Modul 11 Access Control Lists (ACLs)

Pendahuluan

ACL sederhananya digunakan untuk mengijinkan atau tidak paket dari host menuju ke tujuan tertentu. ACL terdiri atas aturan-aturan dan kondisi yang menentukan trafik jaringan dan menentukan proses di router apakah nantinya paket akan dilewatkan atau tidak. Modul ini akan menerangkan standard an extended ACL, penempatan ACL dan beberapa aplikasi dari penggunaan ACL.

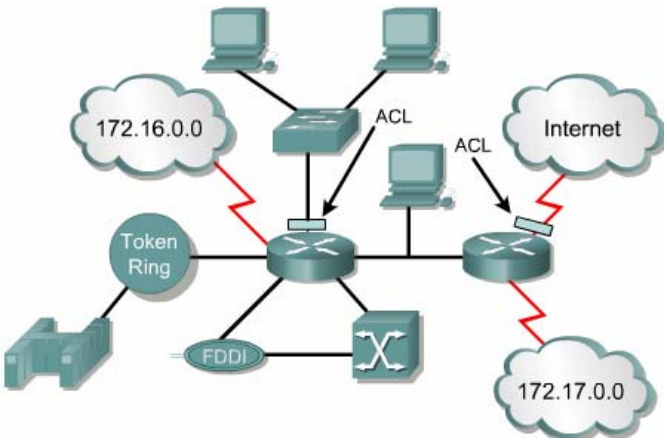
Setelah melalui modul ini diharapkan mahasiswa mampu:

- Menggambarkan perbedaan anatar standard an extended ACL
- Menjelaskan aturan-aturan untuk penempatan ACL
- Membuat dan mengaplikasikan ACL
- Menggambarkan fungsi dari firewall
- Menggunakan ACL untuk mem-blok akses virtual terminal

1. Dasar ACL

1.1 Pendahuluan

ACL adalah daftar kondisi yang digunakan untuk mengetes trfaik jaringan yang mencoba melewati interface router. Daftar ini memberitahu router paket-paket mana yang akan diterima atau ditolak. Penerimaan dan penolakan berdasarkan kondisi tertentu.

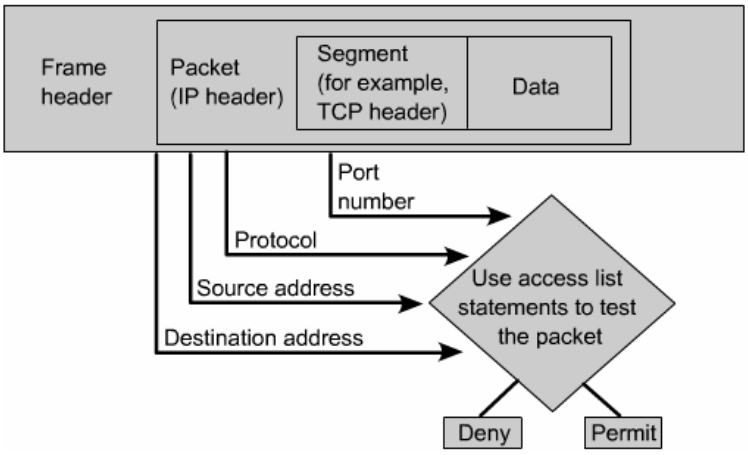


Gambar 1.1 ACL

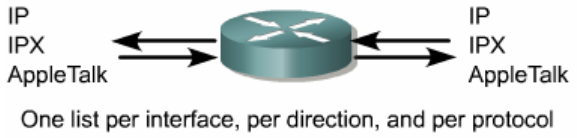
Untuk mem-filter trafik jaringa, ACL menentukan jika paket itu dilewatkan atau diblok pada interface router. Router ACL membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port.

ACL harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACL harus didefinisikan setiap protokol pada interface. ACL kontrol trafik pada satu arah dalam interface. Dua ACL terpisah harus dibuat untuk mengontrol trafik inbound dan outbound. Setiap interface boleh memiliki banyak protokol dan arah yang sudah didefinisikan. Jika router mempunyai dua interface diberi IP, AppleTalk

dan IPX, maka dibutuhkan 12 ACL. Minimal harus ada satu ACL setiap interface.



Gambar 1.2 Cisco ACL memeriksa paket pada header upper-layer

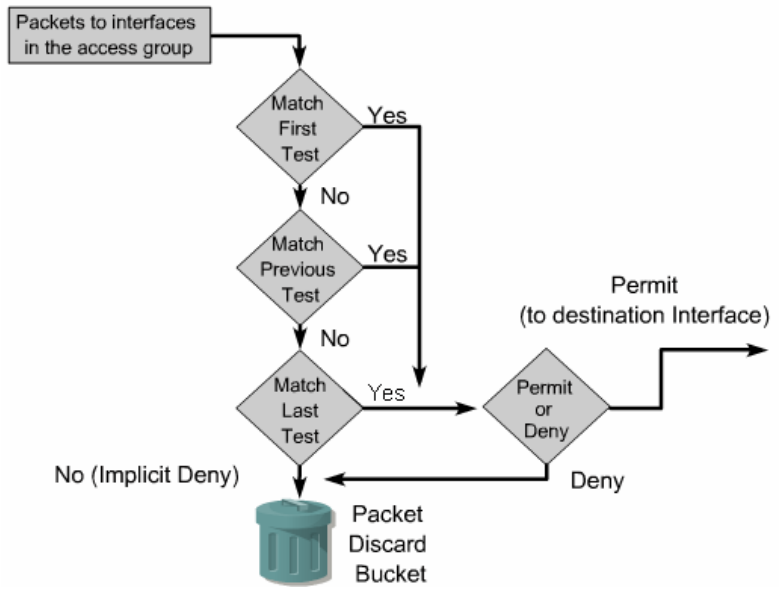


Gambar 1.3 Grup access list dalam Router

Berikut ini adalah fungsi dari ACL:

- Membatasi trafik jaringan dan meningkatkan unjuk kerja jaringan. Misalnya, ACL memblok trafik video, sehingga dapat menurunkan beban jaringan dan meningkatkan unjuk kerja jaringan.
- Mengatur aliran trafik. ACL mampu memblok update routing. Jika update tidak dibutuhkan karena kondisi jaringan, maka bandwidth dapat dihemat.
- Mampu membrikan dasar keamanan untuk akses ke jaringan. Misalnya, host A tidak diijinkan akses ke jaringan HRD dan host B diijinkan.
- Memutuskan jenis trafik mana yang akan dilewatkan atau diblok melalui interface router. Misalnya, trafik email dilayani, trafik telnet diblok.
- Mengontrol daerah-daerah dimana klien dapat mengakses jaringan.
- Memilih host-hots yang diijinkan atau diblok akses ke segmen jaringan. Misal, ACL mengijinkan atau memblok FTP atau HTTP.

1.2 Cara kerja ACL



Gambar 1.4 Cara kerja ACL

Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses.

Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jika alamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound. Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch ke interface itu. Selanjutnya router memriksa apakah interface tujuan mempunyai ACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paket cocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paket dienkapsulasi di layer 2 dan di-forward keluar interface device berikutnya.

1.3 Membuat ACL

Ada dua tahap untuk membuat ACL. Tahap pertama masuk ke mode global config kemudian memberikan perintah **access-list** dan diikuti dengan parameter-parameter. Tahap kedua adalah menentukan ACL ke interface yang ditentukan.

Dalam TCP/IP, ACL diberikan ke satu atau lebih interface dan dapat memfilter trafik yang masuk atau trafik yang keluar dengan menggunakan perintah **ip access-group** pada mode configuration interface. Perintah **access-group** dikeluarkan harus jelas dalam interface masuk atau keluar. Dan untuk membatalkan perintah cukup diberikan perintah **no access-list list-number**.

Aturan-aturan yang digunakan untuk membuat access list:

- Harus memiliki satu access list per protokol per arah.
- Standar access list harus diaplikasikan ke tujuan terdekat.
- Extended access list harus harus diaplikasikan ke asal terdekat.
- Inbound dan outbound interface harus dilihat dari port arah masuk router.
- Pernyataan akses diproses secara sequencial dari atas ke bawah sampai ada yang cocok. Jika tidak ada yang cocok maka paket ditolak dan dibuang.
- Terdapat pernyataan **deny any** pada akhir access list. Dan tidak kelihatan di konfigurasi.
- Access list yang dimasukkan harus difilter dengan urutan spesifik ke umum. Host tertentu harus ditolak dulu dan grup atau umum kemudian.
- Kondisi cocok dijalankan dulu. Diijinkan atau ditolak dijalankan jika ada pernyataan yang cocok.
- Tidak pernah bekerja dengan access list yang dalam kondisi aktif.
- Teks editor harus digunakan untuk membuat komentar.
- Baris baru selalu ditambahkan di akhir access list. Perintah **no access-list x** akan menghapus semua daftar.
- Access list berupa IP akan dikirim sebagai pesan ICMP host unreachable ke pengirim dan akan dibuang.
- Access list harus dihapus dengan hati-hati. Beberapa versi IOS akan mengaplikasikan default deny any ke interface dan semua trafik akan berhenti.
- Outbound filter tidak akan mempengaruhi trafik yang asli berasal dari router local.

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Gambar 1.5 protokol dengan ACL berdasar nomor

```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
0.255.255.255
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Gambar 1.6 perintah access-group

1.4 Fungsi dari wildcard mask

Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address. Wildcard mask mewakili proses yang cocok dengan ACL mask-bit. Wildcard mask tidak ada hubungannya dengan subnet mask.

Wildcard mask dan subnet mask dibedakan oleh dua hal. Subnet mask menggunakan biner 1 dan 0 untuk mengidentifikasi jaringan, subnet dan host. Wildcard mask menggunakan biner 1 atau 0 untuk memfilter IP address individual atau grup untuk diijinkan atau ditolak akses. Persamaannya hanya satu dua-duanya sama-sama 32-bit.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255

Can be written as:
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0

Can be written as:
Router(config)#access-list 1 permit host 172.30.16.29
```

Gambar 1.7 any dan host Option

Ada dua kata kunci di sini yaitu **any** dan host. **Any** berarti mengganti 0.0.0.0 untuk IP address dan 255.255.255.255 untuk wildcard mask. **Host** berarti mengganti 0.0.0.0 untuk mask. Mask ini membutuhkan semua bit dari alamat ACL dan alamat paket yang cocok. Opsi ini akan cocok hanya untuk satu alamat saja.

1.5 Verifikasi ACL

Untuk menampilkan informasi interface IP dan apakah terdapat ACL di interface itu gunakan perintah **show ip interface**. Perintah **show access-lists** untuk menampilkan isi dari ACL dalam router. Sedangkan perintah **show running-config** untuk melihat konfigurasi access list.

```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 2
Serial0/0 is down, line protocol is down
  Internet address is 200.200.2.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
```

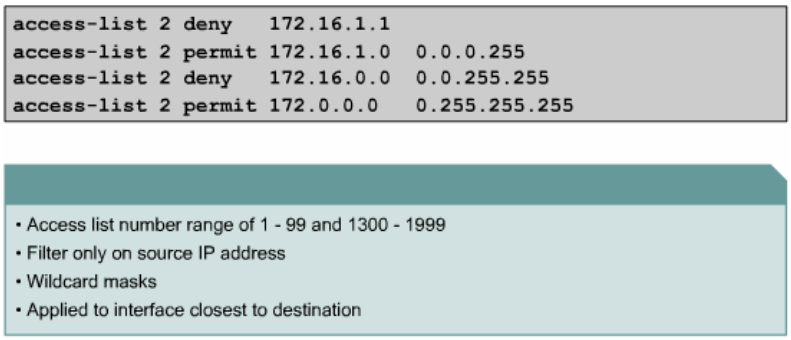
Gambar 1.8 standar ACL

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Gambar 1.9 pernyataan standar ACL

2. Access Control Lists

Standar access-list digunakan untuk mendefinisikan standar ACL dengan nomor antara 1 sampai 99 (dan juga antara 1300 sampai 1999 pada IOS yang baru).



Gambar 2.1 Pernyataan standar ACL

Untuk Cisco IOS Software Release 12.0.1, standar ACL dimulai dengan 1300 sampai 1999 untuk menyediakan kemungkinan ACL 798. Pada gambar di atas ACL pertama, menunjukkan tidak ada wildcard mask. Dan default mask 0.0.0.0 diguanakan. Sintak lengkap perintah ACL adalah:

```
Router(config)#access-list access-list-number deny permit
remark source [source-wildcard] [log]
```

Kata kunci remark membuat access list lebih muda untuk dimengerti. Setiap remark dibatasi sampai 100 karakter. Sebagai contoh:

```
Router(config)#access-list 1 permit 172.69.2.88
```

Lebih mudah lagi dengan entri yang lebih spesifik:

```
Router(config)#access-list 1 remark Permit only Jones
workstation through access-list 1 permit 171.69.2.88
```

Perintah no untuk menghapus ACL:

```
Router(config)#no access-list access-list-number
```

Perintah ip access-group ACL dihubungkan dengan interface:

```
Router(config-if)#ip access-group {access-list-number |
access-list-name} {in | out}
```

Kesimpulan

- ACL adalah daftar urutan pernyataan penerimaan atau penolakan yang dijalankan untuk pengalamatan atau protokol layer atas
- Penempatan dan urutan pernyataan ACL adalah hal yang sangat penting untuk unjuk kerja jaringan
- Standar ACL digunakan untuk memeriksa alamat asal dari paket yang akan dirutekan
- Sedangkan extended ACL digunakan lebih spesifik daripada standar ACL yang menyediakan lebih banyak parameter dan argumen