Lab Guide & Module

Cisco Certified Network Associate 200-301 V.1.1

7. Access Control List

Salah satu skill penting yang harus dikuasai oleh network engineer adalah Access Control Lists (ACLS). Kita dapat menggunakan ACLs untuk permit/deny traffic di jaringan yang kita manage. Standard dan extended ACLs dapat menerapkan sejumlah fitur keamanan, termasuk policy-based routing, quality of service (QoS), Network Address Translation (NAT), dan Port Address Translation (PAT). Kita juga bisa melakukan konfigurasi standard dan extended ACLs pada interface router untuk mengontrol jenis traffic yang diizinkan melalui router tertentu.

Jenis-jenis ACL

- Standard IPv4 ACL: Melakukan filtering berdasarkan IP source host/network saja.
- Extended IPv4 ACL: Melakukan filtering berdasarkan source dan destination IP, Protocol, serta nomor port TCP dan UDP.

Metode Konfigurasi ACL

Kita bisa menggunakan dua metode untuk mengidentifikasi standard maupun extended ACLS:

- Numbered IPv4 ACL: Menggunakan nomor untuk identifikasi.
- Named IPv4 ACL: Menggunakan nama deskriptif atau nomor untuk identifikasi.

Named IP ACLs memberikan fleksibilitas lebih dalam bekerja dengan entri ACL. Selain menggunakan nama yang lebih mudah diingat, menggunakan named ACLs daripada numbered ACLs memungkinkan kita untuk menghapus statement ACL per nomor sequence.

Configuration Guide ACL

- Berdasarkan skenario di lapangan sesuaikan ACL standard atau extended, numbered atau named.
- Hanya satu ACL yang diizinkan per protokol, per direction, dan per interface.
- Susun ACL untuk memungkinkan pemrosesan dari sequence atas ke bawah. Buat statement ACL dari yang spesifik ke yang paling umum.
- Semua ACL memiliki statement implicit deny any di sequence akhir.
- Buat ACL dahulu sebelum memasang ke interface.

- Biasanya, extended ACL dikonfigurasikan sedekat mungkin dengan source traffic. Sebaliknya standard ACL dikonfigurasikan sedekat mungkin dengan destination traffic. Ini dikarenakan standard ACL tidak menentukan alamat tujuan, sehingga kita perlu memasangnya di perangkat yang paling dekat dengan destination traffic.

7.1 Standar ACL

Skenario Standar ACL #1

Blokir network 192.168.10.0/24 dalam mengakses network server 192.168.20.0/24

R3

```
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255

R3(config)#access-list 1 permit any

R3(config)#int fa0/1

R3(config-if)#ip access-group 1 out

R3(config-if)#end

R3#show access-list
```

Untuk skenario ini kita perlu melakukan konfigurasi Standard ACL di Router Interface yang paling dekat dengan destination, yakni R3 Interface Fa0/1.

Percobaan test ping dari PC1:

PC1

```
C:\>ping -n 2 192.168.20.10
```

Percobaan test ping dari R2:

R2

```
R2>ping 192.168.20.10
```

Mari kita lihat perintah verifikasi show access-list di R3. Pastikan sudah ada matches traffic di masing-masing rule ACL.

R3

```
R3#show access-list
```

Skenario Standar ACL #2

Dari network 192.168.10.0/24, hanya perbolehkan IP 192.168.10.2/32 untuk mengakses segmen network server 192.168.20.0/24

R3

```
R3(config)#ip access-list standard 1

R3(config-std-nacl)#5 permit host 192.168.10.2

R3(config-std-nacl)#do show acc
```

Pada activity ini, kita menggunakan Named ACL untuk meng-edit ACL group number 1. Kita perlu menggunakan mode Named ACL dikarenakan pada mode ini, kita dapat mengubah sequence rule ACL secara manual.

Skenario Standar ACL #3

Batasi akses telnet/ssh R3, supaya hanya dapat diakses dari IP host 192.168.10.2 saja.

R3

```
R3(config) #access-list 2 permit host 192.168.10.2

R3(config)#

R3(config)#! lanjut konfigurasi remote access telnet/ssh

R3(config)#

R3(config)#username cisco secret cisco

R3(config)#username idn secret idnmantab
```

```
R3(config)#enable secret cisco

R3(config)#

R3(config)#ip domain-name idn.id

R3(config)#crypto key generate rsa general-key modulus 1024

R3(config)#

R3(config)#line vty 0 4

R3(config-line)#login local

R3(config-line)#access-class 2 in

R3(config-line)#end
```

Pengetesan

PC1

```
C:\>telnet 192.168.20.1
```

R2

```
R2>telnet 192.168.20.1
```

7.2 Extended ACL

Skenario Extended ACL #1

Blokir network 192.168.10.0/24 untuk mengakses server layanan HTTP dan FTP ke server 192.168.20.10. Lalu blokir juga akses ICMP (PING) ke ntwork 192.168.20.0/24

R1

```
R1(config)#ip access-list extended PC-SERVER

R1(config-ext-nacl)#deny tcp 192.168.10.0 0.0.0.255 host 192.168.20.10 eq 80

R1(config-ext-nacl)#deny tcp 192.168.10.0 0.0.0.255 host 192.168.20.20 eq ftp

R1(config-ext-nacl)#deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
```

```
R1(config-ext-nacl)#permit ip any any

R1(config-ext-nacl)#exit

R1(config)#

R1(config)#int range fa0/1

R1(config-if-range)#ip access-group PC-SERVER in

R1(config-if-range)#end
```

Untuk skenario ini kita perlu melakukan konfigurasi Extended ACL di Router Interface yang paling dekat dengan source, yakni R1 Interface Fa0/1.

Skenario Extended ACL #2

- Hanya perbolehkan akses SSH ke R3, dari network 192.168.10.0/24
- blokir akses ping ke semua IP yang ada pada R3.

R3

```
access-list 102 permit tcp 192.168.10.0 0.0.0.255 any eq 22

access-list 102 deny tep any any eq 22

access-list 102 deny icmp 10.0.0.0 0.0.0.255 any echo

access-list 102 permit ip any any

interface Fa0/0

 ip access-group 101 in

interface s0/0/0

 ip access-group 101 in
```

Untuk skenario ini kita dapat melakukan konfigurasi Extended ACL di Router Interface yang mengarah ke R3 dari traffic incoming R1, yakni R3 Interface Fa0/0 dan 50/0/0.