Ćwiczenie – Konfiguracja i weryfikacja list kontroli dostępu w IPv6

Topologia

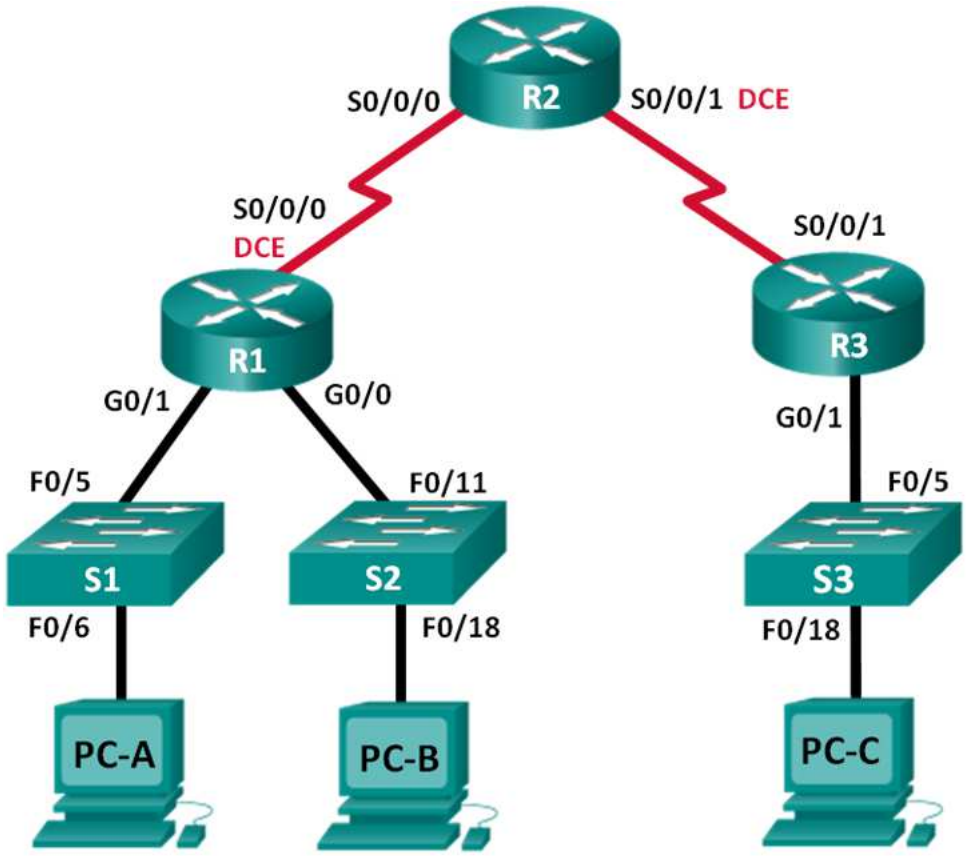

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Brama domyślna
R1	G0/0	2001:DB8:ACAD:B::1/64	Nie dotyczy
	G0/1	2001:DB8:ACAD:A::1/64	Nie dotyczy
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	Nie dotyczy
R2	S0/0/0	2001:DB8:AAAA:1::2/64	Nie dotyczy
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	Nie dotyczy
R3	G0/1	2001:DB8:CAFE:C::1/64	Nie dotyczy
	S0/0/1	2001:DB8:AAAA:2::1/64	Nie dotyczy
S1	VLAN1	2001:DB8:ACAD:A::A/64	Nie dotyczy
S2	VLAN1	2001:DB8:ACAD:B::A/64	Nie dotyczy
S3	VLAN1	2001:DB8:CAFE:C::A/64	Nie dotyczy
PC-A	Karta sieciowa	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	Karta sieciowa	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	Karta sieciowa	2001:DB8:CAFE:C::3/64	FE80::1

Cele

Cześć 1: Zestawienie topologii sieci i inicjacja urządzenia

Cześć 2: Konfiguracja urządzeń i weryfikacja połączeń

Cześć 3: Konfigurowanie i weryfikowanie list kontroli dostępu IPv6

Cześć 4: Edycja ACL IPv6

Scenariusz

Możesz filtrować ruch IPv6 poprzez tworzenie list kontroli dostępu (ACL) i zakładanie ich na interfejsach podobnie do sposobu, w jaki tworzyłeś nazywane listy ACL w IPv4. ACL dla IPv6 są rozszerzone i nazwane. Standardowe i numerowane listy ACL nie są już stosowane z IPv6. Aby zastosować ACL IPv6 do interfejsu VTY, należy użyć nowego polecenia **ipv6 traffic-filter**. Komenda **ipv6 access-class** jest nadal używana do założenia ACL IPv6 na interfejsy.

W tym laboratorium, zastosujesz reguły filtrowania IPv6, a następnie zweryfikujesz się, że występują ograniczenia dostępu, tak jak oczekiwano. Będziesz również edytował ACL IPv6 i zerował liczniki dopasowania.

Uwaga: Routery użyte do przygotowania instrukcji to Cisco 1941 IRS (Integrated Serwices Routers) z zainstalowanym systemem IOS wydanie 15.2(4)M3 (obraz universalk9). Przełączniki użyte do przygotowania instrukcji to Cisco Catalyst 2960s z obrazem systemu operacyjnego Cisco IOS wydanie 15.0(2) (lanbasek9). Do realizacji ćwiczenia mogą być użyte zarówno inne routery oraz przełączniki lub urządzenia z inną wersją systemu IOS. W zależności od użytego modelu urządzenia oraz wersji IOS dostępne komendy oraz komunikaty na ekranie mogą się różnić od tych zamieszczonych w instrukcji. Dostępne interfejsy na poszczególnych typach routerów zostały zebrane w tabeli na końcu niniejszej instrukcji laboratoryjnej.

Uwaga: Upewnij się, że przełączniki nie są skonfigurowane oraz nie przechowują pliku z konfiguracją startową. Jeśli nie jesteś tego pewien skontaktuj się z instruktorem.

Wymagane zasoby

- 3 routery (Cisco 1941 z Cisco IOS wydanie 15.2(4)M3, obraz „universal” lub kompatybilny)

- 3 przełączniki (Cisco 2960 z Cisco IOS wydanie 15.0(2) obraz „lanbasek9” lub kompatybilny)
- 3 komputery PC (Windows 7, Vista lub XP z zainstalowanym emulatorem terminala jak np.: Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco przez port konsolowy.
- Kable ethernetowe i serialowe jak pokazano na rysunku topologii sieci

Część 1: Zestawienie topologii sieci i inicjacja urządzeń

W części 1, należy zestawić topologie sieci i wyczyścić konfiguracje urządzeń jeśli to konieczne.

Krok 1: Połącz okablowanie zgodnie z topologią.

Krok 2: Zainicjuj i przeładuj routery i przełączniki.

Część 2: Konfiguracja urządzeń i weryfikacja połączeń

W części 2 skonfiguruj podstawowe ustawienia na routerach, przełącznikach i komputerach. Skorzystaj ze schematu sieci oraz tablicy adresacji w zakresie nazw urządzeń i adresacji.

Krok 1: Skonfiguruj adresy IPv6 na wszystkich komputerach PC.

Skonfiguruj globalny adres unicast IPv6 zgodnie z tabelą adresacji. Użyj adresu link-local **FE80::1** dla wszystkich komputerów PC jako bramy domyślnej .

Krok 2: Skonfiguruj przełączniki.

a. Wyłącz DNS lookup.
b. Przypisz nazwy urządzeń.
c. Przypisz domain-name **ccna-lab.com**.
d. Włącz szyfrowanie haseł zapisywanych tekstem jawnym.
e. Utwórz baner MOTD ostrzegający użytkowników, że nieautoryzowany dostęp jest zabroniony.
f. Utwórz lokalną bazę użytkowników z nazwą użytkownika **admin** i hasłem **classadm**.
g. Przypisz **class** jako hasło do trybu uprzywilejowanego EXEC jak hasło szyfrowane.
h. Przypisz **cisco** jako haslo do trybu konsolowego i włącz logowanie.
i. Włącz logowanie na liniach VTY z użyciem lokalnej bazy użytkowników.
j. Wygeneruj klucz kryptograficzny RSA do ssh modulo 1024 bity.
k. Zmień transport na liniach VTY na SSH i Telnet.
l. Przypisz adres IPv6 do VLAN 1 zgodnie z tabelą adresacji.
m. Administracyjnie wyłącz wszystkie nieaktywne interfejsy.

Krok 3: Skonfiguruj podstawowe ustawienia wszystkich routerów.

a. Wyłącz DNS lookup.
b. Przypisz nazwy urządzeń.
c. Przypisz domain-name **ccna-lab.com**.
d. Włącz szyfrowanie haseł zapisywanych tekstem jawnym.
e. Utwórz baner MOTD ostrzegający użytkowników, że nieautoryzowany dostęp jest zabroniony.
f. Utwórz lokalną bazę użytkowników z nazwą użytkownika **admin** i hasłem **classadm**.
g. Przypisz **class** jako hasło do trybu uprzywilejowanego EXEC jak hasło szyfrowane.

h. Przypisz **cisco** jako hasło do trybu konsolowego i włącz logowanie.

i. Włącz logowanie na liniach VTY z użyciem lokalnej bazy użytkowników.

j. Wygeneruj klucz kryptograficzny RSA do ssh modulo 1024 bity.

k. Zmień transport na liniach VTY na SSH i Telnet.

Krok 4: Skonfiguruj ustawienia IPv6 na R1.

a. Skonfiguruj adres unicast IPv6 na interfejsie G0/0, G0/1, i S0/0/0.

b. Skonfiguruj adres link-local IPv6 na interfejsie G0/0, G0/1 i S0/0/0. Użyj adresu link-local **FE80::1** na wszystkich trzech interfejsach.

c. Ustaw częstotliwość zegara interfejsu S0/0/0 na 128000.

d. Włącz interfejsy.

e. Włącz IPv6 unicast routing.

f. Skonfiguruj routing domyślny dla IPv6 na interfejs S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Krok 5: Skonfiguruj ustawienia IPv6 na R2.

a. Skonfiguruj adres unicast IPv6 na interfejsie S0/0/0 i S0/0/1.

b. Skonfiguruj adres link-local IPv6 na interfejsie S0/0/0 i S0/0/1. Użyj adresu link-local **FE80::2** na wszystkich trzech interfejsach.

c. Ustaw częstotliwość zegara interfejsu S0/0/1 na 128000.

d. Włącz interfejsy.

e. Włącz IPv6 unicast routing.

f. Skonfiguruj trasy statyczne IPv6 dla ruchu do podsieci na R1 i R3.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Krok 6: Skonfiguruj ustawienia IPv6 na R3.

a. Skonfiguruj adres unicast IPv6 na interfejsie G0/1 i S0/0/1.

b. Skonfiguruj adres link-local IPv6 na interfejsie G0/1 i S0/0/1. Użyj adresu link-local **FE80::1** na wszystkich trzech interfejsach.

c. Włącz interfejsy.

d. Włącz IPv6 unicast routing.

e. Skonfiguruj routing domyślny dla IPv6 na interfejs S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

Krok 7: Sprawdź łączność.

a. Ping z każdego PC do wszystkich innych komputerów PC w sieci powinien się powieść.

b. Telnet do R1 z każdego PC w sieci.

c. SSH do R1 z każdego PC w sieci.

d. Telnet do S1 z każdego PC w sieci.

e. SSH do S1 z każdego PC w sieci.

f. Rozwiąż problemy z łącznością w sieci na tym etapie, ponieważ listy ACL tworzone w części 3 niniejszego laboratorium będą ograniczać dostęp do niektórych obszarów w sieci.

Część 3: Konfiguracja i weryfikacja IPv6 ACLs

Krok 1: Skonfiguruj i zweryfikuj ograniczenia VTY na R1.

a. Załóż ACL, aby tylko hosty z sieci 2001:db8:acad:a::/64 mogły się telnetować do R1. Natomiast wszystkie hosty mają mieć dostęp do R1 tylko poprzez ssh.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any
R1(config-ipv6-acl)# permit tcp any any eq 22
```

b. Załóż RESTRICT-VTY ACL na linie VTY R1.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

c. Wyświetl nową ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
    permit tcp any any eq 22 sequence 20
```

d. Zweryfikuj, że RESTRICT-VTY ACL umożliwia ruch telnet tylko z sieci 2001:db8:acad:a::/64.

Jak RESTRICT-VTY ACL umożliwia tylko hostom z sieci 2001:db8:acad:a::/64 na dostęp za pomocą Telnet do R1?

_____

_____

_____

_____

Co powoduje drugi wpis zezwalający w RESTRICT-VTY ACL?

_____

Krok 2: Zabroń dostępu poprzez Telnet do sieci 2001:db8:acad:a::/64.

a. Załóż ACL o nazwie RESTRICTED-LAN, która będzie blokować dostęp za pomocą Telnet do sieci 2001:db8:acad:a::/64.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

b. Załóż ACL RESTRICTED-LAN na interfejsie G0/1 dla ruchu wychodzącego.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

c. Telnet do S1 z PC-B i PC-C w celu weryfikacji, że protokół Telnet został zablokowany. Użyj SSH do połączenia się na S1 z PC-B w celu weryfikacji, że jest on wciąż osiągalny za pomocą SSH. Rozwiąż problemy jeśli to konieczne.

d. Użyj komendy **show ipv6 access-list** do wyświetlenia listy RESTRICTED-LAN.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
```

```
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
    permit ipv6 any any (45 matches) sequence 30
```

Zauważ, że każdy komunikat identyfikuje liczbę dopasowań do zastosowanej reguły, które wystąpiły od momentu założenia listy ACL na interfejsie.

e. Użyj komendy **clear ipv6 access-list** do zresetowania liczników dopasowań listy ACL RESRICTED-LAN.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

f. Wyświetl ponownie ACL za pomocą komendy **show access-lists** w celu potwierdzenia, że liczniki zostały skasowane.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any sequence 30
```

Część 4: Edycja list ACL dla protokołu IPv6

W części 4, należy dokonać edycji listy RESTRICTED-LAN stworzonej w części 3. Dobrą praktyką postępowania jest usunięcie listy z interfejsu przed jej edycją. Po edycji można ją z powrotem zastosować na interfejsie.

Uwaga: Wielu administratorów tworzy kopię listy i edytuje kopię. Kiedy edycja jest skończona administrator usuwa starą listę i zakłada nową na interfejs. Taki sposób postępowania powoduje, ze lista jest na swoim miejscu i filtruje ruch do momentu, kiedy jest gotowa nowa lista ACL. Przy takim sposobie postępowaniu sieć pozostaje bez ochrony na bardzo krótki czas.

Krok 1: Usuń ACL z interfejsu.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Krok 2: Użyj komendy show access-lists do zobaczenia ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (36 matches) sequence 30
```

Krok 3: Wprowadź nową regułę do ACL używając sekwencyjnego numerowania.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host
2001:db8:acad:a::a eq 23 sequence 15
```

Co robi nowy wpis zezwalający?

_____

Krok 4: Wprowadź nowy wpis na końcu ACL.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Uwaga: Ten nowy wpis dopuszczający ruch jest użyty tylko w celu pokazania jak dodać wpis na końcu listy ACL. Ta reguła nie będzie nigdy wykorzystana (brak przypasowania) ponieważ wpis wyżej pasuje do wszystkiego.

Krok 5: Użyj komendy show access-lists command do przeglądnięcia zmian w ACL.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
    permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (124 matches) sequence 30
    permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Uwaga: Komenda **do** może być użyta do wykonania dowolnej komendy w trybie uprzywilejowanym, podczas, gdy jesteśmy w trybie konfiguracji ogólnej.

Krok 6: Usuń wpis w ACL.

Użyj komendy **no** do skasowania wpisu „permit”, który chwilę wcześniej dodałeś.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Krok 7: Użyj komendy show access-list RESTRICTED-LAN w celu wyświetlenia ACL.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
    permit ipv6 any any (214 matches) sequence 30
```

Krok 8: Załóż ponownie listę RESTRICTED-LAN na interfejsie G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Krok 9: Przetestuj zmiany w ACL.

Połącz się z PC-B do S1 przez Telnet. Rozwiąż problemy jeśli to konieczne.

Do przemyślenia

1. Co powoduje zwiększanie się licznika przy wpisie **permit ipv6 any any** w liście ACL RESTRICTED-LAN?

   _____

2. Jakiej komendy użyłbyś do skasowania liczników w liście ACL na linii VTY?

   _____

Tabela – podsumowanie interfejsów routera

Podsumowanie interfejsów routera				
Model routera	**Interfejs ethernetowy #1**	**Interfejs ethernetowy #2**	**Interfejs szeregowy #1**	**Interfejs szeregowy #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Uwaga: Aby dowiedzieć się, jaka jest konfiguracja sprzętowa routera, obejrzyj interfejsy, aby zidentyfikować typ routera oraz aby określić liczbę interfejsów routera. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Tabela ta zawiera identyfikatory możliwych kombinacji interfejsów szeregowych i Ethernet w urządzeniu. Tabela nie zawiera żadnych innych rodzajów interfejsów, mimo iż dany router może jakieś zawierać Przykładem może być interfejs ISDN BRI. Łańcuch w nawiasie jest skrótem, który może być stosowany w systemie operacyjnym Cisco IOS przy odwoływaniu się do interfejsu..