LABORATORIUM PROJEKTOWANIE I OBSŁUGA SIECI KOMPUTEROWYCH II

Data wykonania ćwiczenia:	25.04.2023
Rok studiów:	3
Semestr:	6
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	8

Temat: Packet Tracer - Konfigurowanie i modyfikowanie standardowych list ACL IPv4

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Packet Tracer - Konfigurowanie i modyfikowanie standardowych list ACL IPv4

Bezpieczeństwo sieci i kontrola przepływu ruchu są ważnymi kwestiami przy projektowaniu i zarządzaniu sieciami IP. Możliwość konfigurowania odpowiednich reguł do filtrowania pakietów, w oparciu o ustalone zasady bezpieczeństwa, jest cenną umiejętnością.

W tym ćwiczeniu zostaną skonfigurowane reguły filtrowania dla dwóch lokalizacji biznesowych reprezentowanych przez R1 i R3. Kierownictwo ustanowiło pewne zasady dostępu między sieciami LAN znajdującymi się w R1 i R3, które należy wdrożyć. Router Edge znajdujący się pomiędzy R1 i R3 został dostarczony przez usługodawcę internetowego nie będzie miał żadnych list ACL. Nie uzyskasz dostępu administracyjnego do routera Edge, ponieważ możesz kontrolować tylko własny sprzęt i zarządzać nim.

Część 1: Weryfikacja łączności

W pierwszej części czeka nas seria testów połączeń między urządzeniami

Z PC-A, wykonaj ping do PC-C i PC-D. Czy powiodły się?

Tak

Z R1, wykonaj ping do PC-C i PC-D. Czy powiodły się?

Tak

Z PC-C, wykonaj ping do PC-A i PC-B. Czy powiodły się?

Tak

Z R3, wykonaj ping do PC-A i PC-B. Czy powiodły się?

Tak

Czy wszystkie komputery mogą wysłać ping do serwera pod numerem 209.165.200.254?

Tak

Część 2: Konfiguracja i weryfikacja standardowych numerowanych oraz nazywanych list ACL

Krok 1: Skonfiguruj numerowaną standardową listę ACL.

Standardowe listy ACL filtrują tylko w oparciu o adres źródłowy. Typową najlepszą praktyką dla standardowych list ACL jest konfigurowanie i stosowanie listy ACL jak najbliżej miejsca docelowego. Dla pierwszej listy dostępu w tym działaniu utwórz standardową numerowaną listę ACL, która umożliwia ruchowi ze wszystkich hostów w sieci 192.168.10.0/24 i wszystkim hostom z sieci 192.168.20.0/24 dostęp do wszystkich hostów w sieci 192.168.30.0/24 sieć. Zasady bezpieczeństwa stanowią również, że na końcu wszystkich list ACL powinien znajdować się wpis kontroli dostępu (ACE) deny any, zwany także instrukcją ACL.

Jakiej maski blankietowej użyjesz, aby umożliwić wszystkim hostom z sieci 192.168.10.0/24 dostęp do sieci 192.168.30.0/24?

`0.0.0.255`

Zgodnie z zalecanymi przez firmę Cisco najlepszymi praktykami, na którym routerze umieszczałbyś tę ACL?

`R3`

Na którym interfejsie można umieścić tę ACL? W jakim kierunku byś ją zastosował?

```
Interfejs G0/0/0. Lista kontroli dostępu (ACL) powinna zostać zastosowana do ruchu
wychodzącego.

moglibyśmy umieścić ACL na interfejsie S0/1/1 routera R3 dla ruchu przychodzącego.
Należy jednak podkreślić, że taka konfiguracja spowodowałaby również blokowanie
ruchu z sieci LAN R1 do sieci 192.168.40.0/24
```

a) Skonfiguruj ACL na R3. Użyj numeru 1 listy dostępu.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b) Zastosuj ACL na odpowiednim interfejsie we właściwym kierunku.

```
R3(config)# interface g0/0/0
R3(config-if)# ip access-group 1 out
```

c) Sprawdź numerowaną ACL.

Korzystanie z różnych poleceń show może pomóc w sprawdzeniu składni i umieszczeniu list ACL w routerze.

Którego polecenia użyjesz, aby zobaczyć całą listę dostępu 1 ze wszystkimi wpisami kontroli dostępu ACE?

```
R3# show access-lists 1

lub

R3# show access-lists
```

Jakiego polecenia użyłbyś, aby zobaczyć, gdzie lista dostępu została zastosowana i w jakim kierunku?

```
R3# show ip interface g0/0/0

lub
```

```
R3# show ip interface
```

1. Na R3 wydaj polecenie show access-lists 1.

```
R3# show access-list 1
Standard IP access list 1
    permit 192.168.10.0, wildcard bits 0.0.0.255
    permit 192.168.20.0, wildcard bits 0.0.0.255
    deny any
```

2. Na R3 wydaj polecenie show ip interface g0/0/0.

```
R3# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound access list is not set
<Output omitted>
```

3. Przetestuj ACL, aby sprawdzić, czy zezwala na ruch z sieci 192.168.10.0/24 do sieci 192.168.30.0/24.

Z wiersza poleceń PC-A wykonaj ping na adres IP PC-C. Czy polecenia ping zostały wykonane pomyślnie?

Tak

4. Przetestuj listę ACL, aby sprawdzić, czy zezwala na ruch z sieci 192.168.20.0/24 do sieci 192.168.30.0/24.

Z wiersza poleceń PC-B wykonaj ping na adres IP PC-C. Czy polecenia ping zostały wykonane pomyślnie?

Tak

5. Czy ping z PC-D do PC-C powinien się powieść? Wykonaj ping z PC-D do PC-C, aby zweryfikować odpowiedź.

Nie, to że się nie powodzi potwierdza nam że ASL działa poprawnie

d) Z wiersza poleceń R1, ponownie wykonaj ping na adres IP PC-C.

```
R1# ping 192.168.30.3
```

Czy test ping zakończył się sukcesem? Wyjaśnij.

Pingi nie powiodły się. Kiedy wykonujesz pinga z routera, używa on jako adresu źródłowego najbliższego interfejsu do celu. Pingi miały adres źródłowy 10.1.1.1. Lista dostępu na R3 zezwala jedynie na dostęp sieciom 192.168.10.0/24 i 192.168.20.0/24.

e) Wydaj ponownie komendę show access-lists 1. Należy zauważyć, że dane wyjściowe polecenia wyświetlają informacje dotyczące liczby dopasowania każdego ACE do ruchu, który dotarł do interfejsu Gigabit Ethernet 0/0/0.

```
R3# show access-lists 1
Standard IP access list 1
    permit 192.168.10.0 0.0.0.255 (4 match(es))
    permit 192.168.20.0 0.0.0.255 (4 match(es))
    deny any (4 match(es))
```

Krok 2: Wykonaj konfigurację nazywanej standardowej listy ACL.

Utwórz nazwaną standardową ACL zgodną z następującymi zasadami: zezwalaj na ruch ze wszystkich hostów z sieci 192.168.40.0/24 do wszystkich hostów w sieci 192.168.10.0/24. Ponadto zezwalaj na dostęp tylko komputera PC-C do sieci 192.168.10.0/24. Nazwa tej listy dostępu ma być następująca BRANCH-OFFICE-POLICY.

Zgodnie z zalecanymi przez firmę Cisco najlepszymi praktykami, na którym routerze umieszczałbyś tę ACL?

R1

Na którym interfejsie można umieścić tę ACL? W jakim kierunku byś ją zastosował?

ACL powinna być zastosowana na wychodzącym ruchu na G0/0/0. Umieszczenie jej na ruchu przychodzącym w S0/0/0 na R1 spowoduje zablokowanie wszelkiego ruchu z sieci LAN R3 do sieci 192.168.20.0/24.

a) Utwórz standardową ACL o nazwie BRANCH-OFFICE-POLICY na R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Spójrz na pierwszy ACE na liście dostępowej. Jaki jest inny sposób napisania tego?

permit 192.168.30.3 0.0.0.0

b) Zastosuj ACL na odpowiednim interfejsie we właściwym kierunku.

```

```

```
R1# config t
R1(config)# interface g0/0/0
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c) Zweryfikuj nazwaną ACL.

1. Na R1 wydaj polecenie show access-lists 1.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit host 192.168.30.3
    20 permit 192.168.40.0 0.0.0.255
```

Czy istnieje jakaś różnica między tą ACL na R1 a ACL na R3? Jeśli tak, to co to jest?

Chociaż w wierszu 30 nie ma jawnego polecenia "deny any" na routerze R1, jest ono domyślne. Warto to podkreślić. Dodanie przez nich jawnego wpisu "deny any" jest dobrą praktyką i wzmacnia zrozumienie działania list ACL, ponieważ taki wpis pojawia się w wyniku polecenia "show access-lists". Łatwo jest zapomnieć o domyślnym "deny any" podczas rozwiązywania problemów z ACL, co może prowadzić do blokowania ruchu, który powinien być dozwolony.

2. Na R1 wydaj polecenie show ip interface g0/0/0, aby sprawdzić, czy lista ACL jest skonfigurowana na interfejsie.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Output omitted>
```

Przetestuj ACL. Z wiersza poleceń na PC-C, wyślij ping na adres IP PC-A. Czy pingi się powiodły?

Tak

3. Przetestuj ACL, aby upewnić się, że tylko host PC-C ma dostęp do sieci 192.168.10.0/24. Należy wykonać rozszerzony ping i użyć adresu G0/0/0 na R3 jako źródła. Wykonaj ping na adres IP PC-A.

```
R3# ping
Protocol [ip]:
```

```
Target IP address: 192.168.10.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.30.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
U.U.U
```

Czy polecenia ping zostały wykonane pomyślnie?

Nie

4. Przetestuj listę ACL, aby sprawdzić, czy zezwala na ruch z sieci 192.168.40.0/24 do sieci 192.168.10.0/24. Z wiersza poleceń PC-D wykonaj ping na adres IP PC-A.

Czy polecenia ping zostały wykonane pomyślnie?

Tak

Część 3: Modyfikacja standardowych list ACL

W biznesie często zmieniają się zasady bezpieczeństwa. Z tego powodu listy ACL mogą wymagać modyfikacji. W części 3 zostanie zmieniona jedna z wcześniej skonfigurowanych list ACL, tak aby była zgodna z wprowadzoną nową zasadą zarządzania.

Spróbuj wysłać ping do serwera pod adresem 209.165.200.254 z PC-A. Zauważ, że ping nie powiódł się. ACL na R1 blokuje powrót ruchu internetowego do PC-A. Dzieje się tak dlatego, że adres źródłowy w zwracanych pakietach nie mieści się w zakresie dozwolonych adresów.

Zarząd postanowił, że ruch powracający z sieci 209.165.200.224/27 powinien mieć pełny dostęp do sieci 192.168.10.0/24. Zarząd chce również, aby listy ACL na wszystkich routerach były zgodne ze spójnymi regułami. Wpis ACE deny any powinien być umieszczony na końcu wszystkich list ACL. Należy zmodyfikować listę ACL BRANCH-OFFICE-POLICY.

Do tej listy ACL zostaną dodane dwa dodatkowe wiersze. Można to zrobić na dwa sposoby:

OPCJA 1: Wydanie polecenia no ip access-list standard BRANCH-OFFICE-POLICY w trybie konfiguracji globalnej. Spowoduje to usunięcie listy ACL z routera. W zależności od routera IOS może wystąpić jeden z następujących scenariuszy: wszelkie filtrowanie pakietów zostanie anulowane, a wszystkie pakiety będą przepuszczane przez router; lub, ponieważ nie usunąłeś polecenia ip access-group z interfejsu G0/1, filtrowanie jest nadal realizowane. Niezależnie od tego, po usunięciu listy ACL można ponownie wpisać całą ACL lub wyciąć ją i wkleić z edytora tekstu.

OPCJA 2: Możesz modyfikować listy ACL w miejscu, dodając lub usuwając określone wiersze w samej liście ACL. Może się to przydać, zwłaszcza w przypadku list ACL, które są długie. Ponowne wpisywanie całej listy ACL lub wycinanie i wklejanie może z łatwością prowadzić do błędów. Modyfikowanie określonych linii w ACL jest łatwe do wykonania.

Dla tego działania użyj opcji 2.

Krok 1: Modyfikowanie nazwanej standardowej listy ACL .

a) Na R1 wydaj polecenie show access-lists 1.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0 0.0.0.255 (5 matches)
```

b) Dodaj dwa dodatkowe wiersze na końcu listy ACL. W trybie konfiguracji globalnej zmodyfikuj listę ACL, BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c) Sprawdź listę ACL.

1. Na R1 wydaj polecenie show access-lists 1.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny any
```

Czy musisz zastosować BRANCH-OFFICE-POLICY do interfejsu G0/1 na R1?

`Nie, ip access-group BRANCH-OFFICE-POLICY wciąż działa na intefejsie G0/1`

2. Przetestuj listę ACL, aby sprawdzić, czy umożliwia ruch powrotny z sieci 209.165.200.224/27 do sieci 192.168.10.0/24. Z komputera PC-A wykonaj ping do serwera pod adresem 209.165.200.254.

Czy polecenia ping zostały wykonane pomyślnie?

`Tak`