

Praktikum 3

1. Pengantar

Firewall adalah sebuah perangkat lunak yang digunakan untuk menyaring paket data yang masuk maupun keluar dari sistem.

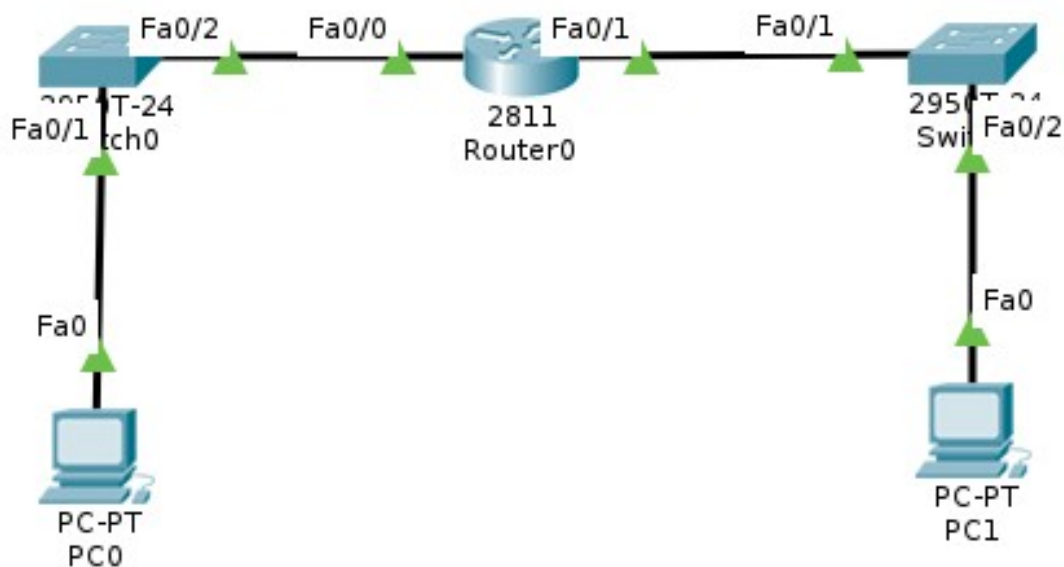
Firewall sendiri memiliki dua macam jenis, yaitu Software Firewall, dan Hardware khusus Firewall.

Praktikum kali ini akan membahas bagaimana melakukan konfigurasi Firewall di Router dan di PC

Dengan menggunakan simulasi PING untuk melakukan pengecekan apakah paket ditolak atau tidak

2. Pembahasan

1. Buatlah topologi seperti dibawah ini



2. Kemudian berikan IP masing-masing Router dan PC

Tempat	IP – Subnet Mask
PC0	192.168.1.2 – 255.255.255.0
Default Gateway	192.168.1.1
Router Fa0/0	
PC1	192.168.2.2 – 255.255.255.0
Default Gateway	192.168.2.1
Router Fa0/1	

3. Konfigurasi Routing Otomatis dengan perintah-perintah ini:

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
```

4. Lakukan tes koneksi dengan perintah PING 192.168.2.2 dari komputer PC0, atau 192.168.1.2 dari komputer PC1

5. Konfigurasi Access-List (Firewall) dengan perintah-perintah ini:

```
Router(config)#access-list 1 deny host 192.168.1.2
Router(config)#interface Fa0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

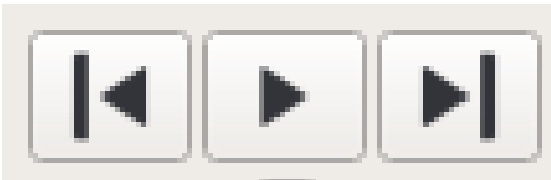
6. Lakukan Simulasi untuk mengecek apakah paket ditolak atau tidak, dari PC0 ke PC1, tekan Icon message di atas atau di samping kanan tergantung versi. Lalu klik ke PC0 ke PC1.



7. Lalu tukar mode dari RealTime ke Simulation Mode:



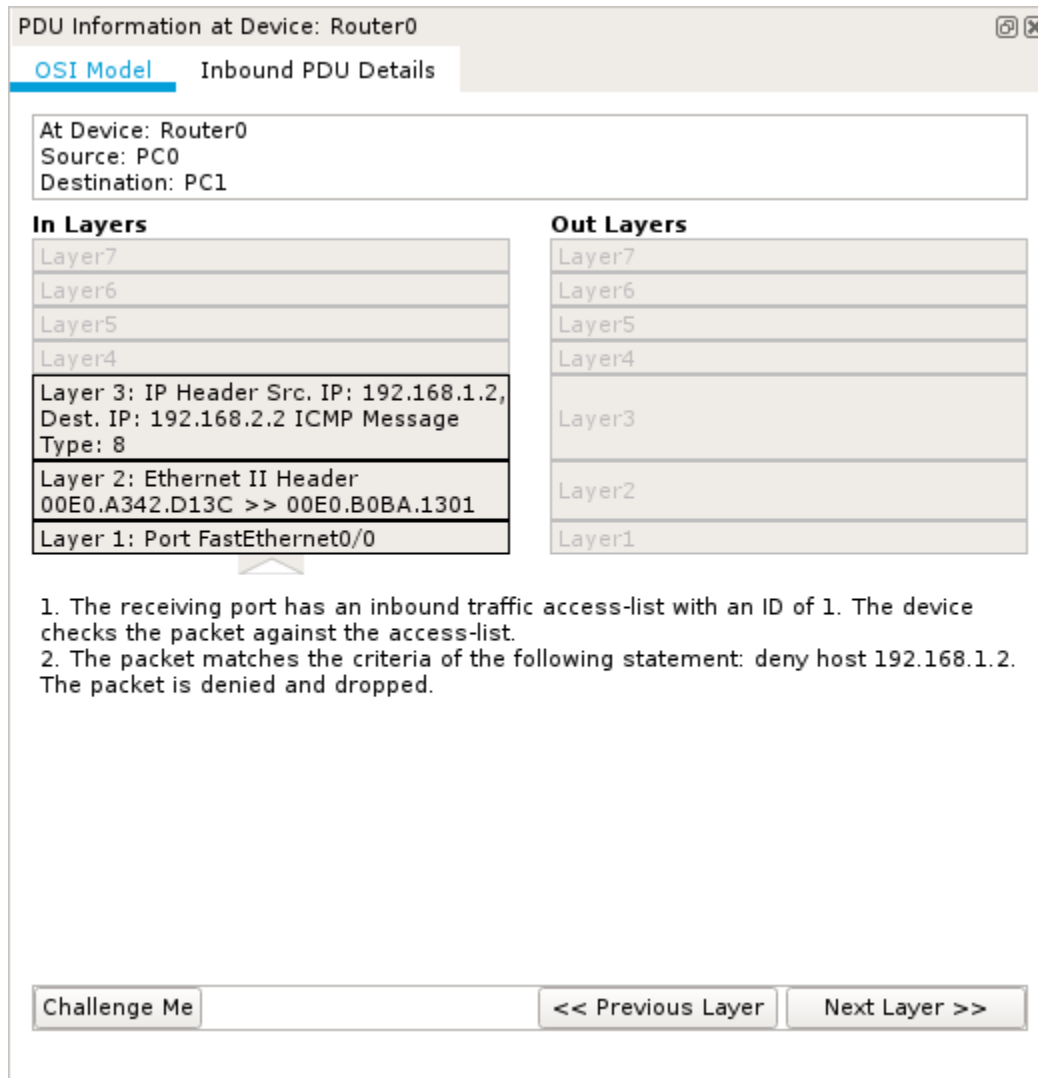
8. Tekan tombol Fast Forward, untuk mengecek di mana paket tersebut akan di drop.



9. Setelah menemukan tempat di mana paket tersebut drop, klik paket di antara Switch0 dan Router0

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	Router0	ICMP
	0.002	--	Router0	ICMP

10. Lalu akan muncul sebuah PDU Information window, lalu klik Layer 3 di window tersebut.



11. Deskripsi no 2 menjelaskan bahwa paket sesuai kriteria dan paket ditolak.

12. Kemudian, hapus Rules yang sudah dikonfigurasi dengan perintah:

```
Router(config)#interface Fa0/0
Router(config-if)#no ip access-group 1 in
Router(config-if)#no ip access-group 1 out
Router(config-if)#exit
Router(config)#no access-list 1
Router(config)#
```

13. Setelah filter dihapus, cek kembali koneksi dengan PING dari PC0 ke PC1 dan harus berhasil.
14. Buka window PC1 dengan cara di klik, lalu klik Firewall. Lalu isi dengan data berikut:



PC1

Physical Config **Desktop** Programming Attributes

Firewall [X]

Service ☒ On ☐ Off

Interface FastEthernet0

Inbound Rules

Action Deny Protocol ICMP

Remote IP 192.168.1.2 Remote Wildcard Mask 0.0.0.255

Remote Port Local Port

Save Remove Add

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Deny	ICMP	192.168.1.2	0.0.0.255	-	-

☐ Top

Action: Deny | Protocol: ICMP | Remote IP 192.168.1.2 | Wildcard Mask: 0.0.0.255 lalu klik Add, dan Service ON

15. Gunakan simulasi kembali untuk mengecek apakah paket di drop atau tidak. Dengan menggunakan cara 7-10. Pastikan terlebih dahulu di mana paket di drop sebelum memilih PDU Information Window.

PDU Information at Device: PC1

OSI Model Inbound PDU Details

At Device: PC1
Source: PC0
Destination: PC1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.2.2 ICMP Message Type: 8	Layer3
Layer 2: Ethernet II Header 00E0.B0BA.1302 >> 0001.4260.637E	Layer2
Layer 1: Port FastEthernet0	Layer1

1. The receiving device has an inbound traffic firewall. The pc checks the packet against the firewall.
2. The packet matches the criteria of the following statement: deny icmp 192.168.1.0 0.0.0.255 any. The packet is denied and dropped.

Challenge Me << Previous Layer Next Layer >>

16. Klik layer 3, lalu baca deskripsi nomor 2. Di sana terdapat informasi bahwa paket dari IP 192.168.1.0 telah di tolak dan di-drop.