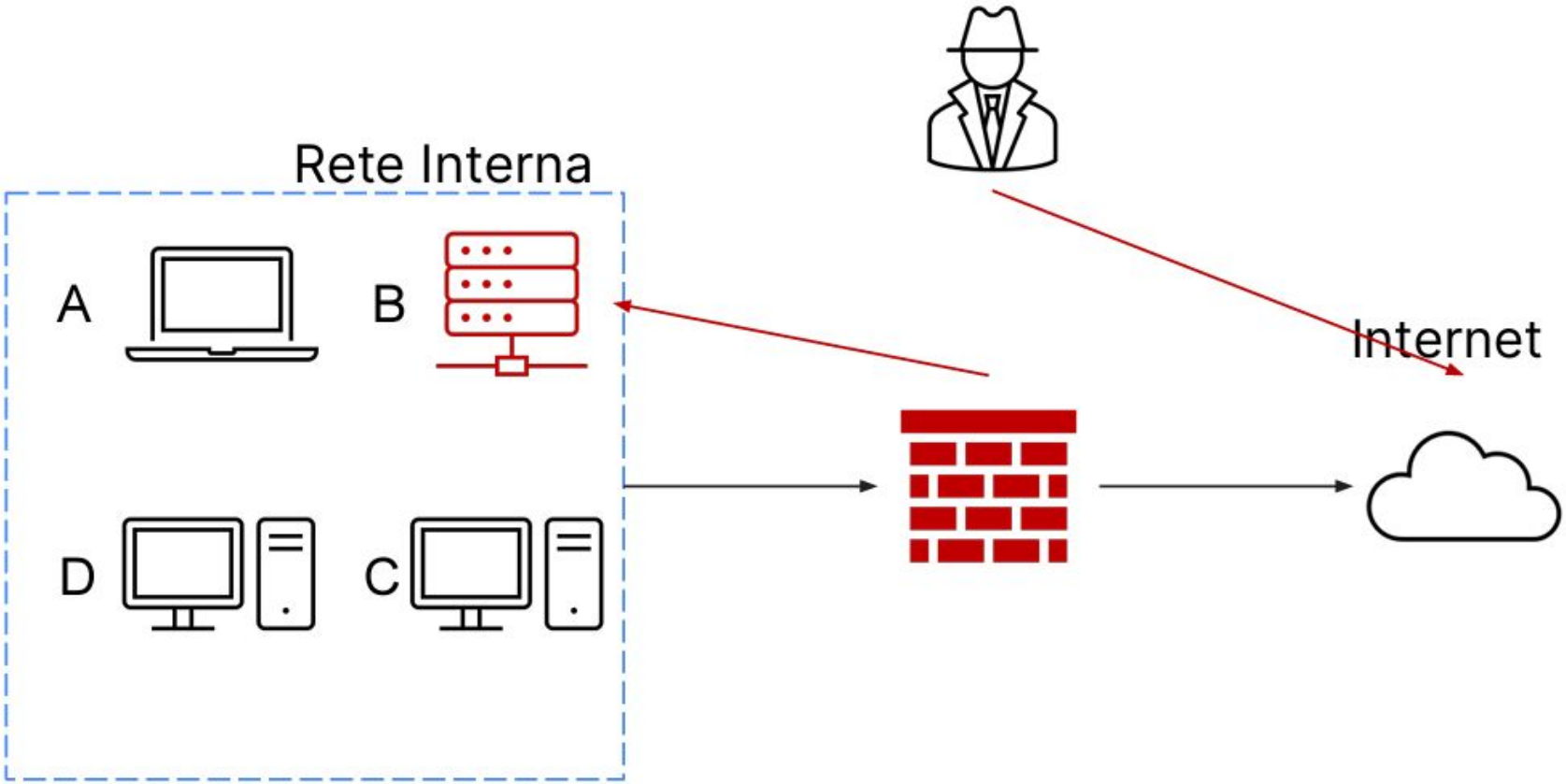
S9L4

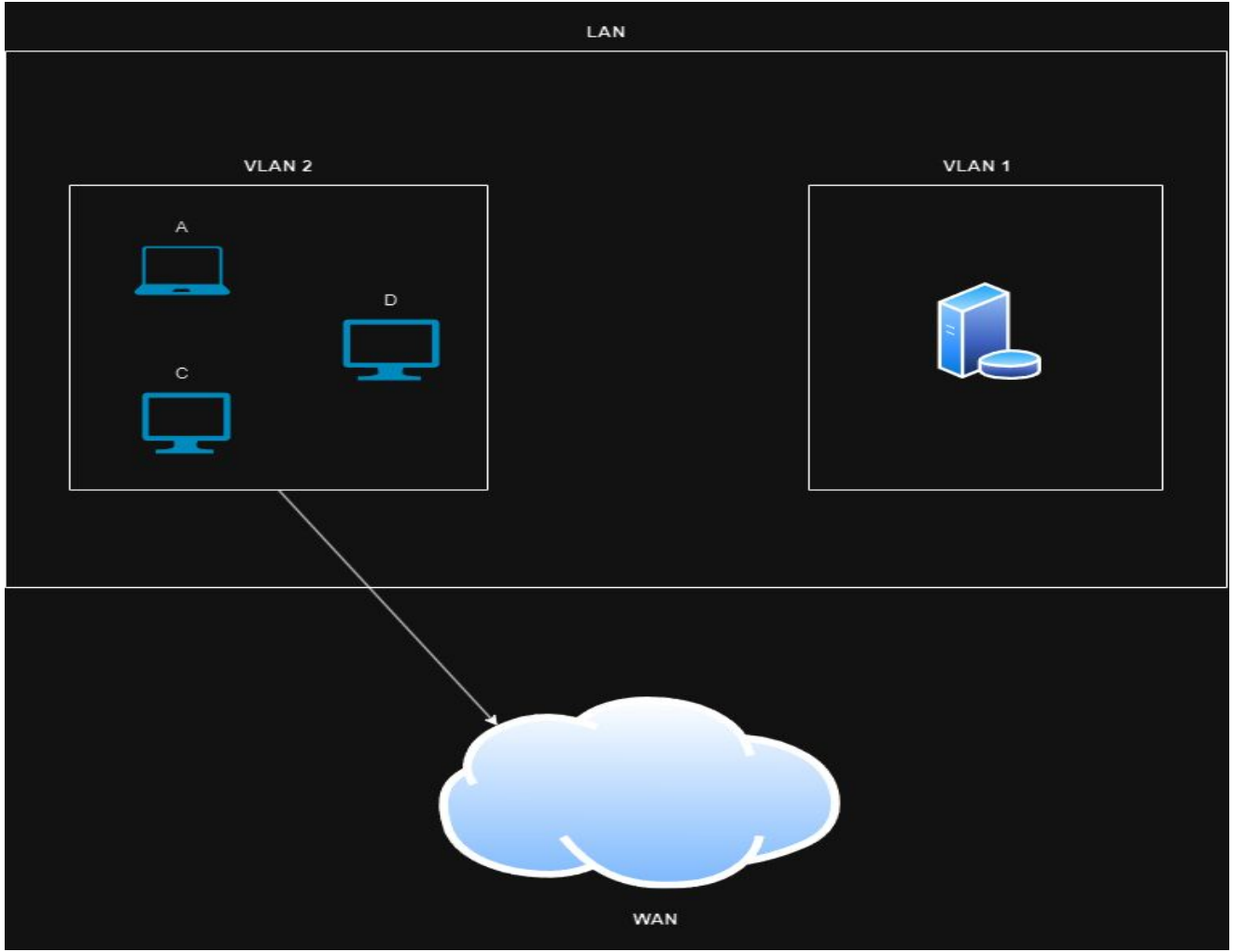
Mi trovo di fronte alla seguente situazione


Rete Interna
A
B
D
C
Internet

Il sistema B, ovvero un database con diversi dischi per lo storage, è stato compromesso interamente da un attaccante, il quale è riuscito a bucare la rete e ad accedere al sistema tramite internet.

L’attaccante potrebbe essere arrivato direttamente a B attraverso internet senza prima passare per uno degli altri 3 host perché il database magari è accessibile pubblicamente, ovvero risulta essere raggiungibile da chiunque su internet.

In una situazione del genere, bisogna procedere segmentando la rete interna


LAN
VLAN 2
A
D
C
VLAN 1
WAN

Vado a segmentare la rete in maniera tale da separare il database (B) dai 3 host (A, C e D). Quindi B finirà in quarantena e verrà anche sconnesso dalla WAN (VLAN 1), mentre A, C e D saranno semplicemente messi in quarantena (VLAN 2).

La quarantena è un tipo di isolamento che include anche il monitoraggio del sistema compromesso. Inoltre, riguardo a B opto anche per la rimozione, o air gap, ovvero, oltre all'isolamento all'interno di una VLAN apposita, lo disconnetto da internet in modo tale da impedire all'attaccante di arrecare ulteriore danno al sistema compromesso e in generale all'azienda.

Il segmento VLAN 2, invece, può essere semplicemente messo in quarantena perché i 3 host vanno monitorati dato che potrebbero essersi connessi B quando ancora facevano parte della stessa rete e potrebbero essere stati compromessi. Non è necessario optare per la rimozione, almeno finché non ci si è resi conto della effettiva non compromissione dei dispositivi. Se uno di essi dovesse risultare compromesso, allora si dovrebbe segmentare ulteriormente VLAN 2 rimuovendo l'host problematico. Se dovessero risultare compromessi tutti e 3, allora l'intera VLAN 2 dovrebbe essere rimossa.

Siccome l'attaccante, come è stato detto, ha compromesso interamente il database, bisogna gestire adeguatamente lo smaltimento o il riutilizzo del sistema. Le due tecniche migliori in tal senso sono *purge* e *destroy*.

Nel caso di purge, adotterei non solo un approccio logico per la rimozione dei contenuti sensibili come ad esempio sovrascrivere i dischi più e più volte (*clear*), ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Invece, nel caso di *destroy*, oltre a meccanismi logici e fisici, si utilizzano tecniche di laboratorio che distruggono completamente il sistema, come ad esempio la fusione o la saldatura dei componenti hardware.

Ovviamente, la scelta della tecnica da adottare in questo caso dipenderà dalla volontà di riutilizzare o meno B. Infatti, se optassi per destroy sarei ovviamente sicuro di aver tolto di mezzo tutta la roba compromessa, tuttavia l'azienda dovrebbe acquistare un nuovo database. Perciò, se si vuole scegliere in maniera economicamente più conveniente, allora purge è la soluzione.