Packet Tracer - Configurarea ACL-urilor extinse - Scenariul 1

Topologie

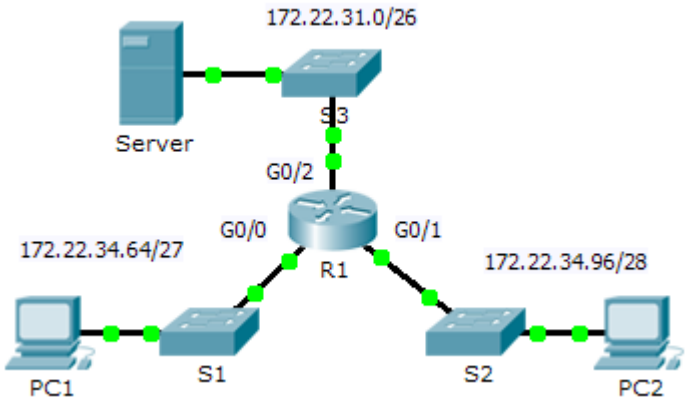

Tabela de Adresare

Echipament	Interfață	Adresă IP	Masca de subrețea	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Obiective

Partea 1 : Configurați , Aplicați și Verificați un ACL Extins Numerotat

Partea 1 : Configurați , Aplicați și Verificați un ACL Extins Numerotat

Context/Scenariu

Doi angajați au nevoie de acces la serviciile furnizate de server. **PC1** are nevoie doar de acces **FTP** în timp ce PC2 are nevoie doar de acces la web. Ambele calculatoare pot da ping la server, dar nu își pot da ping între ele.

Part 1: Configurați, aplicați și verificați un ACL Extins Numerotat

Step 1: Configurați un ACL pentru a permite FTP și ICMP.

a. Din modul de configurare global din **R1**, introduceți următoarea comandă pentru a determina numărul valid pentru o listă de acces extinsă.

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

```
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

b. Adăugați **100** la comandă, urmat de un semn de întrebare.

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

c. Pentru a permite trafic FTP, introduceți **permit**, urmat de un semn de întrebare.

```
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. Acest ACL permite FTP și ICMP. ICMP este afișat mai sus, dar FTP nu, deoarece FTP folosește TCP. Deci introduceți TCP. Introduceți **tcp** pentru a rafina ajutorul ACL.

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

e. Observați că puteți filtra doar PC1 folosind **cuvântul** cheie host sau ați putea permite orice host. În acest caz, orice echipament care are o adresă ce aparține rețelei 172.22.34.64/27 este permis. Introduceți adresa de rețea, urmată de un semn de întrebare.

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

f. Calculați masca wildcard determinând opusul binar al măștii de subrețea.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.00011111 = 0.0.0.31

g. Introduceți masca wildcard, urmată de un semn de întrebare.

```
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. Configurați adresa de destinație. În acest scenariu, filtrăm traficul pentru o singură destinație, serverul. Introduceți cuvântul cheie **host** urmat de adresa IP a serverului.

```
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. Observați că una din opțiuni este **<cr>** (carriage return). Cu alte cuvinte, puteți apăsa **Enter** iar regula va permite tot traficul TCP. În orice caz, permitem doar traficul FTP; așadar, introduceți cuvântul cheie **eq**, urmat de un semn de întrebare pentru a afișa opțiunile disponibile. Apoi, introduceți **ftp** și apăsați pe **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. Creați o a doua listă de acces pentru a permite traficul ICMP (ping, etc.) de la PC1 la Server. Observați că numărul listei de acces rămâne la fel și că un anumit tip de trafic ICMP nu trebuie specificat.

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

k. Restul traficului nu este acceptat, în mod implicit.

Step 2: Aplicați ACL-ul pe interfața corectă pentru a filtra traficul.

Din **perspectiva** lui R1, traficul la care se aplică ACL 100 este de tip inbound din rețeaua conectată la interfața Gigabit Ethernet 0/0. Intrați în modul de configurare al interfeței și aplicați ACL-ul.

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

Step 3: Verificați implementarea ACL.

a. Ping de la **PC1** la **Server**. În cazul în care comenzile ping nu se realizează cu succes , verificați adresele IP înainte de a continua.

b. FTP de la **PC1** la **Server**. Atât numele de utilizator, cât și parola sunt cisco.

```
PC> ftp 172.22.34.62
```

c. Ieșiți din serviciul FTP al Serverului.

```
ftp> quit
```

d. Dați ping de la **PC1** la **PC2**. Hostul de destinație ar trebui să fie inaccesibil, deoarece traficul nu a fost permis în mod explicit.

Part 2: Configurați , Aplicați și Verificați un ACL Extins Numerotat

Step 1: Configurați un ACL pentru a permite ICMP și accesul HTTP.

a. ACL-urile denumite încep cu **ip** ca si cuvânt cheie. Din modul de configurare global **al** lui R1, introduceți următoarea comandă, urmată de un semn de întrebare.

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

b. Puteți configura ACL-urile numite standarde și extinse. Această listă de acces filtrează adrese IP de destinație și sursă; așadar, trebuie extinsă. Introduceți **HTTP_ONLY** ca nume. (Pentru notarea în Packet Tracer, numele este case-sensitive.)

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

c. Prompt-ul se modifică. Acum vă aflați în modul de configurare al ACL-urilor numite extinse. Toate echipamentele din LAN **PC2** au nevoie de acces TCP. Introduceți adresa de rețea, urmată de un semn de întrebare.

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

d. O metodă alternativă pentru a calcula un wildcard este de a scădea masca de subrețea din 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. Finalizați declarația specificând adresa serverului așa cum ați procedat la Partea 1 și filtrând traficul www.

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

f. Creați o a doua listă de acces pentru a permite traficul ICMP (**ping, etc**.) de la PC2 la Server. Notă: Prompt-ul rămâne la fel și nu este necesară specificarea unui anumit tip de trafic ICMP.

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

g. Restul traficului nu este acceptat, în mod implicit. Ieșiți din modul de configurare al ACL-ul extins denumit.

Step 2: Aplicați ACL-ul pe interfața corectă pentru a filtra traficul.

Din perspectiva lui **R1**, traficul care accesează lista **HTTP_ONLY** se aplică la inbound-ul său din rețeaua conectată la interfața Gigabit Ethernet 0/1. Intrați în modul de configurare al interfeței și aplicați ACL-ul.

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

Step 3: Verificați implementarea ACL.

a. Dați ping de la **PC2** la Server. Dacă ping-urile nu se realizează, verificați adresele IP înainte de a continua.

b. Conectați-vă prin **FTP** de la PC2 la Server. Conexiunea ar trebui să eșueze.

c. Deschideți browser-ul web pe **PC2** și introduceți adresa IP a Serverului ca **URL**. Conexiunea ar trebui să se realizeze cu succes.