LABORATORIUM PROJEKTOWANIE I OBSŁUGA SIECI KOMPUTEROWYCH II

Data wykonania ćwiczenia:	17.04.2023
Rok studiów:	3
Semestr:	6
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	7

Temat: Konfigurowanie numerowanych standardowych list ACL IPv4 / Konfigurowanie nazywanych standardowych list ACL IPv4

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Konfigurowanie numerowanych standardowych list ACL IPv4

Część 1: Planowanie implementacji listy ACL

Krok 1: Zbadaj 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 z niego 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.

b) Na routerze R2 powinny zostać zaimplementowane następujące zasady:

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:

- 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 weryfikacja standardowej listy 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 żadnej zasady. Aby zezwolić na wszelki pozostały ruch sieciowy, należy użyć następującego polecenia:

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

c) Przed zastosowaniem listy kontroli dostępu na interfejsie w celu filtrowania ruchu najlepiej jest przejrzeć jej zawartość by sprawdzić, czy będzie ona filtrować ruch zgodnie z oczekiwaniami.

```
R2# show access-lists
Standard IP access list 1
10 deny 192.168.11.0 0.0.0.255
20 permit any
```

d) Aby lista ACL faktycznie filtrowała ruch, musi zostać zastosowana. Zastosuj tę listę ACL umieszczając ją na interfejsie GigabitEthernet 0/0 dla ruchu wychodzącego. Uwaga: W rzeczywistej sieci operacyjnej nie jest dobrą praktyką, aby stosować niesprawdzone listy dostępu do aktywnego interfejsu.

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#end
R2#
```

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 ACL odrzuca cały ruch, który nie pasuje do żadnej zasady. Aby przepuścić cały pozostały ruch, należy utworzyć drugą zasadę dla listy ACL 1.

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

```
R3>enable
R3#
R3#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
```

```
R3(config-if)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#end
```

c) Sprawdź, czy lista dostępu jest poprawnie skonfigurowana.

```
R3# show access-lists
Standard IP access list 1
10 deny 192.168.10.0 0.0.0.255
20 permit any
```

d) Zastosuj tę listę ACL umieszczając ją na interfejsie GigabitEthernet 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) 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.

c) Wydaj ponownie polecenie show access-lists na routerach R2 i R3. Powinieneś zobaczyć dane wyjściowe wskazujące liczbę pakietów, które pasują do każdego wpisu listy dostępu. Uwaga: Liczba dopasowań wyświetlanych dla routerów może być różna ze względu na liczbę wykonanych testów ping.

```
R2# show access-lists
Standard IP access list 1
10 deny 192.168.11.0 0.0.0.255 (4 match(es))
20 permit any (8 match(es))
```

```
```

```
R3# show access-lists
Standard IP access list 1
10 deny 192.168.10.0 0.0.0.255 (4 match(es))
20 permit any (8 match(es))
```

Konfigurowanie nazywanych standardowych list ACL IPv4

Część 1: Konfigurowanie i stosowanie nazwanej 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.

```
R1# show access-lists
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4 (4 match(es))
20 permit host 192.168.100.100 (4 match(es))
30 deny any (8 match(es))
```