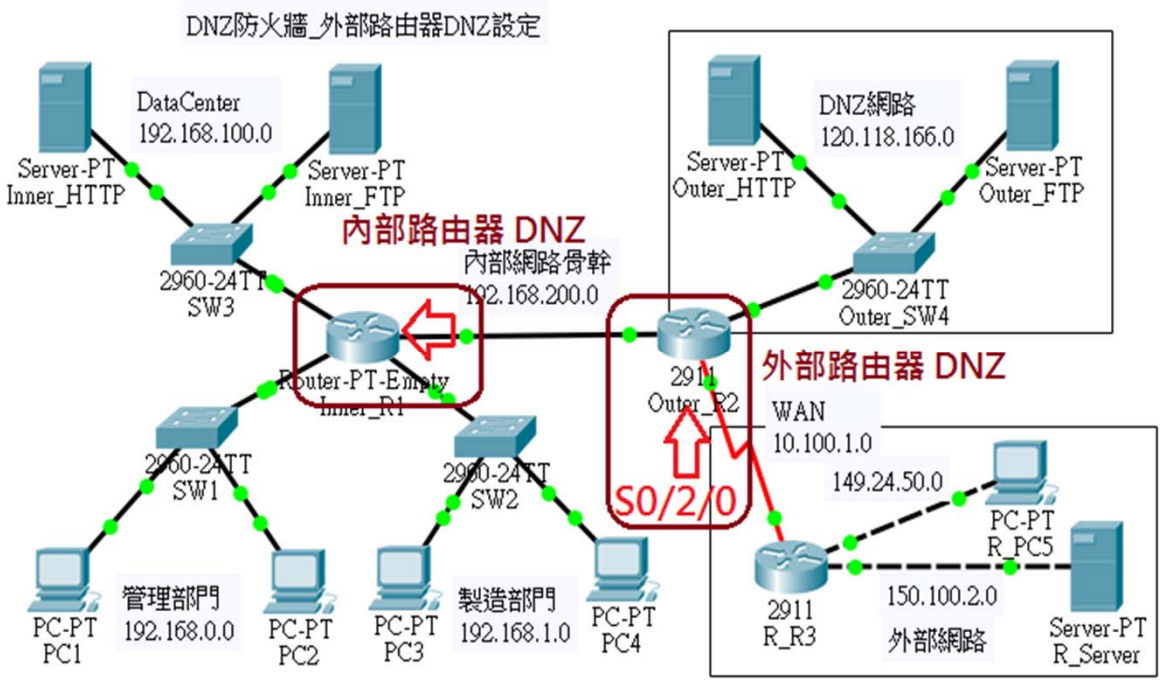
9-6-6 外部路由器 DNZ 規劃 (一)

- 內部路由器管制
  - 禁止外部主機存取內部任何資源，內部主機可以存取外部資源。
  - DNZ 網路上主機可以與內部網路主機相互連線。
- 外部路由器管制
  - 允許外部可以任意存取 DNZ 網路內伺服器。
  - 允許外部網路可以測試 (Ping) DNZ 網路下主機。
  - 允許內部網路主機可以任意進出。



9-6-6 外部路由器 DNZ 規劃 (二)

管制 DNZ 網路機制：DNZ-ACL 規則

Outer_R2(Gi0/1) 外部路由器：DNZ-ACL								
編號	Permit/ deny	封包類型	來源		目的		方向	備註
			IP	port	IP	port		
1	permit	ip	any		120.118.166.0/24		in	
2	permit	ip	120.118.166.0/24		any		out	
3	permit	ip	192.168.0.0/16		any		out	
4	permit	ip	any		192.168.0.0/16		in	
5	deny	ip	any		any			

9-6-6 外部路由器 DNZ 規劃 (三)

- 設定 DNZ-ACL-out 規則

```
Outer_R2> en
Outer_R2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Outer_R2(config)#ip access-list extended DNZ-ACL-out
Outer_R2(config-ext-nacl)#permit ip 120.118.166.0 0.0.0.255 any
Outer_R2(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 any
Outer_R2(config-ext-nacl)#deny ip any any
Outer_R2(config-ext-nacl)#exit
Outer_R2(config)#do show access-list DNZ-ACL-out
Outer_R2(config)#int s0/2/0
Outer_R2(config-if)#ip access-group DNZ-ACL-out out
```

- 設定 DNZ-ACL-in 規則

```
Outer_R2(config)#ip access-list extended DNZ-ACL-in
Outer_R2(config-ext-nacl)#permit ip any 120.118.166.0 0.0.0.255
Outer_R2(config-ext-nacl)#permit ip any 192.168.0.0 0.0.255.255
Outer_R2(config-ext-nacl)#deny ip any any
Outer_R2(config-ext-nacl)#exit
Outer_R2(config)#do show access-list DNZ-ACL-in
Outer_R2(config)#int s0/2/0
Outer_R2(config-if)#ip access-group DNZ-ACL-in in
```

- 測試
  - R_PC5 ping 192.168.200.1