Packet Tracer - Konfigurowanie nazywanych standardowych list ACL IPv4

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	F0/0	192.168.10.1	255.255.255.0	nd.
	F0/1	192.168.20.1	255.255.255.0	
	E0/0/0	192.168.100.1	255.255.255.0	
	E0/1/0	192.168.200.1	255.255.255.0	
File Server	Karta sieciowa	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	Karta sieciowa	192.168.100.100	255.255.255.0	192.168.100.1
PC0	Karta sieciowa	192.168.20.3	255.255.255.0	192.168.20.1
PC1	Karta sieciowa	192.168.20.4	255.255.255.0	192.168.20.1
PC2	Karta sieciowa	192.168.10.3	255.255.255.0	192.168.10.1

Cele

Część 1: Konfigurowanie i stosowanie nazywanych standardowych list ACL

Część 2: Weryfikowanie implementacji list ACL

Wprowadzenie / Scenariusz

Główny administrator sieci zlecił Ci zadanie polegające na utworzeniu standardowej nazywanej listy ACL blokującej dostęp do serwera plików. Serwer plików zawiera bazę danych dla aplikacji internetowych. Dostęp do serwera plików musi mieć tylko stacja robocza programu Web Manager PC1 i serwer sieci Web. Należy odmówić pozostałego ruchu do serwera plików.

Instrukcje

Część 1: Konfigurowanie i stosowanie nazywanej standardowej listy ACL

Krok 1: Przed skonfigurowaniem i implementacją ACL sprawdź łączność w sieci.

Testy ping z wszystkich trzech stacji roboczych do **Web Server** i **File Server** powinny się powieść.

Krok 2: Wykonaj konfigurację nazywanej standardowej listy ACL.

a. Skonfiguruj następującą nazywaną listę ACL na **R1**.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# permit host 192.168.100.100
```

```
R1(config-std-nacl)# deny any
```

Uwaga: Dla celów punktacji w nazywanej ACL uwzględniana jest wielkość liter, a instrukcje muszą być w tej samej kolejności, jak pokazano na rysunku.

b. Użyj polecenia **show access-lists**, aby sprawdzić zawartość listy dostępu przed zastosowaniem jej na interfejsie. Upewnij się, że nie zostały źle wpisane żadne adresy IP i że instrukcje są w prawidłowej kolejności.

```
R1# show access-lists
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

Krok 3: Zastosuj nazywaną listę ACL.

a. Zastosuj wychodzącą listę ACL na interfejsie Fast Ethernet 0/1.

Uwaga: W rzeczywistej sieci operacyjnej stosowanie listy dostępu do aktywnego interfejsu nie jest dobrą praktyką i należy ich unikać, jeśli to możliwe.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

b. Zapisz konfigurację.

Część 2: Weryfikowanie implementacji listy ACL

Krok 1: Sprawdź konfigurację listy ACL oraz jej zastosowanie na interfejsie.

Użyj komendy **show access-lists** aby zweryfikować konfigurację ACL. Użyj komendy **show run** lub **show ip interface fastethernet 0/1** aby sprawdzić, czy lista ACL jest prawidłowo zastosowana na interfejsie.

Krok 2: Sprawdź, czy lista ACL działa poprawnie.

Testy ping z wszystkich trzech stacji roboczych do **Web Server** powinny się powieść, ale tylko ping z komputera **PC1** i **Web Server** do **File Server** powinien zakończyć się powodzeniem. Powtórz polecenie **show access-lists**, aby zobaczyć liczbę pakietów dopasowanych do poszczególnych instrukcji.