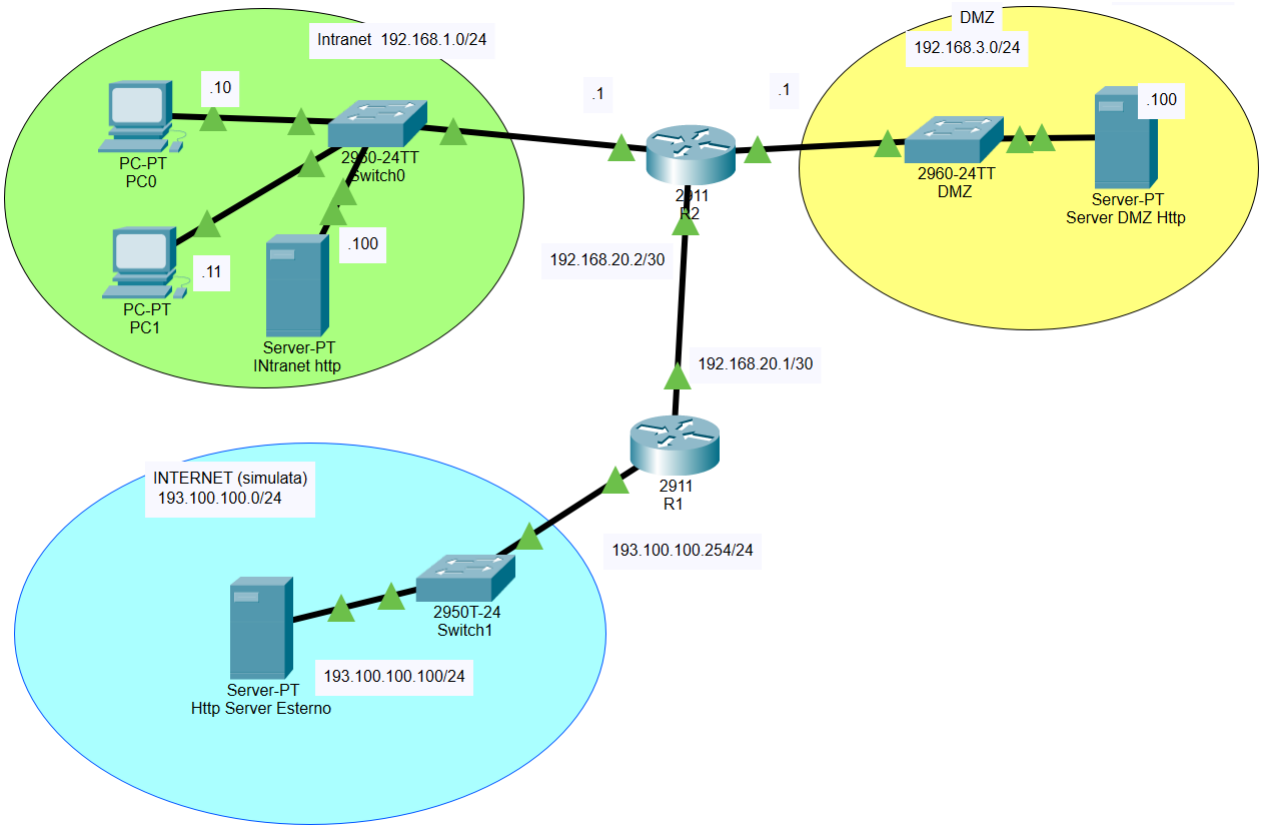
Dmz



Obiettivo

Si vuole collegare ad Internet una LAN, disegnata in alto, composta da:

- un router R2 avente funzionalità di firewall packet filtering
- una Intranet contenente un server http e due PC sui quali deve essere disponibile l'accesso Web della intranet
- una DMZ, nella quale è situato un Web server che risponde all'indirizzo IP 192.168.3.100.
- Per eseguire il collegamento ad Internet si è acquistato il router R1 e lo si è connesso alla rete del provider con indirizzo IP 193.100.100.254

NOTE:

- Per semplicità di configurazione, si rappresenta la rete Internet esterna con il solo router R1, fornito dal provider, che vede collegato, tramite switch un Web Server avente indirizzo IP 193.100.100.100
- Sempre per semplicità non sono state introdotte regole di natting.
- Il firewall, rappresentato dal router R2 con tre schede di rete GigaEthernet, va configurato con delle semplici regole di packet filtering.

Scopo dell'esercizio

- Si devono porre in essere delle ACL extended sul router R2, che funge da firewall di tipo packet filtering, in modo che non sia, in alcun modo, possibile collegarsi, dall'esterno, al server web della rete Intranet .
- Il server web in Intranet deve essere raggiungibile dal solo dal server della DMZ e dai PC dell'intranet
- Gli host dell'intranet devono potersi collegare a qualsiasi host esterno (quindi deve essere consentito il traffico di risposta).
- Tutti i pacchetti ICMP devono essere disabilitati ad eccezione del ping

Tabella degli indirizzi

Dispositivo	Interfaccia	Indirizzo IPv4	Maschera	IPv4 Def. Gateway
R1	G0/0	192.168.3.1	255.255.255.0	N/A
	G0/1	192.168.20.2	255.255.255.252	N/A
	G0/2	192.168.1.1	255.255.255.0	N/A
R2	G0/0	193.100.100.254	255.255.255.0	N/A
	G0/1	192.168.20.1	255.255.255.252	N/A
Server Intranet http	NIC	192.168.1.100	255.255.255.0	192.168.1.1
PC0	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC1	NIC	192.168.1.11	255.255.255.0	192.168.1.1
Server DMZ Http	NIC	192.168.3.100	255.255.255.0	192.168.3.1
Server Http Esterno	NIC	193.100.100.100	255.255.255.0	193.100.100.254

Configurazione R1

```
Router >enable
Router #configure terminal
Router(config)#hostname R1


R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 193.100.100.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.20.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

Configurazione R2

```
Router>enable
Router#configure terminal
Router(config)#hostname R2

R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)#interface GigabitEthernet0/1
R2(config-if)#ip address 192.168.20.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)#interface GigabitEthernet0/2
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

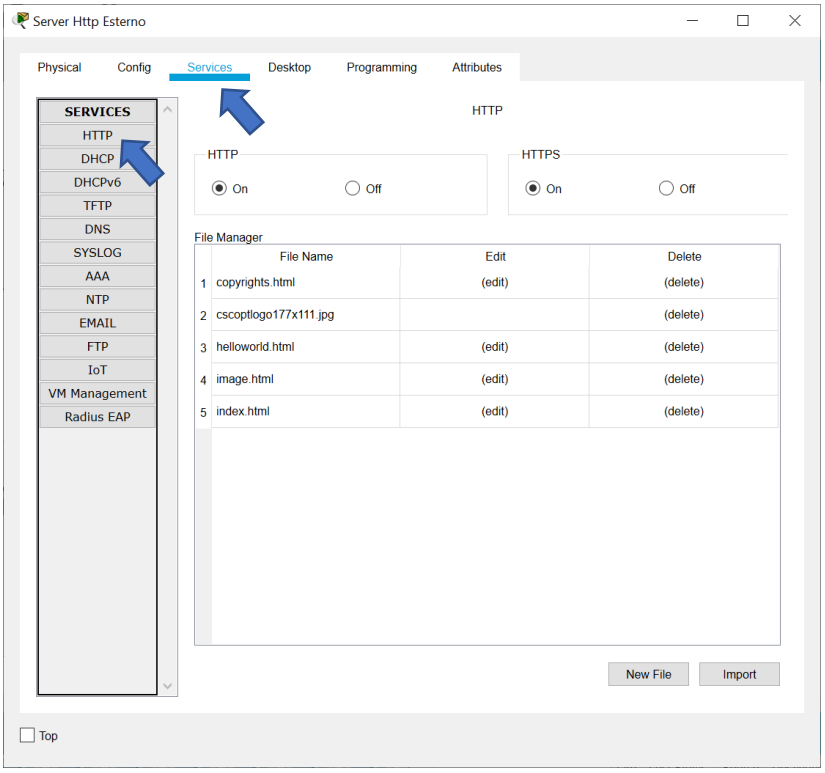
Inserimento delle rotte statiche su R1 e R2

```
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.20.2
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.20.2

R2(config)#ip route 193.100.100.0 255.255.255.0 192.168.20.1
```

Definizione delle pagine index.html sui server

Sono presenti 3 web server. In ogni server, per prima cosa, bisogna attivare il servizio http entrando nella scheda services, selezionando http (On)



Per personalizzare la pagina index.html, basta cliccare sul edit in corrispondenza del file index.html al punto 5 della tabella.
Inseriamo in coda al codice html contenuto una riga di intestazione che indichi il server in cui ci troviamo.

Nel Server Http Esterno inseriamo la riga:

<h1>SERVER HTTP ESTERNO</h1>

Nel Server Intranet http inseriamo la riga:

<h1>SERVER HTTP INTRANET</h1>

Nel Server DMZ http inseriamo la riga:

<hi>SERVER HTTP INTERNO</h1>

Impostazione delle ACL su R2
Impostiamo l'ACL per i pacchetti tcp in entrata sull 'interfaccia GigaEthernet 0/1 permettendo a tutto il traffico http, qualsiasi sia l'host di provenienza, diretto al server web in DMZ avente indirizzo 192.168.3.100.

```
R2(config)#access-list 110 permit tcp any 192.168.3.100 0.0.0.0 eq 80
```

Consentiamo inoltre il traffico di risposta ai ping inoltrati

```
R2(config)#access-list 110 permit icmp any any echo-reply
```

Nota: le regole sopra descritte, essendo di tipo extended, devono essere numerate con un valore compreso fra 100 e 199

Dopo aver regolato l'accesso alla dmz dobbiamo abilitare l'accesso a internet da parte degli host presenti nella intranet. Attualmente il traffico di risposta a una richiesta http risulterebbe bloccata. Quando un client della Intranet si collega al server web in Internet riceve i pacchetti di risposta su porte con valore superiore a 1024 e questo tipo di traffico viene bloccato con le regole finora impostate.

```
R2(config)#access-list 110 permit tcp any 192.168.1.0 0.0.0.255 gt 1024
```

Per controllare che tutto sia a posto eseguiamo il comado

```
R2#show access-lists
Extended IP access list 110
     10 permit tcp any host 192.168.3.100 eq www
     20 permit icmp any any echo-reply
     30 permit tcp any 192.168.1.0 0.0.0.255 gt 1024
```

E' importante ricordare che il router applica, per ogni pacchetto, le regole, nello stesso ordine con il quale sono state scritte e che se nessuna delle regole è soddisfatta il pacchetto viene scartato.
Applichiamo infine l' ACL all'interfaccia GigaEthernet 0/1 per il traffico in ingresso

```
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip access—group 110 in
```