Master Jaringan

panduan untuk belajar menjadi master jaringan yang meliputi : CISCO , DEBIAN , LINUX , MATERI , MIKROTIK , and OTHER

ACCESS LIST di Cisco Packet Tracer

Penulis **Unknown**

CISCO

Assalamualaikum wr.wb
kali ini saya akan share tentang cara menggunakan ACL yang berguna untuk memfilter packet, sebelum kita masuk ke konfigurasi lebih dulu kita harus tahu apa itu ACL?

A. Pengertian

Access List digunakan untuk mem-filter paket yang akan masuk maupun keluar dari Router. Dimana ada paket ingin masuk/keluar maka akan diproses terlebih dahulu di Access List ini. Maka jika ada paket yang tidak sesuai kriteria maka akan di drop , sesuai dengan kebijakan yang kita buat.
Yang perlu diketahui tentang Access List ini adalah : Metode dalam penerapan ACL :

• Inbound access-list : Paket akan difilter ketika masuk.

• Outbound access-list : Paket akan difilter ketika ingin keluar.

ACL dibagi menjadi 2 Jenis :

• Standard Access List : Melakukan filtering berdasarkan IP Host atau network Source nya saja. Standar ACL menggunakan nomer ACL 1 – 99.

• Extended Access List : Penerapan Filteringnya lebih spesifik, bisa melakukan filtering berdasarkan destination , protocol dan port yang digunakan. Extended ACL menggunakan Nomer ACL 100 – 199 .

Terdapat 3 Opsi dalam penerapan ACL :

• Permit : Mengijinkan

• Deny : Menolak

• Remark : Memberikan komentar

B. Latar Belakang

dengan adanya ACL ini kita dapat mengatur jika ada yang mau difilter packet - packet tertentu agar tidak melewati router sehingga packet tersebut tidak akan sampai pada server

C. Persiapan Software dan Hardware

- PC dengan sistem operasi bebas
- aplikasi packet tracer
- modul

D. Maksud dan Tujuan

1. Dapat memahami lebih dalam tentang fungsi ROUTER
2. Dapat menkonfigurasi router agar bisa mengkonfigurasi ACL
3. Dapat memefilter packet sesuai dengan yang kita inginkan

E. Tahapan dan Pelaksanaan

akan ada 2 tahapan untuk praktek kali ini :

Standard Access List

1 pertama buka aplikasi cisco terlebih dahulu

2 lalu kita buat topologi seperti berikut :

3 pertama kita konfigurasi IPnya sesuai dengan topologi diatas, agar lebih mudah kita gunakan DHCP server pada router

4 konfigurasi pada router 1 :

```
Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gi 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#ip dhcp pool dhcp1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#ex
Router(config)#ip dhcp e
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#int gi 0/0
Router(config-if)#ip address 12.12.12.1 255.255.255.0
Router(config-if)#no sh
```

5 lalu pada router 0 :

```
Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)#int gi 0/0
Router(config-if)#ip address 12.12.12.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#int gi 0/1
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#ip dhcp pool dhcp2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.2
Router(dhcp-config)#ip dhcp excluded-address 192.168.2.2
Router(config)#
```

6 lalu kita lakukan Routing pada kedua router tersebut :

Router 1 :

```
Router(config)#ip route 192.168.2.0 255.255.255.0 12.12.12.2
```

Router 0 :

```
Router(config)#ip route 192.168.1.0 255.255.255.0 12.12.12.1
```

7 sekarang kita coba ping dari client ke server

8 sekarang baru kita konfigurasinya untuk ACL, kita akan memfilter PC 1 agar tidak bisa mengirim packet ke server, untuk topologi diatas kita akan konfigurasi interface gi 0/0 pada router 0, perintahnya adalah sebagai berikut :

```
Router(config)#access-list 1 deny 192.168.1.3 0.0.0.0
Router(config)#access-list 1 permit any
Router(config)#int gi0/1
Router(config-if)#ip access-group 1 out
```

9 lalu sekarang kita coba tes ping dari PC 1 :

terbukti bahwa PC 2 tidak bisa ping ke server karena kita tadi telah memfilter PC tersebut agar tidak bisa mengirim packet ke server

10 sekarang kita tes ping dari PC 0 :

PC 1 bisa ping ke server karena tidak di filter

11 sekarang kita coba untuk memfilter satu network, jika kita membuat access list yang baru maka access list yang lama akan terhapus, jadi tidak masalah jika nomer access listnya kita ganti nomernya selama noomer nya 1 - 99

12 untuk memfilter satu network yang kita masukan adalah network lalu wildcard dari network tersebut :

```
Router(config-if)#Router(config)#access-list 2 deny 192.168.1.0
0.0.0.255
Router(config)#access-list 2 permit any
Router(config)#int gi0/1
Router(config-if)#ip access-group 2 out
Router(config-if)#
```

13 lalu kita coba tes dengan ping ke server, PC 0 :

14 PC 1 :

Extended Access List

Selanjutnya kita masuk ke bagian Extended nya , dengan extended ini kita bisa menfilter paket lebih spesifik , baik dari port , protocol dan destinationnya. Kalau standard hanya bisa mentraffic berdasarkan source saja. Extended ini menggunakan nomer ACL 100 – 199. Kita masih melanjutkan lab sebelumnya jadi , topologi nya masih sama

1 pertama buka aplikasi cisco terlebih dahulu

2 lalu buatlah topologi seperti berikut :

3 konfigurasi IPnya sesuai topologi, untuk cara nya bisa dilihat pada konfigurasi di atas tadi saat bab Standart Access List, jadi saya tidak akan menampilkanya lagi

4 langsung ke konfigurasi ACL nya, untuk konfigurasi kali ini kita konfigurasi pada Router yang paling dekat dengan Client, dan juga jika tadi nomernya harus 1 - 99 untuk Extended ini kita harus menggunakan nomer 100 - 199

5 untuk praktek kali ini kita akan melakukan drop www pada PC 0, sehingga PC tersebut tidak akan bisa mengakses WEB server tapi masih bisa ping, untuk melakukanya bisa menggunakan perintah seperti berikut :

```
Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 deny tcp 192.168.1.2 0.0.0.0 host
192.168.2.1 eq 80
Router(config)#access-list 100 permit ip any any
Router(config)#int gi 0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

6 sekarang kita coba tes dengan ping dari PC 0 ke server :

kita masih bisa ping karena yang kita filter tadi cuma port 80 nya yaitu port untuk WEB server

7 sekarng kita coba dari PC 0 tersebut mengakses WEB server :

terbukti PC 0 tidak bisa mengakses WEB server dikarenakan pada router 1 tadi telah dikonfigurasi ACL untuk memfilter PC tersebut agar tidak bisa mengirim packet melalui PORT 80

8 sekarng kita coba mengakses WEB server melalui PC 1 :

di situ terbukti bahwa PC 1 bisa mengakses WEB server karena tadi yang difilter cuma PC 0

9 untk melihat ACL yang di deny dan permit kita bisa menggunakan perintah "show accesst-list [nomer ACL]"

disitu terlihat ada 12 paket yang di deny dan 9 packet yang di permit

F. Referensi

- **modul cisco IDN.pdf**

G. Hasil dan Kesimpulan

dari praktek di atas menunjukan bahwa kita bisa memfilter packet yang di kirim sesuai dengan yang kita inginkan , dengan cara mengkonfigurasi ACL pada router sehingga router tidak akan bisa di lewati packet seperti yang telah kita konfigurasi

4 comments

Balas

LOVELYZ TRILOGY August 27, 2019 at 1:53 PM

Warning!! SPAM has been detected!

Balas

Salsabila Amalia Febra November 14, 2019 at 2:10 PM

pusinggg sumpah

Balas

Anonymous February 10, 2021 at 2:36 PM

Min berarti aclnya gimana?

Balas

Anonymous December 27, 2023 at 10:43 PM

min kalo ingin merubah nilai dari prority acl gimana saya ingin rulenya bisa tempatnya diatas

Emoticon

Enter Comment

Cari artikel...

Blog Archive

- September (12)
- August (40)
- July (35)

Label

- CISCO
- DEBIAN
- LINUX
- MATERI
- MIKROTIK
- OTHER

Mengenai Saya

Unknown

View my complete profile

Popular Post

ACCESS LIST di Cisco Packet Tracer

Assalamualaikum wr.wb kali ini saya akan share tentang cara ...

Cara instalasi debian 8.5

assalamualaikum wr. wb. kali ini saya akan share tentang car...

SOAL! Membuat Jaringan gabungan Routing BGP dan OSPF

Assalamualaikum wr.wb Saya mendapat soal dari suatu master ci...

Kategori

Pilih Kategori

Artikel Terbaru

About

Google today announced IT admins can now apply policies to Chrome on Android and iOS, in addition to Windows, Mac, Linux, and Chrome OS.

Web Tools

- Contact Form
- Disclaimer
- Privacy Policy
- Sitemap
- Terms of Service

Newsletter

Berlangganan artikel terbaru dari blog ini langsung via email.

Email address Submit