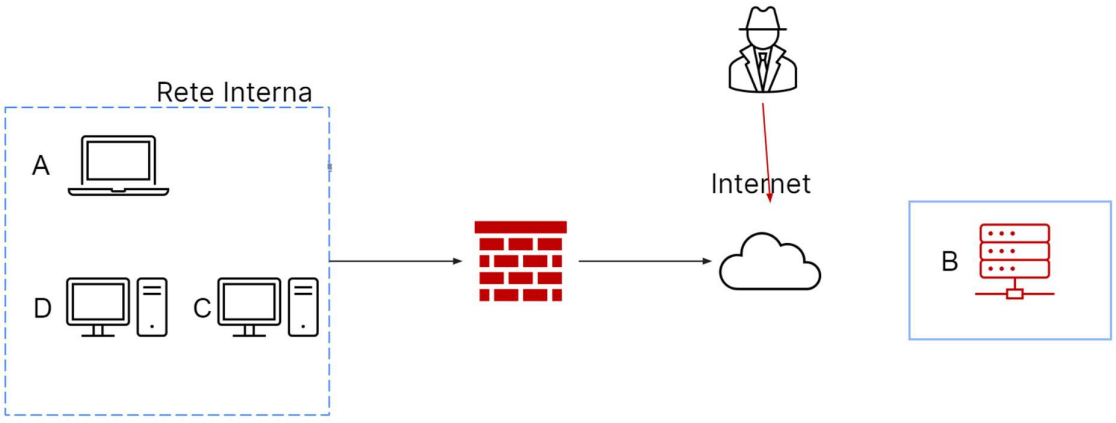
Esercizio Epicode 29/06/2023

Il sistema B, dopo essere stato compromesso interamente da un attaccante, è andato sotto il processo di **Isolamento**, come mostrato in figura. Ovvero il sistema infetto è stato completamente disconnesso dalla rete per restringere l'accesso alla rete interna da parte dell'attaccante. Sia l'attaccante che il sistema B hanno comunque ancora accesso ad Internet e l'accattante ha ancora accesso al sistema B.



In figura, vediamo la tecnica della **Rimozione**, in cui il sistema B è stato completamente rimosso sia da rete interna che da internet, in modo tale da impedire l'accesso alla macchina infettata dall'attaccante.



La differenza tra il metodo **Purge** ed il metodo **Destroy** è:

nel **Purge** si procede con la rimozione dei dati tramite l'uso di magneti. Il device non viene distrutto, anche se gli HDD risultano inutilizzabili a causa del processo che li danneggia.

Nel **Destroy** si procede con la distruzione vera e propria del device tramite varie tecniche, tra cui disintegrazione o trapanazione.

Il metodo **Clear** pulisce il device utilizzando, per esempio una tecnica nota come "factory reset", in cui i dati vengono sovrascritti innumerevoli volte per riportare il device nello stato iniziale. Queste tecniche vengono definite "logiche".