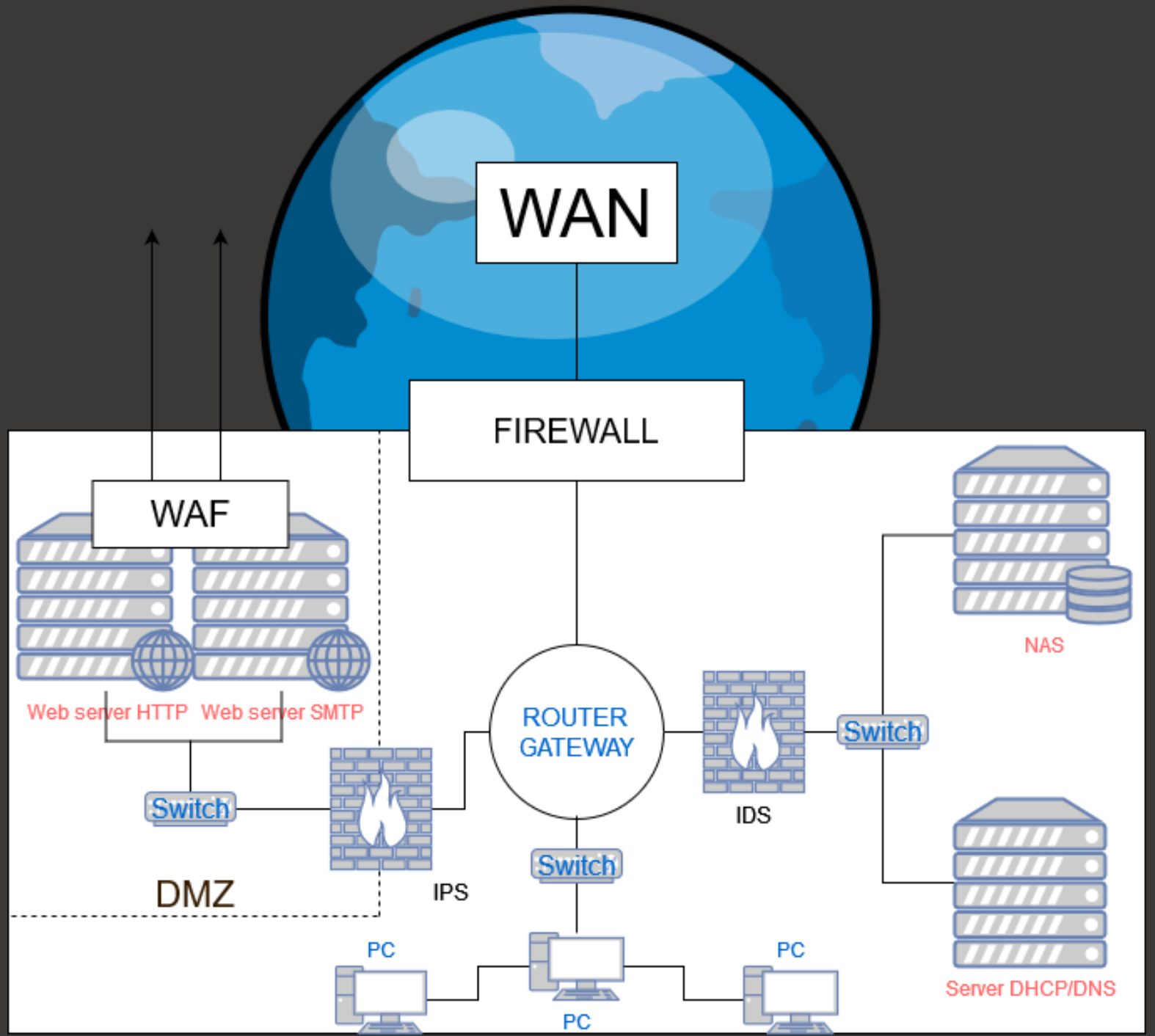
Il diagramma di rete sottostante è completo di:
-Zona di internet (WAN)
-Zona demilitarizzata (DMZ)
-Zona interna, con firewall perimetrale.

Partendo dal firewall perimetrale. Si chiama così perché sta a cavallo tra la WAN e la LAN.
In questo caso (nel 99% dei casi al giorno d'oggi) si utilizza il filtraggio "stateful", che è ottimo per le connessioni in uscita dalla nostra rete interna.
Ogni dispositivo nella rete ha una sua ACL (Access Control List) che viene aggiornata ogni volta che ci si connette ad un sito.

Nella DMZ invece abbiamo i server che sono "esposti" al web (in questo caso un server HTTP ed uno SMTP).
Per proteggerli utilizziamo il WAF (Web Application Firewall) che legge l'IP e la porta del mittente, ma soprattutto, analizza i pacchetti. Se nota qualcosa che non va, li blocca.

Non è l'unica linea di difesa però, all'interno della rete sono installati anche un IDS (Intrusion Detection System) ed un IPS (Intrusion Prevention System).
L'IPS previene interamente un tentativo di intrusione, ma ha spesso dei falsi-positivi.
L'IDS invece notifica soltanto la probabile intrusione, senza prender nessun'azione.
Vista la natura dell'IPS, è ottimale utilizzarlo per separare la DMZ dal resto della rete interna, poiché usarlo per separare i PC utente dai server interni, potrebbe provocare parecchia latenza e disagi (per esempio per accedere a dei file importanti). Quindi mantenere la sicurezza adeguata con un IDS, mantenendo l'efficienza, è consigliato.


WAN
FIREWALL
WAF
Web server HTTP
Web server SMTP
Switch
DMZ
IPS
ROUTER
GATEWAY
IDS
Switch
Switch
NAS
Server DHCP/DNS
PC
PC
PC