Packet Tracer – Konfiguracja rozszerzonych list ACL – Scenariusz 3

Topologia

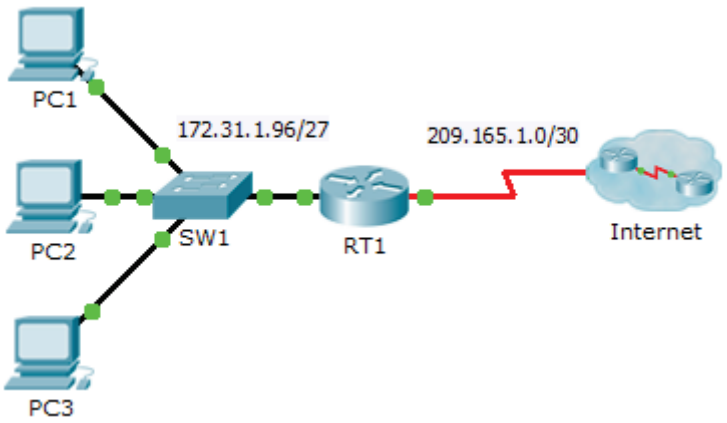

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
RT1	G0/0	172.31.1.126	255.255.255.224	Nie dotyczy
	S0/0/0	209.165.1.2	255.255.255.252	Nie dotyczy
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.

Część 1: Konfiguracja rozszerzonej nazywanej listy ACL

Użyj jednej nazwanej ACL, aby wdrożyć 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 rozszerzoną nazwaną listę ACL, która będzie blokować dostęp **PC1** do usług HTTP i HTTPS na **Server1** i **Server2**. Ponieważ nie da się bezpośrednio obserwować podsieci serwerów w Internecie, potrzebne są cztery zasady.

   Jakie polecenie rozpoczyna tworzenie nazwanej ACL?

b. Zapisz wyrażenie, które blokuje dostęp z **PC1** do **Server1** tylko dla protokołu HTTP (port 80).

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

d. Zapisz wyrażenie, które blokuje dostęp z **PC1** do **Server2** tylko dla protokołu HTTP.

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

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

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

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

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

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

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

Krok 4: Zezwól na cały pozostały ruch IP.

Domyślnie lista kontroli dostępu odrzuca cały ruch, który nie pasuje do dowolnej reguły na liście. Jakie polecenie zezwoli na cały pozostały ruch?

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 również od relacji ruchu w odniesieniu do **RT1**.

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

a. Jakie komendy zastosują ACL na właściwym interfejsie i we właściwym kierunku?

Krok 2: Przetestuj dostęp dla każdego komputera.

a. Otwórz strony internetowe znajdujące się na **Server1** i **Server2** za pomocą przeglądarki internetowej na **PC1** używając protokołów HTTP i HTTPS.

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 Kroki 2a do 2c z **PC2** i **PC3,** aby sprawdzić prawidłowe działanie listy dostępu.