S3-L5
Firewall

Nell'esempio da me portato, quello che ho cercato di rappresentare è un'azienda avente 2 server in grado di erogare servizi: un server con servizio **http** e uno con servizio **smtp** attivo. In questo caso, la funzione di firewall è affidata ai router opportunamente configurati da CLI.

Il quadrato in alto a sinistra rappresenta una rete esterna (internet) in grado di collegarsi ai server per poter sfruttare i servizi.
Qui ho integrato anche un server DNS in grado di convertire gli indirizzi ip dei server target in nomi facilmente comprensibili.

L'azienda è strutturata su più livelli, proprio come la sua sicurezza.
In alto (rettangolo giallo) abbiamo la **DMZ**, ovvero un'area facilmente accessibile dagli utenti esterni, in cui troviamo i 2 server adibiti a **http** e **smtp**.
Poiché si tratta di server che devono garantire una certa velocità di risposta, in quest'area non è possibile applicare misure di sicurezza troppo stringenti, in quanto si avrebbero ripercussioni sulla qualità del servizio offerto.
Si tratta quindi anche dell'area più a rischio attacchi esterni e pertanto i server sono stati confinati in un'area detta appunto **DMZ** chiusa tra 2 firewall:

- il primo è il punto di accesso per gli utenti esterni è avrà misure di sicurezza abbastanza blande (in questo caso ho cercato di filtrare il traffico permettendo l'ingresso solo agli indirizzi ip diretti alle porte **80** e **25**);
- il secondo separa la **DMZ** dalla rete interna e avrà misure di sicurezza più dure (in questo caso, a puro scopo di esempio, ho filtrato le connessioni sulla porta **23**, permettendo comunque la comunicazione tra l'area dipendenti e la dmz).

Scendendo di livello troviamo l'area dipendenti, una rete più interna all'azienda, ma non bisognosa di grandi misure di sicurezza.
Essa è a sua volta separata dall'area amministrazione da un firewall in grado di bloccare tutto il traffico in entrata. In questo modo, all'area amministrativa sarà permesso comunicare con le aree soprastanti, ma a queste ultime non sarà possibile dialogare con l'area amministrativa. Questo aumenta esponenzialmente la sicurezza di questo livello, parliamo infatti di un livello più "delicato".
Stessa situazione la ritroviamo all'ultimo livello, una stanza in cui è presente un server contenente dati importanti per l'azienda. In questo caso abbiamo un firewall che blocca tutte le comunicazioni fatta eccezione per quelle che arrivano dall'area amministrativa.

Di seguito riporto le configurazioni utilizzate per i router:

- **Router 1:**
  10 permit tcp any host 192.168.0.2 eq www (23 match(es))
  20 permit tcp any host 192.168.0.3 eq smtp
  30 deny ip any any
  (Regole in ingresso)

- **Router 2:**

10 deny tcp any 192.168.1.0 0.0.0.255 eq telnet
20 permit ip any any

- **Router 3:**
  10 deny ip any any

- **Router 4:**
  10 permit tcp 192.168.4.0 0.0.0.255 host 192.168.6.2
  20 deny ip any any