

Una zona DMZ è una rete che protegge la rete locale interna di un'organizzazione dal traffico non attendibile. L’obiettivo di una DMZ è consentire agli host di accedere a reti non attendibili, tra cui Internet, garantendo la sicurezza della propria rete.

Il firewall si mette direttamente dietro il router e può essere configurato per analizzare il traffico in entrata, filtrando le minacce che arrivano al dispositivo. Con firewall perimetrale (posizionato subito prima di internet, per proteggere l'infrastruttura IT) si intende, il 'muro' a protezione della struttura IT. Si tratta di misure di sicurezza che se attuate in modo corretto bloccano gli accessi indesiderati.

L’IDS (Intrusion Detection System) esegue un monitoraggio continuo sulla rete, identificando per tempo possibili attacchi alla rete. Rileva intrusioni o attività sospette.

Il componente IDS l’ho posizionato dopo lo switch perchè va posizionato in punti critici della rete come switch, gateway o server per massimizzare la copertura.

L’IPS () invece monitora il traffico di rete alla ricerca di potenziali minacce e le blocca automaticamente, interrompendo le connessioni pericolose, eliminando i contenuti dannosi o attivando altri dispositivi di sicurezza.

Il componente IPS invece l’ho posizionato prima della zona DMZ, così da avere un sistema di prevenzione delle intrusioni (IPS). Potrebbe essere configurato per bloccare qualsiasi traffico diverso dalle richieste HTTPS

La differenza tra IDS e IPS è quasi minima. Hanno gli stessi programmi ma vengono configurati in maniera diversa e l’IPS è attivo, mentre l’IDS è passivo.