**LAPORAN PRAKTIKUM LAB**

**ACL(Access Control List)**

**Untuk memenuhi Tugas Mata Kuliah Jaringan Komputer Lanjut**

Dosen pengampu :

**Farizqi Panduardi, S.ST. M.T**



Disusun oleh :

Erica Septiyana (361955401165 / 2F)

**PROGRAM STUDI DIPLOMA III**

**TEKNIK INFORMATIKA**

**POLITEKNIK NEGERI BANYUWANGI**

**2021**

**Modul 9 ACL**

**(Acces Control List)**

Access Control Lists digunakan untuk menguji trafik jaringan yang mencoba melewati interface router. ACLs ini diimplementasikan pada router yang dijadikan gateway yang menghubungkan jaringan LAN dan WAN. Untuk mem-filter trafik jaringan, ACLs menentukan jika paket itu dilewatkan atau diblok pada interface router. Router ACLs membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port. Tanpa Access list, semua paket bisa terpancarkan ke semua bagian dari jaringan. ACLs harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACLs harus didefinisikan setiap protokol pada interface. ACLs kontrol trafik pada satu arah dalam interface.

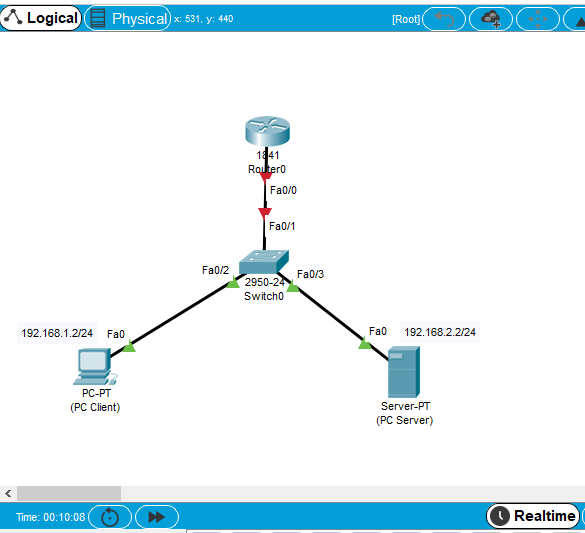
Setiap interface boleh memiliki banyak protokol dan arah yang sudah didefinisikan. Jika router mempunyai dua interface diberi IP, AppleTalk dan IPX, maka dibutuhkan 12 ACL. Minimal harus ada satu ACLs setiap interface. Ketika sudah di ketahui apa yang akan di filter, langkah berikutnya adalah untuk menentukan lalu lintas mana yang akan di filter. Perangkat lunak Cisco IOC mempergunakan pemfilteran logika dari sebuah ACL yang salah satunya sebagai sebuah paket yang masuk ke dalam interface atau keluar dari interface. Setelah memiliki pilihan router dimana akan di letakkan access list, dan harus memilih interface dimana akan digunakan access logika, sebagaimana menggunakan logika untuk inbound (Ketika sebuah ACL diterapkan pada paket inbound di sebuah interface, paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan)atau outboundpaket (Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut diroute ke outbound interface dan diproses melalui ACL malalui antrian).

Menerapkan ACL menyebabkan router menganalisa setiap paket arah spesifik yang melalui interface tersebut dan mengmbil tindakan yang sesuai. Rule yang harus di ikuti ketika ingin membandingkan paket dengan ACL :

* Paket selalu dibandingkan dengan setiap baris dari ACL secara berurutan
* Paket hanya dibandingkan baris-baris ACL sampai terjadi kecocokan
* Terdapat statement “tolak” yang tersembunyi (impilicit deny) pada setiap akhir baris ACL, ini artinya bila suatu paket tidak cocok dengan semua baris kondisi pada ACL, paket tersebut akan ditolak.

**Praktikum :**

1. Membuat jaringan seperti berikut dengan menggunakan 1 router, i switch dan 2 PC.



1. Merubah IP di PC dan menambahkan gateway

PC Client dengan perintah:

# ifconfig eth0 192.168.1.2 netmask 255.255.255.0

# route add -net default gw 192.168.1.1

PC Server dengan perintah:

# ifconfig eth0 192.168.2.2 netmask 255.255.255.0

# route add -net default gw 192.168.2.1

1. Setting IP di masing-masing interface Router

* Konfigurasi port fastethernet dan berikan ip address pada port tersebut Konfigurasi pada interface fastethernet 0/0. Dengan perintah :

Router(config)# interface fastethernet 0/0

Router(config-if) # ip address 192.168.1.1 255.255.255.0

Router(config-if) # no shutdown

Router(config-if) # CTRL+Z

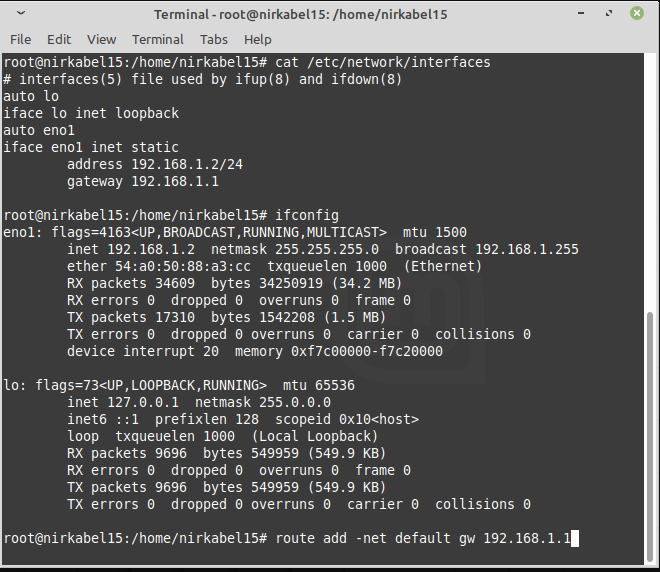
* Konfigurasi pada interface fastethernet 0/1. Dengan Perintah :

Router(config)# interface fastethernet 0/1

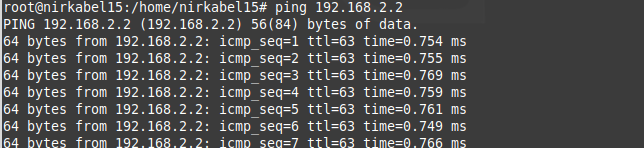
Router(config-if) # ip address 192.168.2.1 255.255.255.0

Router(config-if) # no shutdown

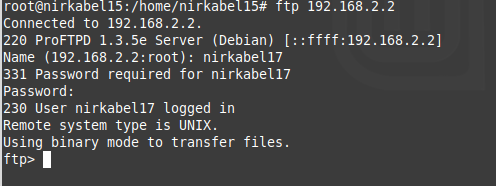
1. Tes koneksi dari PC Client ke PC Server
2. Melihat ip address dan gateway



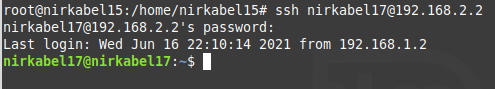
1. Ping dari Client ke Server



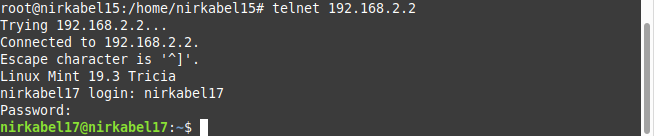
1. Tes ftp dari client ke server



1. Ssh dari client ke server 192.168.2.2

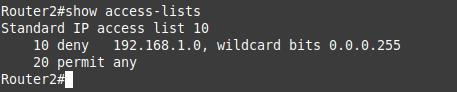


1. Telnet dari pc client ke server 192.168.2.2

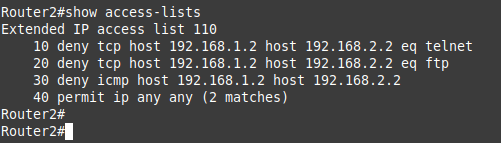


1. Setting ACL pada Router, kemudian hapus ACL yang sebelumnya. Buat suatu rule di router seperti berikut : Tolak akses Telnet, FTP dan pinng dari PC Client, ijinkan akses web dan SSH dari PC Client.

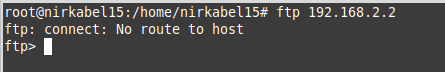
* ACL sebelumnya:



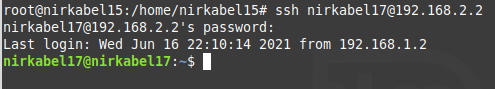
* ACL pada Ping, Telnet, dan FTP



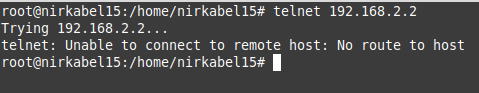
1. Melakukan tes koneksi FTP, SSH, Telnet, dan Ping kembali
2. Tes FTP



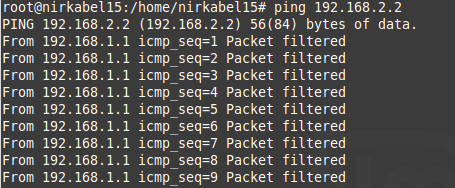
1. Tes SSH



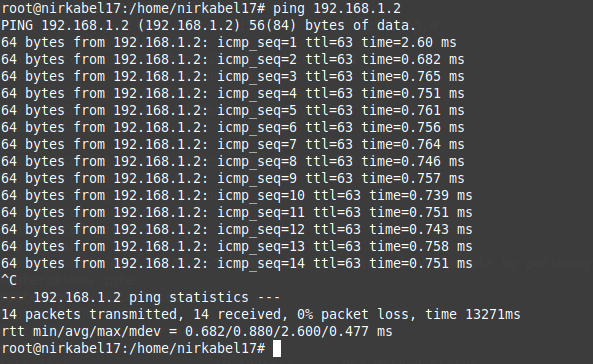
1. Tes Koneksi Telnet



1. Tes Koneksi Ping



1. Tes Koneksi Web Server ke Client



**Kesimpulan :**

ACL digunakan untuk memfilter paket-paket yang keluar masuk jaringan melalui router. Dalam praktikum ini kita dapat melakukan koneksi dari Web server ke client dann dari Ssh ke client, hal ini karena akses ACL hanya diberikan ke FTP, Telnet, dan Ping.