DMZ

Network for anything that has to be reachable from the internet. Acts as a buffer zone between WAN and the internal network.

Permitted devices

Only hosts that sit in front of public services. They accept connections from outside and pass them on to the right internal application. Nothing else lives here.

Access

The DMZ can reach the specific application services it fronts, and the internet for certificates and updates. It can't reach Trusted, and it can't reach the rest of Servers. Requires granular firewall management.

Notes

- DMZ hosts are managed from the inside. The connection starts from within the network, so there is no inbound path from the DMZ into the internal zones.
- New public services get published through this zone, never straight from an internal one.

Why it's set up this way

Anything exposed to the internet gets attacked first. Keeping it isolated means a compromise here doesn't hand over the rest of the network. In the future, consider a dual-dmz setup.

Revision #2
Created 2026-11-20 19:08:35 UTC by Henry
Updated 2026-11-20 19:32:33 UTC by Henry