MODUL 7
NAT dan PROXY

TUJUAN PEMBELAJARAN:

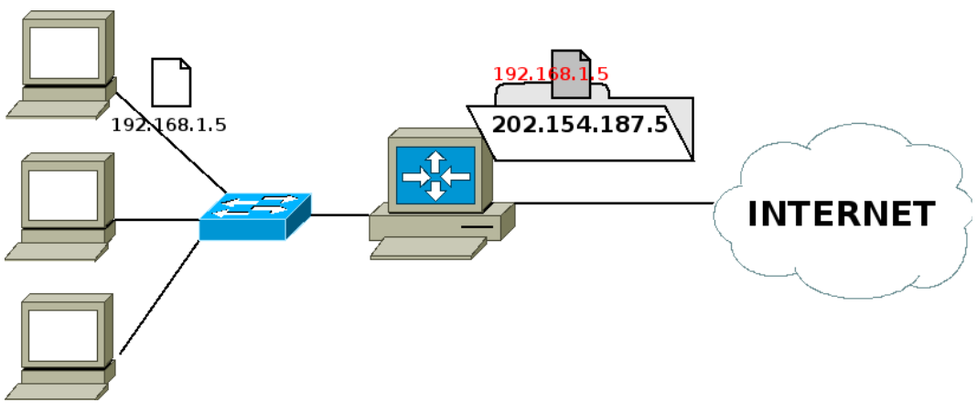
Setelah melaksanakan praktikum ini, mahasiswa diharapkan :

1. Mengerti dan memahami cara kerja dan fungsi dari NAT
2. Mampu membangun aplikasi Proxy
3. Mampu membangun transparent proxy dan proxy bertingkat

DASAR TEORI

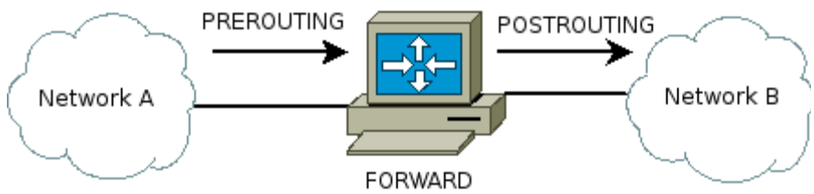
Network Address Translation (NAT)

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

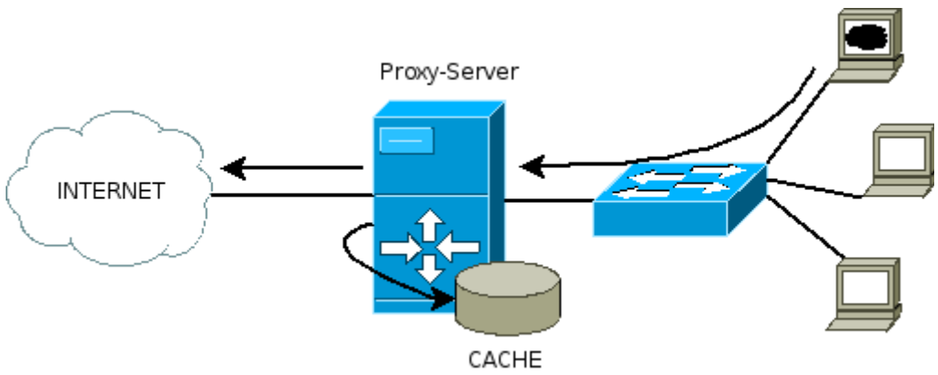
Proses NAT dilakukan pada data yang akan meninggalkan ROUTER. Sehingga pada iptables untuk pengolahan NAT dilakukan pada chain POSTROUTING. Rule yang diberikan kepada paket data tersebut adalah MASQUERADE.
Langkah-langkah membangun NAT dengan iptables pada Linux Router:
1. Tentukan NIC mana yang terkoneksi 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.

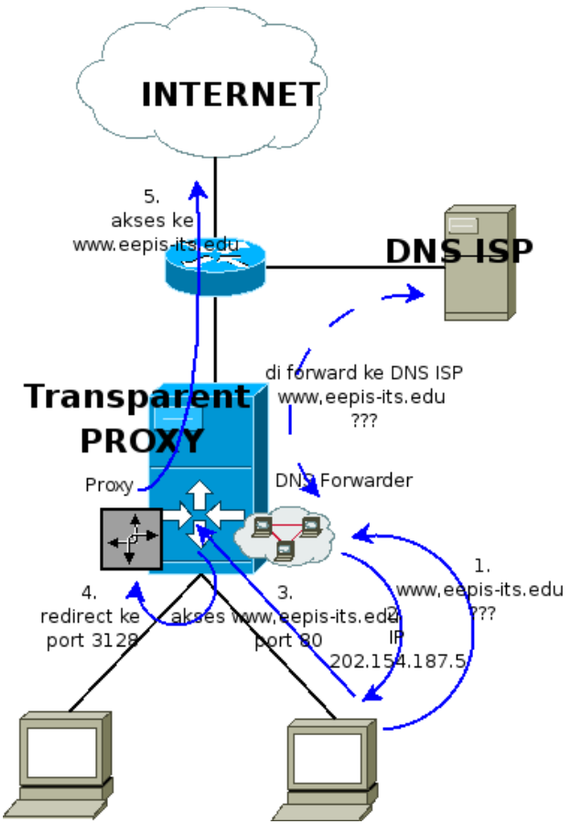
Transparent Proxy

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 :

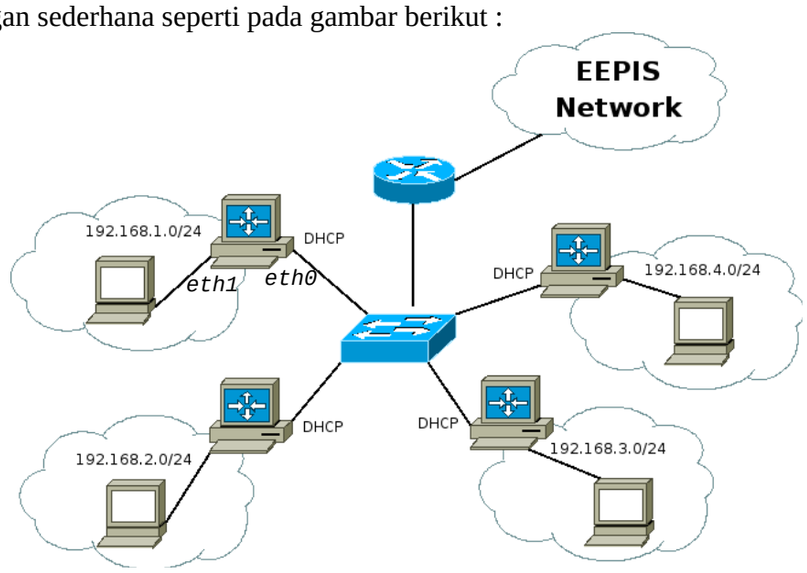
- Sebuah komputer sebagai *client*, dengan 1 NIC Card
- Sebuah komputer sebagai router, dengan 2 NIC Card
- *Hub/switch* sebagai penghubung jaringan
- Kabel jaringan secukupnya

TUGAS PENDAHULUAN

1. Apa perbedaan yang mendasar antara proxy server dan NAT ?
2. Jelaskan penggunaan perintah cache_peer pada proxy dan berikan contohnya ?

PERCOBAAN

Bangun jaringan sederhana seperti pada gambar berikut :



Gb 5. Topologi Praktikum

NB :
Pastikan tidak ada firewall di PC Router. Hapus dengan perintah :

```
# iptables –F
# iptables –t nat -F
```

A. Network Address Translation (NAT)

1. Pada PC Router, setting sebagai berikut :
   a. Setting dengan IP pada eth0 dan eth1

```
# dhclient     => lakukan pada eth0 yang terhubung ke switch utama
# ifconfig eth1 192.168.1.1 netmask 255.255.255.0
```

   b. Aktifkan ip_forward pada PC Router untuk melakukan proses routing :

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. Setting pada PC Client

```
# ifconfig eth0 192.168.1.2 netmask 255.255.255.0
# route add –net default gw 192.168.1.1
```

3. Lakukan tes koneksi dari PC Client dan catat hasilnya

```
# ping 192.168.1.1     => ke gateway masing-masing kelompok
# ping 192.168.50.1    => ke Cisco Router
```

   Lakukan juga tes koneksi ke arah server PENS:

```
# mtr 202.9.85.3
# mtr www.eepis-its.edu
```

   Buka website (beri setting no proxy) dan arahkan ke :
   http://www.eepis-its.edu

4. Tambahkan NAT pada PC router, dengan IP network sesuai dengan jaringan masing-masing

```
# iptables –t nat –A POSTROUTING –s 192.168.1.10/24 –j MASQUERADE
```

5. Catat hasil iptables pada PC Router

```
# iptables –t nat –nL
```

6. Ulangi langkah 3 dan bandingkan hasilnya.

B. Proxy Server

B.1 Akses koneksi berbasis proxy

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 tes koneksi ke arah server PENS (pastikan TIDAK TERKONEKSI)

```
# mtr 202.9.85.3
# mtr www.eepis-its.edu
```

   Buka website (beri setting no proxy) dan arahkan ke :
   http://www.eepis-its.edu
   http://mis.eepis-its.edu
   http://umm.eepis-its.edu
   http://noc.eepis-its.edu

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 mengakses ke jaringan luar.

```
# vim /etc/squid/squid.conf
```

Cari bagian berikut dan tambahkan rule:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
acl kelompok1 src 192.168.1.0/24 192.168.2.0/24
http_access allow kelompok1

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all
```

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. Ulangi langkah 3 dan bandingkan hasilnya.

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
```

B.2 Pembatasan koneksi pada suatu website dengan proxy

1. Pertahankan konfigurasi diatas.
2. Buat file untuk menolak beberapa halaman website :

```
#  vim  /etc/squid/tolak
mis.eepis-its.edu
noc.eepis-its.edu
```

3. Tambahkan konfigurasi pada file berikut :

```
# vim /etc/squid/squid.conf
```

Cari bagian berikut dan tambahkan rule (perhatikan susunan rule-nya)

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
acl tolak dstdomain "/etc/squid/tolak"
http_access deny tolak

acl kelompok1 src 192.168.1.0/24 192.168.2.0/24
http_access allow kelompok1
```

4. Ulangi langkah B.1 6-8 dan bandingkan hasilnya.

B.3 Pembatasan koneksi user dengan proxy (user authentication)

1. Pertahankan konfigurasi diatas
2. Buatlah account untuk user (missal nafisa) yang akan melakukan koneksi

```
#touch  /etc/squid/squid_passwd
#chmod  o+r  /etc/squid/squid_passwd
#htpasswd  /etc/squid/squid_passwd  nafisa
```

NB: Jika perintah htpasswd tidak bisa maka harus diinstall dulu

```
#apt-get install apache2
```

3 Tambahkan konfigurasi pada file berikut :

```
# vim /etc/squid/squid.conf

# auth_param basic program /usr/lib/squid/ncsa_auth /usr/etc/passwd
```

Hilangkan komentar pada perintah diatas dan lakukan perubahan sebagai berikut :

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd

Tambahkan perintah berikut (perhatikan susunan rule-nya) :

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
acl tolak dstdomain "/etc/squid/tolak"
http_access deny tolak

acl ncsa_users proxy_auth REQUIRED
http_access allow ncsa_users

acl kelompok1 src 192.168.1.0/24 192.168.2.0/24
http_access allow kelompok1
```

4. Ulangi langkah B.1 6-8 dan bandingkan hasilnya.
   Seharusnya ketika user melakukan koneksi ke web server, maka akan muncul notifikasi sebagai berikut :

B.4 Penggunaan cache_peer dengan proxy

1. Lakukan akses keluar dari jaringan PENS :
   misal http://www.detik.com dan http://www.facebook.com

   NB : Seharusnya tidak bisa, karena di PENS terdapat parent proxy.

2. Tambahkan konfigurasi pada file berikut :

```
# vim /etc/squid/squid.conf

#  TAG: cache_peer
#     To specify other caches in a hierarchy, use the format:
#
#           cache_peer hostname type http-port icp-port [options]
#
#     For example,
#
#     #                                        proxy  icp
#     #          hostname             type     port   port  options
#     #          -------------------- -------- ----- -----  -----------
#     cache_peer parent.foo.net       parent    3128  3130  proxy-only default
#     cache_peer sib1.foo.net         sibling   3128  3130  proxy-only
#     cache_peer sib2.foo.net         sibling   3128  3130  proxy-only
#
#           type:  either 'parent', 'sibling', or 'multicast'.
cache_peer proxy2.eepis-its.edu parent 443 0 proxy-only no-digest no-netdb-
exchange default login=user:pass

never_direct allow all
```

3. Restart aplikasi squid
```
# /etc/init.d/squid restart
```

4. Ulangi langkah B.4 no 1 dan bandingkan hasilnya.

C. 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 untuk meresolv nama dari domain tersebut.

Bagian DNS (di PC Router)

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 202.9.85.3)
```
forwarders {
      202.9.85.3;
};
```

5. Restart aplikasi DNS
```
# /etc/init.d/bind9 restart
```

Bagian Proxy (di PC Router)

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
```

7. Restart aplikasi squid dengan cara :
```
# /etc/init.d/squid restart
```

Bagian Firewall (di PC Router)

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 -A 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 (PC Client)

9. Pada Client jalankan “nslookup www.eepis-its.edu” dengan menggunakan terminal
10. Akses ke website http://www.eepis-its.edu atau http://www.detik.com

LAPORAN RESMI

Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Tugas akan diberikan pada waktu praktikum.