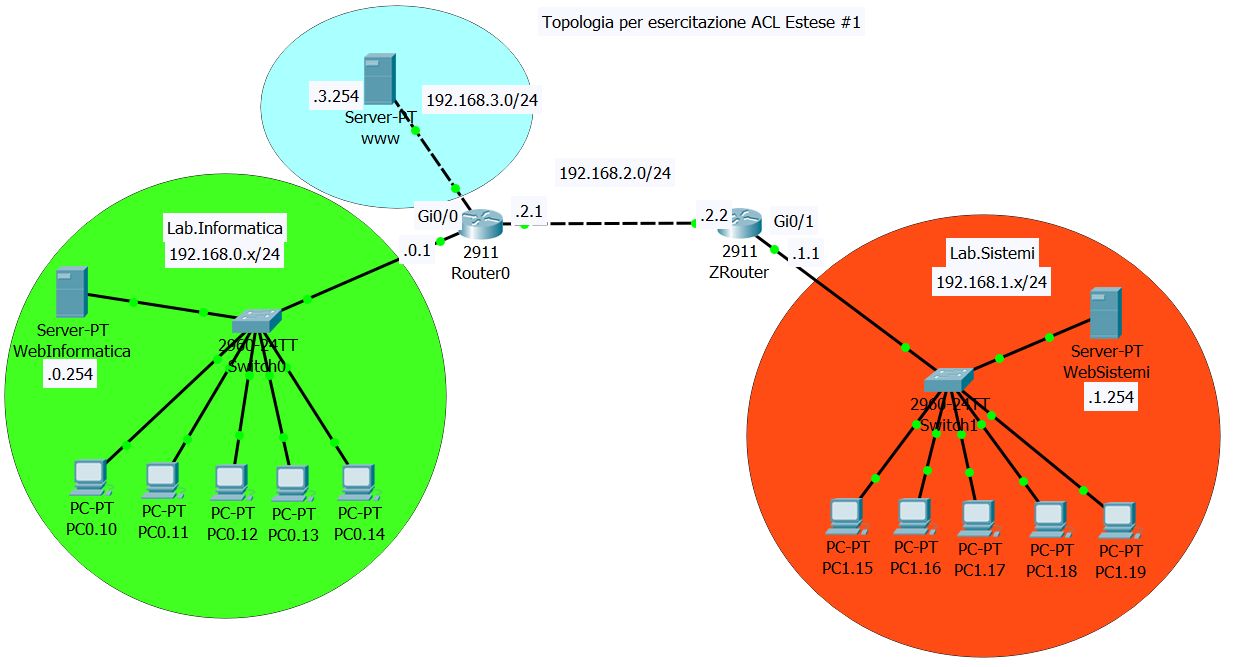
**Esercitazione di Laboratorio Sistemi e Reti**

**Sicurezza – ACL Estese #1**

*a.s. 2017/2018*



**Esercizio 1**

1. **\*Tutti i PC** dellarete Lab.Sistemi **devono poter accedere** allarete Lab.Informatica

ZRouter(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255

ZRouter#conf terminal

ZRouter(config)#interface Gi0/1

ZRouter(config-if)#ip access-group 100 in

1. **\*Nessun PC** dellarete Lab.Sistemi **deve poter accedere** allarete Lab.Informatica

ZRouter(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255

ZRouter#conf terminal

ZRouter(config)#interface Gi0/1

ZRouter(config-if)#ip access-group 100 in

1. **\*Tutti i PC** della rete Lab.Sistemi **possono accedere** al server web (www) della DMZ dellarete Lab.Informatica, ma non possono accedere alla rete privata (verde) di Lab.Informatica

ZRouter(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.254 eq 80

ZRouter(config)# access-list 100 ip deny any any

ZRouter#conf terminal

ZRouter(config)#interface Gi0/1

ZRouter(config-if)#ip access-group 100 in

1. **\*Tutti i PC** della rete Lab.Informatica **non possono navigare** sul **server web aziendale** (*www*) tranne il server *WebInformatica* che può farlo.

ZRouter(config)# access-list 100 permit tcp host 192.168.0.254 host 192.168.3.254 eq 80 established

ZRouter(config)#access-list 100 deny tcp 192.168.0.0 0.0.0.255 host 192.168.3.254 eq 80

ZRouter#conf terminal

ZRouter(config)#interface Gi0/0

ZRouter(config-if)#ip access-group 100 in

1. **\*Tutti i PC** della rete Lab.Informatica **non possono uscire dalla rete aziendale (verde),** **non possono** navigare sui **server web aziendale** (*www*) e *WebInformatica* ma possono navigare su *WebSistemi*. Attenzione alla configurazione impossibile.

ZRouter(config)#access-list 100 permit tcp 192.168.0.0 0.0.0.255 host 192.168.1.254 eq 80

ZRouter(config)# access-list 100 deny ip any any

ZRouter#conf terminal

ZRouter(config)#interface Gi0/0

ZRouter(config-if)#ip access-group 100 in

**Osservazioni**: se permetto IP implicitamente (default) consento anche di usufruire dei servizi. Per evitare quindi l’accesso ai servizi pur garantento la connettività (ping) prima si fa il deny dei servizi e poi il permit dell’IP