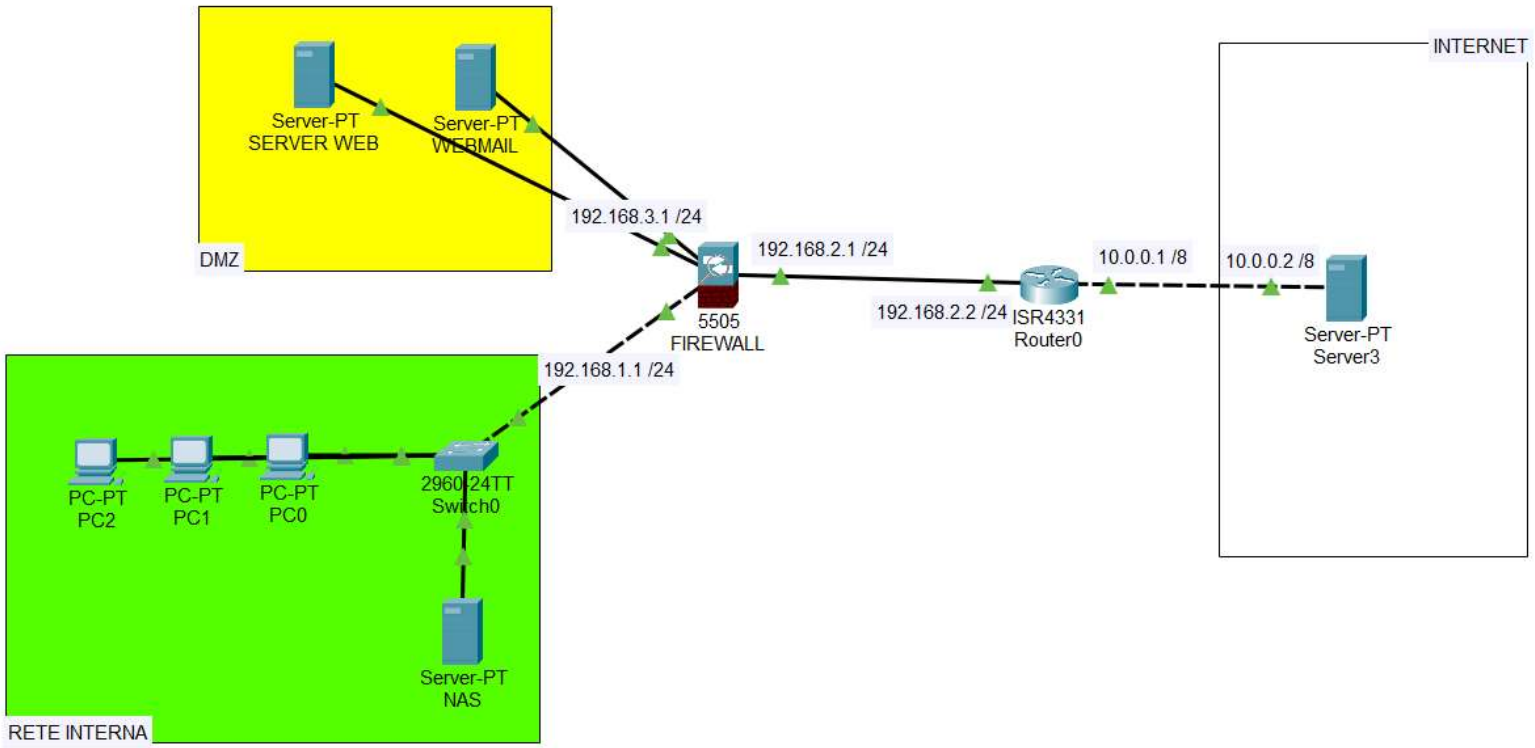

I computer della rete aziendale locale possono comunicare liberamente con la rete DMZ poichè sul firewall sarà impostata una ACL Access-control list che permetterà ai computer aziendali di accedere ai server nella rete DMZ. Le Access Control Lists (Access-list) sono il metodo con cui il firewall determina se il traffico è autorizzato o rifiutato. Il segmento di rete dell'ISP è collegato all'interfaccia Ethernet0/0 ed è etichettato all'esterno con un livello di protezione pari a 0. La rete interna è stata collegata a Ethernet0/1 e contrassegnata come interna con un livello di protezione di 100 (il massimo). Il segmento DMZ, in cui risiede il server Web e il server Webmail è collegato a Ethernet 0/2 ed etichettato come DMZ (può essere impostato livello di protezione tra 0 e 100).

Pertanto, senza aggiungere alcun ACL alla configurazione:

- Gli host all'interno (livello di protezione 100) possono connettersi agli host sulla DMZ (livello di protezione 70).
- Gli host interni (livello di protezione 100) possono connettersi agli host esterni (livello di protezione 0).
- Gli host sulla DMZ possono connettersi agli host esterni (livello di protezione 0).

Tuttavia non è vero il contrario, il traffico viene rifiutato quando:

- Gli host esterni (livello di protezione 0) non possono connettersi agli host interni (livello di protezione 100).
- Gli host all'esterno (livello di protezione 0) non possono connettersi agli host sulla DMZ.

Poiché il traffico dall'esterno alla rete DMZ viene rifiutato dal firewal, gli utenti su Internet non possono raggiungere il server Web, bisogna autorizzare esplicitamente questo traffico.
Gli utenti su Internet possano accedere al server Web sulla porta TCP 80 e Webmail porta 25.