Praktikum Jaringan Komputer 2

Modul 4

# NAT dan Proxy

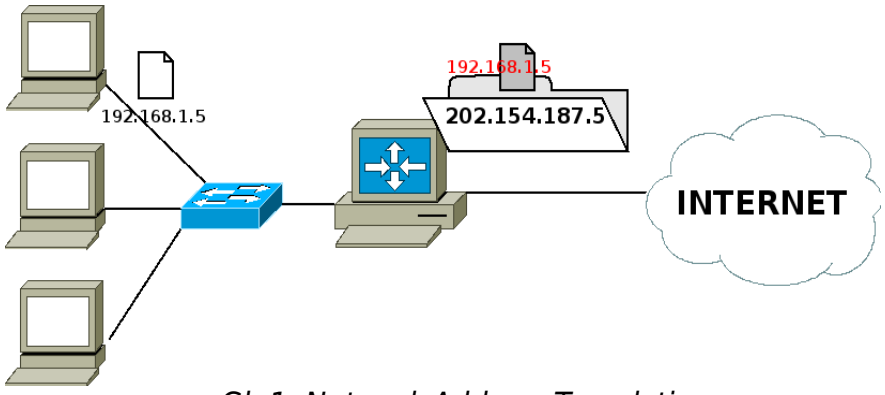
**TUJUAN:**

1. Mahasiswa memahami cara kerja dan fungsi dari NAT
2. Mahasiswa mampu membangun aplikasi PROXY
3. Mahasiswa mampu menggunakan teknik redirect untuk transparant proxy

**DASAR TEORI:**

**Network Address Translation (NAT)**

Pada jaringan komputer, proses Network Address Translation (NAT) adalah proses penulisan ulang (masquerade) pada alamat IP asal (source) dan/atau alamat IP tujuan (destination), setelah melalui router atau firewall. NAT digunakan pada jaringan dengan workstation yang menggunakan IP Private supaya dapat terkoneksi ke Internet dengan menggunakan satu atau lebih IP Public. Ilustrasi NAT terlihat pada Gb. 1.

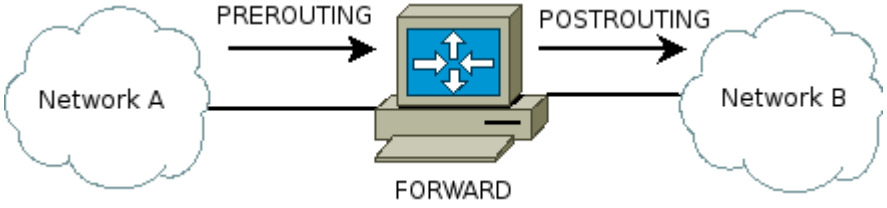



*Gb 1. Network Address Translation*

Pada mesin Linux, untuk membangun NAT dapat dilakukan dengan menggunakan iptables (Netfilter). Dimana pada iptables memiliki tabel yang mengatur NAT.

Pada tabel NAT, terdiri dari 3 chain (Gb. 2) yaitu:

- PREROUTING, digunakan untuk memilah paket yang akan diteruskan
- POSTROUTING, digunakan untuk memilah paket yang telah diteruskan
- FORWARD, digunakan untuk memilih paket yang melalui router.




*Gb 2: Tabel NAT pada iptables*

Proses NAT dilakukan pada data yang akan meninggalkan ROUTER. Sehingga pada iptables untuk pengolahan NAT dilakukan pada chain POSTROUTING. Rule yang diberikan kepada paket data tersebut adalah MASQUERADE.

Langkah-langkah membangun NAT dengan iptables pada Linux Router:

1. Tentukan NIC mana yang terkoneksi ke internet dan yang terkoneksi ke LAN
2. Tentukan Network Address dari LAN, misal 192.168.1.0/24
3. Menambahkan Rule di iptables

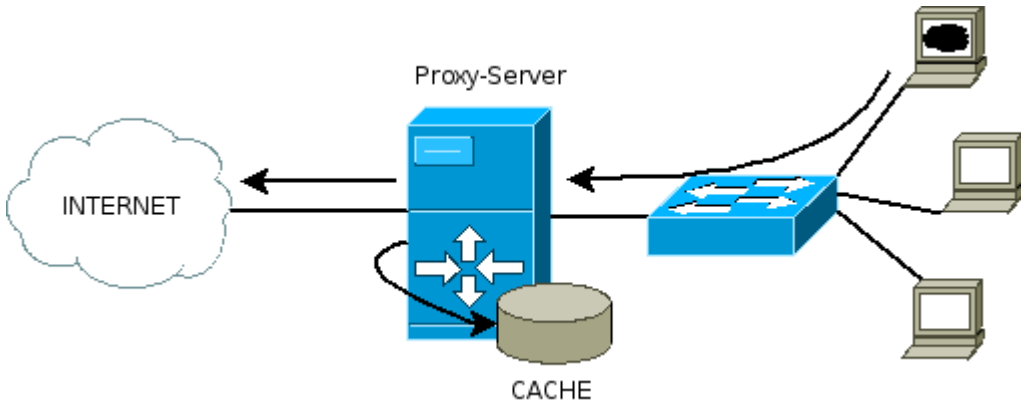
```
# iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
```

Dengan menggunakan NAT ini, IP dari LAN akan dapat terkoneksi ke jaringan yang lain, tetapi tidak dapat diakses dari jaringan lain.

**Proxy-Server**

Proxy server adalah sebuah server pada jaringan komputer yang memberikan pelayanan pada komputer client untuk dapat melakukan koneksi tidak langsung (indirect connection) dengan jaringan yang lainnya.

Client meminta koneksi ke arah proxy server kemudian server melakukan koneksi ke arah server tujuan, atau mengambil data dari dalam tempat penyimpanan sementara (cache). Ilustrasi Proxy dapat dilihat pada Gb. 3.




*Gb 3: Proxy Server dan cache*

Untuk mesin Linux, dapat menggunakan aplikasi “squid”. Dimana pada squid tersebut dapat melakukan pembatasan akses.

File konfigurasi squid berada di direktori /etc/squid/, dan file konfigurasinya bernama “squid.conf”. Squid menggunakan port tertentu untuk menerima request dari client, defaultnya adalah 3128.

Untuk menggunakan proxy, client dapat merubah preferences / options pada software web browsernya dengan mengarahkan IP proxy dan portnya.

**TRANSPARENT PROXY**

Transparent proxy adalah suatu cara supaya client dapat tetap mengakses ke jaringan lain tanpa harus memasukkan IP proxy server pada web browsernya.

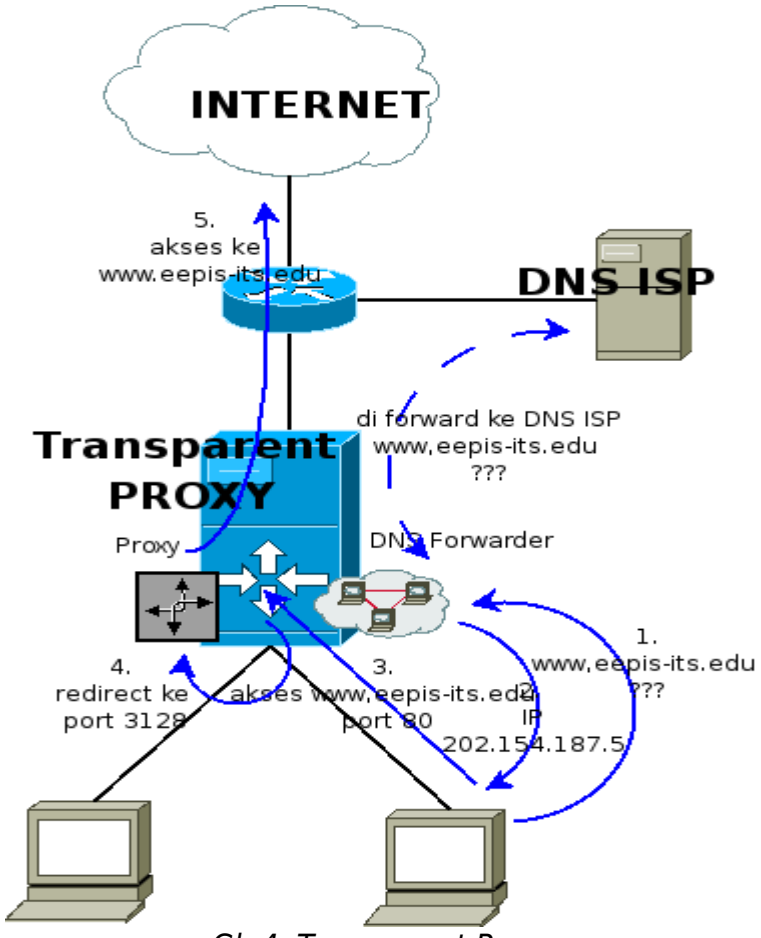
Cara kerja dari tranparent proxy adalah :

1. PC Client akan menanyakan pada DNS no IP dari site yang akan diakses, DNS server akan melanjutkan (forward) request DNS tersebut ke Server DNS suatu ISP.
2. Setelah mendapatkan balasan PC Client akan mengakses web.
3. PC Client yang akan mengakses suatu web di internet (tcp 80), paket requestnya akan ditangkap terlebih dahulu oleh PC Router.
4. Paket yang tertangkap akan dibelokkan (REDIRECT) ke arah port aplikasi proxy, sehingga yang awalnya mengakses ke port 80 akan dipindahkan ke port 3128.

Komponen yang diperlukan untuk membangun transparent proxy adalah :

- Aplikasi proxy, pada praktikum ini menggunakan “squid”
- Aplikasi REDIRECT, pada praktikum ini menggunakan “iptables”
- Aplikasi DNS forwarder (optional), pada praktikum ini menggunakan “bind9”

Ilustrasi cara kerja transparent proxy dapat dilihat di Gb. 4.




*Gb 4: Transparent Proxy*

**PERALATAN**

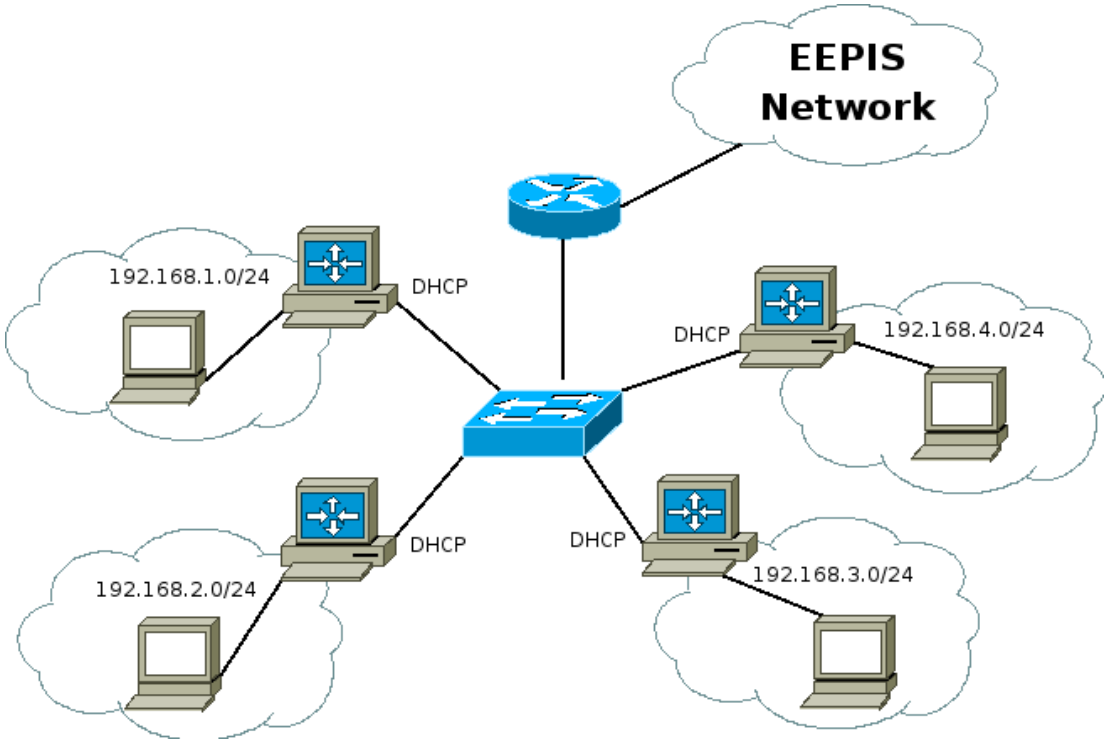
1. PC Router dengan 2 NIC atau lebih
2. PC Client (windows atau linux)
3. Switch

Catat semua langkah dan hasil yang dilakukan pada laporan sementara !!!

**LANGKAH-LANGKAH PRAKTIKUM**

Network Address Translation

1. Siapkan jaringan seperti pada gambar topologi (Gb. 5) dan pastikan tidak ada firewall di mesin PC router !!! (hapus dengan iptables -F dan iptables -t nat -F)




*Gb 5: Topologi Praktikum*

2. Pada PC router, ethernet yang mengarah ke switch menggunakan IP DHCP, sedangkan ethernet yang mengarah ke LAN diberikan IP dengan blok terakhir 1. Contoh pada jaringan 192.168.1.0/24 diberi IP 192.168.1.1.
3. Aktifkan IP-forwarding : # echo 1 > /proc/sys/net/ipv4/ip_forward
4. Pada PC client diberikan alamat IP static sesuai dengan jaringannya. Misal jaringan 192.168.1.0/24 diberi IP 192.168.1.100.
5. Pastikan PC client dan PC router bisa saling terkoneksi dengan melakukan ping atau traceroute (mtr).
   Contoh :
   - Dari PC client
     # ping 192.168.1.1
   - Dari PC router
     # ping 192.168.1.100

6. Lakukan mtr ke arah IP server ns1.eepis-its.edu (202.154.187.2) dan ke arah PC client di jaringan lainnya dari PC client maupun PC router.
   # mtr 202.154.187.2
   # mtr 192.168.2.55
7. Tambahkan NAT pada PC router, dengan IP network sesuai dengan jaringan masing-masing
   # iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
8. Catat hasil iptables pada PC router
   # iptables -t nat -nL
9. Lakukan mtr ke arah IP server ns1.eepis-its.edu dan ke arah PC client di jaringan lainnya
10. Buka website http://noc.eepis-its.edu dari PC client. (buat screenshotnya)

PROXY-SERVER

1. Pastikan belum terinstall aplikasi proxy di mesin pc router, dengan cara :
   # dpkg -P squid
2. Hapus rule NAT di pc router
   # iptables -t nat -F
3. Lakukan ping atau mtr dari PC client ke arah server noc.eepis-its.edu (202.154.187.2) dan pastikan TIDAK terkoneksi !!!
4. Lakukan installasi aplikasi proxy “squid” di mesin PC router
   # apt-get install squid
5. Rubah konfigurasi pada /etc/squid/squid.conf di mesin PC router, supaya memperbolehkan IP client di jaringannya dapat mengakseske jaringan luar.
   # vim /etc/squid/squid.conf
   Cari bagian :
   #acl our_networks src 192.168.1.0/24 192.168.2.0/24
   #http_access allow our_networks
   tips: Pada vim dapat dilakukan dengan : ESC – tekan tombol / - ketik “our_network”
   Rubah menjadi : (isi dengan IP jaringan dan hilangkan tanda # didepannya)
   acl our_networks src 192.168.1.0/24
   http_access allow our_networks
   Simpan file konfigurasi tersebut dengan “:wq”
6. Restart aplikasi squid dengan cara :
   # /etc/init.d/squid restart
7. Pada PC client, buka aplikasi web browser (iceweasel), rubah preferences untuk proxy. Isikan dengan IP mesin proxy dan portnya.
   Contoh :
   HTTP Proxy : 192.168.1.1 dengan port : 3128
8. Pada PC Client, lakukan akses ke alamat web http://noc.eepis-its.edu atau http://www.eepis-its.edu (Tidak mengakses ke INTERNET !!!)
9. Pada PC router, tampilkan report dari client yang menggunakan proxy. File report ada di /var/log/squid/access.log
   # tail -f /var/log/squid/access.log

TRANSPARENT PROXY

1. Matikan preferences untuk menggunakan Proxy pada web browser di PC Client
2. Akses ke web http://www.eepis-its.edu, seharusnya akses akan gagal dengan web browser gagal untuk meresolv nama dari domain tersebut.

Bagian DNS

3. Pada PC router lakukan installasi aplikasi DNS "bind9"
   # apt-get install bind9
4. Rubah konfigurasi pada file /etc/bind/named.conf.options
   # vim /etc/bind/named.conf.options
   Rubah bagian : (hilangkan tanda // di depannya)
   // query-source address * port 53;
   Menjadi :
   query-source address * port 53;
   Rubah bagian :
   // forwarders {
   //  0.0.0.0;
   // };
   Menjadi : (hilangkan tanda // dan ganti IP 0.0.0.0 menjadi IP DNS – ISP 202.154.187.2)
   forwarders {
   202.154.187.2;
   };
5. Restart aplikasi DNS
   # /etc/init.d/bind9 restart

Bagian Proxy

6. Rubah konfigurasi file /etc/squid/squid.conf pada mesin PC Router
   # vim /etc/squid/squid.conf
   Rubah bagian :
   http_port 3128
   Menjadi : (menambahkan kata "transparent")
   http_port 3128 transparent
   Simpan dengan "ESC - :wq"
7. Restart aplikasi squid dengan cara :
   # /etc/init.d/squid restart

Bagian Firewall

8. Tambahkan aturan firewall pada mesin PC Router untuk membelokkan request ke DNS (udp 53) dan ke WEB (tcp 80)
   # iptables -nL -t nat
   Menambahkan redirect untuk WEB ke arah port proxy
   # iptables -t nat -I PREROUTING -s 192.168.1.0/24 -p tcp –dport 80 -j REDIRECT –to-ports 3128
   Menambahkan redirect untuk DNS ke arah bind9

# iptables -t nat -I PREROUTING -s 192.168.1.0/24 -p udp –dport 53 -j REDIRECT –to-ports 53

Lihat isi firewall dengan iptables -t nat -nvL

Bagian akses

9. Pada Client jalankan “nslookup www.eepis-its.edu” dengan menggunakan terminal
10. Akses ke website http://www.eepis-its.edu atau http://noc.eepis-its.edu
11. Pada mesin PC router, catat hasil akses dengan cara :

    # tail -f /var/log/squid/access.log

**TUGAS**

1. Gambar topologi keseluruhan dari praktikum ini
2. Catat konfigurasi proxy pada file “/etc/squid/squid.conf” dengan cara

```
# grep -v "^#" /etc/squid/squid.conf | sed -e '/^$/d'
```

**REFERENSI**


1. NAT - wikipedia, http://en.wikipedia.org/wiki/Network_address_translation
2. Proxy server – wikipedia, http://en.wikipedia.org/wiki/Proxy_server
3. squid – doc
4. man iptables

Data Praktikum Modul 4 : NAT dan PROXY

NRP :
Nama :
Hari/Tgl :

Network Address Translation (NAT)

1. Gambar Topologi

2. ping dan mtr sebelum ada NAT

3. Penambahan rule NAT

4. ping dan mtr setelah ada NAT

Proxy Server

1. ping atau mtr setelah NAT dihapus

2. akses web dengan preferences di web browser

3. Menampilkan laporan akses pada file /var/log/squid/access.log

Transparent PROXY

1. Akses web dengan mematikan preferences pada web browser

2. Hasil iptables -nvL -t nat

3. Hasil laporan akses dari file /var/log/squid/access.log

4. Hasil percobaan nslookup

5. Hasil akses dengan web browser