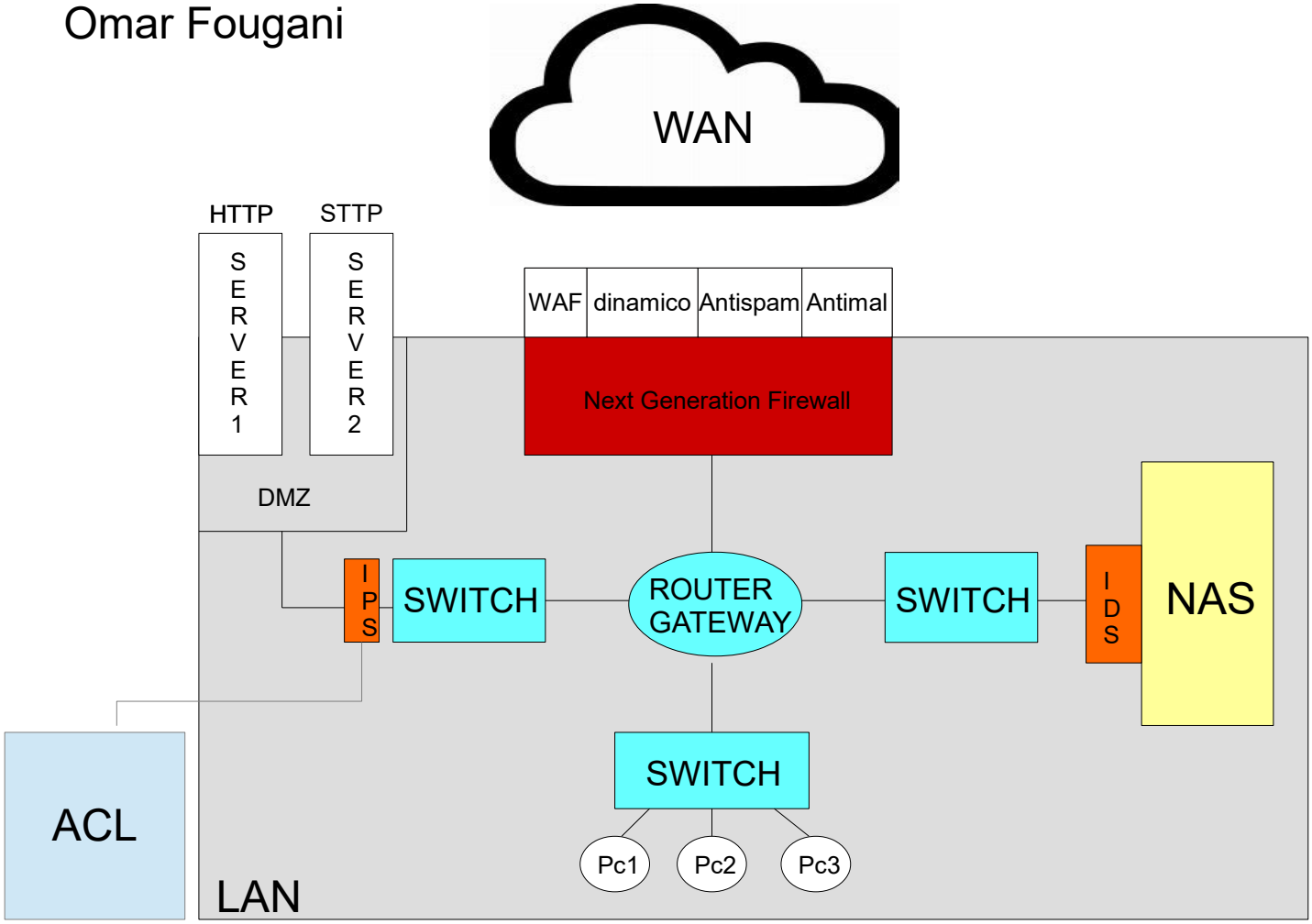
Omar Fougani



Questa è la rappresentazione di una rete e le sue varie componenti.

I pacchetti provenienti da una rete esterna si ritroveranno a dover superare una serie di protezioni e filtraggi.
In primis abbiamo il Firewall della nostra rete aziendale, della LAN, semplificando.
Come firewall ho utilizzato il “Next generation Firewall” comprendente il filtro dinamico; antimalware e antispam; il WAF che fa da filtraggio per il contenuto,leggendo il destinatario e mittente verificando se il pacchetto è malevolo. E' 1° livello di sicurezza ed è presente su tutti i livelli di ISO/OSI.
La DMZ (zona demilitarizzata) è dove vi sono i nostri server Web - Mail sono HTTP e STTP. La DMZ è la zona raggiungibile dall'esterno, quindi da tutto il mondo. (qui entra poi in gioco il WAF).
A protezione del nostro NAS inserisco un IDS o IPS che fungono da allarme e ti avvisano, dopo aver spacchettato il pacchetto, e dopo aver fatto confronti con la tabella ACL, se vi sono rischi. IPS a differenza del primo, blocca/permette l'accesso del pacchetto(il problema però sta nell'individuare i falsi positivi).
Sostanzialmente conviene tenere un IPS nella zona demilitarizzata,affinchè il traffico venga controllato automaticamente. A protezione del nostro NAS probabilmente convengono entrambi, dipende dalle nostre risorse. Ma di base utiliziamo l'IDS e decidiamo di conseguenza se i pacchetti sono o meno malevoli.