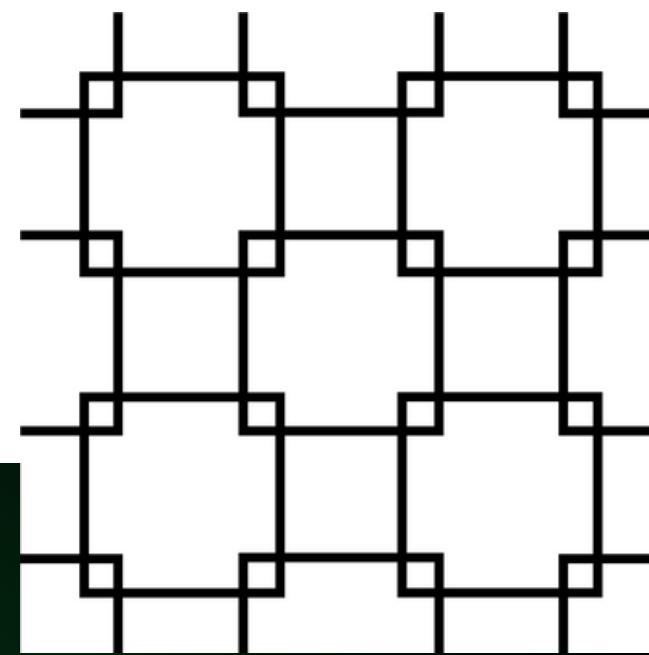


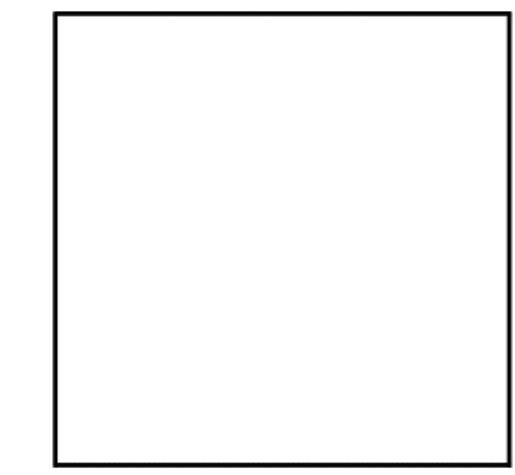
INCIDENT RESPONSE

In data odierna, il Sig. Rossi ha subito un attacco e ci ha chiesto di intervenire tempestivamente per gestire la criticità e ripristinare il sistema in modo da renderlo nuovamente utilizzabile e sicuro.

Modalità di gestione di un sistema compromesso



Segmentazione

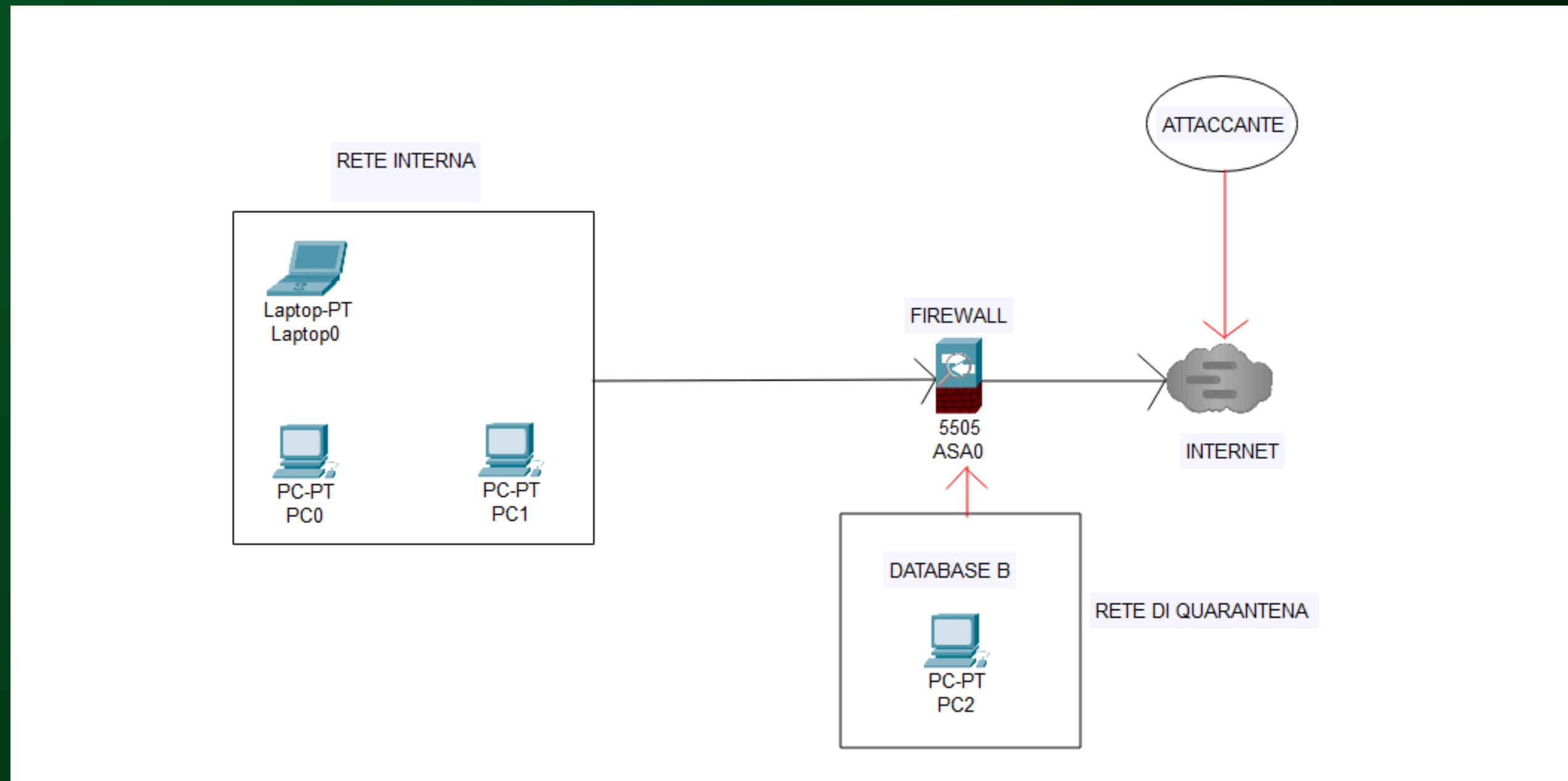


isolamento



Segmentazione

Se avviene un incidente, è possibile isolare il sistema compromesso (nel nostro caso il sistema B) creando una **VLAN**, in modo da contenere la diffusione del malware e impedire all'attaccante di muoversi per l'intera rete aziendale. Tuttavia, è buona pratica effettuare la segmentazione prima che avvenga un incidente.



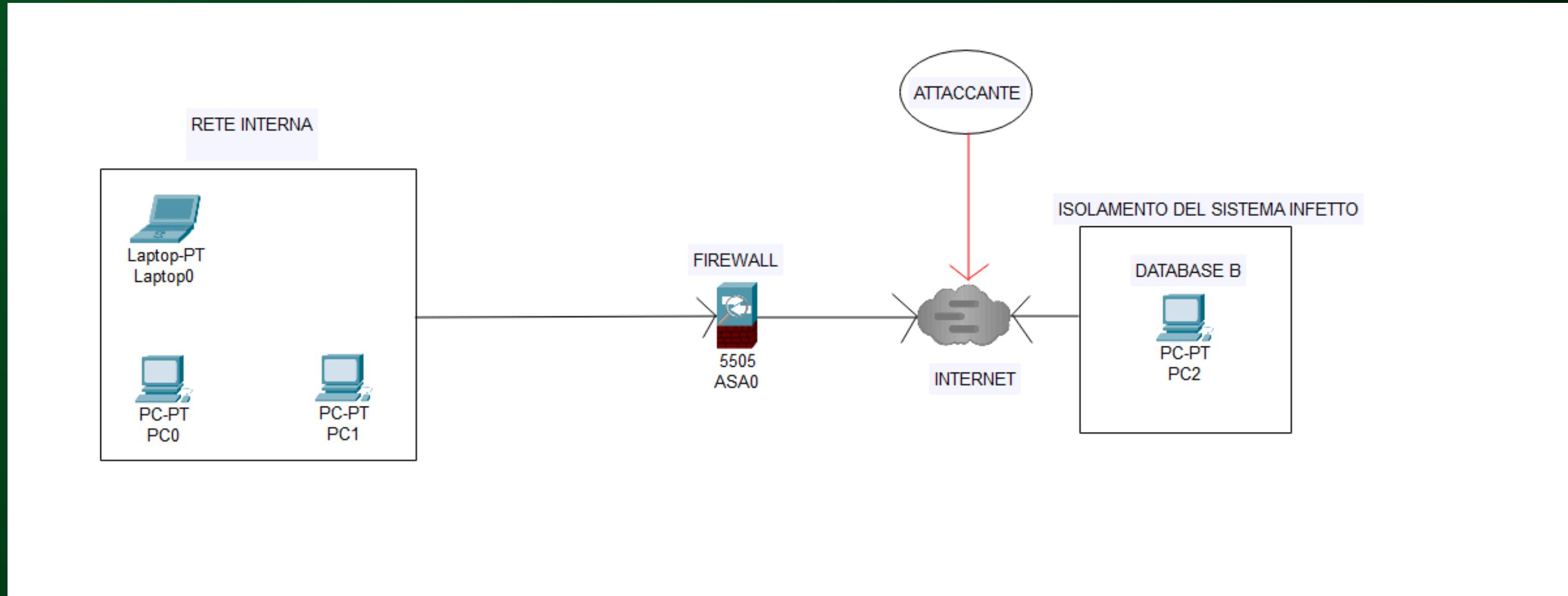
Creiamo una VLAN dedicata al sistema compromesso, chamata “**rete di quarantena**” (come in figura). Questo avrà una doppia utilità:

- Evitare che l'attaccante arrivi ai sistemi della rete non ancora compromessi
- Creare un ambiente sicuro dove poter analizzare, anche in un secondo momento, il malware (per esempio all'interno di una **sandbox**)



Isolamento

Questa tecnica prevede la **disconnessione fisica** del dispositivo dalla rete; sebbene impedisca il propagarsi del malware o il funzionamento delle backdoor, annienta l'accessibilità ai dati, creando disagi al business aziendale.



Abbiamo 2 opzioni (scegliamo in base alle policy aziendali):

- Isolare il sistema B dalla rete aziendale, ma permettergli di collegarsi comunque ad internet (come in figura)
- Isolare completamente il sistema B da internet, ma ciò impedirà ai dipendenti di avere accesso rapido alle risorse aziendali

Rimozione dell'incidente

Non basta aver isolato il sistema infetto; bisogna anche mettere in sicurezza ciò che più vale all'interno di un'azienda: i **dati**. La diffusione di dati sensibili, infatti, può causare (oltre ad un'enorme perdita finanziaria) anche delle ripercussioni legali.



RECUPERO DATI

Esistono 2 approcci per il recupero di dati da dischi compromessi :

- Reconstruction: se il sistema non è stato interamente compromesso, possiamo recuperare le parti non intaccate ed eliminare quelle compromesse
- Rebuilding: se il sistema è stato interamente compromesso oppure non conosciamo appieno la gravità del danno, dovremo ricostruire interamente il sistema

Esistono 3 principali modalità per distruggere file o dispositivi non più sicuri:

Distruzione dei File/Dispositivi compromessi

Clear

I dati presenti sul dispositivo vengono sovrascritti più volte con tecniche “logiche” per essere sicuri che non rimanga traccia dei dati malevoli. Si tratta di un ripristino dati di fabbrica.

Purge

Oltre all’approccio logico, si utilizzano magneti per la rimozione dei dati.

Destroy

Si tratta dell’eliminazione “fisica” del dispositivo su cui sono presenti i dati. Questo approccio può avvalersi anche di sofisticate tecnologie di laboratorio.