Packet Tracer - Configurarea ACL-urilor extinse - Scenariul 3

Topologie

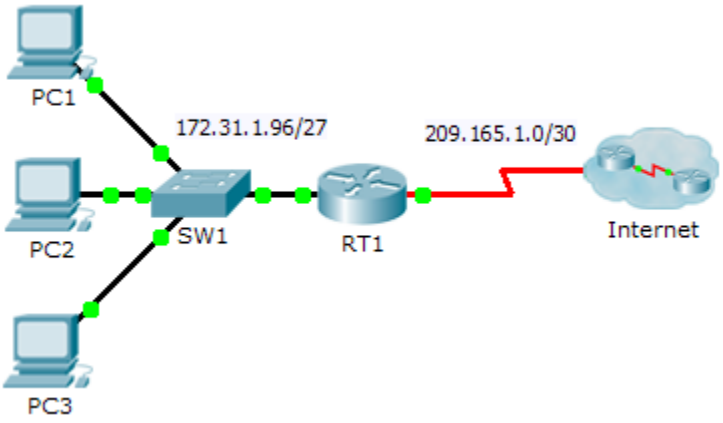

Tabela de Adresare

Dispozitiv	Interfață	Adresă IP	Mască de subrețea	Default Gateway
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	N/A
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254		
Server2	NIC	64.103.255.254		

Obiective

Partea 1 : Configurați un ACL Extins Denumit

Partea 2 : Aplicați și Verificați ACL-ul Extins

Condiții/Scenariu

În acest scenariu , dispozitive specifice unui LAN le sunt permise mai multe servicii aflate pe internet.

Part 1: Configurați un ACL Extins Numit

Folosiți un ACL denumit pentru a implemente următoarea politică:

- Blocați accesul HHTP și HTTPS de la PC1 către **Server1** și **Server2.** Serverele sunt în interiorul norului și doar dumneavoastră știți adresele lor IP.
- Blocați accesul FTP de la PC2 către **Server1** și **Server2**.
- Blocați acces-ul ICMP de la PC3 la **Server1** și **Server2**.

Notă: Din motive de notare, trebuie să configurați declarațiile în ordinea specificată în pașii ce urmează:

Step 1: Interziceți PC1 din a accesa serviciile HTTP și HTTPS pe Server1 și Server2.

a. Creați o listă de acces IP extinsă numită ACL care va interzice accesul lui PC1 la serviciile HTTP și HTTPS de pe **Server1** și **Server2**. Pentru că este imposibil să observați direct subrețea serverelor de pe Internet , patru reguli sunt necesare.

Care este comanda pentru a începe un ACL numit ?

b. Înregistrați afirmația care interzicfe accesul de la **PC1** la **Server1** , doar pentru HTTP (port 80).

c. Înregistrați afirmația care interzice accesul de la **PC1** la **Server1** , doar pentru HTTPS (port 443).

d. Înregistrați afirmația care interzice accesul de la **PC1** la **Server2** , doar pentru HTTP.

e. Înregistrați afirmația care refuză accesul de la **PC1** la **Server2** , doar pentru HTTPS.

Step 2: Interziceți PC2 din a accesa serviciile FTP pe Server1 și Server2.

a. Înregistrați afirmația care interzice accesul de la **PC2** la **Server1** , doar pentru FTP (numai port 21).

b. Înregistrați afirmația care interzice accesul de la **PC2** la **Server2** , doar pentru FTP (doar port 21).

Step 3: Interziceți PC3 din a da ping la Server1 și Server2.

a. Înregistrați afirmația care interzice accesul ICMP de la **PC3** la Server1.

b. Înregistrați afirmația care interzice accesul ICMP de la **PC3** la Server2.

Step 4: Permiteți restul traficului IP.

În mod implicit , lista de acces impiedică tot traficul care nu se potrivește cu regulile din listă. Ce comandă permite restul traficului?

Part 2: Aplicați și Verificați ACL Extins

Traficul ce urmează a fi filtrat vine de la rețeaua 172.31.1.96/27 și este detinat pentru rețelele la distanță. Plasamanetul adecvat ACL de asemenea depinde de relația dintre trafic cu privire la RT1.

Step 1: Aplicați ACL-ul la interfața corectă și în direcția corectă.

a. Care sunt comenzile de care aveți nevoie pentru a aplica ACL-ul la interfața corectă și direcția corectă ?

Step 2: Testați accesul pentru fiecare PC.

a. Accesați website-urile de pe **Server1** și **Server2** folosind Web Browser-ul de la PC1 și folosind ambele protocoale HTTP și HTTPS.

b. Accesați FTP-ul de pe **Server1** și **Server2** folosind PC1. Username-ul și parola sunt "cisco".

c. Ping **Server1** și **Server2** de la PC1.

d. Repetați Pasul 2a până la 2c cu **PC2** și **PC3** pentru a verifica funcționarea corespunzătoare a listei de acces.