



Il **router** permette il passaggio dalla **zona di internet** alla **DMZ** (*demilitarized zone*), all'interno della quale bisogna garantire l'utilizzo della rete per **servizi necessari** (mail, shopping online, a seconda delle necessità dell'azienda).

Per garantire la protezione di rete (e quindi dei dati e dei servizi necessari all'azienda) da minacce esterne, utilizzeremo un **firewall** (posto tra **DMZ** e **rete interna**) per regolamentare il traffico di rete in entrata e in uscita. Il firewall perimetrale protegge al contempo la **rete interna**, non connessa, poiché autorizzando soltanto il viaggio di alcune informazioni, posso garantire la separazione tra **rete interna**, **dmz** e l'**esterno** grazie al **filtraggio** (per esempio: filtraggio statico). Possiamo anche utilizzare dei comandi specifici nel filtraggio, chiamati **azioni**. Alcuni comandi possibili del firewall sono:

1. **Allow** (consente di lasciar passare il pacchetto di informazioni)
2. **Drop** (non lascia passare il pacchetto ma non avverte la sorgente)
3. **Deny** (non lascia passare il pacchetto ma informa la sorgente)