

## Packet Tracer – Demonstracja działania listy kontroli dostępu

### Cele

Część 1: Weryfikacja lokalnego połączenia i testowanie listy kontroli dostępu

Część 2: Usuwanie listy kontroli dostępu i ponowne testowanie

### Wprowadzenie

Niniejsze ćwiczenie demonstruje użycie listy kontroli dostępu (ACL) w celu zablokowania komunikatów ping tak, by nie dotarł on do hostów znajdujących się w zdalnych sieciach. Po usunięciu listy ACL z konfiguracji, komunikaty ping nie będą blokowane.

### Tabela adresacji

| Urządzenie | Interfejs      | Adres IP / Prefiks |
|------------|----------------|--------------------|
| R1         | G0/0           | 192.168.10.1/24    |
|            | G0/1           | 192.168.11.1/24    |
|            | S0/0/0         | 10.1.1.1/30        |
| R2         | S0/0/0         | 10.10.1.2/30       |
|            | S0/0/1         | 10.10.1.5/30       |
| R3         | G0/0           | 192.168.30.1/24    |
|            | G0/1           | 192.168.31.1/24    |
|            | S0/0/1         | 10.10.1.6/24       |
| PC1        | Karta sieciowa | 192.168.10.10/24   |
| PC2        | Karta sieciowa | 192.168.10.11/24   |
| PC3        | Karta sieciowa | 192.168.11.10/24   |
| PC4        | Karta sieciowa | 192.168.30.12/24   |
| Serwer DNS | Karta sieciowa | 192.168.31.12/24   |

### Instrukcje

#### Część 1: Weryfikacja lokalnego połączenia i testowanie listy kontroli dostępu

**Krok 1:** Użyj komendy ping do urządzeń znajdujących się w sieci lokalnej aby sprawdzić komunikację.

- W wierszu poleceń komputera **PC1** wykonaj ping do komputera **PC2**.
- W wierszu poleceń komputera **PC1**, wykonaj ping do komputera **PC3**.

Dlaczego test ping się powiódł?

### Krok 2: Użyj komendy ping do urządzeń znajdujących się w sieciach zdalnych by sprawdzić działanie ACL.

- W wierszu poleceń komputera **PC1**, wykonaj ping do komputera **PC4**.
- W wierszu poleceń komputera **PC1**, wykonaj ping do **Serwer DNS**.

Dlaczego test ping nie powiódł się? (**Wskazówka**: Użyj trybu symulacji lub wyświetl konfigurację routera, aby to zbadać).

## Część 2: Usuń listę ACL i powtórz test

### Krok 1: Aby zbadać konfigurację ACL, użyj komend show.

- Przejdź do interfejsu wiersza poleceń R1. Użyj komend **show run** i **show access-lists** aby wyświetlić aktualnie skonfigurowane listy ACL. Użyj komendy **show access-lists**, aby szybko wyświetlić aktualne listy ACL. Wpisz komendę **show access-lists** a następnie spację i znak zapytania (?), aby wyświetlić dostępne opcje:

```
R1# show access-lists ?
<1-199> ACL number
WORD ACL name
<cr>
```

Jeżeli znasz numer lub nazwę listy ACL, to możesz filtrować wyjście komendy **show**. Aczkolwiek **R1** ma tylko jedną listę ACL; w związku z tym komenda **show access-lists** jest wystarczająca.

```
R1#show access-lists
Standard IP access list 11
 10 deny 192.168.10.0 0.0.0.255
 20 permit any
```

Pierwszy wiersz listy ACL blokuje wszystkie pakiety pochodzące z sieci **192.168.10.0/24**, która obejmuje echa protokołu ICMP (Internet Control Message Protocol) (żądania ping). Druga linia listy ACL zezwala na cały ruch **IP** z dowolnego (**any**) źródła przez router.

- Aby ACL wpłynęło na działanie routera, musi być zastosowana na interfejsie w określonym kierunku. W tym scenariuszu lista ACL jest używana do filtrowania ruchu wychodzącego interfejsem. W związku z tym cały ruch opuszczający określony interfejs R1 będzie sprawdzany pod kątem listy ACL 11.

Można wyświetlić informacje dotyczące protokołu IP za pomocą komendy **show ip interface**, ale lepsze jest po prostu użycie polecenia **show run**. Aby uzyskać pełną listę interfejsów, do których można zastosować listę ACL, oraz listę wszystkich skonfigurowanych list ACL, należy użyć następującego polecenia:

```
R1# show run | include interface|access
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface Serial0/0/0
  ip access-group 11 out
interface Serial0/0/1
```

```
interface Vlan1
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
```

Drugi symbol „|” tworzy warunek OR, który pasuje do 'interface' LUB 'access '. Ważne jest, aby żadne spacje nie były uwzględniane w warunku OR. Użyj jednego lub obu tych poleceń, aby znaleźć informacje na temat listy ACL.

Do jakiego interfejsu i w jakim kierunku zastosowana jest ACL?

### Krok 2: Usuń listę ACL 11 z konfiguracji.

Do usuwania list ACL z konfiguracji służy komenda **no access list** *[number of the ACL]*. Polecenie **no access-list** używane bez argumentów powoduje usunięcie wszystkich list ACL skonfigurowanych na routerze. Polecenie **no access-list** *[number of the ACL]* usuwa tylko określoną listę ACL. Usunięcie listy ACL z routera nie powoduje usunięcia listy ACL z interfejsu. Polecenie, które stosuje ACL do interfejsu, musi zostać usunięte oddzielnie.

- a. Na interfejsie Serial0/0/0 usuń listę dostępu 11, która została wcześniej zastosowana do interfejsu jako filtr **wychodzący**:

```
R1(config)# interface s0/0/0
R1(config-if)# no ip access-group 11 out
```

- b. Aby usunąć listę ACL, w trybie konfiguracji globalnej wpisz następującą komendę:

```
R1(config)# no access-list 11
```

- c. Upewnij się, że test ping z komputera **PC1** do **DNS Server** i **PC4** kończy się powodzeniem.