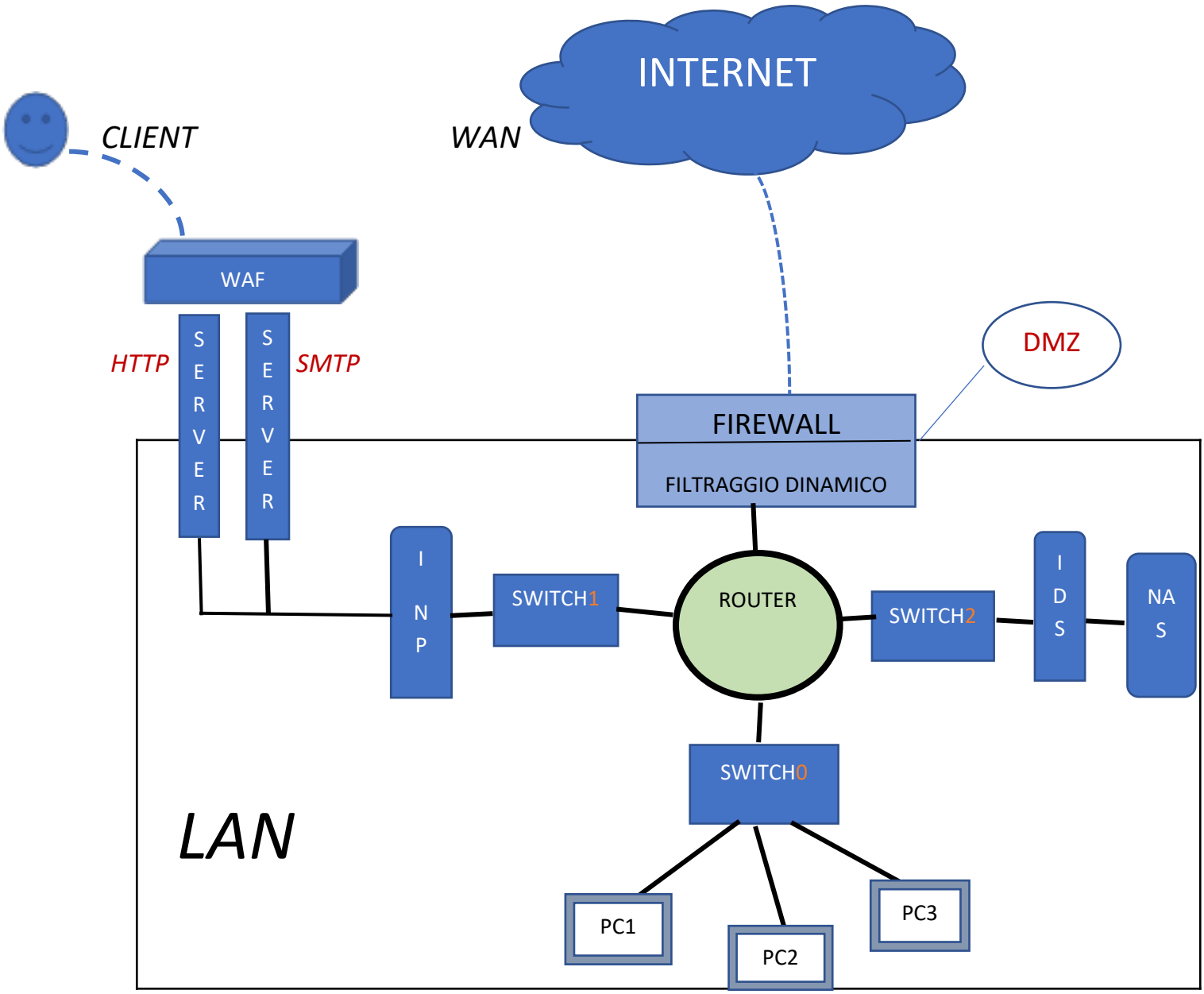

***SPIEGAZIONE DELLA RETE

Abbiamo qua sopra il disegno di una rete, composta da:una zona di internet; una zona DMZ ; una rete interna.In queste zone i dispositivi si cambiano informazioni tra di loro comunicando tramite indirizzo IP. Tuttavia il cambio di informazione tra dispositivi di due zone si fa in modo diverso in fuzione che la rete interna sia privata o pubblica.In seguito spiegheremo come si svolgono questi cambiamenti di informazione nel caso in cui la rete interna è pubblica o privata e il ruolo che giocca ogni dipositivo.

Generalmente, Se la rete interna è privata(tipo quella di un'azienda) ,la communicazione tra una rete interna e una rete esterna si fa dall'interno verso l'esterno.In questo caso sul disegno sopra alcuni dispositivi come: il WAF , SERVEUR HTTP e SMTP ,INP e IDS non saranno necessario perché

sono utilizzati quando la rete interna è publica.Nel caso rappresentato sopra La zona di internet è costituita da un reseau WAN(Wide Area Network) che è una rete globale di computer interconessi che utilizzano il protocollo di comunicazione TCP/IP.

La zona DMZ(Demilitaried Zone) è un area posta tra la rete esterna internet e la rete interna LAN(Local Area Network);consente ai dispositivi esterni di accedere a tali servizi senza entrare direttamente nella rete interna.in caso di rete interna privata, abbiamo in questa zono un Firewall che è un dispositivo di sicurezza che permette di filtrare il traffico in ingresso e in uscita;in questo caso il Firewall esegue un filtraggio Dinamico.

Nella zona interna,abbiamo: un ROUTER che instrada i pachetti tra PC e Server NAS.I SWITCH che in generale consentono di collegare diversi dispositivi all'interno di una rete locale, in questo caso collegano i PC con Router e il Router con Serveur NAS.. se la rete interna fosse publica il Switch1 avrebbe collegato il Router con IPS e il Switch2 con l'IDS. Poi abbiamo La NAS che è un dispositivo di archiviazione dati centralizzato ; Per finire abbiamo i PC che sono dispositivi elettronici capace di elaborare,immagazzinare e condividere informazioni.

Come detto prima se la rete interna è pubblica allora useremo in questo caso: il WAF,Sever http e smtp , IPS ,IDS.anche se rappresentati in questo modo sul disegno, questi dispositivi sono collocati nella DMZ e permettono tramitte Server http e smtp, ai dispositivi esterni di accedere agli informazioni quello che non sarebbe possibile se la rete interna fosse privata.A questo punto facciamo faccia a un problema se lasciamo il sistema così gli attacanti avranno libero accesso ai dati;Per evitare questo usiamo un WAF che è un tipo di Firewall progettato specificamente per proteggere le applicazioni web da attachi e minacce esterni .

Il WAF in questo caso apre e verifica tutti i file che vengono dai clienti per verificare che non ci sono minaccie alla sicurezza delle Applicazioni web andando a controllare la base di dato che contiene malware registrati.

IPS e IDS sono dispositivi di sicurezza utili nel caso un attacante riesce a attraversare il livello di sicurezza del WAF.L'IPS segnala e blocca attività sospesa o minacce alla sicurezza; IDS segnala solo l'attaco ma non lo blocca raggione per la qualle l'abbiamo messo in seconda posizione su nostro disegno.