

DMZ

Demilitarized zone

Una DMZ (demilitarized zone) è un segmento isolato di LAN (una "sottorete") raggiungibile sia da reti interne che esterne che permette, però, connessioni esclusivamente verso l'esterno: gli host attestati sulla DMZ non possono connettersi alla rete aziendale interna.

Tale configurazione viene normalmente utilizzata per permettere ai server posizionati sulla DMZ di fornire servizi all'esterno senza compromettere la sicurezza della rete aziendale interna nel caso una di tali macchine sia sottoposta ad un attacco informatico: per chi si connette dall'esterno dell'organizzazione la DMZ è infatti una sorta di "strada senza uscita" o "vicolo cieco".

Solitamente sulla DMZ sono infatti collegati i server pubblici (ovvero quei server che necessitano di essere raggiungibili dall'esterno della rete aziendale - ed anche dalla rete internet - come, ad esempio, server mail, web server e server DNS) che rimangono in tal modo separati dalla LAN interna, evitando di comprometterne l'integrità.

Una DMZ può essere creata attraverso la definizione di policies distinte su uno o più firewall. Le connessioni dalle reti esterne verso la DMZ sono solitamente controllate tramite il protocollo PAT (Port Address Translation).