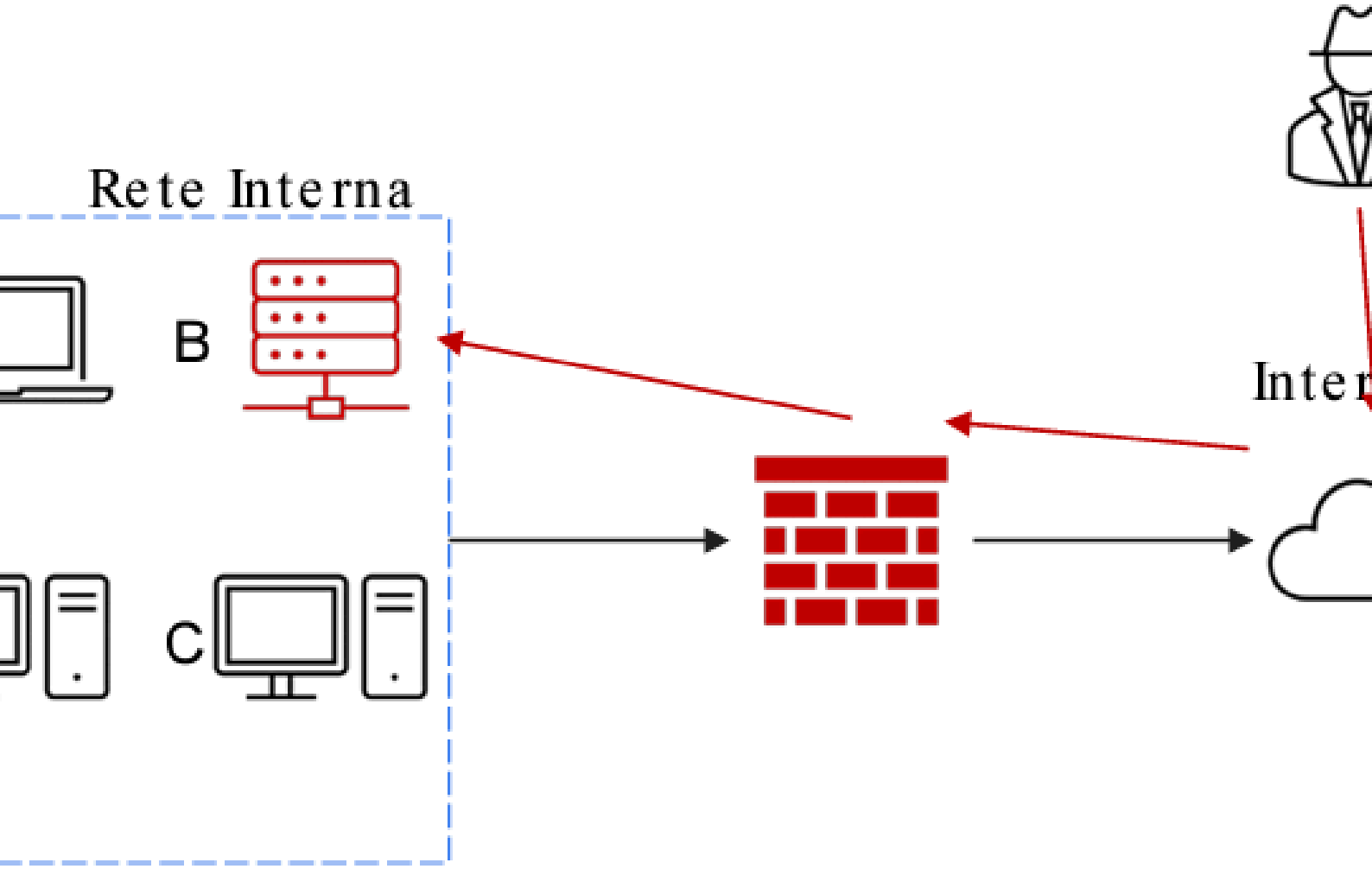
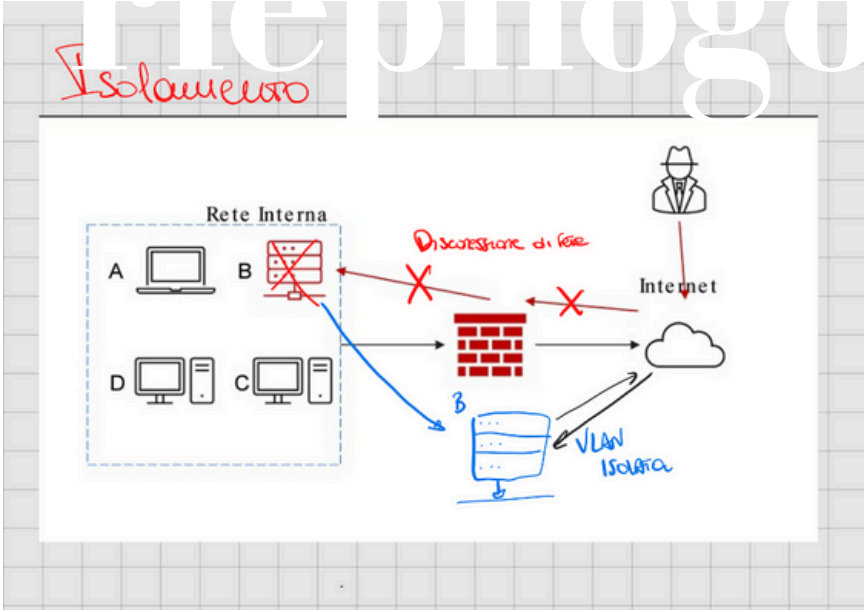
S9L4



Sarah Ortiz

Isolamento

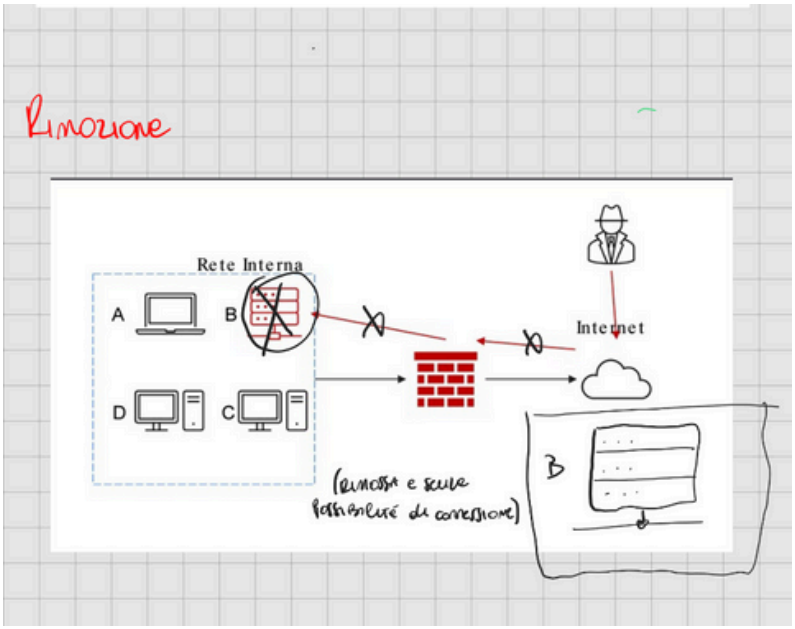


L'isolamento è il processo di separazione di un sistema compromesso dal resto della rete per impedire che il malware o l'attacco in corso possa propagarsi ad altri sistemi.

Vi sono due tecniche di Isolamento:

- la disconnessione della rete tramite software o scollegando fisicamente il cavo di rete. Il suo scopo è impedire che il sistema infetto possa comunicare con altri sistemi della rete interna o con Internet.
- Creare una VLAN isolata, assegnando il sistema infetto a una VLAN dedicata e isolata dal resto della rete. il cui scopo è contenere il traffico di rete del sistema compromesso in una rete virtuale separata, prevenendo la propagazione del malware.

Rimozione



La rimozione è il processo di eliminazione del malware o del software dannoso da un sistema compromesso per ripristinarlo a uno stato sicuro.
la tecnica utilizzata:

- spostare fisicamente o logicamente il sistema B in una posizione isolata per poter utilizzarlo senza rischi per il resto della rete. Lo scopo è quello di lavorare sul sistema B senza il rischio di contaminazione della rete interna.

Purge

Purge è il processo di rimozione dei dati in modo che non possano essere recuperati nemmeno con strumenti avanzati di recupero dati. Questo processo assicura un livello di sicurezza più elevato rispetto a Clear, rendendo i dati irrecuperabili anche con tecniche sofisticate. Metodi utilizzati:

- Sovrascrittura completa
- Cancellazione crittografica
- Demagnetizzazione

Destroy

Destroy è il processo di distruzione fisica del supporto di memorizzazione, garantendo che i dati non possano essere recuperati in alcun modo. Questo è il metodo più sicuro e definitivo per eliminare i dati sensibili. Metodi utilizzati:

- Triturazione
- Incenerimento
- Fusione o scioglimento
- Perforazione o frantumazione

Clear

Clear è il processo di rimozione dei dati in modo che non possano essere recuperati tramite strumenti standard di recupero dati. Questo processo rende i dati inaccessibili a chiunque utilizzi software o tecniche di recupero dati comunemente disponibili. Metodi utilizzati:

- Cancellazione software
- Formattazione