Laboratorium 3 – Filtrowanie ruchu z wykorzystaniem rozszerzonych list kontroli dostępu

Cele ćwiczenia

Celem ćwiczenia jest wdrożenie w sieci IP list kontroli dostępu (ang. Access Control List – ACL), umożliwiających sterowanie dostępem do określonych usług na serwerach. Zastosowane zostaną dwa typy ACL, tj. rozszerzone (ang. extended) i nazywane (ang. named).

Celami szczegółowymi ćwiczenia są:

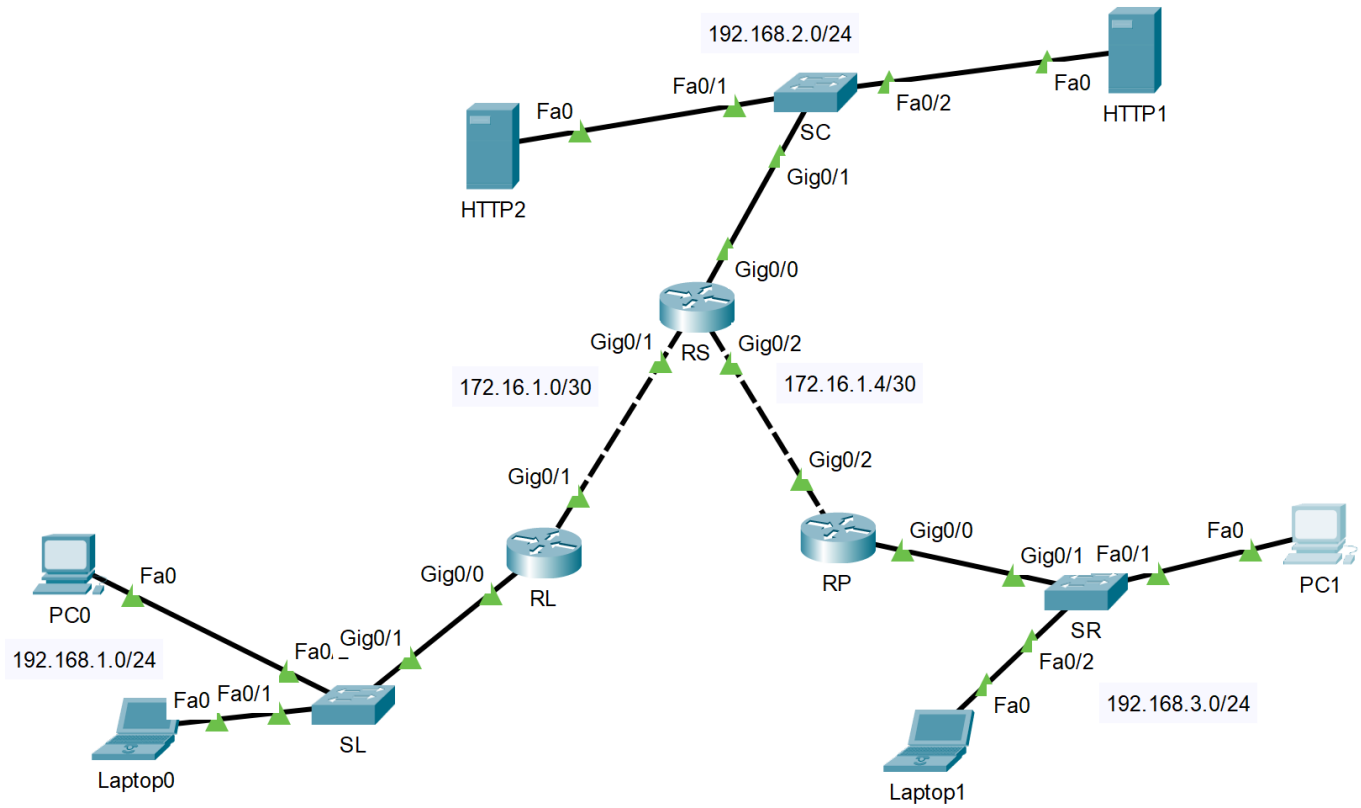
1. Konfiguracja rutingu RIP w sieci operatora.
2. Konfiguracja filtru (w postaci extended ACL) zezwalającego na obsługę ruchu ICMP w określonej sieci IP.
3. Konfiguracja filtru (w postaci named ACL) zezwalającego na obsługę ruchu http w określonej sieci IP.

Opis topologii logicznej i fizycznej sieci

1. Komputer PC0 o adresie IP 192.168.1.**2**/24 połączony łączem FastEthernet z portem FastEthernet 0/2 przełącznika SL
2. Komputer Laptop0 o adresie IP 192.168.1.**3**/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SL
3. Port GigabitEthernet 0/1 przełącznika SL połączony z portem GigabitEthernet 0/0 rutera RL o adresie 192.168.1.**1**/24
4. Port GigabitEthernet 0/1 rutera RL o adresie 172.16.1.**1**/30 połączony z portem GigabitEthernet 0/1 rutera RS o adresie 122.16.1.**2**/30

5. Port GigabitEthernet 0/2 rutera RS o adresie 172.16.1.**5**/30 połączony z portem GigabitEthernet0/2 rutera RP o adresie 172.16.1.**6**/30
6. Port GigabitEthernet 0/0 rutera RS o adresie 192.168.2.**1**/24 połączony z portem GigabitEthernet0/1 przełącznika SC
7. Serwer HTTP1 o adresie 192.168.2.80/24 połączony z portem przełącznika Fa0/2 przełącznika SC
8. Serwer HTTP2 o adresie 192.168.2.23/24 połączony z portem przełącznika Fa0/1 przełącznika SC
9. Port GigabitEthernet 0/0 rutera RP o adresie 192.168.3.**1**/24 połączony z portem GigabitEthernet 0/**1** przełącznika SR
10. Komputer PC1 o adresie IP 192.168.3.**2**/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SR
11. Komputer Laptop1 o adresie IP 192.168.3.**3**/24 połączony łączem FastEthernet z portem FastEthernet 0/2 przełącznika SR

Graficzną reprezentację opisanej topologii przedstawiono na poniższym rysunku



Przebieg ćwiczenia

Połączenie urządzeń zgodnie z topologią przedstawioną w poprzednim rozdziale

Nadanie adresów IP urządzeniom końcowym

1. Komputer PC0
    a. Adres 192.168.1.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.1.1 z maską 24 bitową
2. Komputer Laptop0
    a. Adres 192.168.1.3 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.1.1 z maską 24 bitową
3. Serwer HTTP2
    a. Adres 192.168.2.23 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.2.1 z maską 24 bitową
4. Serwer HTTP1
    a. Adres 192.168.2.80 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.2.1 z maską 24 bitową
5. Komputer PC1
    a. Adres 192.168.3.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.3.1 z maską 24 bitową
6. Komputer Laptop1
    a. Adres 192.168.3.3 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.3.1 z maską 24 bitową

Konfiguracja interfejsów sieciowych ruterów

1. Ruter RL

```
Router>enable

Router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname RL
```

```
RL(config)#interface gigabitEthernet 0/0

RL(config-if)#ip address 192.168.1.1 255.255.255.0

RL(config-if)#no shutdown

RL(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

RL(config)#interface gigabitEthernet 0/1

RL(config-if)#ip address 172.16.1.1 255.255.255.252

RL(config-if)#no sh


RL(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

2. Ruter RS

```
RS(config)#interface gigabitEthernet 0/1
RS(config-if)#ip address 172.16.1.2 255.255.255.252
RS(config-if)#no sh
RS(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

RS(config-if)#exit
RS(config)#interface gigabitEthernet 0/0
RS(config-if)#ip address 192.168.2.1 255.255.255.0
RS(config-if)#no sh

RS(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

RS(config)#int gigabitEthernet 0/2
RS(config-if)#ip address 172.16.1.5 255.255.255.252

RS(config-if)#no sh

RS(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
```

3. Ruter RP

```
Router>enable

Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname RP

RP(config)#int gig 0/2

RP(config-if)#ip add 172.16.1.6 255.255.255.252

RP(config-if)#no sh

RP(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/2, changed state to up

RP(config)#int gig 0/0

RP(config-if)#ip add 192.168.3.1 255.255.255.0

RP(config-if)#no sh
```

```
RP(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
```

Sprawdzenie poprawności konfiguracji interfejsów ruterów:

```
Router#show ip interface brief
```

Uruchomienie rutingu RIP na wszystkich ruterach:

```
RL>ena

RL#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RL(config)#router rip

RL(config-router)#version 2

RL(config-router)#network 192.168.1.0

RL(config-router)#network 172.16.1.0

RL(config-router)#


RS>ena

RS#conf t

Enter configuration commands, one per line. End with CNTL/Z.

RS(config)#router rip

RS(config-router)#version 2

RS(config-router)#network 172.16.1.0
```

```
RS(config-router)#network 172.16.1.4
RS(config-router)#network 192.168.2.0
RS(config-router)#

RP>ena
RP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RP(config)#router rip
RP(config-router)#version 2
RP(config-router)#network 172.16.1.4
RP(config-router)#network 192.168.3.0
RP(config-router)#
```

Konfiguracja filtru ACL umożliwiającego przesyłanie wiadomości ICMP z sieci 192.168.1.0/24 do 192.168.2.0

Określenie sieci źródłowej i docelowej oraz do ruchu typu ICMP powoduje, że ACL powinna być listą rozszerzoną i powinna zostać nałożona na interfejsie GE0/0 rutera RL (jak najbliżej źródła). Poniżej przedstawiono konfigurację rozszerzone listy kontroli dostępu. Zwróć uwagę na dostępne opcje, o których możesz się dowiedzieć posługując się znakiem zapytania.

1. Konfiguracja listy kontroli dostępu

```
RL>enable
RL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
RL(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
RL(config)#access-list 110 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
RL(config)#access-list 110 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
RL(config)#access-list 110 permit icmp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
RL(config)#access-list 110 permit icmp 192.168.1.0 ?
```

```
    A.B.C.D  Source wildcard bits

  RL(config)#access-list 110 permit icmp 192.168.1.0 0.0.0.255 ?

    A.B.C.D  Destination address

    any      Any destination host

    host     A single destination host

  RL(config)#access-list 110 permit icmp 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255 ?

    <0-256>               type-num

    echo                  Echo (ping)

    echo-reply            Echo reply

    host-unreachable      Host unreachable

    net-unreachable       Net unreachable

    port-unreachable      Port unreachable

    protocol-unreachable  Protocol unreachable

    ttl-exceeded          TTL exceeded

    unreachable           All unreachables

    <cr>

  RL(config)#access-list 110 permit icmp 192.168.1.0 0.0.0.255 any

  RL(config)#

  RL#

  %SYS-5-CONFIG_I: Configured from console by console
```

Pamiętaj, że domyślnym ostaniem wpisem w ACL jest deny any any.

2. Nałożenie ACL na właściwym interfejsie rutera RL

```
RL#show access-lists
Extended IP access list 110
    10 permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

RL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RL(config)#interface gigabitEthernet 0/0
RL(config-if)#ip access-group 110 in
```

Sprawdzenie poprawności działania ACL

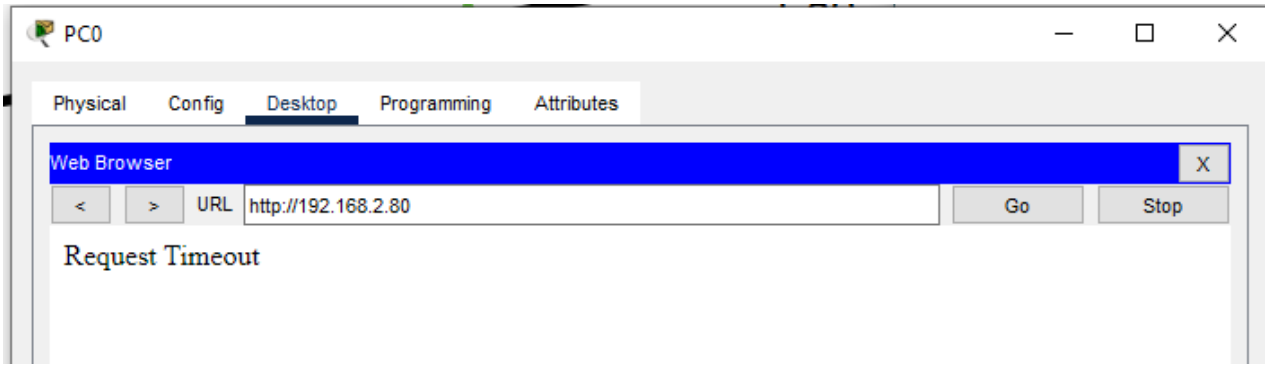
1. Wyślij ICMP Echo Request (ping) z PC0 do serwera HTTP1. ICMP jest w grupie permit, zatem ping powinien zakończyć się sukcesem, jak na poniższym rysunku:

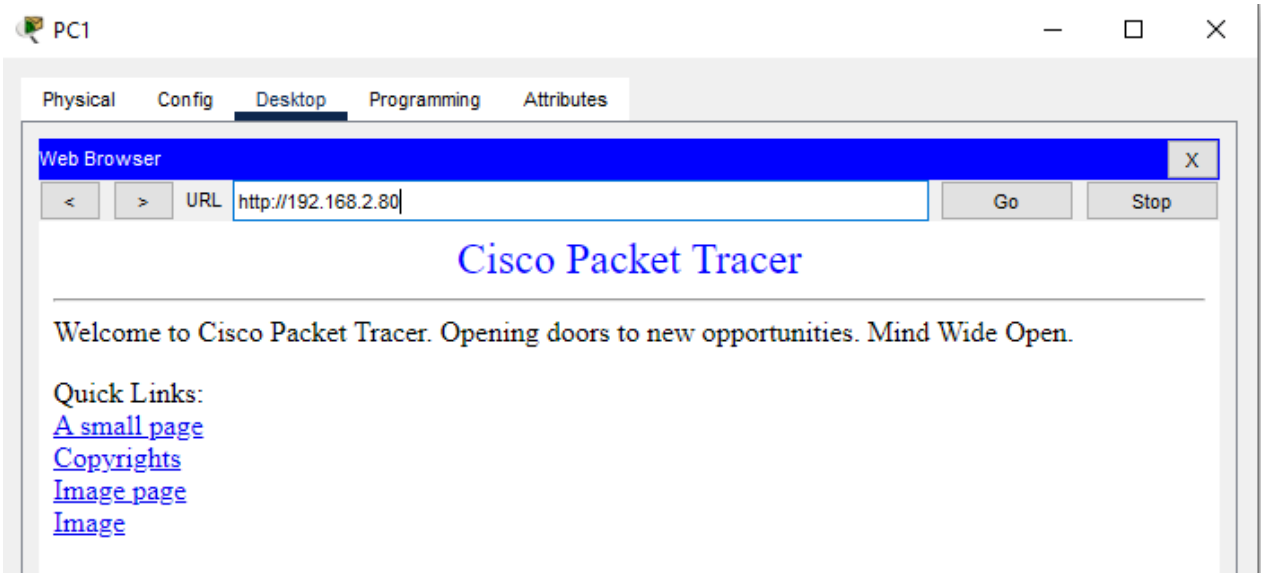
```
C:\>ping 192.168.2.80

Pinging 192.168.2.80 with 32 bytes of data:

Reply from 192.168.2.80: bytes=32 time<1ms TTL=126
Reply from 192.168.2.80: bytes=32 time<1ms TTL=126
Reply from 192.168.2.80: bytes=32 time=1ms TTL=126
Reply from 192.168.2.80: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2. Wyślij ICMP Echo Request (ping) z PC0 do serwera PC1. ICMP jest w grupie permit, jednak sieć docelowa 192.168.3.0 jest w grupie blokowanych połaczeń (wyjaśnij dlaczego). Zatem powinniśmy otrzymać poniższą odpowiedź:

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

3. Sprawdzenie możliwości nawiązania łączności z serwerem http (192.168.2.80), na porcie 80. Sprawdź możliwość nawiązania takiego połączenia z komputera PC0 oraz PC1. W przypadku PC0 nie powinno się to powieść, a w przypadku PC1 -tak. Przykładowe zrzuty ekranu umieszczono poniżej:





Konfiguracja filtru ACL w postaci nazywanej listy rozszerzonej

Zastosowany zostanie filtr zezwalający na przesyłanie z sieci 192.168.3.0 tylko ruchu http. W tym celu należy zdefiniować nazywaną rozszerzoną listę ACL (ang. named extended ACL), przepuszczającą ruch http z sieci 192.168.3.0 tylko do serwera HTTP1 (192.168.2.80). Określenie sieci źródłowej i hosta docelowego, powoduje, że ACL powinna być nałożona na interfejsie GE0/0 rutera RP (jak najbliżej źródła). Ograniczenie do konkretnego typu ruchu (http) powoduje z kolei, że konieczne jest zastosowanie listy rozszerzonej. Poniżej przedstawiono konfigurację rozszerzonej nazywanej listy kontroli dostępu. Zwróć uwagę na dostępne opcje, o których możesz się dowiedzieć posługując się znakiem zapytania.

1. Konfiguracja nazywanej listy kontroli dostępu

```
RP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RP(config)#ip access-list extended ?
  <100-199>  Extended IP access-list number
  WORD       name
RP(config)#ip access-list extended Tylko-HTTP1
```

```
RP(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host
192.168.2.80 eq www

RP#sh access-lists

Extended IP access list Tylko-HTTP1

    10 permit tcp 192.168.3.0 0.0.0.255 host 192.168.2.80 eq www
```

2. Nałożenie nazywanej listy kontroli dostępu na właściwy interfejs rutera RP

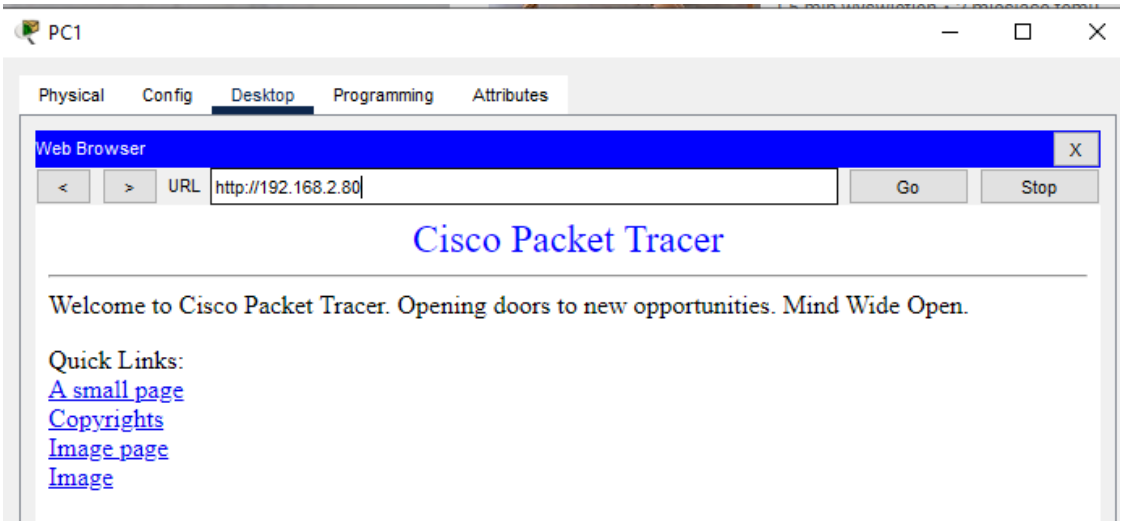
```
RP#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

RP(config)#int gigabitEthernet 0/0

RP(config-if)#ip access-group Tylko-HTTP1 in
```

Sprawdzenie poprawności działania ACL

1. Wyślij ICMP Echo Request (ping) z PC1 do serwera HTTP1. ICMP jest w grupie domyślnej „deny any”, zatem ping powinien zakończyć się porażką:

```
C:\>ping 192.168.2.80

Pinging 192.168.2.80 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.2.80:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

2. Sprawdzenie możliwości nawiązania łączności z serwerem http (192.168.2.80), na porcie 80.



3. Sprawdzenie możliwości nawiązania łączności z serwerem http (192.168.2.80), na porcie 80.