

Zona DMZ

Zona applicativi critici

Rete aziendale divisa in zona DMZ e zona applicativi critici.

Router Gateway: viene posizionato prima del firewall perimetrale nella struttura della rete perché è responsabile dell’instradamento del traffico tra le diverse reti, inclusa la DMZ e la rete esterna. Il router gateway ha la funzione di indirizzare il traffico in base alle regole di routing configurate, in modo che il traffico venga instradato correttamente attraverso il firewall perimetrale.

Firewall perimetrale a filtraggio dinamico: si trova tra la rete interna LAN e la rete esterna WAN (solitamente internet). Blocca tutte le connessioni che hanno origine dall’esterno verso l’interno e consente quelle che hanno origine dall’interno verso l’esterno.

Monitora lo stato delle connessioni di rete, tenendo traccia delle informazioni collegate ad esse, come ad esempio gli indirizzi IP. Queste informazioni servono per valutare se il traffico in arrivo è legittimo o meno: se il traffico in arrivo corrisponde ad una connessione che è stata stabilita internamente (cioè l’IP da cui ha origine la connessione è salvato nella sua tabella di memoria), il firewall lo lascia passare, altrimenti blocca il traffico.

DMZ: è una parte della rete aziendale che si trova sempre tra la rete interna LAN e la rete esterna WAN. E’ progettata per ospitare servizi e risorse che devono essere accessibili dall’esterno, come server web, server di posta elettronica ecc… Serve quindi anche per eludere un limite del firewall a filtraggio dinamico, cioè la comunicazione dall’esterno verso l’interno; questa diventa possibile con la DMZ solo verso i dispositivi associati agli indirizzi IP presenti in DMZ.

La DMZ è configurata in modo da isolare questi servizi dalla rete interna, riducendo così il rischio di compromissione della sicurezza in caso di attacco dall’esterno. La DMZ non fornisce la stessa protezione della rete interna, quindi è necessario implementare misure di sicurezza aggiuntive come l’IDS(sistemi di rilevamento delle intrusioni) e l’IPS (sistema di prevenzione delle intrusioni).

IDS: è un software che funge da sistema di rilevazione passivo. Avverte con un messaggio di alert l’amministratore del sistema nel caso qualcuno di non autorizzato stia provando ad accedere al dispositivi da esso protetto (in questo caso il NAS). Il soggetto non autorizzato potrebbe essere qualche attaccante esterno che sia riuscito ad eludere i controlli del firewall, oppure qualcuno interno alla rete LAN.

IPS: a differenza dell’IDS, dopo aver individuato la presenza di un possibile attacco, non si limita ad informare l’amministratore del sistema, ma attiva immediatamente delle azioni di protezioni adeguate. La configurazione dell’IPS deve essere molto accurata affinché quest’ultimo non rilevi azioni normali dell’utente come anomale e pericolose e quindi bloccarle (“falsi positivi”).

NAS: dispositivo di archiviazione di dati collegato ad una rete locale che fornisce accesso centralizzato ai dati e ai file per gli utenti e i dispositivi all’interno della rete.