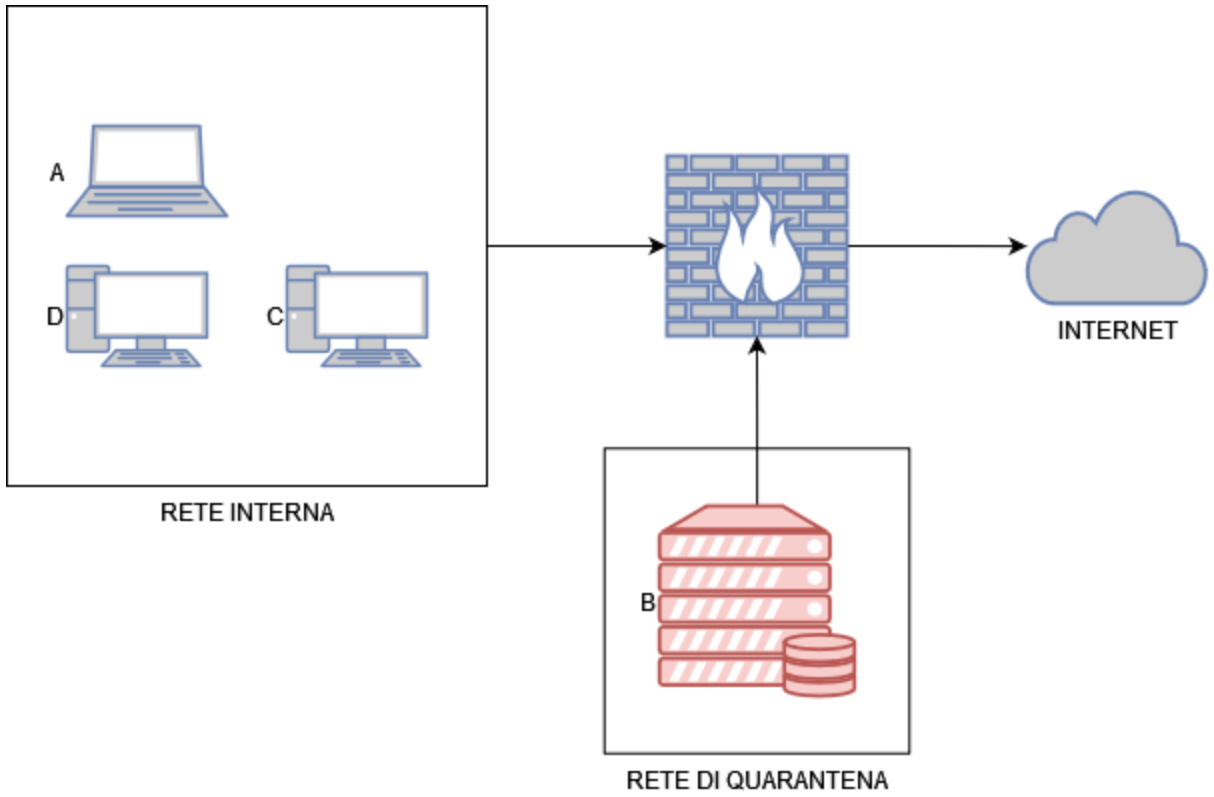
Nel caso un attaccante riuscisse a prendere controllo di un dispositivo all'interno di una rete e quest'ultima non fosse segmentata, avrebbe facile accesso anche al resto dei dispositivi nella rete.
La segmentazione (come nello schema a fianco) è un'ottima tecnica di prevenzione. Può essere fatta tramite l'uso di una (o più) VLAN o tramite il subnetting.
Così facendo sarebbe anche un ottimo modo per contenere i danni.

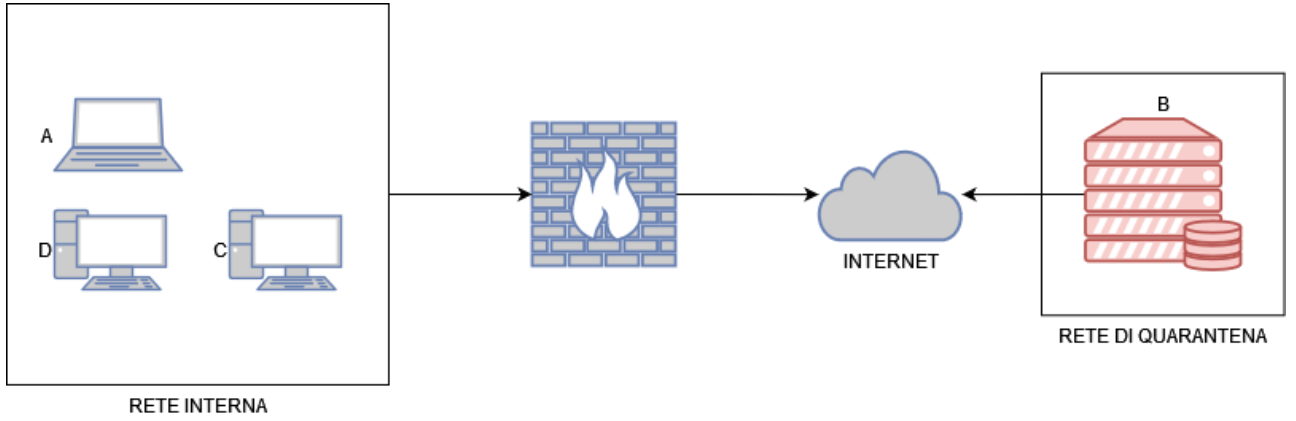
Nel caso di uno storage compromesso, si possono adottare varie tecniche, tra cui:
-Purge: si ha un approccio logico (es. la formattazione), ma si affianca ad un approccio fisico, tipo l'utilizzo di magneti forti nel caso degli HDD per rendere inaccessibili determinate informazioni.

-Destroy: è l'approccio più drastico per lo smaltimento degli storage compromessi. Oltre alle tecniche logiche, si tratta di distruggere (letteralmente) l'eventuale drive, cercandolo di "disintegrare" nel modo più minuzioso possibile onde evitare a tutti i costi il recupero delle informazioni su esso contenute.



Le altre due tecniche di contenimento ed isolamento sono rispettivamente:

-Di isolamento: consiste nel rimuovere interamente il dispositivo infetto dalla rete interna. Viene usato nel caso in cui la semplice segmentazione non dovesse bastare.
In questo caso l'attaccante può avere ancora accesso alla macchina compromessa tramite internet.



-Di rimozione: è il sistema più drastico, si tratta di rimuovere il dispositivo infetto interamente dalla rete interna e dalla rete internet, in modo da impedire l'accesso alla macchina tramite internet da parte dell'attaccante.