Laboratorium - Konfiguracja i weryfikacja rozszerzonych list ACL IPv4

Topologia

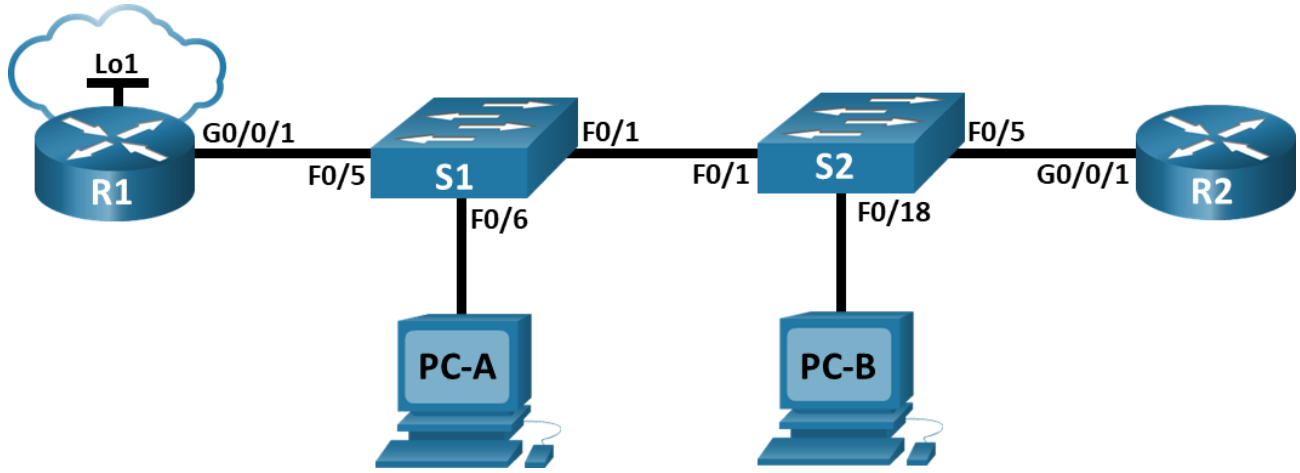

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0/1	nd.	nd.	nd.
	G0/0/1.20	10.20.0.1	255.255.255.0	
	G0/0/1.30	10.30.0.1	255.255.255.0	
	G0/0/1.40	10.40.0.1	255.255.255.0	
	G0/0/1.1000	nd.	nd.	
	Loopback 1	172.16.1.1	255.255.255.0	
R2	G0/0/1	10.20.0.4	255.255.255.0	nd.
S1	VLAN 20	10.20.0.2	255.255.255.0	10.20.0.1
S2	VLAN 20	10.20.0.3	255.255.255.0	10.20.0.1
PC-A	Karta sieciowa	10.30.0.10	255.255.255.0	10.30.0.1
PC-B	Karta sieciowa	10.40.0.10	255.255.255.0	10.40.0.1

Tabela VLAN

VLAN	Nazwa	Przypisany interfejs
20	Management	S2: F0/5
30	Operations	S1: F0/6
40	Sales	S2: F0/18
999	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2
1000	Native	nd.

Cele

Część 1: Utworzenie sieci oraz konfigurowanie podstawowych ustawień urządzenia

Część 2: Konfigurowanie i weryfikacja rozszerzonych list kontroli dostępu

Wprowadzenie / Scenariusz

Otrzymałeś zadanie skonfigurowania list kontroli dostępu w sieci małej firmy. ACL są jednym z najprostszych i najbardziej bezpośrednich sposobów kontrolowania ruchu w warstwie 3. R1 będzie obsługiwać połączenie internetowe (symulowane przez interfejs Loopback 1) i udostępnianie trasie domyślnej routerowi R2. Po zakończeniu konfiguracji początkowej firma ma określone wymagania bezpieczeństwa ruchu, które są odpowiedzialne za wdrożenie.

Uwaga: Routery używane w praktycznych laboratoriach CCNA to Cisco 4221 z Cisco IOS XE wydanie 16.9.4 (obraz universalk9). Przełączniki używane w laboratoriach to Cisco Catalyst 2960 z Cisco IOS wydanie 15.2 (2) (obraz lanbasek9). Można używać Innych routerów lub przełączników oraz wersji Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS, dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Przejrzyj tabelę podsumowującą interfejsy routera w celu określenia poprawnych identyfikatorów interfejsów.

Uwaga: Upewnij się, że konfiguracje startowe routerów i przełączników zostały wykasowane. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane zasoby

- 2 routery (Cisco 4221 z uniwersalnym obrazem Cisco IOS XE Release 16.9.4 lub porównywalny)
- 2 przełączniki (Cisco 2960 z Cisco IOS Release 15.2(2) obraz lanbasek9 lub porównywalny)
- 2 komputery PC (Windows z emulatorem terminala takim jak Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco IOS za pośrednictwem portów konsoli
- Kable Ethernet zgodnie z przedstawioną topologią

Instrukcje

Część 1: Zbuduj sieć i skonfiguruj podstawowe ustawienia urządzeń.

Krok 1: Zbuduj sieć zgodnie z topologią.

Połącz wymagane urządzenia oraz kable tak, jak pokazano na schemacie topologii.

Krok 2: Skonfiguruj podstawowe ustawienia dla każdego routera.

a. Przypisz routerowi nazwę.

b. Wyłącz wyszukiwanie DNS, aby router nie próbował tłumaczyć niepoprawnie wprowadzonych poleceń, tak jakby były one nazwami hostów.

c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.

e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.

f. Zaszyfruj hasła zapisane jawnym tekstem.

g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

h. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Krok 3: Wykonaj podstawową konfigurację przełączników.

a. Przypisz nazwę urządzenia do przełącznika.

b. Wyłącz wyszukiwanie DNS, aby router nie próbował tłumaczyć niepoprawnie wprowadzonych poleceń, tak jakby były one nazwami hostów.

c. Przypisz **class** jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.

d. Przypisz **cisco** jako hasło konsoli i włącz logowanie.

e. Przypisz **cisco** jako hasło do VTY oraz włącz logowanie.

f. Zaszyfruj hasła zapisane jawnym tekstem.

g. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

h. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

Część 2: Konfiguracja sieci VLAN na przełącznikach.

Krok 1: Utwórz sieci VLAN na przełączniku.

a. Utwórz i nazwij wymagane sieci VLAN na każdym przełączniku z powyższej tabeli.

b. Skonfiguruj interfejs zarządzania i bramę domyślną na każdym przełączniku, korzystając z informacji o adresie IP z tabeli adresowania.

c. Przypisz wszystkie nieużywane porty przełącznika do sieci VLAN ParkingLot, skonfiguruj je w trybie dostępu statycznego i dezaktywuj je administracyjnie.

Uwaga: Polecenie interface range jest pomocne, aby wykonać to zadanie z minimalną koniecznych poleceń.

Krok 2: Przypisz sieci VLAN do odpowiednich interfejsów przełącznika.

a. Przypisz używane porty do odpowiedniej sieci VLAN (określonej w powyższej tabeli VLAN) i skonfiguruj je w trybie dostępu statycznego.

b. Wydaj polecenie **show vlan brief** i sprawdź, czy sieci VLAN są przypisane do odpowiednich interfejsów.

Część 3: Konfiguracja połączeń trunk

Krok 1: Ręcznie skonfiguruj interfejs trunk F0/1.

a. Zmień tryb przełączania na interfejsie F0/1, aby wymusić trunking. Pamiętaj, aby to zrobić na obu przełącznikach.

b. W ramach konfiguracji łącza trunk ustaw natywną sieć jako VLAN 1000 na obu przełącznikach. Komunikaty o błędach mogą być tymczasowo wyświetlane, gdy oba interfejsy są skonfigurowane z różnymi natywnymi sieciami VLAN.

c. W ramach innej części konfiguracji łącza trunk określ, że tylko sieci VLAN 10, 20, 30 i 1000 mogą korzystać z łącza.

d. Wydaj polecenie **show interfaces trunk**, aby zweryfikować porty trunk, natywną sieć VLAN i dozwolone sieci VLAN na łączu trunk.

Krok 2: Ręcznie skonfiguruj interfejs trunk F0/5 na S1.

a. Skonfiguruj F0/5 na S1 z tymi samymi parametrami trunk co F0/1. To jest trunk do routera.

b. Zapisz konfigurację bieżącą do pliku konfiguracji startowej.

c. Użyj polecenia **show interfaces trunk**, aby sprawdzić ustawienia trunk.

Część 4: Konfiguracja routingu

Krok 1: Skonfiguruj routing między sieciami VLAN na R1.

a. Aktywuj interfejs G0/0/1 na routerze.

b. Skonfiguruj podinterfejsy dla każdej sieci VLAN zgodnie z tabelą adresowania IP. Wszystkie podinterfejsy używać będą enkapsulacji 802.1Q. Upewnij się, że podinterfejs dla natywnej sieci VLAN nie ma przypisanego adresu IP. Dołącz opis dla każdego podinterfejsu.

c. Skonfiguruj interfejs Loopback 1 na R1 z adresowaniem z powyższej tabeli.

d. Użyj polecenia **show ip interface brief**, aby sprawdzić, czy podinterfejsy działają.

Krok 2: Skonfiguruj interfejs g0/0/1 R2 przy użyciu adresu z tabeli i domyślnej trasy z następnym przeskokiem 10.20.0.1

Część 5: Konfiguracja zdalnego dostępu

Krok 1: Skonfiguruj wszystkie urządzenia sieciowe do podstawowej obsługi SSH.

a. Utwórz lokalnego użytkownika z nazwą użytkownika SSHadmin i zaszyfrowanym hasłem $cisco123!

b. Użyj **ccna-lab.com** jako nazwy domeny.

c. Wygeneruj zestaw kluczy kryptograficznych o module 1024-bitowym.

d. Skonfiguruj pierwsze pięć wierszy VTY na każdym urządzeniu, aby obsługiwały tylko połączenia SSH i uwierzytelniały się w lokalnej bazie danych użytkowników.

Krok 2: Włącz bezpieczne, uwierzytelnione usługi internetowe na R1.

a. Włącz serwer HTTPS na R1.

```
R1(config)# ip http secure-server
```

b. Skonfiguruj R1, aby uwierzytelniać użytkowników próbujących połączyć się z serwerem WWW.

```
R1(config)# ip http authentication local
```

Część 6: Weryfikacja łączności

Krok 1: Skonfiguruj hosty PC.

Skonfiguruj adresy IP na komputerach zgodnie z tabelą adresacji.

Krok 2: Wykonaj następujące testy. Wszystkie powinny się powieść.

Uwaga: Aby ping zakończył się pomyślnie, może być konieczne wyłączenie zapory ogniowej komputera.

Od	Protokół	Cel
PC-A	Ping	10.40.0.10
PC-A	Ping	10.20.0.1
PC-B	Ping	10.30.0.10
PC-B	Ping	10.20.0.1
PC-B	Ping	172.16.1.1
PC-B	HTTPS	10.20.0.1
PC-B	HTTPS	172.16.1.1
PC-B	SSH	10.20.0.1
PC-B	SSH	172.16.1.1

Część 7: Konfigurowanie i weryfikacja rozszerzonych list kontroli dostępu.

Po zweryfikowaniu podstawowej łączności firma wymaga wdrożenia następujących zasad zabezpieczeń:

Zasada 1: Sieć Sales nie może łączyć się przez SSH z siecią Management (ale inne protokoły SSH są dozwolone).

Zasada 2: Sieć Sales nie może uzyskać dostępu do adresów IP w sieci Management przy użyciu żadnego protokołu internetowego (HTTP/HTTPS). Sieć Sales nie ma również dostępu do interfejsów R1 za pomocą dowolnego protokołu www. Dozwolony jest cały inny ruch www (uwaga — Sales może uzyskać dostęp do interfejsu Loopback 1 na R1).

Zasada 3: Sieć Sales nie może wysyłać żądań echo ICMP do sieci Operations lub Management. Dozwolone są żądania echa ICMP do innych miejsc docelowych.

Zasada 4: Sieć Operations nie może wysyłać żądań echo ICMP do sieci Sales. Dozwolone są żądania echo ICMP do innych miejsc docelowych.

Krok 1: Przeanalizuj sieć i wymagania polityki bezpieczeństwa, aby zaplanować implementację listy ACL.

Krok 2: Opracuj i zastosuj rozszerzone listy dostępu, które będą zgodne z oświadczeniami dotyczącymi zasad bezpieczeństwa.

Krok 3: Sprawdź, czy zasady zabezpieczeń są wymuszane przez wdrożone listy dostępu.

Wykonaj następujące testy. Oczekiwane wyniki są przedstawione w tabeli:

Od	Protokół	Cel	Wynik
PC-A	Ping	10.40.0.10	Nie przeszedł
PC-A	Ping	10.20.0.1	Ukończono pomyślnie
PC-B	Ping	10.30.0.10	Nie przeszedł
PC-B	Ping	10.20.0.1	Nie przeszedł
PC-B	Ping	172.16.1.1	Ukończono pomyślnie
PC-B	HTTPS	10.20.0.1	Nie przeszedł
PC-B	HTTPS	172.16.1.1	Ukończono pomyślnie
PC-B	SSH	10.20.0.4	Nie przeszedł
PC-B	SSH	172.16.1.1	Ukończono pomyślnie