Ćwiczenie – Konfiguracja i weryfikacja standardowych i rozszerzonych list kontroli dostępu ACL

Topologia

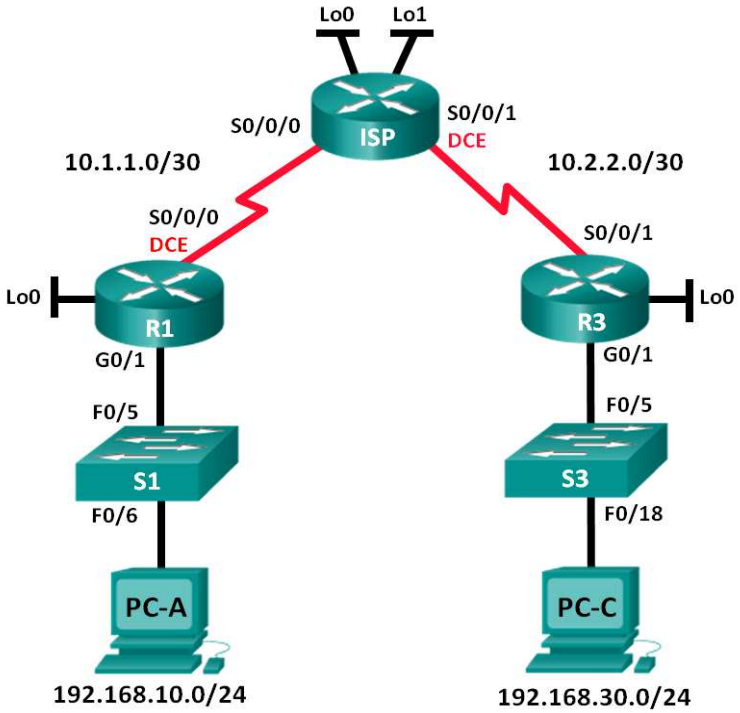

Tabela adresacji

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
	Lo1	209.165.201.1	255.255.255.224	Nie dotyczy
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.
- Konfiguracja i weryfikacja ograniczeń dostępu na liniach VTY.
- Wyzwanie – Konfiguracja list kontroli dostępu na przełączniku S1

Część 4: Modyfikacja standardowych list kontroli dostępu ACL

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

Część 5: Konfiguracja i weryfikacja rozszerzonych numerowanych i nazywanych list kontroli dostępu

- Konfiguracja, instalacja i weryfikacja rozszerzonych numerowanych list kontroli dostępu.
- Konfiguracja, instalacja i weryfikacja rozszerzonych nazywanych list kontroli dostępu.

Część 6: Modyfikacja i weryfikacja rozszerzonych list kontroli dostępu

Wprowadzenie

Bezpieczeństwo sieci jest ważnym aspektem podczas projektowania oraz zarządzania siecią IP. Umiejętność konfigurowania zasad filtrowania pakietów jest pożądaną umiejętnością. Rozszerzone listy kontroli dostępu (ACL) są bardzo skuteczne. Oferują one znacznie większą kontrolę ruchu niż standardowe listy ACL, zarówno pod względem rodzaju filtrowanego ruchu jak również możliwości zdefiniowania źródła oraz miejsca docelowego ruchu sieciowego.

Podczas tego laboratorium twoim zadaniem będzie skonfigurowanie reguł filtrowania ruchu dla dwóch biur, których sieci LAN są przyłączone do routerów R1 i R3. Zarząd firmy ustalił określone zasady dostępu między sieciami LAN obsługiwanymi 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 przełączniku 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.

i. Uruchom dostęp WWW na routerze R1 w celu zasymulowania serwera WWW z lokalnym uwierzytelnianiem dla użytkownika **admin**.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

j. Uruchom dostęp WWW na R3 i ISP. Użyj tych samych parametrów jak powyżej.

k. Na routerze R3 włącz protokół SSH.

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

l.

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 skonfigurowania przed zastosowanie 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? _____

e. Otwórz przeglądarkę na komputerze PC-A i przejdź do adresu http://209.165.200.225 na ISP. Zostaniesz poproszony do podania nazwy użytkownika i hasła. Użyj **admin** jako nazwy użytkownika i **class** jako hasła. Jeśli zostaniesz zachęcony do zaakceptowania certyfikatu, zaakceptuj go. Router załaduje Cisco Configuration Professional (CCP) Express w oddzielnym oknie. Możesz być wezwany do podania nazwy użytkownika i hasła . Użyj **admin** jako nazwy użytkownika i **class** jako hasła.

f. Otwórz przeglądarkę na komputerze PC-C i przejdź do strony http://10.1.1.1 na R1. Zostaniesz poproszony do podania nazwy użytkownika i hasła. Użyj **admin** jako nazwy użytkownika i **class** jako hasła. Jeśli zostaniesz zachęcony do zaakceptowania certyfikatu, zaakceptuj go. Router załaduje Cisco Configuration Professional (CCP) Express w oddzielnym oknie. Możesz być wezwany do podania nazwy użytkownika i hasła. Użyj **admin** jako nazwy użytkownika i **class** jako hasła.

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 uzyj 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. Utwórz 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? _____

Krok 3: Konfiguracja i weryfikacja ograniczeń dostępu na liniach VTY.

W tym kroku utworzysz i zastosujesz nazywane listy ACL w celu ograniczenia zdalnego dostępu do routera poprzez linie vty. Po utworzeniu list ACL przetestujesz je i zweryfikujesz poprzez dostęp do routera przy użyciu protokołu Telnet z różnych adresów IP.

a. Utwórz standardową nazywaną listę ACL **ADMIN-MGT** na routerze R1. Utwórz wpis zezwalający na ruch od administratora PC-A (192.168.10.3) i dodatkowy wpis zezwalający na dostęp z adresów od 192.168.10.4 do 192.168.10.7. Zauważ, że pierwszy wpis dotyczy pojedynczego adresu poprzez

użycie wpisu host. Zamiast tego można użyć komendy permit 192.168.10.3 0.0.0.0. Drugi wpis zezwala na ruch z adresów 192.168.10.4 do 192.168.10.7 poprzez użycie maski blankietowej 0.0.0.3, która jest odwróceniem maski sieciowej 255.255.255.252.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# permit host 192.168.10.3
R1(config-std-nacl)# permit 192.168.10.4 0.0.0.3
R1(config-std-nacl)# exit
```

Nie ma potrzeby konfigurowania indywidulanych blokad, ponieważ na końcu listy znajduje się wpis **deny any**.

b. Przypisz utworzoną listę ACL do linii vty.

```
R1(config)# line vty 0 15
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

W celu zdalnego dostępu i weryfikacji, czy utworzona lista działa poprawnie zostanie użyty protokół Telnet.

Uwaga: SSH jest bezpieczniejszy od Telnetu; jednakże SSH wymaga aby urządzenia sieciowe były odpowiednio skonfigurowane. Na tym laboratorium Telnet używany jest dla wygody.

c. Otwórz wiersz poleceń na komputerze PC-A i sprawdź czy możliwa jest komunikacja z routerem przy użyciu polecenia **ping**.

d. Z komputera PC-A połącz się do routera R1 przy użyciu protokołu Telnet. Wejdź do trybu uprzywilejowanego po wpisaniu hasła. Po poprawnym zalogowaniu zobaczysz baner powitalny i znak zachęty routera.

Czy udało się połączyć z routerem? _____

e. Wpisz **exit** i naciśnij Enter w celu zamknięcia połączenia Telnet.

f. Zmień adres IP komputera na 192.168.10.100 w celu sprawdzenia czy lista ACL blokuje ruch z nieuprawnionych adresów IP.

g. Połącz się do routera przez Telnet jeszcze raz. Czy połączenie zakończyło się sukcesem?

_____

Jaki komunikat się pojawił?

_____

h. Zmień adres IP komputera PC-A na jeden z zakresu od 192.168.10.4 do 192.168.10.7 w celu sprawdzenia czy lista ACL zezwala na ruch z ustawionego zakresu IP. Po zmianie adresu połącz się ponownie do routera przy użyciu protokołu Telnet.

Czy połączenie zakończyło się sukcesem?

_____

_____

i. W trybie uprzywilejowanym routera R1 użyj komendy **show ip access-lists** i naciśnij Enter. Zauważ jak system IOS pokazuje liczbę poprawnych powiązań do danego wpisu ACE (w nawiasie).

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.10.3 (2 matches)
    20 permit 192.168.10.4, wildcard bits 0.0.0.3 (2 matches)
```

Ze względu na dwa połączenia Telnet do routera, każde z adresu IP pasującego do jednego wpisu ACE, istnieją połączenia pasujące do obydwu wpisów ACE.

Dlaczego do każdego wpisu ACE są dwa powiązania skoro wykonane zostało tylko po jednym połączeniu z każdego adresu IP?

_____

_____

_____

W jaki sposób można określić, w którym momencie protokół Telnet powoduje dwa powiązania podczas jednego połączenia Telnet?

_____

_____

_____

_____

j. Na routerze R1 wejdź do trybu globalnej konfiguracji.

k. Wejdź do trybu konfiguracji list dostępu ADMIN-MGT i dodaj wpis **deny any** na końcu listy.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

Uwaga: Ze względu na niejawny wpis **deny any** na końcu każdej listy nie ma potrzeby dodawania wyraźnego wpisu **deny any**. Jednakże wpis ten może być przydatny administratorowi w celu sprawdzenia ile razy wykonano połączenia, które zostały zablokowane.

l. Połącz się z komputera PC-B do R1 przy użyciu protokołu Telnet. Spowoduje to powstanie powiązania do wpisu **deny any** na liści kontroli dostępu.

m. W trybie uprzywilejowanym użyj komendy **show ip access-lists i** naciśnij Enter. Powinny być teraz widoczne powiązania do wpisu **deny any**.

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
    10 permit 192.168.10.3 (2 matches)
    20 permit 192.168.10.4, wildcard bits 0.0.0.3 (2 matches)
    30 deny any (3 matches)
```

Połączenia Telnet zakończone niepowodzeniem, powodują więcej powiązań do wpisu deny any, niż połączenia zakończone sukcesem. Dlaczego?

_____

Krok 4: Wyzwanie – Konfiguracja list kontroli dostępu na przełączniku S1

a. Bez odnoszenia się do konfiguracji routera R1 spróbuj skonfigurować listę ACL na przełączniku, zezwalającą na dostęp tylko z komputera PC-A.

b. Przypisz listę ACL do linii vty przełącznika S1. Pamiętaj, że na przełączniku jest więcej linii vty niż na routerze.

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 uzyj 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, 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? _____

d Przed przystąpieniem do dalszej części zadań **usuń wszystkie listy dostępu z routerów R1 i R3**

Część 5. Konfiguracja i weryfikacja rozszerzonych numerowanych i nazywanych list kontroli dostępu

Rozszerzone listy kontroli dostępu (ACL) mogą filtrować ruch na wiele różnych sposobów. Rozszerzone listy mogą filtrować po źródłowym adresie IP, numerze portu źródłowego, docelowym adresie IP, porcie docelowym jak również po różnych protokołach i usługach.

Zasady bezpieczeństwa są następujące:

1. Zezwól na ruch WWW pochodzący z sieci 192.168.10.0/24 skierowany do dowolnej sieci.
2. Zezwól na połączenia SSH do interfejsu szeregowego R3 z komputera PC-A.
3. Zezwól użytkownikom w sieci 192.168.10.0/24 na dostęp do sieci 192.168.20.0/24.

4. Zezwól na ruch www pochodzący z sieci 192.168.30.0/24 i skierowany do R1 na port www oraz do sieci 209.165.200.224/27 na ISP. Sieć 192.168.30.0/24 nie może mieć dostępu do żadnej innej sieci za pomocą protokołu www.

Patrząc na zasady bezpieczeństwa wyszczególnione powyżej, potrzebujesz dwóch ACL aby spełnić wymagane zasady bezpieczeństwa. Według najlepszych praktyk, rozszerzone listy kontroli dostępu ACL powinny być najbliżej źródła jak to tylko możliwe. Postąpimy zgodnie z tymi praktykami przy implementowaniu tych zasad.

Krok 1: Konfiguracja numerowanej rozszerzonej listy kontroli dostępu na R1 w celu realizacji zasady bezpieczeństwa nr 1 i 2.

Użyjesz numerowanej listy rozszerzonej ACL na R1. Jaki jest zakres dla rozszerzonych list ACL?

_____

a. Skonfiguruj ACL na R1. Użyj numeru 100 dla listy ACL.

```
R1(config)# access-list 100 remark Allow WWW & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

Co oznacza 80 na końcu powyższej komendy?

_____

Na jakim interfejsie ACL 100 powinna być założona?

_____

_____

W którym kierunku powinna być założona ACL?

_____

_____

b. Załóż ACL 100 na interfejs S0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Sprawdź ACL 100.

1. Otwórz przeglądarkę internetową na PC-A, otwórz stronę WWW http://209.165.200.225 (ISP router). Zadanie powinno zakończyć się sukcesem. Rozwiąż problemy, jeśli tak się nie stało.

2. Zestaw połączenie SSH z PC-A do R3 używając 10.2.2.1 jako adresu IP. Zaloguj się używając **admin** i **class** jako dane uwierzytelniające. Powinno zakończyć się sukcesem. Rozwiąż problemy jeśli nie.

3. Z trybu uprzywilejowanego EXEC na R1 wydaj komendę **show access-lists**.

```
R1# show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
    20 permit tcp any any eq www (111 matches)
```

1. Z linii komend PC-A wydaj komendę ping na adres 10.2.2.1. Wyjaśnij otrzymany rezultat.

_____

_____

_____

Krok 2: Konfiguracja nazywanej rozszerzonej listy ACL na R3 w celu realizacji zasady bezpieczeństwa nr 3.

a. Skonfiguruj politykę bezpieczeństwa na R3. Nazwij listę WWW-POLICY.

```
R3(config)# ip access-list extended WWW-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. Zastosuj listę WWW-POLICY na interfejsie S0/0/1.

```
R3(config-ext-nacl)# interface S0/0/1
R3(config-if)# ip access-group WWW-POLICY out
```

c. Zweryfikuj listę WWW-POLICY.

1. Z trybu uprzywilejowanego na R3 w trybie linii komand, wydaj komendę **show ip interface s0/0/1**.

   Jak, jeśli jest, nazywa się ACL? _____

   W jakim kierunku została zastosowana lista ACL? _____

2. Otwórz przeglądarkę internetową na PC-C i wejdź na stronę http://209.165.200.225 (ISP router). Dostęp powinien być możliwy, Jeśli nie, rozwiąż problemy.
3. Z PC-C, otwórz sesję WWW do http://10.1.1.1 (R1). Dostęp powinien być możliwy, Jeśli nie, rozwiąż problemy.
4. Z PC-C, otwórz sesję WWW do http://209.165.201.1 (ISP router). Dostęp powinien być niemożliwy. Jeśli nie, rozwiąż problemy.
5. Z linii komend PC-C, wykonaj ping do PC-A. Zapisz jaki jest rezultat i dlaczego?

   _____

Część 6. Modyfikacja i weryfikacja rozszerzonej listy kontroli dostępu

Ponieważ lista dostępu zastosowana na routerach R1, R2 i R3 nie pozwala na komunikaty ping, ani żaden inny ruchu pomiędzy sieciami LAN na R1 i R3, kierownictwo zdecydowało, że powinien być możliwy cały ruch pomiędzy sieciami 192.168.10.0/24 i 192.168.30.0/24. Zmodyfikuj obie listy dostępu na R1 i R3.

Krok 1: Modyfikacja ACL 100 na R1.

a. Z trybu uprzywilejowanego EXEC na routerze R1 wydaj komendę **show access-lists**.

   Ile linii zawiera ta lista dostępu? _____

b. Wejdź w tryb konfiguracji globalnej i zmodyfikuj ACL na R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```

c. Wydaj komendę **show access-lists**.

   Gdzie pojawiła się nowo dodana linia w liście ACL 100?

   _____

Krok 2: Modyfikacja nazywanej listy ACL WWW-POLICY na R3.

a. W trybie uprzywilejowanym EXEC na R3 wydaj komendę **show access-lists**.

   Ile linii zawiera ta lista dostępu? _____

b. Wejdź w tryb konfiguracji globalnej i zmodyfikuj ACL na R3.

```
R3(config)# ip access-list extended WWW-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

c. Wydaj komendę **show access-lists** w celu weryfikacji, że nowa linia została dodana na końcu listy.

Krok 3: Weryfikacja zmodyfikowanych list kontroli dostępu (ACL).

a. Z PC-A, wykonaj polecenie ping na adres IP komputera PC-C. Czy ping zakończył się sukcesem?

_____

b. Z PC-C, wykonaj polecenie ping na adres IP komputera PC-A. Czy ping zakończył się sukcesem?

_____

a. Dlaczego ACL działa natychmiast w stosunku do wysłanych komunikatów ping zaraz po tym jak została zmieniona?

_____

Krok 4: Wyzwanie – Blokowanie ruchu FTP.

a. Utwórz listę dostępu, która zablokuje dostęp do usługi FTP na routerze ISP z komputera PC-A. Pozostałe komputery z sieci 192.168.10.0/24 powinny mieć dostęp do usługi.

Zweryfikuj poprawność działania utworzonej listy dostępu.

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?

_____

_____

_____

_____

_____

3. Dlaczego uważnie trzeba planować i testować listy kontroli dostępu?

_____

_____

4. Które z typów list kontroli dostępu są lepsze: standardowe czy rozszerzone?

_____

_____

_____

_____

5. Dlaczego pakiety hello i aktualizacje routingu OSPF nie są blokowane przez domniemany wpis kontroli dostępu **deny any** (ACE) lub listy ACL zastosowane na routerach R1 i R3?

_____

_____

_____

_____

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.				