Packet Tracer– Konfigurowanie standardowych list ACL

Topologia

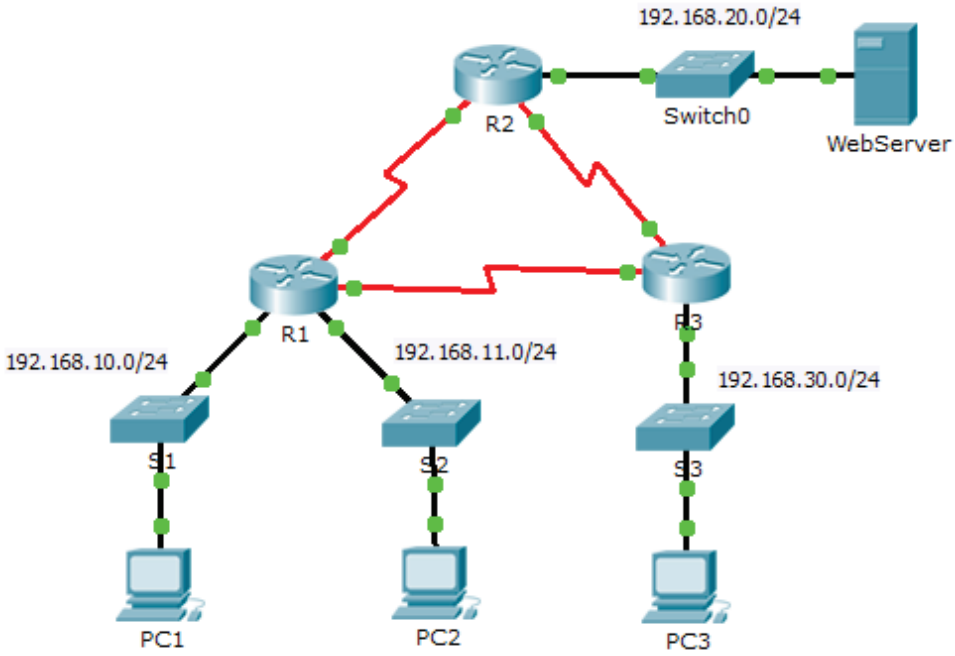

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	F0/0	192.168.10.1	255.255.255.0	Nie dotyczy
	F0/1	192.168.11.1	255.255.255.0	Nie dotyczy
	S0/0/0	10.1.1.1	255.255.255.252	Nie dotyczy
	S0/0/1	10.3.3.1	255.255.255.252	Nie dotyczy
R2	F0/0	192.168.20.1	255.255.255.0	Nie dotyczy
	S0/0/0	10.1.1.2	255.255.255.252	Nie dotyczy
	S0/0/1	10.2.2.1	255.255.255.252	Nie dotyczy
R3	F0/0	192.168.30.1	255.255.255.0	Nie dotyczy
	S0/0/0	10.3.3.2	255.255.255.252	Nie dotyczy
	S0/0/1	10.2.2.2	255.255.255.252	Nie dotyczy
PC1	Karta sieciowa	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Karta sieciowa	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Karta sieciowa	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	Karta sieciowa	192.168.20.254	255.255.255.0	192.168.20.1

Cele

Część 1: Planowanie implementacji list ACL

Część 2: Konfigurowanie, stosowanie i weryfikowanie standardowych list ACL

Wprowadzenie / Scenariusz

Standardowe listy kontroli dostępu (ACL) są skryptami konfiguracji routera, które pozwalają na akceptowanie lub odrzucanie pakietów w oparciu o filtrowanie pakietów na podstawie adresu źródłowego. Niniejsze ćwiczenie koncentruje się na definiowaniu kryteriów filtrowania, konfigurowaniu standardowych list ACL, przyporządkowywaniu ich do interfejsów routera oraz weryfikowaniu i badaniu implementacji list ACL. Routery, adresy IP oraz protokół routingu EIGRP (Enhanced Interior Gateway Routing Protocol) zostały już skonfigurowane.

Część 1: Planowanie implementacji ACL

Krok 1: Sprawdź bieżącą konfigurację sieci.

Przed zastosowaniem listy kontroli dostępu w sieci ważne jest, aby sprawdzić czy istnieje pełna komunikacja między wszystkimi systemami. Sprawdź, czy sieć ma pełną łączność, wybierając kolejne komputery PC i wykonując ping na pozostałe urządzenia w sieci. Testy ping wykonywane do każdego urządzenia powinny się powieść.

Krok 2: Określ dwie zasady zabezpieczeń sieciowych i zaplanuj implementacje ACL.

a. Na routerze **R2** powinny zostać zaimplementowane następujące zasady zabezpieczeń sieciowych:

- Sieć 192.168.11.0/24 nie powinna mieć dostępu do **WebServer** znajdującego się w sieci 192.168.20.0/24.
- Cały pozostały ruch jest dozwolony.

Aby zablokować dostęp z sieci 192.168.11.0/24 do **WebServer** posiadającego adres 192.168.20.254 bez wpływu na pozostały ruch sieciowy, listę ACL należy utworzyć na routerze **R2**. Lista kontroli dostępu musi być umieszczona na interfejsie wyjściowym podłączonym do **WebServer**. Aby przepuścić pozostały ruch sieciowy, na routerze **R2** musi zostać utworzona druga zasada.

b. Na routerze **R3** powinny zostać zaimplementowane następujące zasady zabezpieczeń sieciowych:

- Sieć 192.168.10.0/24 nie powinna mieć dostępu do sieci 192.168.30.0/24.
- Cały pozostały ruch jest dozwolony.

Aby zablokować dostęp z sieci 192.168.10.0/24 do sieci 192.168.30.0/24 bez wpływu na pozostały ruch sieciowy, należy listę ACL utworzyć na routerze **R3**. Lista ACL musi być umieszczona na interfejsie wyjściowym podłączonym do **PC3**. Aby przepuścić pozostały ruch sieciowy, na routerze **R3** musi zostać utworzona druga zasada.

Część 2: Konfigurowanie, stosowanie i weryfikowanie standardowych list ACL

Krok 1: Wykonaj konfigurację i zastosuj standardową numerowaną listę ACL na R2.

a. Utwórz listę ACL o numerze 1 na routerze **R2**, zawierającą polecenie blokujące dostęp z sieci 192.168.11.0/24 do sieci 192.168.20.0/24.

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

b. Domyślnie lista kontroli dostępu odrzuca cały ruch, który nie pasuje do zasady. Aby zezwolić na wszelki pozostały ruch sieciowy, należy użyć następującego polecenia:

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

c. Aby lista ACL faktycznie filtrowała ruch, musi zostać zastosowana. Zastosuj tę listę ACL, umieszczając ją na interfejsie Gigabit Ethernet 0/0 dla ruchu wychodzącego.

```
R2(config)# interface GigabitEthernet0/0
```

```
R2(config-if)# ip access-group 1 out
```

Krok 2: Wykonaj konfigurację i zastosuj standardową numerowaną listę ACL na R3.

a. Utwórz listę ACL o numerze 1 na routerze **R3** , zawierającą polecenie blokujące dostęp z komputera **PC1** znajdującego się w sieci 192.168.10.0/24 do sieci 192.168.30.0/24.

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

b. Domyślnie lista kontroli dostępu odrzuca cały ruch, który nie pasuje do zasady. Aby przepuścić cały pozostały ruch, należy utworzyć drugą zasadę dla listy ACL 1.

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

c. Zastosuj tę listę ACL, umieszczając ją na interfejsie Gigabit Ethernet 0/0 dla ruchu wychodzącego.

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

Krok 3: Sprawdź konfigurację list ACL oraz ich działanie.

a. Na routerach **R2** i **R3** wpisz komendy **show access-list** , aby sprawdzić konfigurację ACL. Aby zweryfikować lokalizację list ACL, użyj komendy **show run** lub **show ip interface gigabitethernet 0/0** .

b. Za pomocą dwóch list ACL, umieszczonych we właściwych miejscach, ruch w sieci jest ograniczony zgodnie z zasadami wyszczególnionymi w części 1. Wykonaj następujące testy w celu potwierdzenia właściwego funkcjonowania list ACL:

- Ping wysłany z 192.168.10.10 do 192.168.11.10 zakończył się sukcesem.
- Ping wysłany z 192.168.10.10 do 192.168.20.254 zakończył się sukcesem.
- Ping wysłany z 192.168.11.10 do 192.168.20.254 zakończył się niepowodzeniem.
- Ping z 192.168.10.10 to 192.168.30.10 zakończył się niepowodzeniem.
- Ping wysłany z 192.168.11.10 do 192.168.30.10 zakończył się sukcesem.
- Ping wysłany z 192.168.30.10 do 192.168.20.254 zakończył się sukcesem.