Packet Tracer - Konfiguracja rozszerzonych list ACL IPv4 - Scenariusz 2

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
RT1	G0/0	172.31.1.126	255.255.255.224	nd.
	S0/0/0	209.165.1.2	255.255.255.252	
PC1	Karta sieciowa	172.31.1.101	255.255.255.224	172.31.1.126
PC2	Karta sieciowa	172.31.1.102	255.255.255.224	172.31.1.126
PC3	Karta sieciowa	172.31.1.103	255.255.255.224	172.31.1.126
Server1	Karta sieciowa	64.101.255.254		
Server2	Karta sieciowa	64.103.255.254		

Cele

Część 1: Konfiguracja rozszerzonej nazywanej listy ACL

Część 2: Zastosowanie i weryfikacja rozszerzonej listy ACL

Wprowadzenie / Scenariusz

W tym scenariuszu, określone urządzenia z sieci lokalnej dopuszczone są do różnych usług umieszczonych na serwerach znajdujących się w Internecie.

Instrukcje

Część 1: Konfiguracja rozszerzonej nazywanej listy ACL

Skonfiguruj jedną nazwaną listę ACL, aby zaimplementować następujące zasady:

- Blokuj ruch HTTP i HTTPS kierowany z **PC1** do **Server1** i **Server2**. Serwery są wewnątrz chmury i tylko ty znasz ich adresy IP.
- Blokuj dostęp FTP z **PC2** do **Server1** i **Server2**.
- Blokuj dostęp ICMP z **PC3** do **Server1** i **Server2**.

Uwaga: Do celów punktacji, należy skonfigurować wyrażenia w kolejności określonej w następujących krokach.

Krok 1: Odmów dostępu PC1 do usług HTTP i HTTPS na Server1 i Server2.

a. Utwórz nazwaną rozszerzoną listę dostępu IP na routerze RT1, która odmówi komputerowi **PC1** dostępu do usług HTTP i HTTPS **Server1** i **Server2**. Wymagane są cztery instrukcje kontroli dostępu.

Jakie jest polecenie rozpoczynające konfigurację rozszerzonej listy dostępu o nazwie **ACL**?

b. Rozpocznij konfigurację listy ACL od instrukcji, która odmawia dostępu z **PC1** do **Server1**, tylko dla HTTP (port 80). Sprawdź w tabeli adresacji adresy IP **PC1** i **Server1**.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
```

c. Następnie wprowadź wyrażenie, które blokuje dostęp z **PC1** do **Server1** tylko dla protokołu HTTPS (port 443).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
```

d. Wprowadź wyrażenie, które blokuje dostęp z **PC1** do **Server2** tylko dla protokołu HTTP. Adres IP **Server2** można znaleźć w tabeli adresacji.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
```

e. Wprowadź wyrażenie, które blokuje dostęp z **PC1** do **Server2** tylko dla protokołu HTTPS.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

Krok 2: Blokuj dostęp PC2 do usług FTP na Server1 i Server2.

Adres IP **PC2** można znaleźć w tabeli adresacji.

a. Wprowadź wyrażenie, które blokuje dostęp z **PC2** do **Server1** tylko dla protokołu FTP (tylko port 21).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
```

b. Wprowadź wyrażenie, które blokuje dostęp z **PC2** do **Server2** tylko dla protokołu FTP (tylko port 21).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
```

Krok 3: Zablokuj PC3 komunikaty ping do Server1 i Server2.

Adres IP **PC3** można znaleźć w tabeli adresacji.

a. Wprowadź wyrażenie, które blokuje dostęp ICMP z **PC3** do **Server1**.

```
RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.101.255.254
```

b. Wprowadź wyrażenie, które blokuje dostęp ICMP z **PC3** do **Server2**.

```
RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.103.255.254
```

Krok 4: Zezwól na cały pozostały ruch IP.

Domyślnie lista kontroli dostępu odrzuca cały ruch, który nie pasuje do żadnej reguły na liście. Wprowadź polecenie, które zezwala na cały ruch, który nie odpowiada żadnej ze skonfigurowanych instrukcji listy dostępu.

Krok 5: Przed zastosowaniem jej na interfejsie sprawdź konfigurację listy dostępu.

Przed zastosowaniem listy dostępu należy zweryfikować konfigurację, aby upewnić się, że nie ma błędów typograficznych i że instrukcje są w prawidłowej kolejności. Aby wyświetlić bieżącą konfigurację listy dostępu, należy użyć polecenia **show access-lists** lub **show running-config**.

```
RT1# show access-lists
Extended IP access list ACL
        10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
        20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
        30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
        40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
        50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
```

```
        60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
        70 deny icmp host 172.31.1.103 host 64.101.255.254
        80 deny icmp host 172.31.1.103 host 64.103.255.254
        90 permit ip any any

RT1# show running-config | begin access-list
ip access-list extended ACL
      deny tcp host 172.31.1.101 host 64.101.255.254 eq www
      deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
      deny tcp host 172.31.1.101 host 64.103.255.254 eq www
      deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
      deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
      deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
      deny icmp host 172.31.1.103 host 64.101.255.254
      deny icmp host 172.31.1.103 host 64.103.255.254
      permit ip any any
```

Uwaga: Różnica między wyjściem polecenia **show access-lists** a wyjściem polecenia **show running-config** polega na tym, że polecenie **show access-lists** zawiera numery sekwencyjne przypisane do instrukcji konfiguracyjnych. Te numery sekwencyjne umożliwiają edycję, usuwanie i wstawianie pojedynczych linii w konfiguracji listy dostępu. Numery sekwencyjne określają również kolejność przetwarzania poszczególnych instrukcji kontroli dostępu, zaczynając od najniższego numeru sekwencyjnego.

Część 2: Zastosowanie i weryfikacja rozszerzonej listy ACL

Ruch, który ma być filtrowany, pochodzi z sieci 172.31.1.96/27 i jest przeznaczony dla sieci zdalnych. Odpowiednie umieszczenie ACL zależy od relacji ruchu w odniesieniu do **RT1**. Ogólnie rzecz biorąc, rozszerzone listy dostępu powinny być umieszczone na interfejsie najbliżej źródła ruchu.

Krok 1: Zastosuj ACL do właściwego interfejsu i w prawidłowym kierunku.

Uwaga: W rzeczywistej sieci operacyjnej niesprawdzone listy ACL nigdy nie powinny być stosowane do aktywnego interfejsu. Nie jest to dobra praktyka i może zakłócić działanie sieci.

Na którym interfejsie należy zastosować nazwaną listę ACL i w jakim kierunku?

Wprowadź polecenia konfiguracyjne, aby zastosować listę ACL do interfejsu.

Krok 2: Przetestuj dostęp dla każdego komputera.

a. Uzyskaj dostęp do witryn internetowych **Server1** i **Server2** za pomocą przeglądarki internetowej komputera **PC1**. Użyj protokołów HTTP i HTTPS. Polecenie **show access-lists** umożliwia wyświetlenie instrukcji list dostępu pozwalających na ruch lub odrzucającej go. Wyjście polecenia **show access-lists** wyświetla liczbę pakietów dopasowanych do każdej instrukcji od czasu ostatniego wyczyszczenia liczników lub ponownego uruchomienia routera.

   Uwaga: Aby wyczyścić liczniki na liście dostępu, użyj polecenia **clear access-list counters**.

```
RT1#show ip access-lists
Extended IP access list ACL
10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))
20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

```
50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
70 deny icmp host 172.31.1.103 host 64.101.255.254
80 deny icmp host 172.31.1.103 host 64.103.255.254
90 permit ip any any
```

b. Połącz się FTP z **Server1** i **Server2** używając **PC1**. Nazwa użytkownika i hasło to **cisco**.

c. Wykonaj ping do **Server1** i **Server2** z **PC1**.

d. Powtórz Krok 2a do kroku 2c z **PC2** i **PC3** aby sprawdzić prawidłowe działanie listy dostępu.