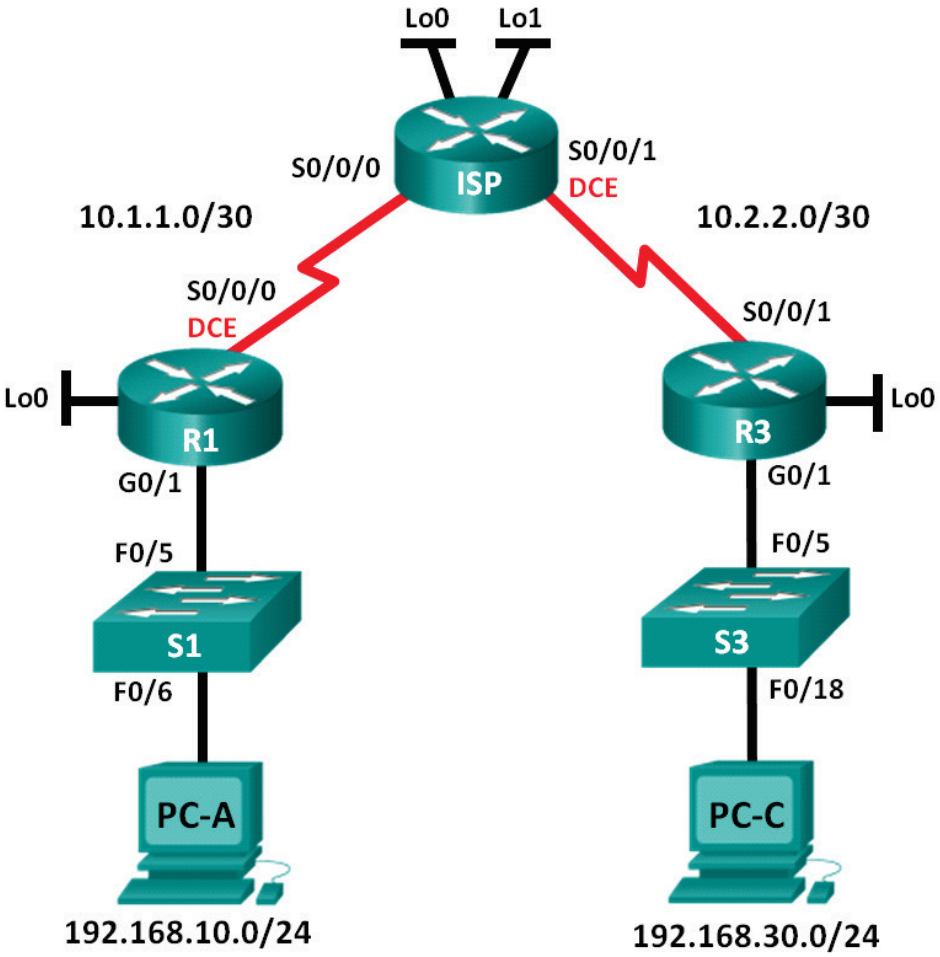
Ćwiczenie – Konfiguracja i weryfikacja rozszerzonych list kontroli dostępu (ACL)

Topologia



Tablica adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.10.1	255.255.255.0	Nie dotyczy
	Lo0	192.168.20.1	255.255.255.0	Nie dotyczy
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Nie dotyczy
ISP	S0/0/0	10.1.1.2	255.255.255.252	Nie dotyczy
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Nie dotyczy
	Lo0	209.165.200.225	255.255.255.224	Nie dotyczy
	Lo1	209.165.201.1	255.255.255.224	Nie dotyczy
R3	G0/1	192.168.30.1	255.255.255.0	Nie dotyczy
	Lo0	192.168.40.1	255.255.255.0	Nie dotyczy
	S0/0/1	10.2.2.1	255.255.255.252	Nie dotyczy
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	Karta sieciowa	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	Karta sieciowa	192.168.30.3	255.255.255.0	192.168.30.1

Cele

Część 1: Połączenie urządzeń według schematu i inicjalizacja urządzeń

Część 2: Konfiguracja urządzeń i weryfikacja łączności

- Konfiguracja podstawowych ustawień na komputerach PC, routerach i przełącznikach.
- Konfiguracja protokołu routingu OSPF na routerach R1, ISP i R3.

Część 3: 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 4: Modyfikacja i weryfikacja rozszerzonych list kontroli dostępu

Scenariusz

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. Kierownictwo firmy ustaliło pewne zasady dostępu między sieciami LAN przyłączonymi do routerów R1 i R3, które należy wdrożyć. Router ISP pomiędzy routerami R1 i R3 nie ma skonfigurowanych żadnych list ACL. Podczas ćwiczenia możesz konfigurować i zarządzać swoimi routerami tj. R1 i R3, gdyż nie będziesz miał dostępu to trybu administracyjnego na routerze ISP.

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)
- 2 przełączniki (Cisco 2960 z Cisco IOS wydanie 15.0(2) obraz „lanbasek9" lub kompatybilny)
- 2 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

• Zestawienie topologii sieci i inicjacja urządzeń

W części I, należy zestawić topologię sieci i wyczyścić konfigurację z urządzeń jeśli to konieczne.

• Połącz sieć zgodnie ze schematem

• Zainicjuj i przeładuj routery i przełączniki

• Konfiguracja urządzeń i weryfikacja połączeń

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

• Skonfiguruj adresy IP na komputerze PC-A i PC-C.

• Skonfiguruj podstawowe ustawienia na routerze R1.

- Wyłącz DNS lookup.
- Skonfiguruj nazwę urządzenia jak to pokazano na schemacie.
- Utwórz interfejs loopback na routerze R1.
- Skonfiguruj adresy IP na interfejsach jak pokazano na schemacie i w tabeli adresacji.
- Skonfiguruj hasło **class** do trybu uprzywilejowanego EXEC.
- Przypisz taktowanie zegara **128000** na interfejsie S0/0/0.
- Przypisz hasło **cisco** dla konsoli i vty oraz włącz dostęp poprzez Telnet. Skonfiguruj **logging synchronous** zarówno dla połączenia konsolowego jak i vty.
- 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
```

• Skonfiguruj podstawowe ustawienia dla routera ISP.

- Wyłącz DNS lookup.
- Skonfiguruj nazwę urządzenia jak pokazano to na schemacie.
- Utwórz interfejs loopback.

- Skonfiguruj adresy IP na interfejsach jak pokazano na schemacie i w tabeli adresacji.
- Skonfiguruj hasło **class** do trybu uprzywilejowanego EXEC.
- Przypisz taktowanie zegara **128000** na interfejsie S0/0/1.
- Przypisz hasło **cisco** dla konsoli i vty oraz włącz dostęp poprzez Telnet. Skonfiguruj **logging synchronous** zarówno dla połączenia konsolowego jak i vty.
- Uruchom dostęp WWW na ISP. Użyj tych samych parametrów jak w kroku 2.

- **Skonfiguruj podstawowe ustawienia na routerze R3.**
  - Wyłącz DNS lookup.
  - Skonfiguruj nazwę urządzenia jak to pokazano na schemacie.
  - Utwórz interfejs loopback.
  - Skonfiguruj adresy IP na interfejsach jak pokazano na schemacie i w tabeli adresacji.
  - Skonfiguruj hasło **class** do trybu uprzywilejowanego EXEC.
  - Przypisz hasło **cisco** do konsoli i skonfiguruj **logging synchronous** na linii konsolowej.
  - Włącz protokół SSH on R3.

```
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
```

  - Uruchom dostęp WWW na R3. Użyj tych samych parametrów jak w kroku 2.

- **(Opcjonalnie) Skonfiguruj ustawienia podstawowe na przełączniku S1 i S3.**
  - Skonfiguruj nazwę urządzenia jak podano w topologii.
  - Skonfiguruj adres IP interfejsu zarządzania jak pokazano w topologii i tabeli adresacji.
  - Wyłącz DNS lookup.
  - Skonfiguruj hasło **class** do trybu uprzywilejowanego EXEC.
  - Skonfiguruj adres bramy domyślnej.

- **Skonfiguruj routing OSPF na R1, ISP i R3.**
  - Przypisz 1 jako ID procesu OSPF i ogłoś wszystkie sieci R1, ISP i R3. Konfiguracja OSPF dla routera R1 jest dołączona
  - jako przykład.

```
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
```

  - Po konfiguracji protokołu OSPF na routerach R1, ISP i R3 zweryfikuj, że wszystkie routery mają kompletną tablicę routingu poprzez jej wyświetlenie. Usuń problemy jeśli takowe występują.

- **Zweryfikuj łączność pomiędzy urządzeniami**

  Uwaga: Bardzo ważne jest sprawdzenie łączności pomiędzy urządzeniami **przed** konfiguracją list kontroli dostępu i ich przypisaniem do interfejsu. Upewnij się, że sieć funkcjonuje poprawnie zanim zaczniesz filtrować wychodzący ruch.

- Z komputera PC-A, wyślij ping do PC-C i interfejsu loopback oraz interfejsu szeregowego na R3.

  Czy ping zakończył się sukcesem? _____

- Z routera R1, wyślij ping do PC-C i interfejsu loopback oraz interfejsu szeregowego na R3.

  Czy ping zakończył się sukcesem? _____

- Z komputera PC-C, wyślij ping do PC-A i interfejsu loopback oraz interfejsu szeregowego na R1.

  Czy ping zakończył się sukcesem? _____

- Z R3, wyślij ping do PC-A i interfejsu loopback oraz interfejsu szeregowego na R1.

  Czy ping zakończył się sukcesem? _____

- Z PC-A, wyślij ping do interfejsu loopback na routerze ISP.

  Czy ping zakończył się sukcesem? _____

- Z PC-C, wyślij ping do interfejsu loopback na routerze ISP.

  Czy ping zakończył się sukcesem? _____

- 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.

- 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.

• Skonfiguruj i zweryfikuj rozszerzone numerowane i nazywane listy ACL.

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:

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

• Skonfiguruj numerowaną rozszerzoną listę 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?

_____
_____

- 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?

_____
_____

_____
_____

- Załóż ACL 100 na interfejs S0/0/0.

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

- Sprawdź ACL 100.
  - 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.
  - 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.
  - 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)
```

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

    _____
    _____

    _____
    _____

    _____
    _____

- **Konfiguracja nazywanej rozszerzonej listy ACL na R3 w celu realizacji zasady bezpieczeństwa nr 3.**
  - 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
```

- 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
```

- Zweryfikuj listę WWW-POLICY.
  - 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?

    _____
  - 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.
  - Z PC-C, otwórz sesję WWW do http://10.1.1.1 (R1). Dostęp powinien być możliwy, Jeśli nie, rozwiąż problemy.
  - Z PC-C, otwórz sesję WWW do http://209.165.201.1 (ISP router). Dostęp powinien być niemożliwy. Jeśli nie, rozwiąż problemy.
  - Z linii komend PC-C, wykonaj ping do PC-A. Zapisz jaki jest rezultat i dlaczego?

    _____
    _____

• 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.

• Zmodyfikuj ACL 100 na R1.

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

  Ile linii zawiera ta lista dostępu? _____
- 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
```

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

  Gdzie pojawiła się nowo dodana linia w liście ACL 100?

  _____
  _____

• Zmodyfikuj ACL nazywaną WWW-POLICY na R3.

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

  Ile linii zawiera ta lista dostępu? _____

- 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
```

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

- **Zweryfikuj zmodyfikowane listy kontroli dostępu (ACL).**
  - Z PC-A, wykonaj polecenie ping na adres IP komputera PC-C. Czy ping zakończył się sukcesem? _____
  - Z PC-C, wykonaj polecenie ping na adres IP komputera PC-A. Czy ping zakończył się sukcesem? _____

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

    _____
    _____

Do przemyślenia

- Dlaczego uważnie trzeba planować i testować listy kontroli dostępu?

  _____
  _____

  _____
  _____

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

  _____
  _____

  _____
  _____

  _____
  _____

  _____
  _____

- 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 2 –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.