




Esercizio S9 L4



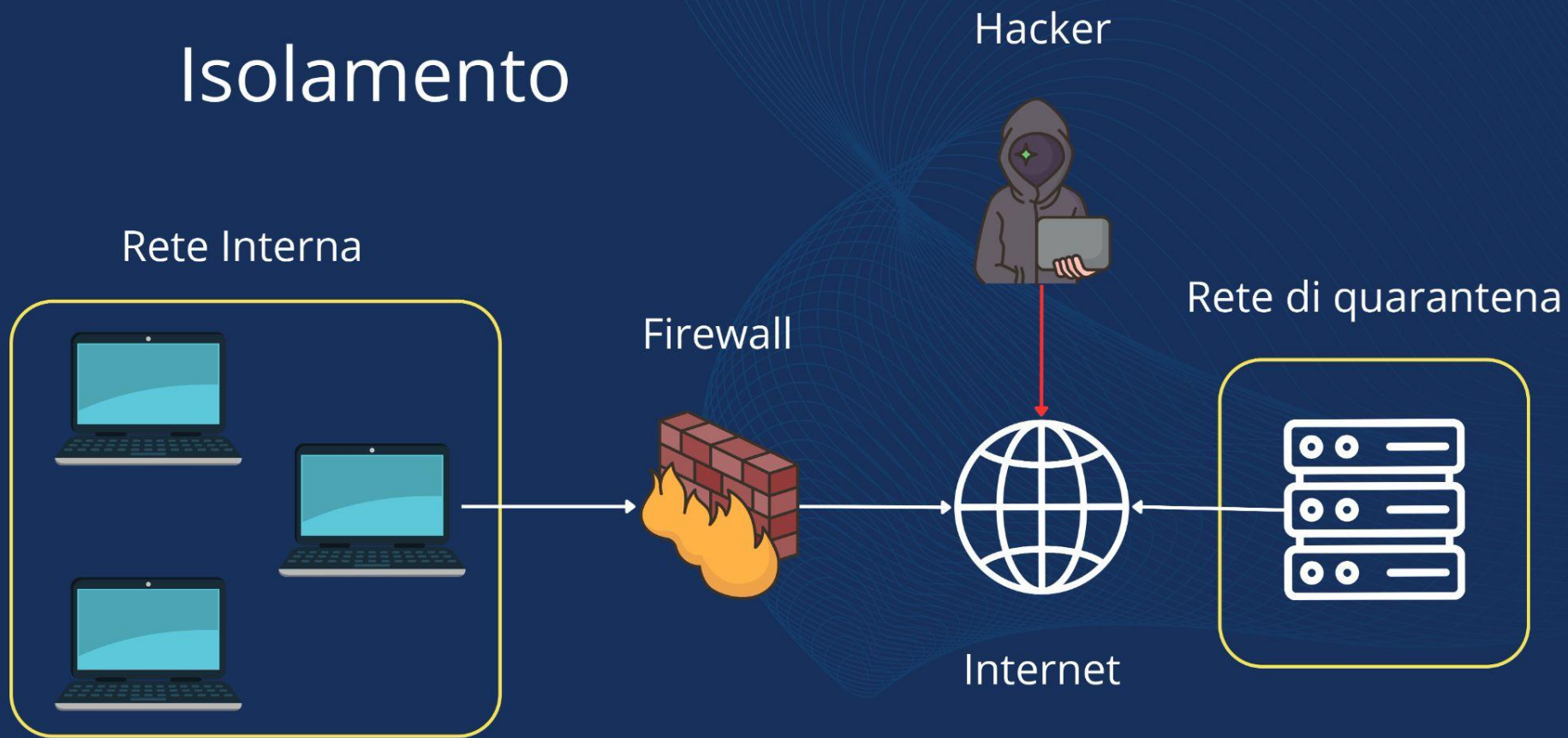
Nelle seguenti due slides sono mostrati degli esempi di isolamento e rimozione di un elemento infetto da una rete.

In entrambi i casi la rete è stata segmentata per limitare la diffusione di malware infetto alla rete interna e per separare l'elemento infetto dalla rete interna.

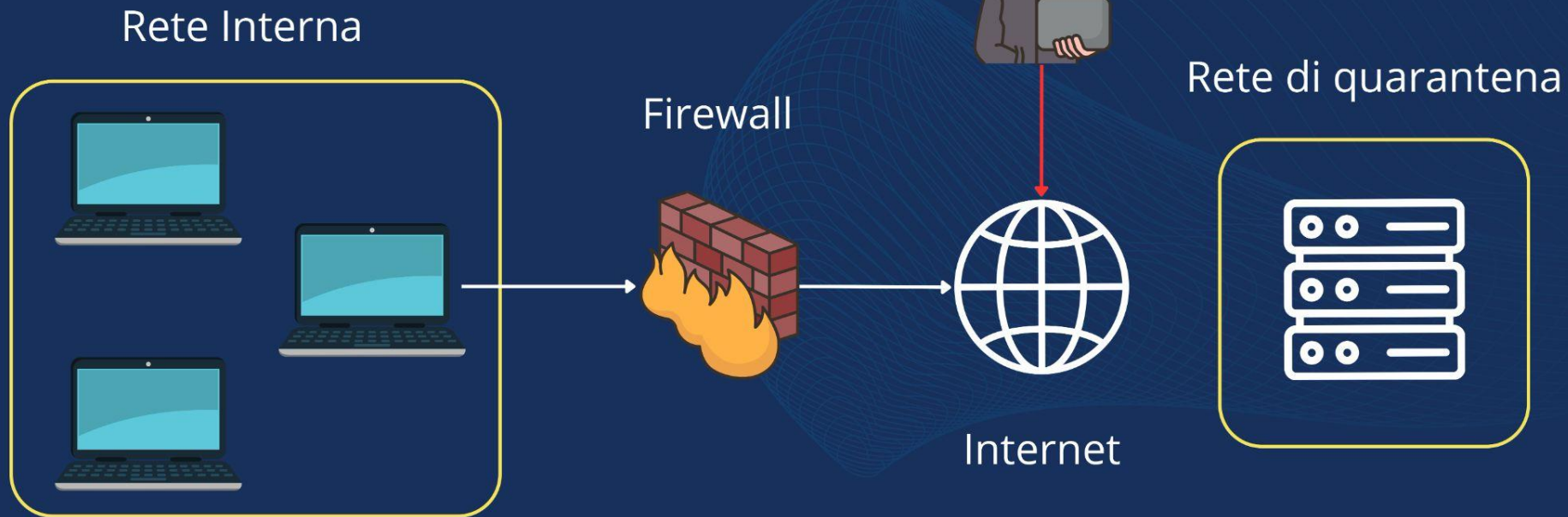
Nel caso dell'isolamento il server infetto è stato spostato in una rete diversa chiamata "Rete di quarantena", in questo modo il server infetto non può più comunicare con le macchine presenti nella rete interna ma può ancora comunicare con internet.

Nel caso della rimozione il server infetto è stato spostato in una rete diversa chiamata "Rete di quarantena", però a differenza dell'isolamento in questo caso il server infetto è stato tagliato fuori da qualsiasi comunicazione e non può connettersi neanche ad internet.

Isolamento



Rimozione





Differenza tra Purge e Destroy.

Quando vogliamo assicurarci che dei file contenuti nei dischi rigidi diventino inaccessibili ed impossibili da reperire possiamo optare per diversi metodi, vediamo in dettaglio due di questi.

Metodo 1 Purge:

Questa tecnica prevede l'utilizzo di magneti molto potenti per smagnetizzare il disco rigido e renderlo illeggibile ed inscrivibile, essenzialmente riducendolo ad un fermacarte.

Metodo 2 Destroy:

Questa tecnica prevede la distruzione fisica del disco rigido mediante incenerimento, alla fine del processo non rimane altro che cenere e di conseguenza non sarà possibile effettuare alcun tipo di analisi per tentare di rintracciare i dati precedentemente contenuti sull'hard disk.