

Packet Tracer - Wdrażanie ACL IPv4 - wyzwanie

Tabela adresacji

Urządzenie	Interfejs	Adres IP
Branch	G0/0/0	192.168.1.1/26
	G0/0/1	192.168.1.65/29
	S0/1/0	192.0.2.1/30
	S0/1/1	192.168.3.1/30
HQ	G0/0/0	192.168.2.1/27
	G0/0/1	192.168.2.33/28
	S0/1/1	192.168.3.2/30
PC-1	Karta sieciowa	192.168.1.10/26
PC-2	Karta sieciowa	192.168.1.20/26
PC-3	Karta sieciowa	192.168.1.30/26
Admin	Karta sieciowa	192.168.1.67/29
Enterprise Web Server	Karta sieciowa	192.168.1.70/29
Branch PC	Karta sieciowa	192.168.2.17/27
Branch Server	Karta sieciowa	192.168.2.45/28
Internet User	Karta sieciowa	198.51.100.218/24
External Web Server	Karta sieciowa	203.0.113.73/24

Cele

- Konfigurowanie routera za pomocą standardowych nazwanych list ACL.
- Konfigurowanie routera za pomocą rozszerzonych nazwanych list ACL.
- Konfigurowanie routera rozszerzonymi listami ACL, aby spełnić określone wymagania komunikacyjne.
- Konfigurowanie ACL w celu kontrolowania dostępu do linii terminala urządzenia sieciowego.
- Konfigurowanie odpowiednich interfejsów routera listami ACL w odpowiednim kierunku.
- Sprawdzanie działania skonfigurowanych list ACL.

Wprowadzenie / Scenariusz

W tym ćwiczeniu skonfigurujesz rozszerzone, standardowe nazwane i rozszerzone nazwane listy ACL w celu spełnienia określonych wymagań komunikacyjnych.

Instrukcje

Krok 1: Sprawdź łączność w sieci nowej firmy

Najpierw należy przetestować łączność w sieci, tak jak jest przed skonfigurowaniem list ACL. Testy ping do wszystkich hostów do wszystkich innych hostów powinny zakończyć się sukcesem.

Krok 2: Skonfiguruj standardowe i rozszerzone listy ACL według wymagań.

Skonfiguruj listy ACL, aby spełniały następujące wymagania:

Ważne wytyczne:

- **Nie** używaj jawnie wpisów deny any na końcu listy ACL.
- Używaj skrótów (**host** i **any**), gdy tylko jest to możliwe.
- Zapisz swoje instrukcje ACL, aby spełnić wymagania w kolejności, w jakiej zostały podane tutaj.
- Umieść listy ACL w najbardziej efektywnej lokalizacji i kierunku.

Wymagania dotyczące listy ACL 1

- Utwórz ACL **101**.
- Zablokuj dostęp FTP do Enterprise Web Server z Internetu.
- Żaden ruch ICMP z Internetu nie powinien być dozwolony do wszystkich hostów w sieci HQ LAN 1
- Zezwalaj na cały pozostały ruch.

Wymagania dotyczące listy ACL 2

- Użyj listy ACL **111**
- Żadne hosty w HQ LAN 1 nie powinny mieć dostępu do serwera Branch.
- Cały pozostały ruch powinien być dozwolony.

Wymagania dotyczące listy ACL 3

- Wykonaj konfigurację nazywaną standardową listą ACL. Użyj nazwy **vty_block**. Nazwa listy ACL musi być dokładnie zgodna z tą nazwą.
- Tylko adresy z sieci HQ LAN 2 powinny mieć dostęp do linii VTY routera HQ.

Wymagania dotyczące listy ACL 4

- Utwórz nazwaną rozszerzoną ACL o nazwie **branch_to_hq**. Nazwa listy ACL musi być dokładnie zgodna z tą nazwą.
- Żadne hosty w żadnej z sieci LAN Branch nie powinny mieć dostępu do sieci HQ LAN 1. Dla każdej sieci LAN Branch należy użyć jednej instrukcji listy dostępu.
- Cały pozostały ruch powinien być dopuszczony.

Krok 3: Sprawdź działanie listy ACL.

- a. Wykonaj następujące testy łączności między urządzeniami w topologii. Zwróć uwagę, czy się powiodły, czy nie.

Uwaga: Użyj polecenia **show ip access-lists**, aby sprawdzić działanie listy ACL. Użyj polecenia **clear access list counters**, aby zresetować liczniki dopasowania.

Wyślij żądanie ping z komputera Branch PC do Enterprise Web Server. Czy polecenie zostało wykonane pomyślnie? Wyjaśnij.

Która instrukcja ACL zezwala lub odrzuca ping między tymi dwoma urządzeniami? Podaj nazwę lub numer listy dostępu, router, na którym została zastosowana, oraz konkretną linię, do której pasował ruch.

Spróbuj wykonać ping z komputera PC-1 w sieci HQ LAN 1 do Branch Server. Czy polecenie zostało wykonane pomyślnie? Wyjaśnij.

Która instrukcja ACL zezwala lub odrzuca ping między tymi dwoma urządzeniami?

Otwórz przeglądarkę sieci Web na External Server i spróbuj wywołać stronę internetową przechowywaną na Enterprise Web Server. Czy kończy się sukcesem? Wyjaśnij.

Która instrukcja ACL zezwala lub odrzuca ping między tymi dwoma urządzeniami?

- b. Przetestuj połączenia z serwerem wewnętrznym z Internetu.

W wierszu poleceń na Internet User PC spróbuj nawiązać połączenie FTP z Branch Server. Czy połączenie FTP powiodło się?

Która lista dostępu powinna zostać zmodyfikowana, aby uniemożliwić użytkownikom z Internetu nawiązywanie połączeń FTP z Branch Server?

Jaki(e) wpis(y) należy dodać do listy kontroli dostępu, aby odmówić tego ruchu?