



**Laboratorium  
Multimedia dan Internet of Things  
Departemen Teknik Komputer  
*Institut Teknologi Sepuluh Nopember***

# **Laporan Akhir Praktikum Jaringan Komputer**

## **Firewall & NAT**

Sebastian Adirian Nugraha - 5024231010

2025

# 1 Langkah-Langkah Percobaan

## 1.1 Firewall

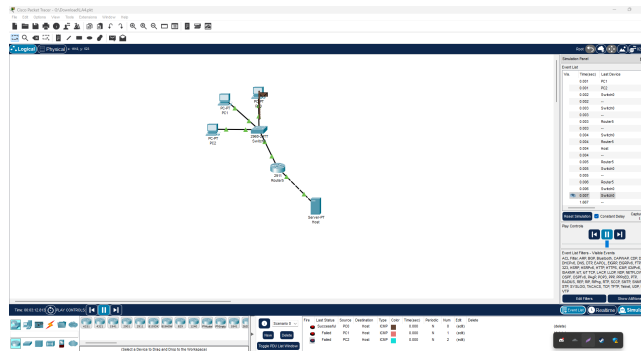
1. Reset Konfigurasi Router Sebelumnya.
2. Connect kembali ke winbox.
3. Masuk menu DHCP Client dan buat new , pilih interface yang terkoneksi dengan internet. Jika sudah dibuat pastikan connection bounded.
4. Buat Address baru pada IPv4 yang terkoneksi pada interface yang terkoneksi dengan client (laptop). Buat dengan Address pada network 192.168.10.1/24.
5. Buat DHCP Server dengan menggunakan fitur DHCP Setup. Gunakan pada network 192.168.10.0, dengan range yang sudah ditentukan dan gunakan dns dari google (8.8.8.8 / 8.8.4.4)
6. Masuk menu IP dan ke bagian Firewall, lalu buka tab NAT. Buat new rule dan chain src-nat pada tab general, pindah ke tab Action dan ganti ke masquerade.
7. Test koneksi terlebih dahulu dengan ping 8.8.8.8 pada terminal router.
8. Kembali ke tab Firewall dan masuk filter rule, buat new filter.
9. untuk ICMP, pada tab general, chain Set ke forward, protocol set ke ICMP, in. interface set ke ether yang terkoneksi dengan laptop. Lalu pada tab action ubah ke drop.
10. Untuk Content Blocking, pada tab general set chain ke forward, protocol tcp, port 80,443, in. interface pada ether yang terkoneksi ke client, dan out. interface pada yang terkoneksi ke internet. Pada tab advanced masukan content sebagai speedtest dan pada tab Action ubah ke drop.
11. Pada router B diset ke mode bridge, dengan mengakses menu bridge dan tambahkan bridge baru.
12. Pada menu bridge ke bagian port dan tambahkan pada bridge yang baru dibuat untuk interface yang terhubung pada router tersebut.
13. Test akses speedtest.net pada laptop yang terhubung pada Router B dan test internet speed pada laptop tersebut.

## 2 Analisis Hasil Percobaan

Pada percobaan ini dilakukan untuk melihat filter yang dilakukan oleh Firewall. Karena Firewall bertugas untuk menangani semua paket data yang masuk ke router, maka Firewall dapat memfilter paket data tersebut berdasarkan karakteristik pada buffer paket data tersebut. Chain pada mode forward berarti segala paket data yang melalui router tersebut akan difilter oleh firewall yang berada pada router tersebut. Firewall juga dapat memfilter berdasarkan protokol yang digunakan misal tcp/udp atau ICMP. Data yang difilter tersebut dapat diteruskan misal di drop yang berarti dimatikan atau

tidak diteruskan ke client. Pada content blocking, kita hanya memblokir semua paket data yang masuk pada content yang mengandung string yang kita filter. Untuk memfilter HTTP dan HTTPS dapat menggunakan protocol TCP/UDP pada port 80 dan 433.

### 3 Hasil Tugas Modul

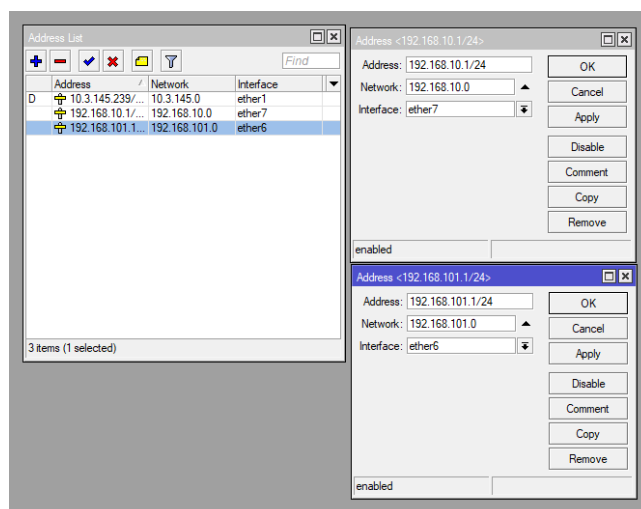


Gambar 1: Firewall ACL Simulation

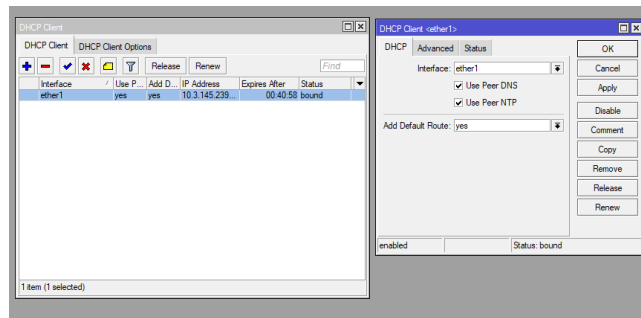
### 4 Kesimpulan

Firewall berperan penting dalam menyaring paket data yang masuk dan keluar router berdasarkan karakteristik tertentu seperti protokol, port, dan isi konten. Dengan menggunakan chain mode forward, firewall dapat memfilter seluruh lalu lintas data yang melewati router. Pemblokiran konten dapat dilakukan dengan mendeteksi string tertentu dalam paket data, terutama pada protokol TCP/UDP dengan port 80 (HTTP) dan 443 (HTTPS).

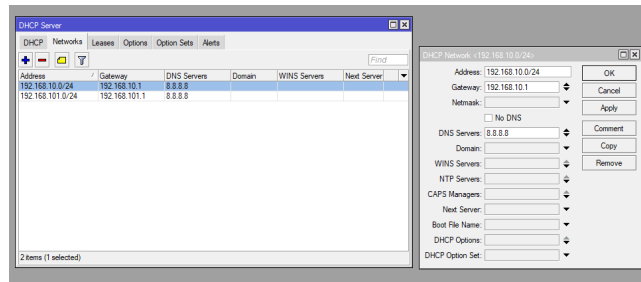
### 5 Lampiran



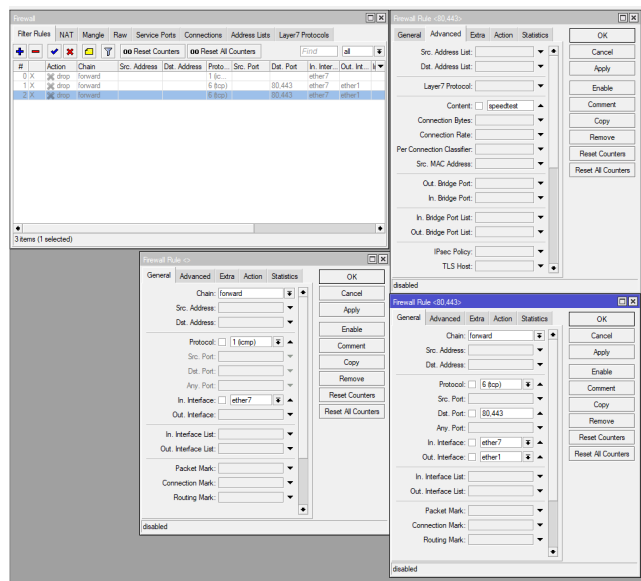
Gambar 2: Addreses Router 1



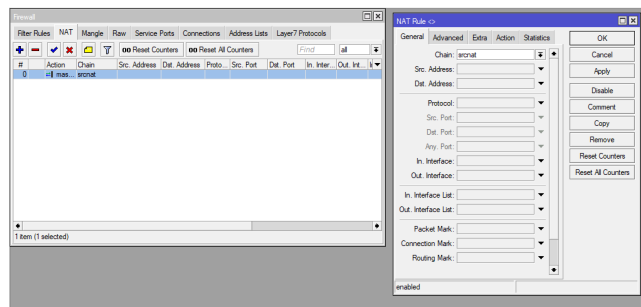
**Gambar 3: DHCP Client Router 1**



**Gambar 4: DHCP Server Router 1**



**Gambar 5: Filter Rule Router 1**



**Gambar 6: NAT Router 1**

```

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

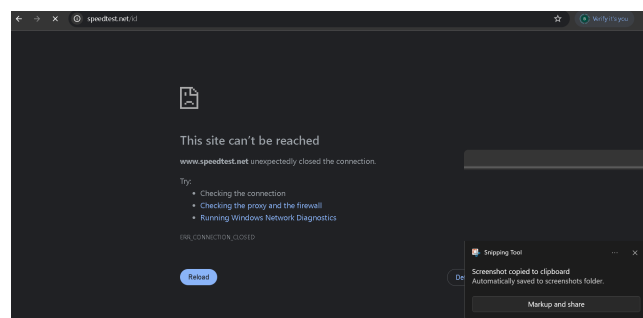
C:\Users\fahri>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 20ms, Average = 20ms

```

**Gambar 7: Ping 8.8.8.8**




**Gambar 8: Speedtest Blocked**

Bridge	Ports	VLANs	MGMTs	Port MGMT Overrides	Filters	NAT	Hosts	MGMTs
#	Interface	Bridge	Isolation	Trusted	Priority (bits)	Path Cost	Role	Root Path
0	eth0	bridge1	no	no	80	10	designated port	
1	eth1	bridge1	no	no	80	10	designated port	

**Gambar 9: Bridge Port**

Bridge Ports VLANs MGMTs Port MGMT Overrides Filters NAT Hosts MGMTs

Filter

Name	Type	L2 MTU	Tx	Rx	Tx Packet (pps)	Rx Packet (pps)	FP Tx	FP Rx	FP Tx Packet (pps)	FP Rx Packet (pps)
R  bridge1	Bridge	1500	0 tps	5.3 kpps	0	11	0 tps	0 tps	0	0

0 tps of 1.0

**Gambar 10: Bridge**



**Gambar 11:** Dokumentasi