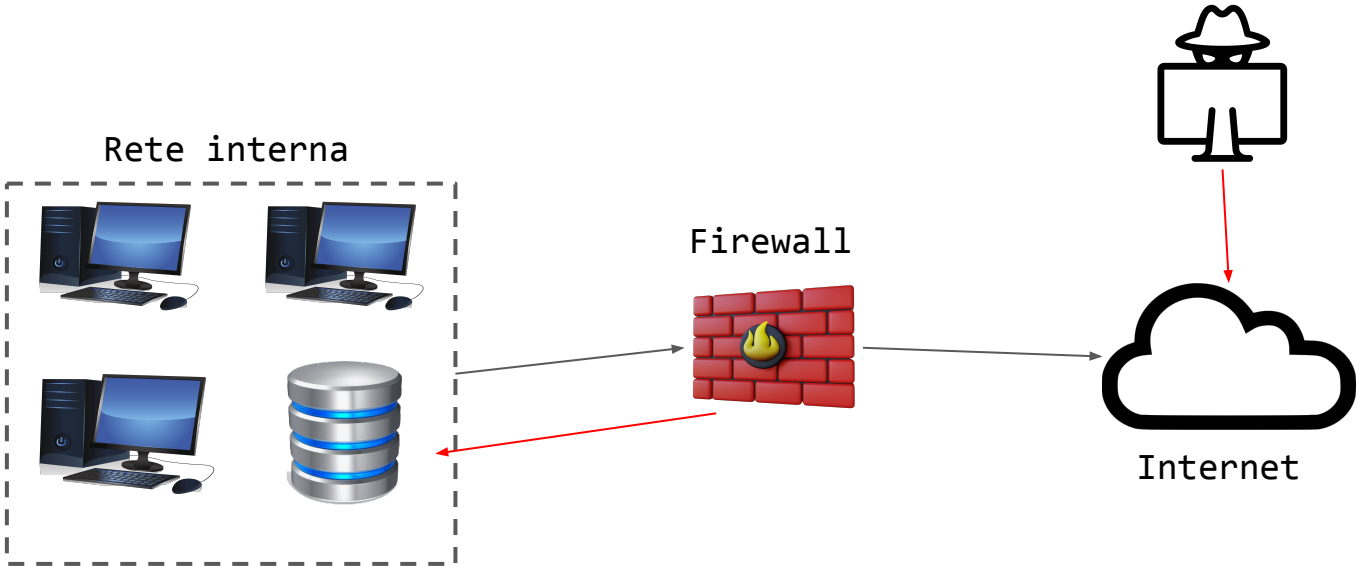
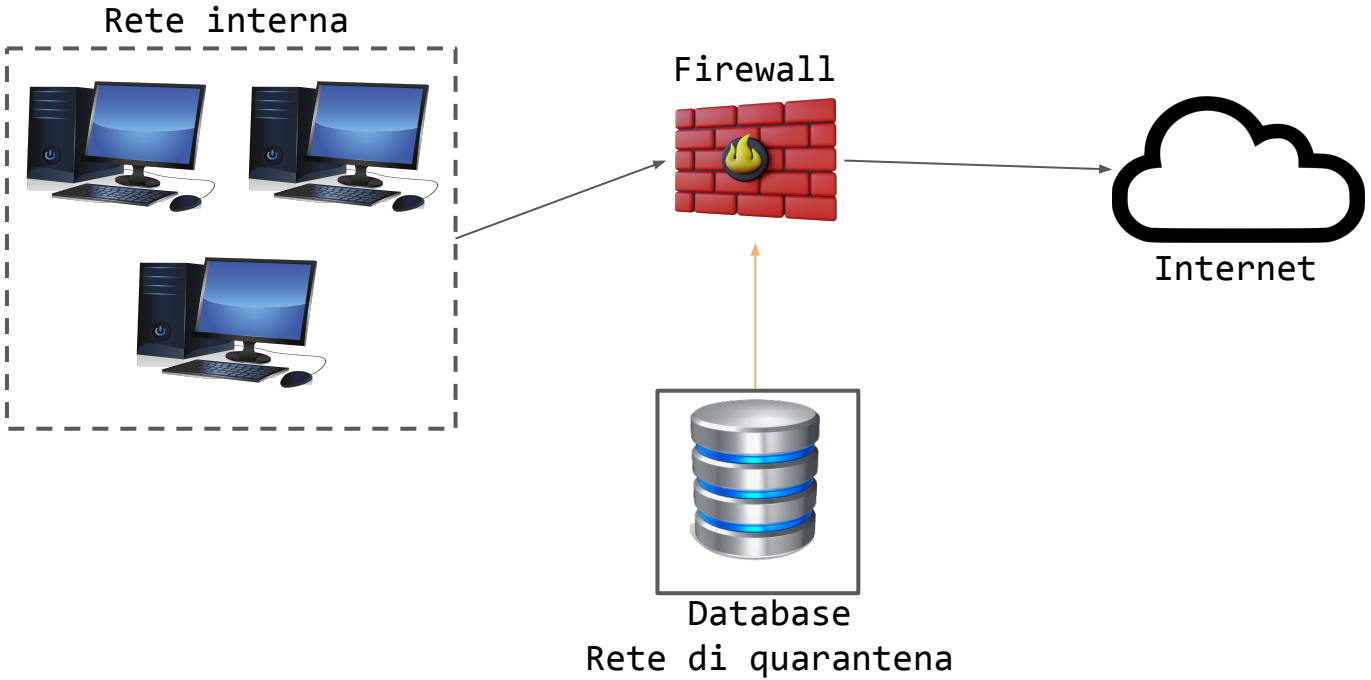
Riferimento: Attacco in corso



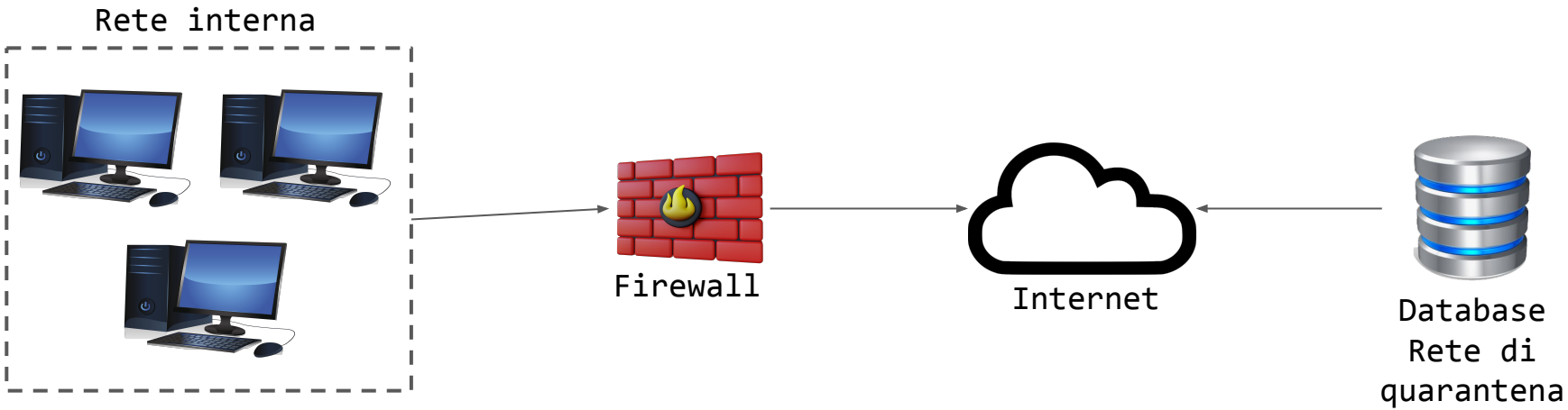
L'esercizio mira a simulare un attacco informatico in cui un database è stato compromesso e richiede la capacità di rispondere rapidamente, isolare il database compromesso e mitigare gli effetti dell'attacco. L'obiettivo principale è proteggere la rete interna e prevenire ulteriori danni all'infrastruttura.

Isolamento: Rete di quarantena



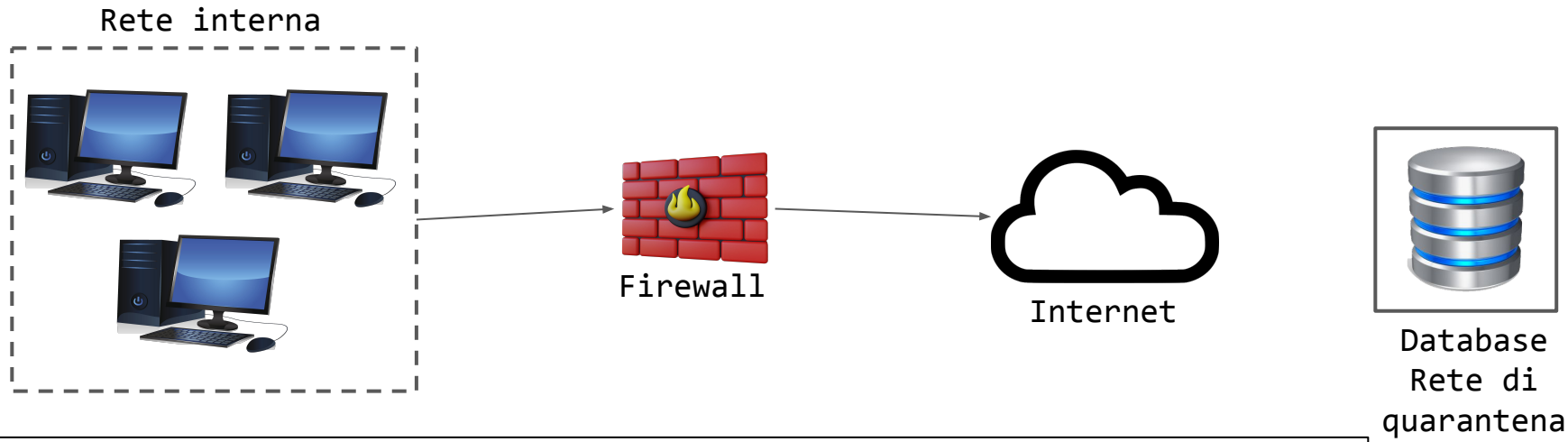
Isolare la macchina compromessa all'interno di una rete di quarantena:
Il primo passo consiste nel creare una rete di quarantena per la macchina bucata. Questa rete dove essere completamente separata dalla rete principale. Possiamo utilizzare il firewall per creare una zona isolata in cui il traffico sia strettamente controllato. In questo modo, l'attaccante non avrà accesso diretto alla rete principale e agli altri sistemi.

Isolamento: Rete di quarantena



Nello schema di seguito viene proposto un approccio alternativo per isolare la macchina compromessa dalla rete principale: collegarla direttamente a Internet. Questa configurazione consente di monitorare attentamente le azioni dell'attaccante al fine di comprendere i suoi movimenti e mitigare la vulnerabilità sfruttata. L'obiettivo è acquisire una conoscenza approfondita dell'attacco per prevenire future intrusioni su altre macchine aziendali.

Rimozione



La completa rimozione del sistema significa disconnettere fisicamente il dispositivo compromesso dalla rete aziendale e interrompere ogni forma di connessione con Internet. Questa azione estrema è solitamente intrapresa quando si ritiene che il sistema compromesso sia compromesso in modo irrimediabile o che la sua presenza possa rappresentare un rischio significativo per l'intera rete.

Purge, Destroy e Clear

Purge: eliminare in modo sicuro e completo dati o informazioni sensibili. In termini di sicurezza informatica, si usa per rimuovere definitivamente un database o file critici per evitare che siano accessibili o recuperabili da persone non autorizzate.

Destroy: la distruzione totale di un elemento o sistema. Nella sicurezza informatica, si riferisce all'eliminazione fisica di un dispositivo di memorizzazione, come un hard disk o una chiavetta USB, in modo che i dati contenuti non possano essere recuperati in alcun modo.

Clear: l'azione di rimuovere o cancellare dati o informazioni presenti in un sistema o dispositivo.
Ad esempio, può significare cancellare i dati da un database o rimuovere informazioni personali da un'app o dispositivo.
Tuttavia, a differenza di "purge" e "destroy", "clear" potrebbe non garantire l'eliminazione completa dei dati e potrebbe essere possibile il loro recupero in determinate circostanze.

In breve, "purge" implica l'eliminazione sicura dei dati, "destroy" indica la distruzione completa di un elemento e "clear" si riferisce alla rimozione o cancellazione dei dati senza garantire la loro eliminazione definitiva.