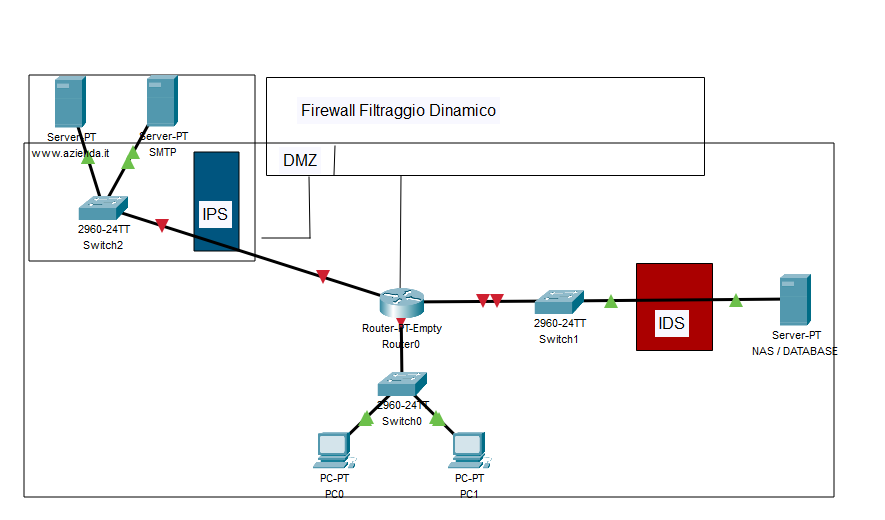
**Report**



Per questa rete aziendale ho deciso di inserire un firewall filtraggio dinamico che si trova nella zona perimetrale per motivi di sicurezza e una facile gestione della memoria che contiene l’indirizzi ip pubblici.

È stato inserito due web server (HTTP e SMTP) quindi possiamo trovare una DMZ che consente ai visitatori del sito Web di ottenere determinati servizi.

L’IPS (Internet Prevention Security) è stato inserito dentro la DMZ per rilevare e agire contro una minaccia in maniera attiva, così da evitare che l’attaccante possa entrare nella LAN.

Dentro la Local Area Network (LAN) troviamo i dispositivi aziendali e il Database principale del cliente dove si trovano tutte le informazioni sensibili, i dispositivi che si trovano dentro la LAN possono comunicare tra di loro senza problemi.

L’IDS (Internet Detection Security) è stato inserito dentro la LAN tra lo switch e il dababase per avere un controllo degli utenti che possono accedere a questa informazione, la persona incaricata della sicurezza potrà gestire il traffico degli indirizzi ip che possono entrare al database e se c’è un movimento strano l’ids dentro la rete interna verso il database aziendale li invierà una notifica, se avessimo messo un sistema di rilevamento IPS avrebbe potuto darci falsi positivi quindi se un utente dentro la stessa rete LAN voleva avere accesso a certe informazioni il sistema di rilevamento poteva bloccare il suo IP privato e la persona non potrà vedere il contenuto del Database.