

STRUTTURA CONCETTUALE DI UN FIREWALL

Un firewall è in sostanza un router con 3 porte ethernet o fastethernet che ha funzionalità di controllo sul traffico in transito (tra le porte) fino al livello 7.

Esistono diversi tipi di firewall sul mercato, sia con un numero inferiore di porte (il minimo comunque è 2) che con un numero maggiore. Inoltre tra i vari modelli offerti variano molto le capacità di controllo sui livelli superiori al quarto.

Ad ogni porta del firewall corrisponde una **zona**, e il firewall viene configurato con delle politiche (policy, o rules) che regolano il traffico in transito tra le varie zone.

Generalmente le tre zone vengono chiamate **trusted** (la rete di fiducia sulla quale ci sono in sostanza i computer che devono essere protetti), la rete **external** (la rete alla quale ci si connette e dalla quale ci si deve “difendere”, e la **DMZ** (demilitarized – demilitarizzata – una rete sotto il dominio di amministrazione dell'azienda che controlla il firewall e sulla quale si posizionano solitamente dei server che devono essere visibili sia dalla trusted che dalla external).

Sostanzialmente le 3 porte non sono differenti l'una dall'altra. La differenza consiste solo nelle policy che solitamente vengono impostate su di esse.

Dato che il firewall esegue routing tra le zone ne consegue che gli host sulle varie zone devono trovarsi su Network IP diverse!