Packet Tracer - Configurarea ACL-urilor Standard

Topologie

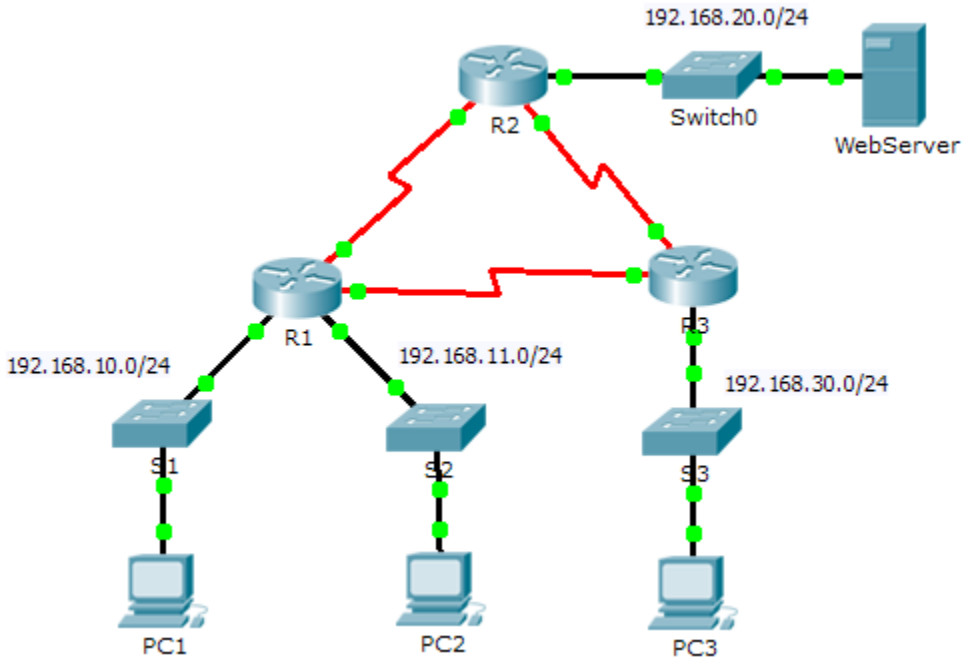

Tabela de Adresare

Dispozitiv	Interfață	Adresă IP	Masca de subreţea	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	F0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	F0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Obiective

Partea 1: Planificați o Implementare de ACL

Partea 2: Configurați, Aplicați și Verificați un ACL Standard

Context/Scenariu

ACL-urile standard sunt script-uri de configurare ale routerului care controlează dacă un router acceptă sau nu pachete în funcție de adresa sursei. Această activitate se concentrează pe definirea criteriului de filtrare, configurarea ACL-urilor standard, aplicarea ACL-urile la interfețele routerului și verificarea și testarea implementării de ACL. Routerele sunt deja configurate, inclusiv adresele IP și rutarea EIGRP (Enhanced Interior Gateway Routing Protocol).

Part 1: Planificați o Implementare de ACL

Step 1: Investigați configurarea rețelei curente.

Înainte de a aplica orice ACL-uri la o rețea, este important să confirmați că aveți conectivitate completă. Verificați dacă rețeaua are conectivitate completă alegând un calculator și dând ping altor echipamente din rețea. Ar trebui să puteți da ping cu succes la orice echipament.

Step 2: Evaluați două politici ale rețelei și planificați implementările de ACL.

a. Următoarele politici de rețea sunt implementate pe R2:

- Rețeaua 192.168.11.0/24 nu poate accesa WebServer din rețeaua **192.168.20.0/24**.

- Restul accesului este permis.

Pentru a restricționa accesul din rețeaua 192.168.11.0/24 la WebServer din 192.168.20.254 fără a interfera cu alt trafic, trebuie creat un ACL pe R2. Lista de acces trebuie plasată pe interfața de ieșire de pe WebServer. Trebuie creată o a doua regulă pe R2 pentru a se permite restul traficului.

b. Următoarele politici de rețea sunt implementare pe R3:

- Rețelei 192.168.10.0/24 nu i se permite să comunice cu rețeaua 192.168.30.0/24.
- Restul accesului este permis.

Pentru a restricționa accesul de la rețeaua 192.168.10.0/24 la rețeaua 192.168.30/24 fără a interfera cu alt trafic, este nevoie de o listă de acces creată pe R3. ACL trebuie plasat pe o interfață de ieșire de pe PC3. Trebuie creată o a doua regulă pe **R3** pentru a se permite restul traficului.

Part 2: Configurați, Aplicați și Verificați un ACL Standard

Step 1: Configurați un ACL numerotat standard pe R2.

a. Creați un ACL folosind numărul 1 pe R2 cu o regulă care împiedică accesul la rețeaua 192.168.20.0/24 din rețeaua 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. În mod implicit, o listă de acces nu permite traficul care nu se încadrează unei reguli. Pentru a permite traficul, configurați următoarea regulă:

```
R2(config)# access-list 1 permit any
```

c. Pentru ca ACL să filtrereze traficul, trebuie aplicat unei anumite operații a router-ului. Aplicați ACL-ul plasându-l pe interfața Gigabit Ethernet 0/0.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Step 2: Configurați și aplicați un ACL standard numerotat pe R3.

a. Creați un ACL folosind numărul 1 pe R3 cu o regulă care împiedică accesul la rețeaua 192.168.30.0/24 din PC1 (92.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. În mod implicit, un ACL împiedică traficul care nu se potrivește cu o regulă. Pentru a permite restul traficului, creați o a doua regulă pentru ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Aplicați ACL-ul plasându-l pe interfața Gigabit Ethernet 0/0 pentru traficul care pleacă.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Step 3: Verificați configurarea și funcționalitatea ACL-ului.

a. Pe **R2** și **R3**, introduceți comanda **show access-list** pentru a verifica configurările ACL. Introduceți comanda **show run** sau **show ip interface gigabitethernet 0/0** pentru a verifica plasările de ACL.

b. Având cele două ACL plasate, traficul de rețea este restricționat în conformitate cu politicile detaliate la Partea 1. Folosiți următoarele teste pentru a verifica implementările ACL:

- Un ping de la 192.168.10.10 la 192.168.11.10 se realizează cu succes.
- Un ping de la 192.168.10.10 la 192.168.20.254 se realizează cu succes.

- Un ping de la 192.168.11.10 la 192.168.20.254 eșuează.
- Un ping de la 192.168.10.10 la 192.168.30.10 eșuează.
- Un ping de la 192.168.11.10 la 192.168.30.10 se realizează cu succes.
- Un ping de la 192.168.30.10 la 192.168.20.254 se realizează cu succes.