

Ćwiczenie – Konfiguracja i weryfikacja standardowych list kontroli dostępu ACL

Topologia

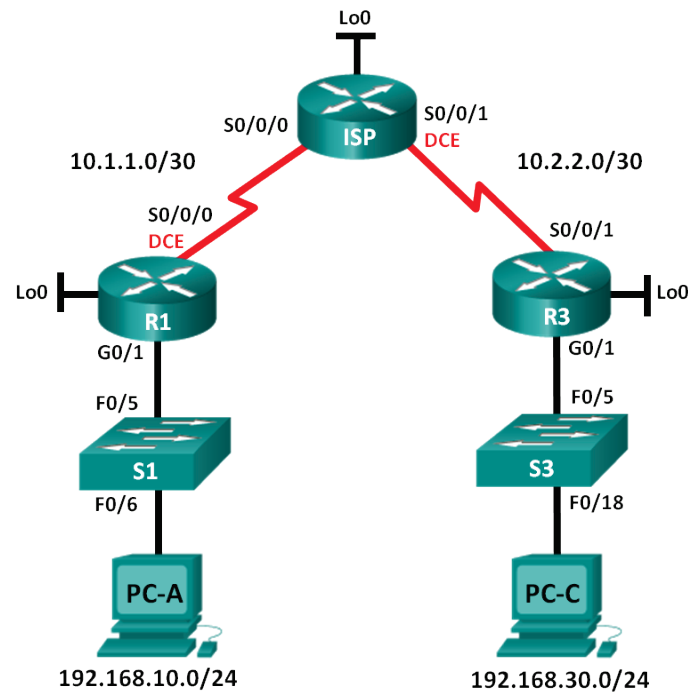


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Cele nauczania

Część 1: Budowa sieci oraz podstawowa konfiguracja urządzeń

- Budowa sieci zgodnie z topologią pokazaną na rysunku.
- Inicjalizacja i ponowne uruchomienie routerów i przełączników.

Część 2: Konfiguracja urządzeń i weryfikacja łączności

- Konfiguracja statycznych adresów IP dla komputerów PC.
- Podstawowa konfiguracja routerów.
- Podstawowa konfiguracja przełączników.
- Konfiguracja routingu OSPF na routerach R1, ISP oraz R3.
- Weryfikacja łączności pomiędzy urządzeniami.

Część 3: Konfiguracja i weryfikacja standardowych numerowanych oraz nazywanych list ACL

- Konfiguracja i weryfikacja standardowych numerowanych list ACL.
- Konfiguracja i weryfikacja standardowych nazywanych list ACL.

Część 4: Modyfikacja standardowych list kontroli dostępu ACL

- Modyfikacja i weryfikacja standardowych nazywanych list ACL.
- Testowanie list ACL.

Wprowadzenie

Bezpieczeństwo sieci jest ważnym aspektem podczas projektowania oraz zarządzania siecią IP. Umiejętność konfigurowania zasad filtrowania pakietów jest pożądaną umiejętnością.

Podczas tego ćwiczenia nauczysz się ustawiać zasady filtrowania dla dwóch sieci biurowych reprezentowanych przez routery R1 oraz R3. Zarząd firmy ustalił określone zasady dostępu między sieciami LAN obsługiwanyymi pomiędzy R1 i R3. Na routerze ISP nie będą skonfigurowane żadne listy ACL. Nie będziesz miał możliwości konfiguracji routera ISP, ponieważ możesz tylko kontrolować własny sprzęt.

Uwaga: Upewnij się, że routery i przełącznik zostały wyczyszczone i nie posiadają konfiguracji startowej. Jeśli nie jesteś pewny/a wezwij instruktora.

Wymagane zasoby

- 3 routery (Cisco 1941 z systemem Cisco IOS Release 15.2(4)M3 universal image lub kompatybilnym)
- 2 przełączniki (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image lub kompatybilnym)
- 2 PC (Windows 7, Vista, lub XP z programem Putty lub innym programem terminalowym)
- Kabel konsolowy do konfiguracji urządzeń Cisco przez port konsolowy
- Kable sieciowe i serialowe pokazane na rysunku topologii

Część 1 Budowa sieci oraz podstawowa konfiguracja urządzeń

W części pierwsze zbudujesz sieć zgodnie z topologią oraz jeśli będzie to potrzebne usuniesz konfigurację urządzeń.

Krok 1: Budowa sieci zgodnie z topologią pokazaną na rysunku.

Krok 2: Inicjalizacja i ponowne uruchomienie routerów i przełączników.

Część 2 Konfiguracja urządzeń i weryfikacja łączności

W części drugiej dokonasz wstępnej konfiguracji routerów, przełączników oraz komputerów zgodnie z tabelą adresacji.

Krok 1: Konfiguracja statycznych adresów IP do komputerów PC.

Krok 2: Podstawowa konfiguracja routerów.

- a. Wyłącz niepożądane zapytania DNS (DNS lookup).
- b. Skonfiguruj nazwy urządzeń zgodnie z topologią.
- c. Utwórz interfejs loopback na każdym routerze zgodnie z tabelą adresacji.
- d. Ustaw adresy IP zgodnie z topologią oraz tabelą adresacji.
- e. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC.
- f. Ustaw taktowanie zegara interfejsu szeregowego DCE na wartość **128000**.
- g. Ustaw **cisco** jako hasło do połączeń konsolowych.
- h. Ustaw **cisco** jako hasło do połączeń wirtualnych w celu uruchomienia dostępu przez Telnet.

Krok 3: (Opcjonalnie) Podstawowa konfiguracja przełączników.

- a. Wyłącz niepożądane zapytania DNS (DNS lookup).
- b. Skonfiguruj nazwy urządzeń zgodnie z topologią.
- c. Skonfiguruj adres IP interfejsu zarządzalnego zgodnie z tabelą adresacji.
- d. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC.
- e. Ustaw bramę domyślną.
- f. Ustaw **cisco** jako hasło do połączeń konsolowych.
- g. Ustaw **cisco** jako hasło do połączeń wirtualnych w celu uruchomienia dostępu przez Telnet.

Krok 4: Konfiguracja routingu OSPF na routerach R1, ISP oraz R3.

- a. Na routerach R1, ISP oraz R3 ustaw ID procesu OSPF równe 1. Dla przykładu poniżej podano konfigurację dla routerów R1 oraz ISP.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.20.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0

ISP(config)# router ospf 1
ISP(config-router)# network 209.165.200.224 0.0.0.31 area 0
ISP(config-router)# network 10.1.1.0 0.0.0.3 area 0
ISP(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

- h. Po skonfigurowaniu routingu OSPF upewnij się, że każdy z routerów w swojej tablicy routingu posiada wpisy do wszystkich sieci. Jeśli tak nie jest popraw konfigurację.

Krok 5: Weryfikacja łączności pomiędzy urządzeniami.

UWAGA: Bardzo ważne jest, aby sieć była poprawnie skonfigurowana przed zastosowaniem list dostępu. Musisz być pewny, że sieć pracuje prawidłowo przed rozpoczęciem filtrowania pakietów.

- a. Z komputera PC-A wykonaj ping do komputera PC-C oraz interfejsu loopback routera R3. Czy pingi zakończyły się sukcesem? _____
- b. Z routera R1 wykonaj ping do komputera PC-C oraz interfejsu loopback routera R3. Czy pingi zakończyły się sukcesem? _____
- c. Z komputera PC-A wykonaj ping do komputera PC-C oraz interfejsu loopback routera R1. Czy pingi zakończyły się sukcesem? _____
- d. Z routera R3 wykonaj ping do komputera PC-A oraz interfejsu loopback routera R1. Czy pingi zakończyły się sukcesem? _____

Część 3: Konfiguracja i weryfikacja standardowych numerowanych oraz nazywanych list ACL

Krok 1: Konfiguracja i weryfikacja standardowych numerowanych list ACL.

Standardowy filtr ruchu ACL bazuje tylko na adresie IP źródła. Typową najlepszą praktyką dla standardowych list ACL jest ich konfiguracja i uruchomienie tak blisko przeznaczenia jak to możliwe. Dla pierwszej listy dostępu utworzysz standardową, numerowaną listę ACL, która zezwala na ruch z wszystkich urządzeń sieci 192.168.10.0/24 oraz sieci 192.168.20.0/24 do wszystkich urządzeń znajdujących się w sieci 192.168.30.0/24. Polityka bezpieczeństwa wymaga, aby na końcu listy ACL obecny był wpis **deny any**.

Jaka maska blankietowa (wildcard mask) powinna być użyta w celu zezwolenia na ruch od wszystkich hostów z sieci 192.168.10.0/24 do hostów z sieci 192.168.30.0/24?

Bazując na polityce bezpieczeństwa rekomendowanej przez Cisco, na którym routerze ustawisz tę listę ACL? _____

Na którym interfejsie uruchomisz tę listę ACL? Do którego kierunku ruchu będzie się ona odnosić?

- a. Skonfiguruj listę ACL na routerze R3. Użyj cyfry 1 jako numeru listy.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

- b. Użyj listy ACL na odpowiednim interfejsie w odpowiednim kierunku.

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

- c. Zweryfikuj numerowaną listę ACL.

Użycie szeregu komend zaczynających się od **show** może być pomocne w weryfikacji składni i lokalizacji list na routerze.

Jakiej komendy użyjesz, aby zobaczyć listę 1 w całości ze wszystkimi listami ACE?

Jakiej komendy użyjesz, aby sprawdzić gdzie została użyta lista oraz w którym kierunku?

- 1 Na routerze R3 użyj komendy **show access-lists 1**

```
R3# show access-list 1
Standard IP access list 1
```

```
10 permit 192.168.10.0, wildcard bits 0.0.0.255
20 permit 192.168.20.0, wildcard bits 0.0.0.255
30 deny any
```

2 Na routerze R3 użyj komendy **show ip interface g0/1**

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Output omitted
```

- 3 Przetestuj listy ACL, aby sprawdzić czy możliwy jest ruch z sieci 192.168.10.0/24 do sieci 192.168.30.0/24. Na komputerze PC-A użyj polecenia ping na adres IP komputera PC-C. Czy wynik był pozytywny? _____
- 4 Przetestuj listy ACL, aby sprawdzić czy możliwy jest ruch z sieci 192.168.20.0/24 do sieci 192.168.30.0/24. Na routerze R1 użyj polecenia ping w rozszerzonej wersji z interfejsu Loopback0 na adres IP komputera PC-C. Czy wynik był pozytywny? _____

R1# ping

Protocol [ip]:

Target IP address: **192.168.30.3**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **192.168.20.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.20.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

- d. Na routerze R1 użyj ponownie polecenia ping na adres IP komputera PC-C.

R1# ping 192.168.30.3

Czy wynik działania polecenia był pozytywny? Dlaczego tak lub dlaczego nie?

Krok 2: Konfiguracja i weryfikacja standardowych nazywanych list ACL.

Stwórz standardową nazywaną listę ACL, która spełnia następujące wymagania: zezwala na ruch z wszystkich hostów z sieci 192.168.40.0/24 do wszystkich urządzeń znajdujących się w sieci 192.168.10.0/24. Dodatkowo zezwól tylko komputerowi PC-C na dostęp do sieci 192.168.10.0/24. Nazwa utworzonej listy powinna być BRANCH-OFFICE-POLICY.

Bazując na polityce bezpieczeństwa rekomendowanej przez Cisco, na którym routerze ustawisz tę listę ACL? _____

Na którym interfejsie uruchomisz tę listę ACL? Do którego kierunku ruchu będzie się ona odnosić?

- a. Stwórz standardową nazywaną listę ACL BRANCH-OFFICE-POLICY na routerze R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Jak inaczej można zapisać pierwszy wpis w powyższej liście ACL?

- b. Użyj listy ACL na odpowiednim interfejsie w odpowiednim kierunku.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

- c. Zweryfikuj listę ACL.

- 1 Na routerze R1 użyj komendy **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit 192.168.30.3
 20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Czy jest jakaś różnica pomiędzy listą na R1 a listą na R3? Jeśli tak, to jaka?

- 2 Na routerze R1 użyj komendy **show ip interface g0/1**.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 Internet address is 192.168.10.1/24
 Broadcast address is 255.255.255.255
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
```

```
Outgoing access list is BRANCH-OFFICE-POLICY
```

```
Inbound access list is not set
```

```
<Output omitted>
```

- 3 Przetestuj listy ACL. Na komputerze PC-C użyj polecenia ping na adres IP komputera PC-A. Czy wynik był pozytywny? _____
- 4 Przetestuj listy ACL, aby sprawdzić, że tylko komputer PC-C może uzyskać dostęp do sieci 192.168.10.0/24. Wykonaj rozszerzony ping z interfejsu G0/1 routera R3 na adres komputera PC-A. Czy wynik był pozytywny? _____
- 5 Przetestuj listy ACL, aby sprawdzić czy możliwy jest ruch z sieci 192.168.40.0/24 do sieci 192.168.10.0/24. Wykonaj rozszerzony ping z interfejsu loopback 0 routera R3 na adres komputera PC-A. Czy wynik był pozytywny? _____

Część 4: Modyfikacja standardowych list kontroli dostępu ACL

Powszechną praktyką związaną z polityką bezpieczeństwa jest modyfikacja list ACL. W zadaniu 4 zmodyfikujesz jedną z list utworzonych wcześniej w celu dopasowania jej do wymagań bezpieczeństwa.

Nowa lista ma spełniać następujące wymagania: użytkownicy z sieci 209.165.200.224/27 powinni mieć pełny dostęp do sieci 192.168.10.0/24. Na wszystkich routerach listy powinny spełniać spójne zadania. Komenda **deny any** powinna zostać dodana na końcu listy. Musisz zmodyfikować listę BRANCH-OFFICE-POLICY.

Musisz dodać dwie dodatkowe linie do tej listy. Można to zrobić na dwa sposoby:

OPCJA 1: Użyj komendy **no ip access-list standard BRANCH-OFFICE-POLICY** w trybie globalnej konfiguracji. Spowoduje to usunięcie całej listy z routera. W zależności od wersji systemu IOS wystąpi jedna z opcji: filtracja ruchu zostanie wyłączona i wszystkie pakiety będą przechodzić przez router, lub ze względu na nieusunięcie komendy **ip access-group** na interfejsie G0/1 ruch będzie cały czas filtrowany. Bez względu na to po usunięciu listy można ją wpisać od nowa lub skopiować i wkleić z edytora tekstu.

OPCJA 2: Możesz modyfikować listy ACL dodając lub kasując określone linie wewnątrz listy. Jest to użyteczne, szczególnie dla bardzo rozbudowanych list. Przepisywanie całej listy lub wycinanie i wklejanie może łatwo prowadzić do błędów. Modyfikowanie określonych linii wewnątrz listy jest łatwiejszym sposobem.

Uwaga: W tym ćwiczeniu użyj opcji 2.

Krok 1: Modyfikacja i weryfikacja standardowych nazywanych list ACL.

- a. Na routerze R1 w trybie uprzywilejowanym użyj komendy **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit 192.168.30.3 (8 matches)
 20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

- b. Dodaj dwie dodatkowe linie na końcu listy. W trybie globalnej konfiguracji zmodyfikuj listę BRANCH-OFFICE-POLICY.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

- c. Zweryfikuj listę ACL.

- 1 Na routerze R1 użyj komendy **show access-lists**

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit 192.168.30.3 (8 matches)
 20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
 30 permit 209.165.200.224 0.0.0.31
 40 deny any
```

Konfiguracja i weryfikacja standardowych list kontroli dostępu ACL

```
30 permit 209.165.200.224, wildcard bits 0.0.0.31
40 deny any
```

Czy musisz zastosować listę BRANCH-OFFICE-POLICY na interfejsie G0/1 routera R1?

- 2 Na routerze ISP użyj polecenia ping w trybie rozszerzonym. Sprawdź czy możliwy jest ruch z sieci 209.165.200.224/27 do sieci 192.168.10.0/24. Musisz wykonać rozszerzony ping z routera ISP z interfejsu loopback 0 na adres komputera PC-A. Czy wynik był pozytywny? _____

Do przemyślenia

1. Standardowe listy ACL to bardzo potężne narzędzie. W jakim celu używa się rozszerzonych list ACL?

2. Typowo listy nazywane wymagają więcej linii niż listy numerowane. Dlaczego więc często stosuje się listy nazywane?

Tabela interfejsów routera

Interfejsy routera				
Model routera	Interfejs Ethernet #1	Interfejs Ethernet #2	Interfejs Serial #1	Interfejs Serial #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 jak router jest skonfigurowany należy spojrzeć na jego interfejsy i zidentyfikować typ urządzenia oraz liczbę jego interfejsów. Nie ma możliwości wypisania wszystkich kombinacji i konfiguracji dla wszystkich routerów. Powyższa tabela zawiera identyfikatory dla możliwych kombinacji interfejsów szeregowych i ethernetowych w urządzeniu. Tabela nie uwzględnia żadnych innych rodzajów interfejsów, pomimo że podane urządzenia mogą takie posiadać np. interfejs ISDN BRI. Opis w nawiasie (przy nazwie interfejsu) to dopuszczalny w systemie IOS akronim, który można użyć przy wpisywaniu komend.