Simulazione di una Rete Aziendale con Docker

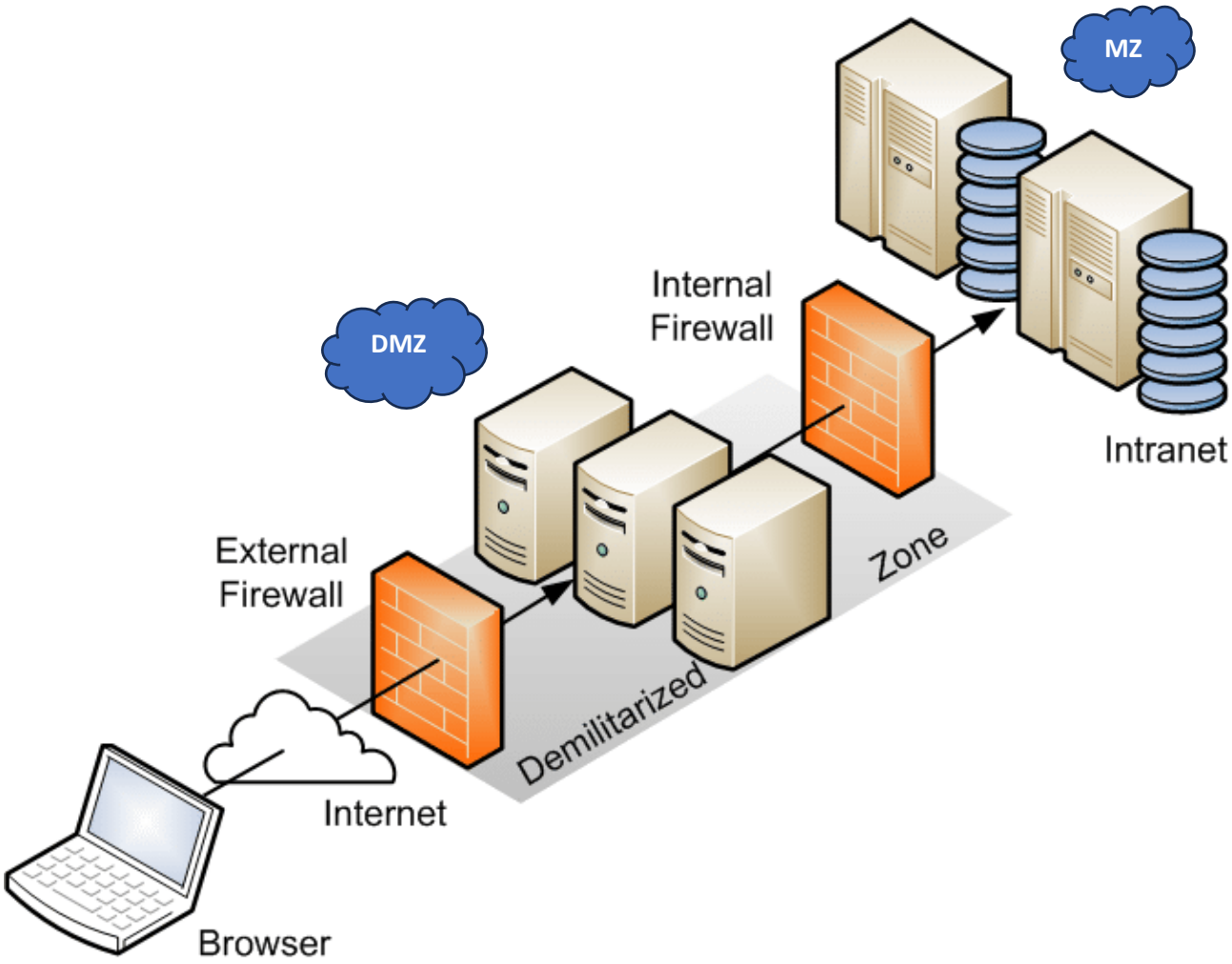
Obiettivo: Costruire un'infrastruttura di rete aziendale utilizzando Docker per simulare un ambiente realistico con diversi livelli di accesso e sicurezza. L'esercizio include la segmentazione della rete, firewall e restrizioni di accesso. Il risultato finale dovrà essere ottenuto mediante lo sviluppo di un file docker-compose.yml che racchiude la soluzione proposta.

Architettura della Rete: La rete sarà suddivisa nei seguenti segmenti:

1. **Zona Pubblica (DMZ)**
    - Ospita servizi accessibili dall'esterno:
        - L’accesso alla rete internet è possibile.
        - Un reverse proxy per gestire il traffico in ingresso.
    - Protetta da firewall con regole di accesso mirate, ad esempio restrizioni a particolari domni (e.g, Facebook)
2. **Zona Interna (MZ)**
    - Contiene servizi aziendali interni con accesso ristretto:
        - Un database server accessibile solo dalla rete privata.
    - Firewall che consente solo connessioni necessarie e non con il mondo esterno, in questo segmento della rete non deve essere prevista alcuna connessione ad internet.
3. **Client Presenti**
    - Simula le postazioni di lavoro con:
        - Sistemi Linux leggeri (Alpine Linux o Debian minimal).

Requisiti Tecnici:

- Tutte le macchine devono essere containerizzate con Docker.
- La comunicazione avviene tramite reti Docker configurate.
- Firewall interni gestiti con iptables o UFW.
- Possibilità di simulare blocchi di accesso a domini specifici (facoltativo)


MZ
DMZ
Internal
Firewall
Intranet
External
Firewall
Zone
Demilitarized
Internet
Browser