Packet Tracer - Konfiguracja rozszerzonych list ACL - Scenariusz 1

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	172.22.34.65	255.255.255.224	nd.
	G0/1	172.22.34.97	255.255.255.240	
	G0/2	172.22.34.1	255.255.255.192	
Server	Karta sieciowa	172.22.34.62	255.255.255.192	172.22.34.1
PC1	Karta sieciowa	172.22.34.66	255.255.255.224	172.22.34.65
PC2	Karta sieciowa	172.22.34.98	255.255.255.240	172.22.34.97

Cele

Część 1: Konfiguracja, zastosowanie i weryfikacja rozszerzonych numerowanych list ACL

Część 2: Konfiguracja, zastosowanie i weryfikacja rozszerzonych nazwanych list ACL

Wprowadzenie / Scenariusz

Dwóch pracowników potrzebuje dostępu do usług świadczonych przez serwer. **PC1** potrzebuje tylko dostępu do FTP, podczas gdy **PC2** potrzebuje tylko dostępu do www. Oba komputery powinny komunikować się podczas testów ping z serwerem, ale nie ze sobą.

Instrukcje

Część 1: Konfigurowanie, zastosowanie i weryfikacja rozszerzonych numerowanych list ACL

Krok 1: Skonfiguruj listę ACL, aby zezwolić na FTP i ICMP z sieci LAN PC1.

a. W trybie konfiguracji globalnej na **R1** wprowadź poniższe polecenie, aby określić pierwszy ważny numer dla rozszerzonej listy dostępu.

```
R1(config)# access-list ?
  <1-99> IP standard access list
  <100-199> IP extended access list
```

b. Dodaj **100** do komendy, a następnie znak zapytania.

```
R1(config)# access-list 100 ?
  deny Specify packets to reject
  permit Specify packets to forward
  remark Access list entry comment
```

c. Aby zezwolić na ruch FTP, wpisz **permit**, a następnie znak zapytania.

```
R1(config)# access-list 100 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
```

d. Po skonfigurowaniu i zastosowaniu ta ACL powinna zezwolić na protokół FTP i ICMP. ICMP jest wymienione powyżej, ale FTP nie. Wynika to z faktu, że protokół FTP jest protokołem warstwy aplikacji, który używa protokołu TCP w warstwie transportowej. Wpisz TCP i znak zapytania dla dokładniejszej pomocy w ACL.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D Source address
  any Any source host
  host A single source host
```

e. Adres źródłowy może reprezentować pojedyncze urządzenie, takie jak PC1, za pomocą słowa kluczowego **host**, a następnie adresu IP PC1. Używanie słowa kluczowego **any** zezwala na dowolny host w dowolnej sieci. Filtrowanie można również wykonać za pomocą adresu sieciowego. W tym przypadku jest to dowolny host, którego adres należy do sieci 172.22.34.64/27. Wpisz ten adres sieciowy, a następnie znak zapytania.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D Source wildcard bits
```

f. Oblicz maskę blankietową określoną jako binarne przeciwieństwo maski podsieci /27.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000**11111** = 0.0.0.31

g. Wpisz maskę blankietową, a następnie znak zapytania.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D Destination address
  any Any destination host
  eq Match only packets on a given port number
  gt Match only packets with a greater port number
  host A single destination host
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  range Match only packets in the range of port numbers
```

h. Skonfiguruj adres docelowy. W tym scenariuszu filtrujemy ruch pod kątem pojedynczego miejsca docelowego, którym jest serwer. Wpisz słowo kluczowe host a następnie adres IP serwera.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
  dscp Match packets with given dscp value
  eq Match only packets on a given port number
  established established
  gt Match only packets with a greater port number
  lt Match only packets with a lower port number
```

```
  neq Match only packets not on a given port number
  precedence Match packets with given precedence value
  range Match only packets in the range of port numbers
  <cr>
```

i. Zauważ, że jedną z opcji jest **cr** (znak powrotu). Innymi słowy możesz nacisnąć **Enter** i wyrażenie to pozwoliłoby na cały ruch TCP. Jednak chcemy pozwolić tylko na ruch FTP; w związku z tym należy wpisać słowo **eq** , a następnie znak zapytania, aby wyświetlić dostępne opcje. Następnie wpisz **ftp** i wciśnij **Enter**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535> Port number
  ftp File Transfer Protocol (21)
  pop3 Post Office Protocol v3 (110)
  smtp Simple Mail Transport Protocol (25)
  telnet Telnet (23)
  www World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

j. Utwórz drugie wyrażenie w liście kontroli dostępu, aby umożliwić ruch ICMP (ping, itp.) z PC1 do Server. Należy zauważyć, że numer listy kontroli dostępu pozostaje taki sam, a specyficzny rodzaj ruchu ICMP nie musi być określony.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

k. Cały pozostały ruch jest domyślnie zabroniony.

l. Wykonaj polecenie **show access-list** i sprawdź, czy lista dostępu 100 zawiera poprawne instrukcje. Zauważ, że instrukcja **deny any any** nie pojawia się na końcu listy dostępu. Domyślne wykonanie listy dostępu jest takie, że jeśli pakiet nie znajdzie dopasowania do instrukcji na liście dostępu, nie jest dozwolony na interfejsie.

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
    20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

Krok 2: W celu filtrowania ruchu zastosuj ACL na odpowiednim interfejsie.

Z punktu widzenia routera **R1**, ruch, którego dotyczy ACL 100, jest przychodzący z sieci podłączonej do interfejsu Gigabit Ethernet 0/0. Wejdź w tryb konfiguracji interfejsu i zastosuj ACL.

Uwaga: W rzeczywistej sieci operacyjnej nie jest dobrą praktyką, aby stosować niesprawdzone listy dostępu do aktywnego interfejsu.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Krok 3: Zweryfikuj implementację listy ACL.

a. Wykonaj komendę ping z PC1 do Server. Jeśli ping zakończy się niepowodzeniem, to sprawdź adresy IP przed dalszym kontynuowaniem.

b. Wykonaj połączenie FTP z PC1 do Server. Nazwa użytkownika i hasło w obu przypadkach to **cisco**.

```
PC> ftp 172.22.34.62
```

c. Wyjdź z usługi FTP.

```
ftp> quit
```

d. Wykonaj ping z PC1 do PC2. Host docelowy powinien być nieosiągalny, ponieważ lista ACL nie zezwalała wprost na ruch.

Część 2: Konfiguracja, zastosowanie i weryfikacja rozszerzonych nazwanych list ACL

Krok 1: Skonfiguruj listę ACL, aby zezwolić na dostęp HTTP i ICMP z sieci LAN PC2.

a. Nazwane listy ACL zaczynają się od słowa kluczowego **ip**. W trybie konfiguracji globalnej na **R1** wprowadź poniższe polecenie, a następnie znak zapytania.

```
R1(config)# ip access-list ?
  extended Extended Access List
  standard Standard Access List
```

b. Możesz skonfigurować nazwane standardowe i rozszerzone listy ACL. Ta lista dostępu filtruje zarówno źródłowe jak i docelowe adresy IP - dlatego też musi być typu extended (rozszerzona). Wpisz **HTTP_ONLY** jako nazwę. (W przypadku oceny Packet Tracer w nazwie jest rozróżniana wielkość liter, a instrukcje listy dostępu muszą być z prawidłową kolejnością).

```
R1(config)# ip access-list extended HTTP_ONLY
```

c. Znak zachęty ulegnie zmianie. Jesteś teraz w trybie konfiguracji rozszerzonych nazywanych ACL. Wszystkie urządzenia w sieci, do której należy **PC2**, muszą mieć dostęp TCP. Wpisz adres sieciowy, a następnie znak zapytania.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
  A.B.C.D Source wildcard bits
```

d. Innym sposobem obliczenia maski blankietowej jest odjęcie maski podsieci od 255.255.255.255.

```
  255.255.255.255
- 255.255.255.240
-----------------
= 0.  0.  0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15
```

e. Zakończ komendę poprzez podanie adresu serwera, tak jak to zrobiłeś w części 1 i dodaj filtrowanie ruchu **www**.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

f. Utwórz drugie wyrażenie w liście kontroli dostępu, aby umożliwić ruch ICMP (ping, itp.) z **PC2** do **Server**. Uwaga: Znaki zachęty pozostają takie same, a specyficzny rodzaj ruchu ICMP nie musi być określony.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

g. Cały pozostały ruch jest domyślnie zabroniony. Wyjdź teraz z trybu konfiguracji rozszerzonych nazywanych ACL.

h. Wykonaj polecenie **show access-list** i sprawdź, czy lista dostępu **HTTP_ONLY** zawiera poprawne instrukcje.

```
R1# show access-lists
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

```
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

Krok 2: W celu filtrowania ruchu zastosuj ACL na odpowiednim interfejsie.

Z punktu widzenia routera **R1**, ruch, którego dotyczy ACL **HTTP_ONLY**, jest przychodzący z sieci podłączonej do interfejsu Gigabit Ethernet 0/1. Wejdź w tryb konfiguracji interfejsu i zastosuj ACL.

Uwaga: W rzeczywistej sieci operacyjnej nie jest dobrą praktyką, aby stosować niesprawdzone listy dostępu do aktywnego interfejsu. Należy tego unikać, jeśli to możliwe.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Krok 3: Zweryfikuj implementację listy ACL.

a. Wykonaj komendę ping z **PC2** do **Server**. Jeśli ping zakończy się niepowodzeniem, to sprawdź adresy IP przed dalszym kontynuowaniem.

b. Z PC2 otwórz przeglądarkę internetową i wprowadź adres IP serwera. Zostanie wyświetlona strona internetowa serwera.

c. Wykonaj połączenie FTP z **PC2** do **Server**. Połączenie powinno zakończyć się niepowodzeniem. Jeśli nie, rozwiąż problemy z instrukcjami listy dostępu i konfiguracjami access-group na interfejsach.