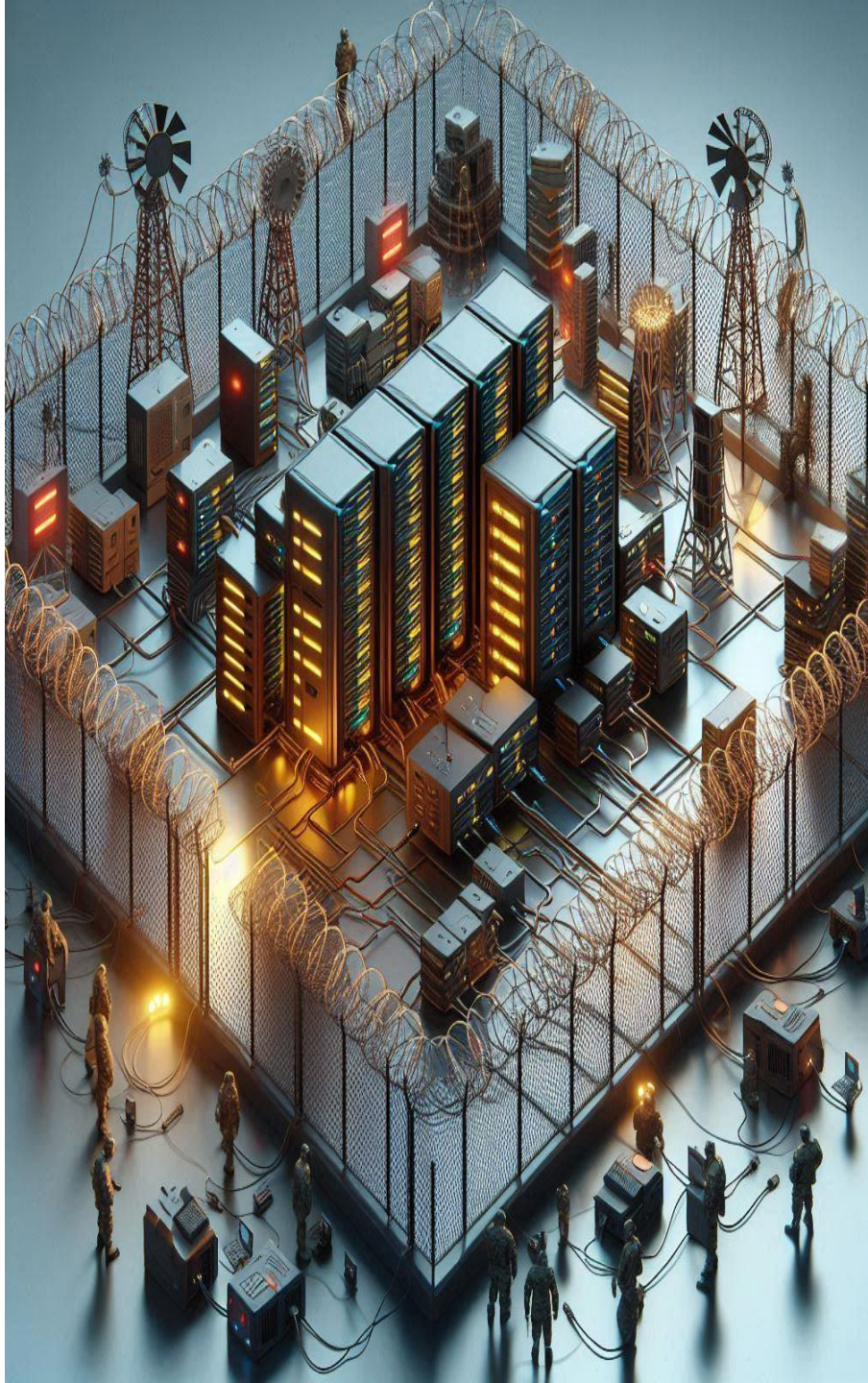
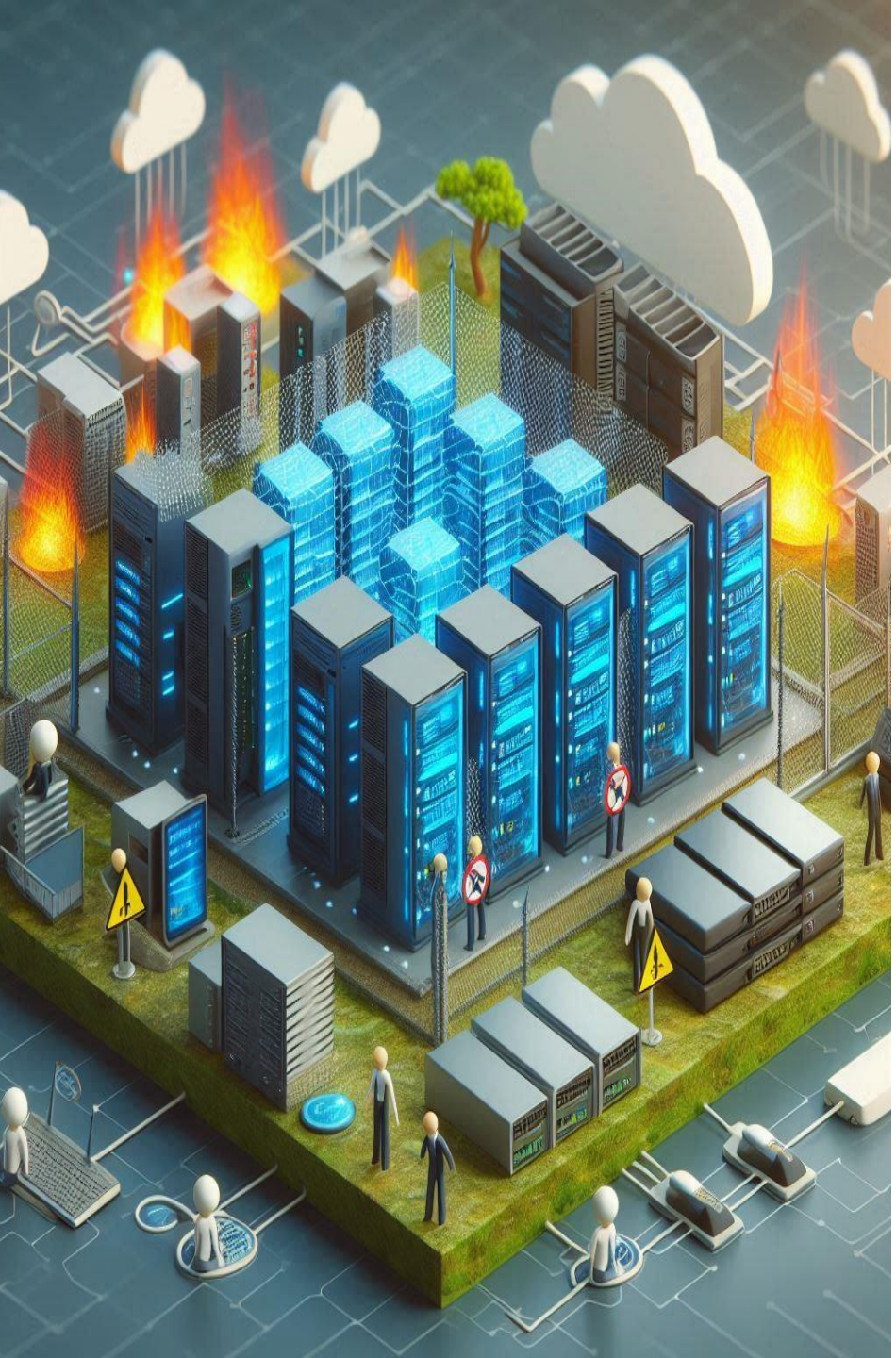

WENET
DMZ
Dr Zare_zardiny
Faraz sarhadi

DMZ (Demilitarized Zone) - A Secure Network Perimeter

A DMZ, or Demilitarized Zone, is a secure network area that sits between an organization's internal network and the public internet. It acts as a buffer zone, allowing limited and controlled access to specific services while protecting the core network from external threats.





The Purpose of a DMZ

1 Isolate Public Services

DMZs allow organizations to to host public-facing services, services, such as web servers or servers or email servers, in a separate, secure network segment.

2 Protect Internal Network Network

By isolating these public-facing facing services, the DMZ helps helps to protect the internal network from potential compromises or attacks.

3 Control Access

DMZs provide a controlled environment where access to and from the from the internal network can be closely monitored and regulated. regulated.

Network Architecture with a DMZ

1

External Network

The untrusted, public network (e.g., the internet) that connects to connects to the DMZ.

2

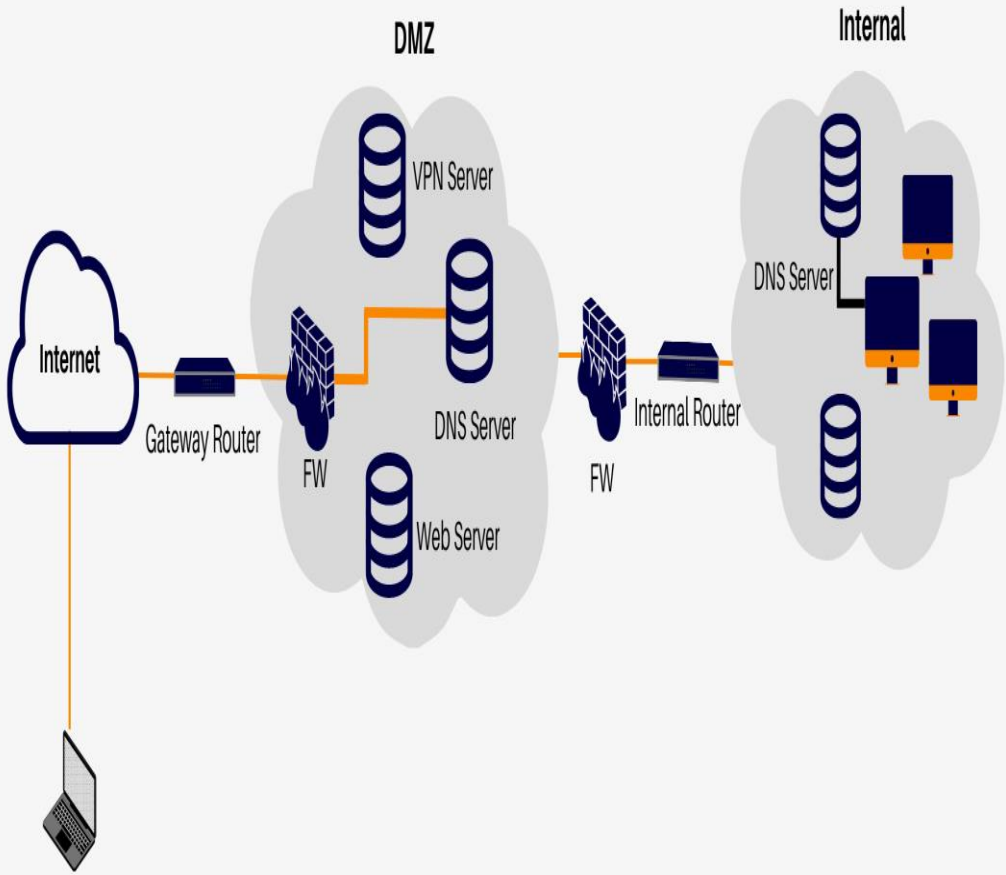
DMZ

The secure, isolated network segment that hosts public-facing facing services.

3

Internal Network

The trusted, internal network that houses the organization's critical critical resources.



zenarmor

Advantages of Implementing a DMZ DMZ

Increased Security

The DMZ provides an additional layer of layer of protection, isolating public services from the internal network.

Access Control

DMZs allow for granular control over over access to and from the internal internal network, improving overall security.

Breach Containment

If a DMZ-hosted service is compromised, the damage is limited to the DMZ, preventing it from spreading to the internal network.

Compliance

DMZs can help organizations meet regulatory requirements and industry industry standards for network segmentation and access control.