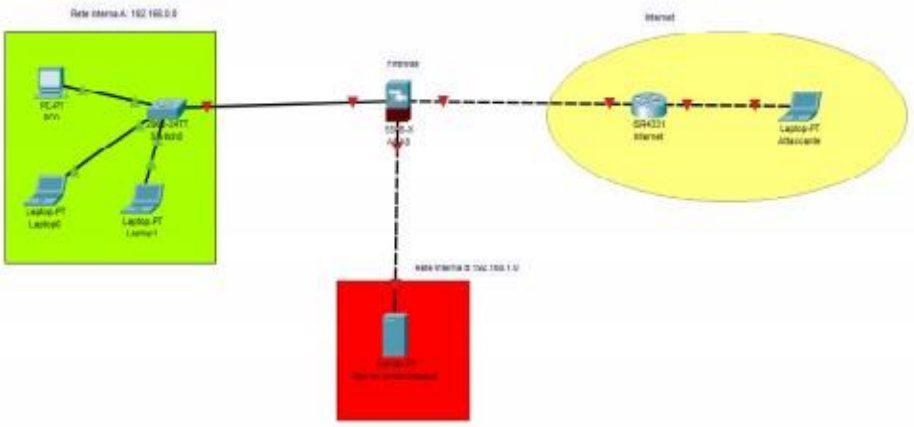
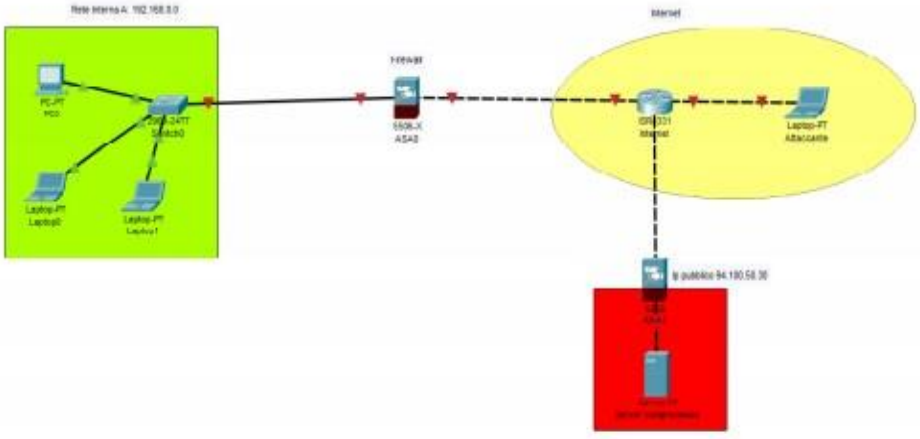
Tipi di gestione di rete

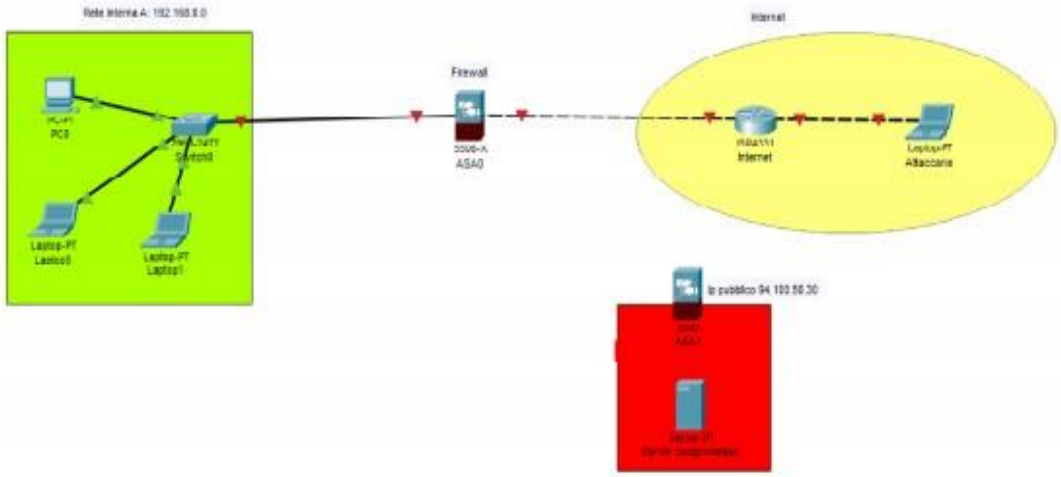
1. Rete di Quarantena: in questo caso il sistema attaccato è separato dagli altri servizi nella rete, creando una rete ad hoc. Questo limita la riproduzione del malware e l'accesso al resto della rete.



2. 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.



3. 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.



Fase di recupero

Durante la fase di recupero, si deve gestire lo smaltimento o il riutilizzo di un disco o di un sistema di storage del sistema compromesso. Prima di fare ciò si deve avere la sicurezza che le informazioni presenti nel componente siano completamente inaccessibili. Per l'eliminazione delle informazioni andremo ad utilizzare due tecniche:

1. Purge: si adotta sia un approccio logico (CLEAR), quindi un approccio read and write. Si va a sovrascrivere più volte. Ad esempio, lo standard DoD 5220.22-M prevede tre passaggi di sovrascrittura, mentre lo standard NIST SP 800-88 prevede fino a sette passaggi. Oppure si utilizza la "factory reset" per riportare il dispositivo allo stato iniziale. In più si sceglie un approccio con tecniche fisiche, come ad esempio l'uso di un magnete potrebbe essere una tecnica utile per distruggere fisicamente i dati su un disco rigido.

2. Destroy: prevede la completa distruzione fisica del disco o del dispositivo di storage in modo da renderlo completamente inutilizzabile e inaccessibile. Ci sono diversi modi per distruggere fisicamente un dispositivo di storage: triturazione, bruciatura o dissolvimento chimico. L'approccio Destroy è irreversibile e una volta che il disco o il dispositivo di storage è stato distrutto, non esiste alcun modo per recuperare i dati in esso contenuti. È importante assicurarsi di aver esaurito tutte le altre opzioni di recupero prima di optare per questo approccio.