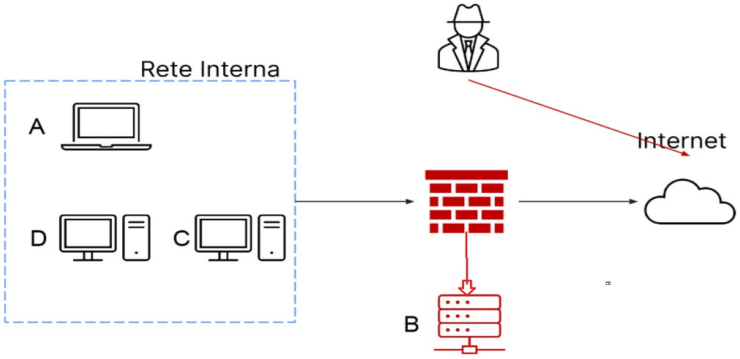
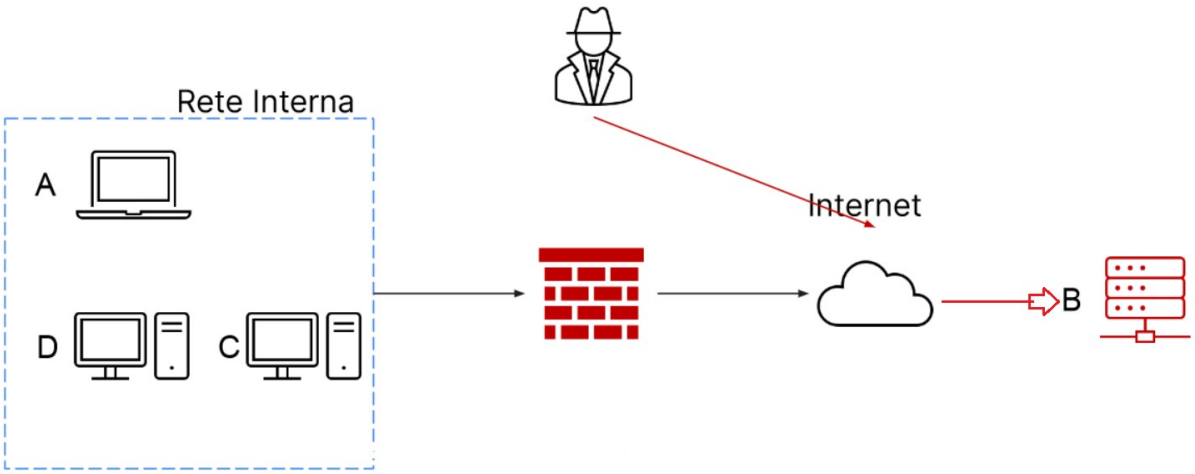
RETE DI QUARANTENA , ISOLAMENTO E RIMOZIONE, PURGE E DESTROY

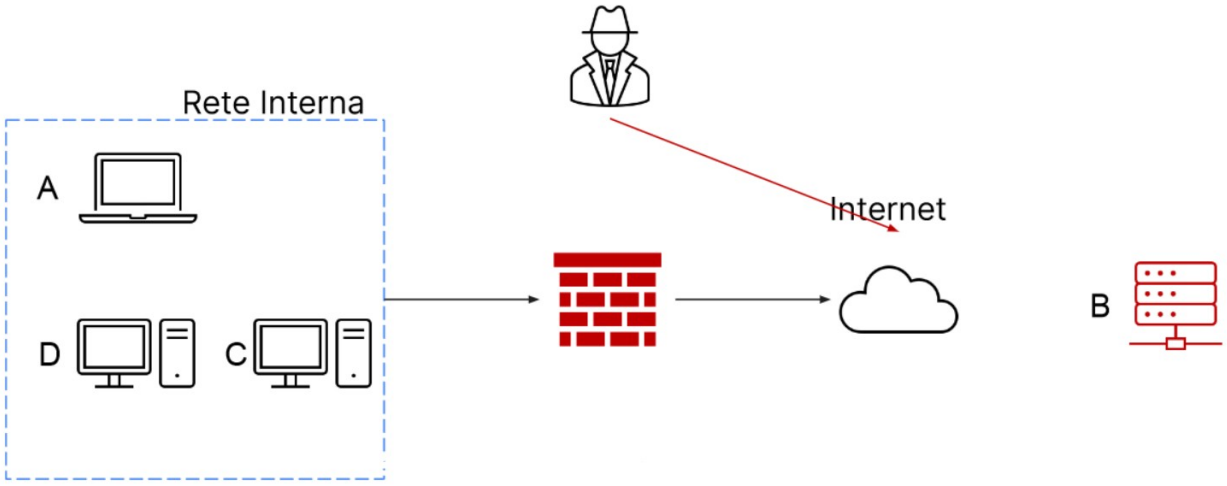
Rete di Quarantena: in questo caso il sistema attaccato è separato dagli altri servizi nella rete, creando una rete ad hoc. Questo limita la riproduzione del malware e l'accesso al resto della rete.



Isolamento: Questo tipo di segmentazione viene utilizzato qualora la tipologia precedente non fosse sufficiente. L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per limitare l'accesso alla rete interna da parte dell'attaccante, ma per l'attaccante è ancora possibile l'accesso al sistema C tramite internet.



Rimozione: Se l'isolamento non bastasse, in questi casi si procede con la tipologia di contenimento più rigorosa, ovvero la rimozione. Come da termine si rimuove sia dalla rete interna sia da internet il sistema infetto, levando all'attaccante l'accesso alla rete interna e alla macchina infetta.



RETE DI QUARANTENA , ISOLAMENTO E RIMOZIONE, PURGE E DESTROY

PURGE

Purge è un metodo di sanificazione dei dati che utilizza sia metodi logici che fisici per cancellare i dati. E il requisito fondamentale è che il recupero dei dati dovrebbe diventare irrealizzabile.

Sotto Purge, sia la sovrascrittura che la distruzione fisica sono tecniche di distruzione accettabili.

NIST Purge viene solitamente condotto in un ambiente di laboratorio. Metodi come la sovrascrittura, la cancellazione dei blocchi e la cancellazione crittografica vengono applicati in Elimina. Tutti questi sono metodi di distruzione logici. Quindi l'unità può essere riutilizzata. Ecco alcuni metodi utilizzati nel metodo di eliminazione.

- **Sovrascrittura:** vengono utilizzati uno o tre passaggi di sovrascrittura per rendere impossibile il ripristino dei dati.
- **Block Erase:** Qui, ogni blocco dei dispositivi di archiviazione viene cancellato elettricamente. Dopo un passaggio del metodo di cancellazione del blocco, gli 1 binari vengono applicati sulle posizioni indirizzabili dall'utente. Quindi la cancellazione del blocco viene eseguita di nuovo.
- **Cancellazione crittografica:** le chiavi di crittografia multimediale (MEK) vengono disinfettate. Ciò rende i dati non recuperabili.

  Vengono utilizzate anche tecniche di distruzione fisica come triturazione, smagnetizzazione e polverizzazione. Questi rendono il dispositivo inutilizzabile. Quindi tecnicamente i dati sono irrecuperabili. Ma le tecniche di distruzione fisica non sono economiche o rispettose dell'ambiente

RETE DI QUARANTENA , ISOLAMENTO E RIMOZIONE, PURGE E DESTROY

CLEAR

NIST Clear viene in genere utilizzato con dati non sensibili. Il metodo utilizza comandi di lettura e scrittura standard per sovrascrivere i dati sul disco.

Affinché la distruzione dei dati sia efficace, tutte le posizioni indirizzabili dall'utente su un disco devono essere distrutte.

La sovrascrittura può essere eseguita solo se non ci sono danni fisici al disco. La sovrascrittura, a volte, non è possibile su tutte le aree del dispositivo da sanificare. Ecco perché questa tecnica viene solitamente utilizzata con dati meno sensibili.

DESTROY

Il metodo destroy viene spesso utilizzato come ultima risorsa quando purge e clear non sono possibili alternative. Viene utilizzato anche quando la verifica della distruzione dei dati con tecniche di eliminazione e cancellazione fallisce.

In base a questo metodo, il supporto non è considerato completamente disinfettato a meno che il recupero dei dati non sia dimostrato fattibile utilizzando tecniche di laboratorio all'avanguardia. Ecco alcune tecniche utilizzate per distruggere i dispositivi.

- Disintegrare
- Polverizzare
- Incenerire
- Sciolto

Tutte queste tecniche distruggeranno completamente il dispositivo. Per questo motivo, non è possibile verificare se la distruzione dei dati è andata a buon fine.