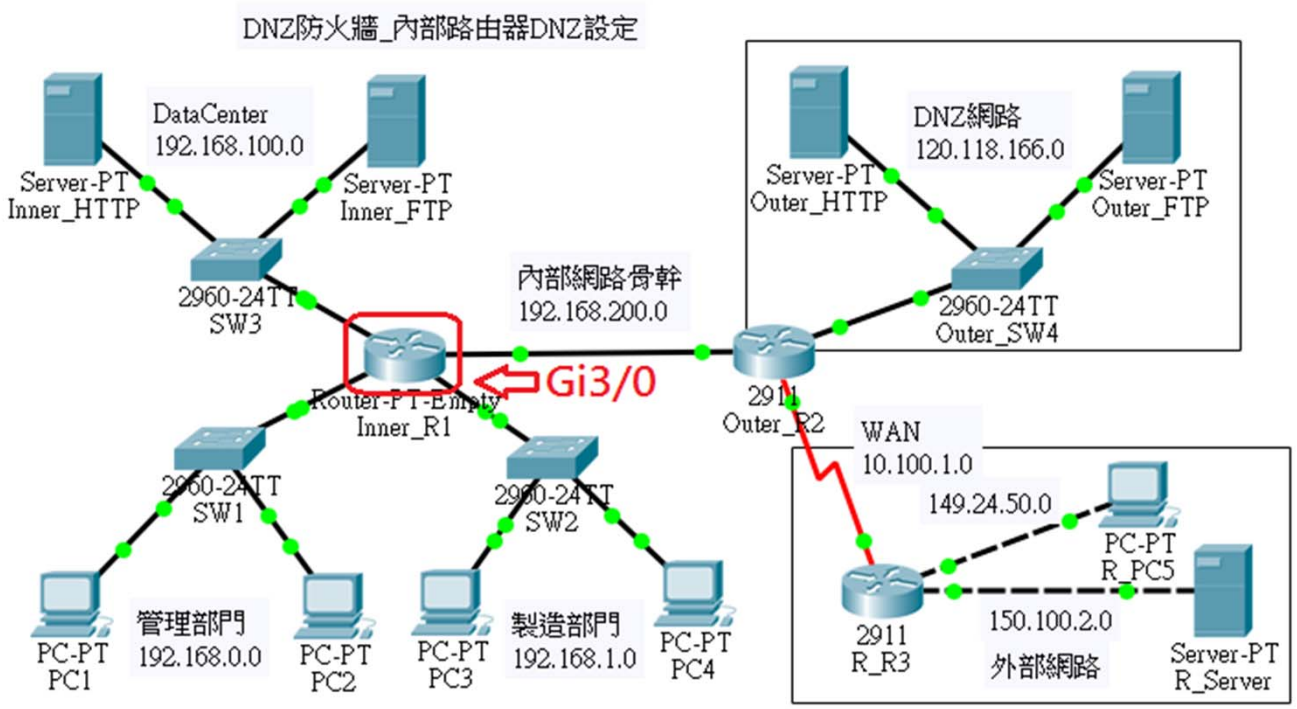
9-6-5 內部路由器 DNZ 規劃 (一)

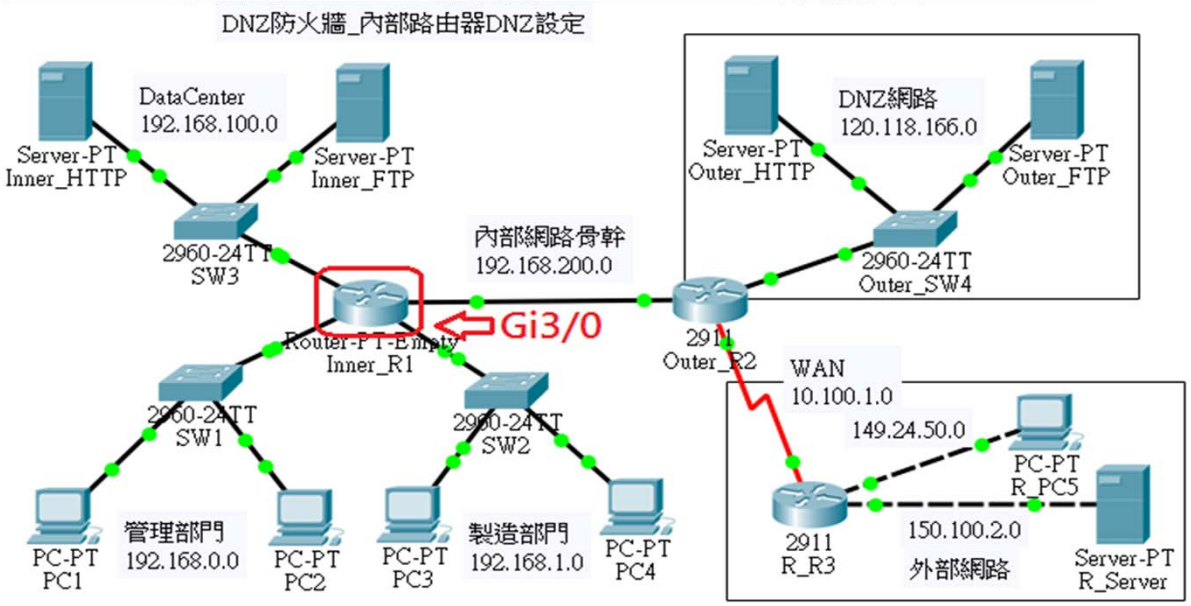
- **DNZ 網路規劃：**
  - 禁止外部主機存取內部任何資源，但內部主機可以存取外部資源。
  - DNZ 網路(120.118.166.0/24) 上主機可以與內部網路相互連線。
  - 允許 PC1 主機(192.168.0.1)與PC3 可登入 Inner_R1 內。
  - DataCenter網路提供內部任何主機存取(沒有管制)。



9-6-5 內部路由器 DNZ 規劃 (二)

- 靜態路由表設定：
  - 以管制封包進出，繞路協定之封包已無法進入。

Router	Destination AD	Network Mask	Net Hop
Inner_R1	120.118.166.0	255.255.255.0	192.168.200.2
	0.0.0.0	0.0.0.0	192.168.200.2
Outer_R2	192.168.0.0	255.255.0.0	192.168.200.1
	0.0.0.0	0.0.0.0	10.100.1.2
R_R3	0.0.0.0	0.0.0.0	10.100.1.1



9-6-5 內部路由器 DNZ 規劃 (三)

Inner-R1 (Gi3/0) 管制機制：

- 允許來源是 120.118.166.0/24網路上主機進入內部網路。
- 允許內部主機連結外部伺服器，但不允許外部主機連結內部伺服器。
- 不允許外部網路主機進入內部網路。

Inner_R1(Gi3/0) 外部路由器：**Inner-DNZ-ACL**								
編號	Permit/ deny	封包類型	來源		目的		方向	備註
			IP	port	IP	port		
1	permit	TCP	192.168.0.0/16	any	any	<1024	out	
2	permit	TCP	any	<1024	192.168.0.0/16	any	in	
3	permit	UDP	192.168.0.0/16	any	any	<1024	out	
4	permit	UDP	any	<1024	192.168.0.0/16	any	in	
5	permit	ip	192.168.0.0/16		120.118.166.0/24		out	
6	permit	ip	120.118.166.0/24		192.168.0.0/16		in	
7	permit	Icmp-echo	192.168.0.0/16		any		out	ping
8	permit	Icmp echo-reply	any		192.168.0.0/16		in	echo

9-6-5 內部路由器 DNZ 規劃 (四)

設定防火牆規則： Inner-DNZ-ACL-out

```
Ineer_R1>en
Ineer_R1#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Ineer_R1(config)#ip access-list extended Inner-DNZ-ACL-out
Ineer_R1(config-ext-nacl)#permit tcp 192.168.0.0 0.0.255.255 any lt 1024
Ineer_R1(config-ext-nacl)#permit udp 192.168.0.0 0.0.255.255 any lt 1024
Ineer_R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.255.255 any echo
Ineer_R1(config-ext-nacl)#permit ip 192.168.0.0 0.0.255.255 120.118.166.0 0.0.0.255
Ineer_R1(config-ext-nacl)#deny ip any any
Ineer_R1(config-ext-nacl)#exit
Ineer_R1(config)#do show access-list Inner-DNZ-ACL-out
Ineer_R1(config)#int gi3/0
Ineer_R1(config-if)#ip access-group Inner-DNZ-ACL-out out
```

Inner-DNZ-ACL-in

```
Ineer_R1(config)#ip access-list extended Inner-DNZ-ACL-in
Ineer_R1(config-ext-nacl)#permit tcp any lt 1024 192.168.0.0 0.0.255.255
Ineer_R1(config-ext-nacl)#permit udp any lt 1024 192.168.0.0 0.0.255.255
Ineer_R1(config-ext-nacl)#permit icmp any 192.168.0.0 0.0.255.255 echo-reply
Ineer_R1(config-ext-nacl)#permit ip 120.118.166.0 0.0.0.255 192.168.0.0 0.0.255.255
Ineer_R1(config-ext-nacl)#deny ip any any
Ineer_R1(config-ext-nacl)#exit
Ineer_R1(config)#do show access-list Inner-DNZ-ACL-in
Ineer_R1(config)#int gi3/0
Ineer_R1(config-if)#ip access-group Inner-DNZ-ACL-in in
Ineer_R1(config-if)#
```

9-6-5 內部路由器 DNZ 規劃 (五)

設定 telnet-ACL 防火牆規則

- 允許 192.168.0.1 與 192.168.1.1 登入

```
Inner_R1(config)#ip access-list standard telnet-ACL
Inner_R1(config-std-nacl)#permit host 192.168.0.1
Inner_R1(config-std-nacl)#permit host 192.168.1.1
Inner_R1(config-std-nacl)#deny any
Inner_R1(config-std-nacl)#exit
Inner_R1(config)#line vty 0 4
Inner_R1(config-line)#password cisco
Inner_R1(config-line)#login
Inner_R1(config-line)#access-class telnet-ACL in
Inner_R1(config-line)#exit
Ineer_R1(config)#enable password User
```

DNZ 防火牆測試

- 允許來源是 120.118.166.0/24網路上主機進入內部網路。
- 允許內部主機連結外部伺服器，但不允許外部主機連結內部伺服器。
- 不允許外部網路主機進入內部網路。