Questa é una configurazione di rete di un'azienda ipotética che ha una rete interna con informazione da proteggere, e anche un sito website e indirizzo Email per il público.

Dal internet arriva molta informazione alla nostra rete, e non tutta é benigna, é per questo che abbiamo inserito varie misure di sicurezza.

- Prima i pacchi arrivano al nostro primo router che permette collegare la nostra rete su internet.
- Poi passa subito per un firewall, dove si filtrano i pacchi maliziosi.
- Dopo questo firewall, si invia il traffico a 3 server:
  - Quello IDS che annalizará ogni pacco in cerca di red flags, e poi enviará questa informazione a seguire il percorso. Questo ci informerá se si prova qualche attacco DoS o TCP dump su nostri server DMZ.
  - Quelli HTTP e Email faranno di DMZ, filtrando ancora piú i pacchetti.
- Dopo la DMZ, il traffico va sul secondo firewall, che filtra ancora di piú.
- Dopo passa tutto da un IPS server, che ci proteggerá di qualsiasi traffico maligno che ha passato per le misure di difesa di prima.
- Finalmente, il resto del traffico puó arrivare all'interno di nostra rete aziendale, compreso con qualsiasi allarma del servizio IDS