ITS
Institut
Teknologi
Sepuluh Nopember

NAT & PROXY SERVER

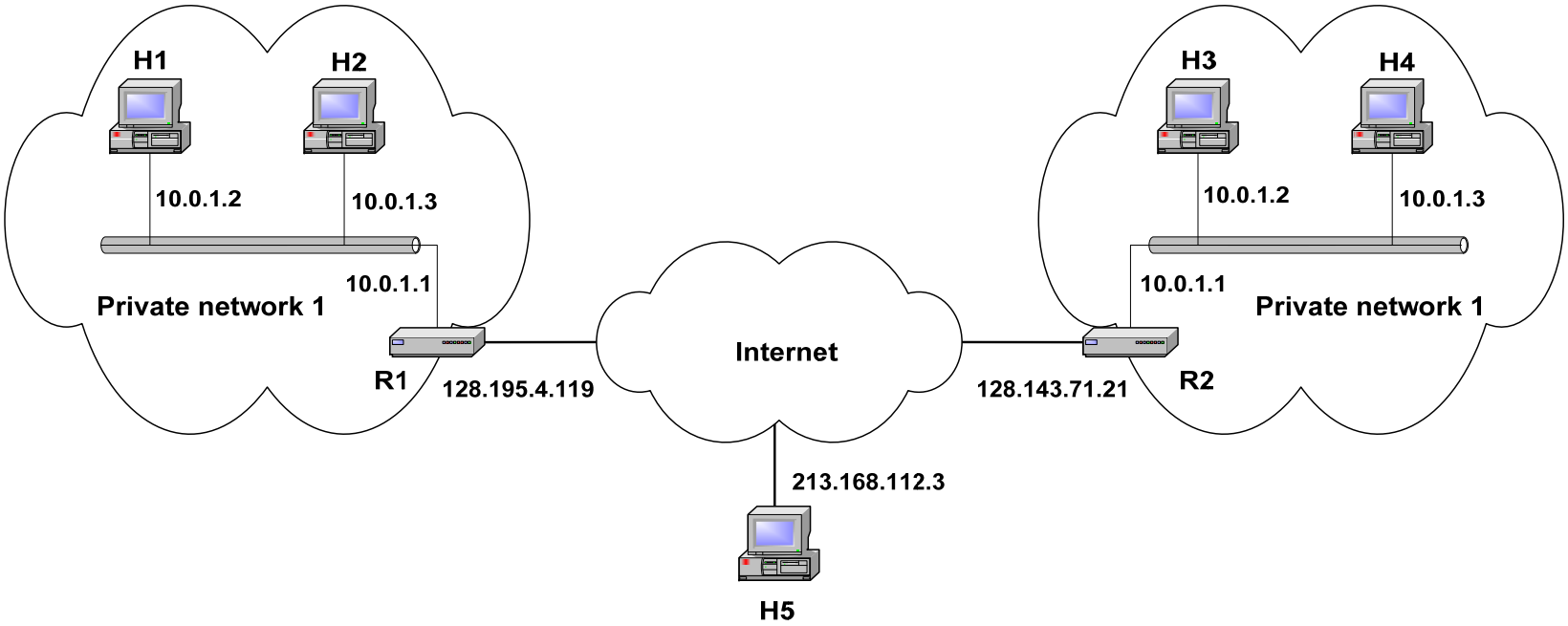
Network Address Translation (NAT)

- NAT adaah sebuah fungsi router yang memetakan alamat IP private (Lokal) ke alamat IP yang dikenal di Internet, shg jaringan private bisa internetan
- NAT merupakan salah satu metode yang memungkinkan host pada alamat private bisa berkomunkasi dengan jaringan di internet
- NAT jalan pada router yang menghubungkan antara private networks dan public Internet, dan menggantikan IP address dan Port pada sebuah paket dengan IP address dan Port yang lain pada sisi yang lain

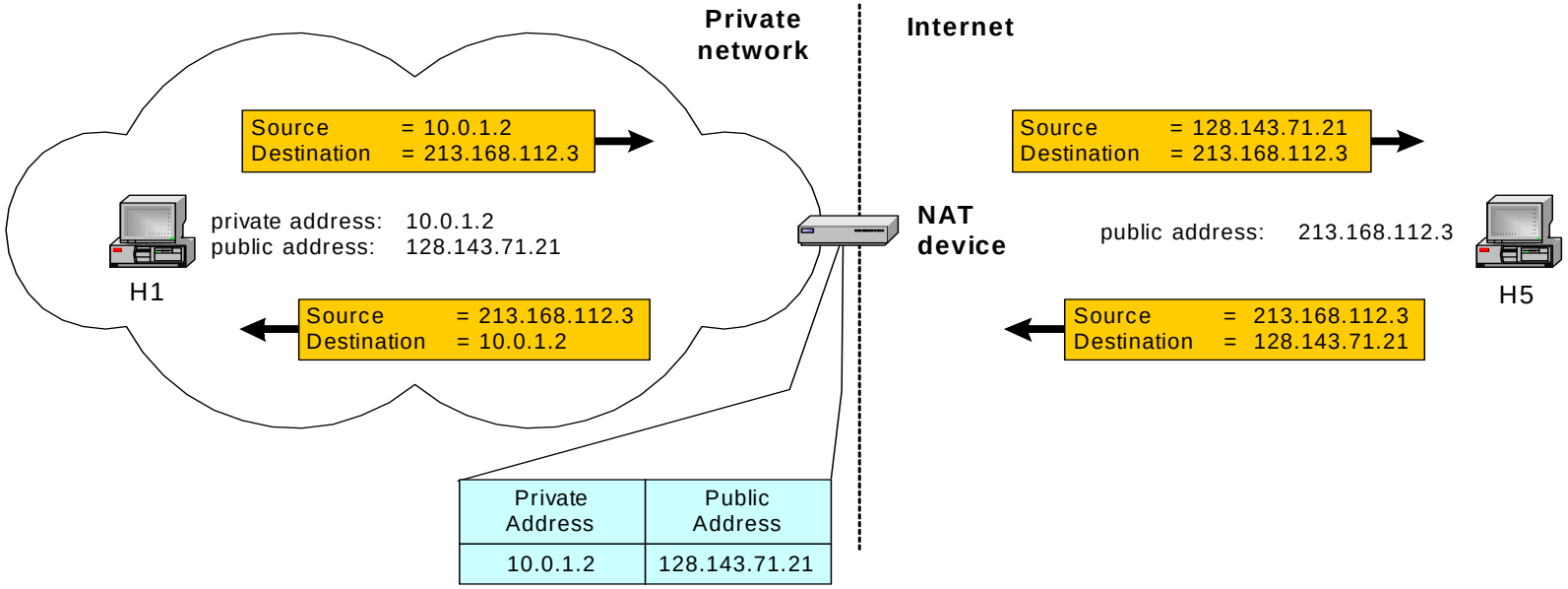
Private Network

- *Private IP* network adalah IP jaringan yang tidak terkoneksi secara langsung ke internet
- IP addresses Private can dirubah sesuai kebutuhan.
  - Tidak teregister dan digaransi menjadi IP Global yang unik
- Umumnya, Jaringan private menggunakan alamat dari range experimental address (*non-routable addresses*):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

Private Addresses



Operasi Dasar NAT



- NAT device mempunyai Tabel Penterjemah

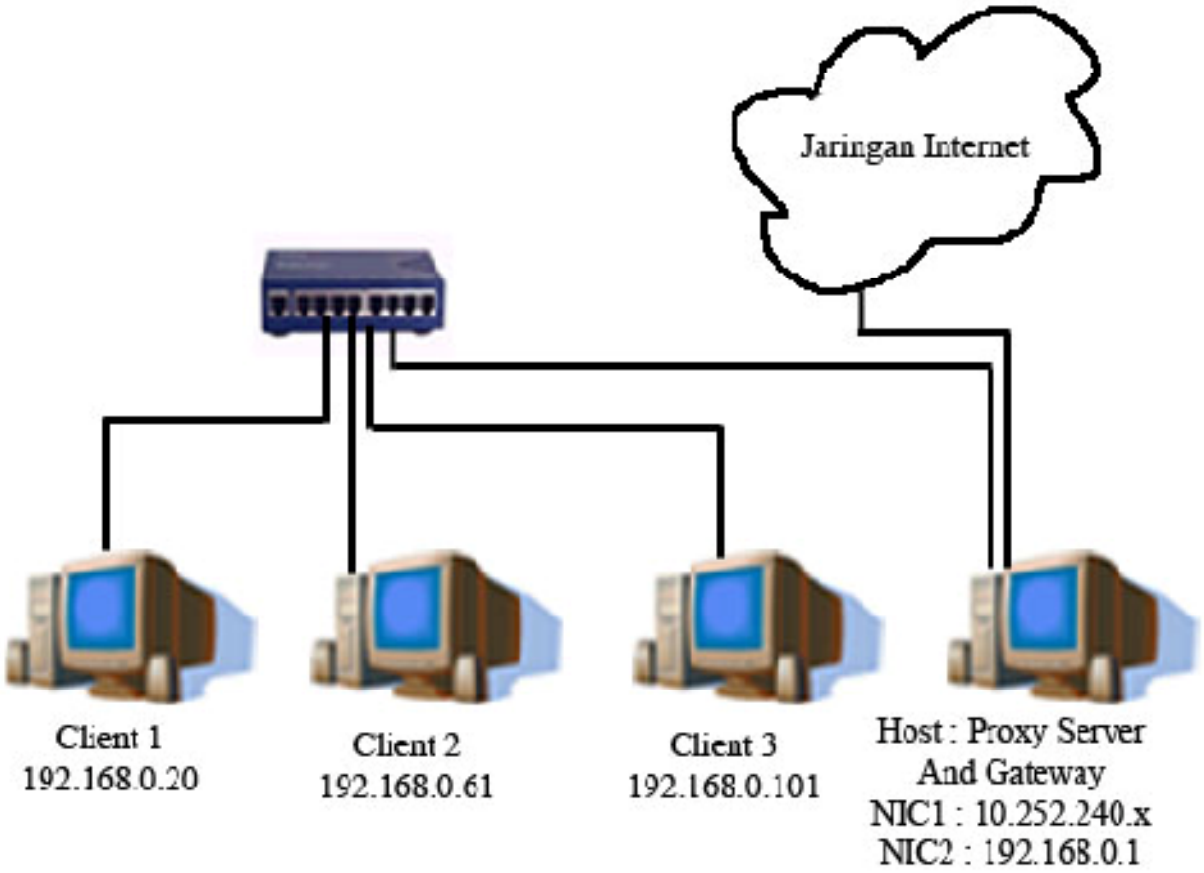
Penggunaan Utama NAT

- Pooling IP address
- Men-support perpindahan ISP tanpa harus merubah konfigurasi pada jaringan lokal
- IP masquerading
- Load balancing servers

Proxy Server

- Proxy merupakan pihak ketiga yang berdiri ditengah-tengah antara kedua pihak yang saling berhubungan dan berfungsi sebagai perantara
- Secara prinsip pihak pertama dan pihak kedua tidak secara langsung berhubungan, akan tetapi masing-masing berhubungan dengan perantara, yaitu proxy

Ilustrasi


Jaringan Internet
Client 1
192.168.0.20
Client 2
192.168.0.61
Client 3
192.168.0.101
Host : Proxy Server
And Gateway
NIC1 : 10.252.240.x
NIC2 : 192.168.0.1

- Pada gambar di atas client1, client2, client3 disebut sebagai pihak pertama
- Sedangkan yang menjadi pihak kedua adalah jaringan internet
- Sebelum keduanya saling berhubungan, mereka harus melewati proxy server

Fungsi Proxy

- Connection Sharing,
- Filtering,
  - Filter Situs-Situs Terlarang,
  - Filter Pengguna Internet,
- Caching,
- Management User's Authentication,
- Management Waktu Akses Internet,
- Management Bandwidth,
- dst

Connection Sharing

- Konsep dasar, pengguna tidak langsung berhubungan dengan jaringan luar atau internet, tetapi harus melewati suatu gateway, yang bertindak sebagai batas antara jaringan lokal dan jaringan luar.
- Gateway ini sangat penting, karena jaringan lokal harus dapat dilindungi dengan baik dari bahaya yang mungkin berasal dari internet, dan hal tersebut akan sulit dilakukan bila tidak ada garis batas yang jelas jaringan lokal dan internet.
- Gateway juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya, dan suatu koneksi ke jaringan luar juga terhubung kepadanya.
- Dengan demikian, koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh gateway secara bersama-sama (connection sharing).
- Dalam hal ini, gateway adalah juga sebagai proxy server, karena menyediakan layanan sebagai perantara antara jaringan lokal dan jaringan luar atau internet

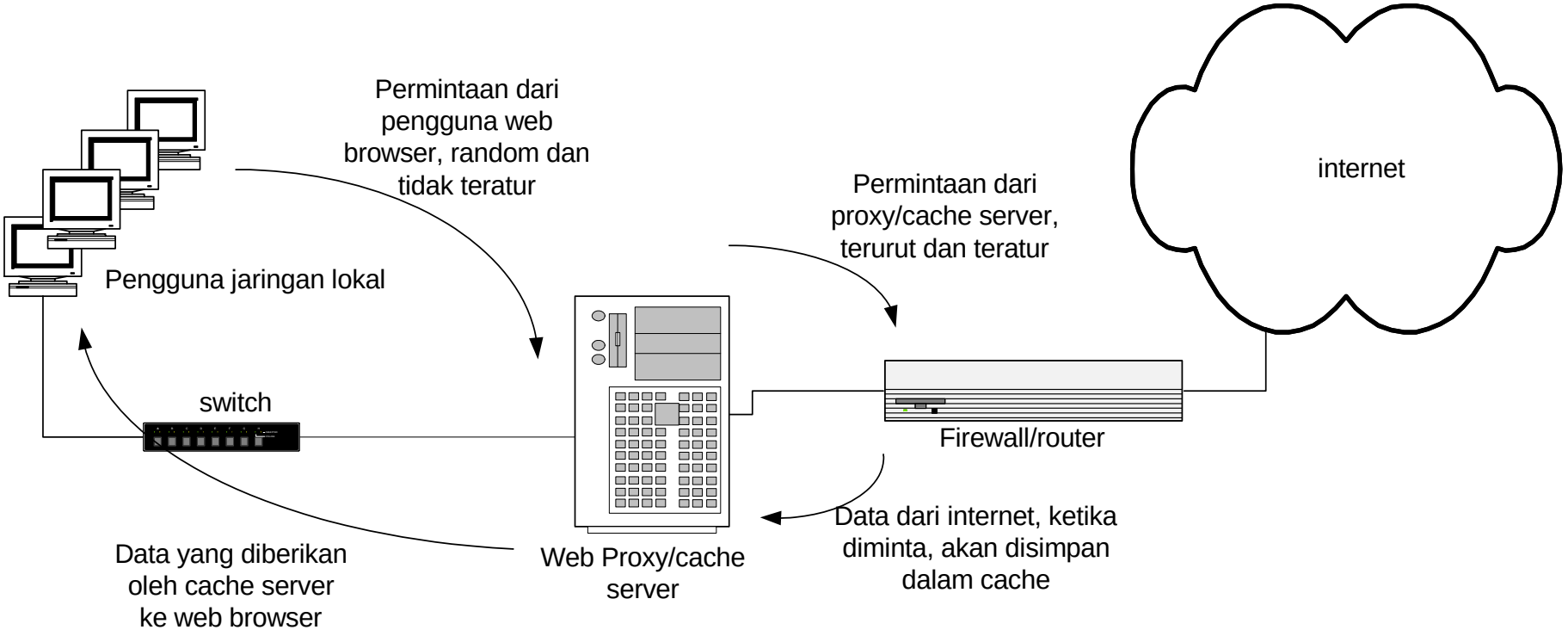
Filtering

- Filter Situs-Situs Terlarang
  - Konsepnya adalah jika ada client yang ingin mengakses situs-situs yang sudah difilter oleh proxy server maka akses akan gagal.
- Filter Pengguna Internet
  - Pengguna Internet sudah didefinisikan di konfigurasi proxy
  - Pendefinisan yang digunakan adalah dengan menggunakan IP Address yang digunakan client
  - Proxy juga bisa mendefinisikan beberapa IP yang tidak bisa akses internet

Caching

- Proxy server memiliki mekanisme penyimpanan obyek-obyek yang sudah pernah diminta dari server-server di internet
- Proxy server yang melakukan proses diatas biasa disebut cache server
- Mekanisme caching akan menyimpan obyek-obyek yang merupakan hasil permintaan dari dari para pengguna, yang didapat dari internet.
- Disimpan dalam ruang disk yang disediakan (cache).

Mekanisme Caching



Caching ...

- Dengan demikian, bila suatu saat ada pengguna yang meminta suatu layanan ke internet yang mengandung obyek-obyek yang sama dengan yang sudah pernah diminta sebelumnya, yaitu yang sudah ada dalam cache, maka proxy server akan dapat langsung memberikan obyek dari cache yang diminta kepada pengguna, tanpa harus meminta ulang ke server aslinya di internet.
- Bila permintaan tersebut tidak dapat ditemukan dalam cache di proxy server, baru kemudian proxy server meneruskan atau memintakannya ke server aslinya di internet

Transparent Proxy

- Salah satu kompleksitas dari proxy pada level aplikasi adalah bahwa pada sisi pengguna harus dilakukan konfigurasi yang spesifik untuk suatu proxy tertentu agar bisa menggunakan layanan dari suatu proxy server
- Agar pengguna tidak harus melakukan konfigurasi khusus, kita bisa mengkonfigurasi proxy/cache server agar berjalan secara benar-benar transparan terhadap pengguna (transparent proxy).
- Transparent Proxy memerlukan bantuan dan konfigurasi aplikasi firewall (yang bekerja pada layer network) untuk bisa membuat transparent proxy yang bekerja pada layer aplikasi

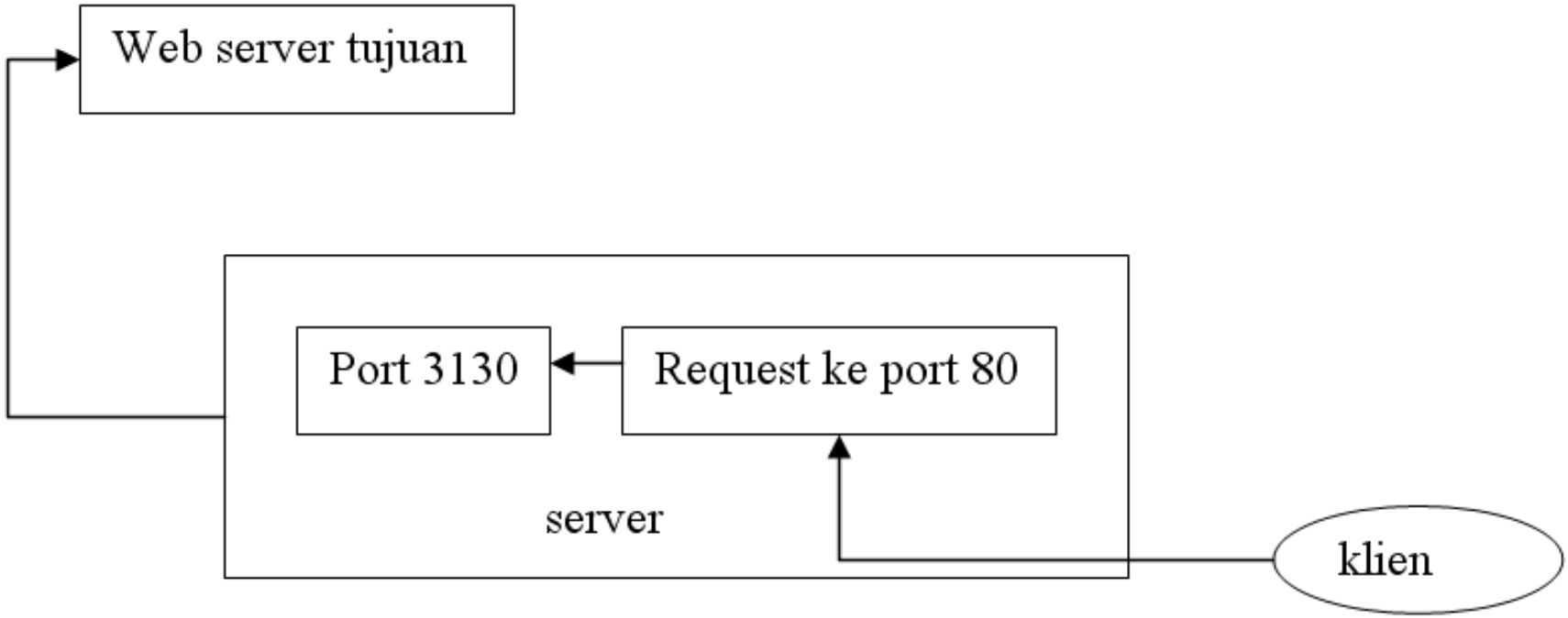
Cara Kerja Transparent Proxy

- Pengguna benar-benar tidak mengetahui tentang keberadaan proxy ini, dan apapun konfigurasi pada sisi pengguna, selama proxy server ini berada pada jalur jaringan yang pasti dilalui oleh pengguna untuk menuju ke internet, maka pengguna pasti dengan sendirinya akan "menggunakan" proxy/cache ini.
- Cara membuat transparent proxy adalah dengan membelokkan arah (redirecting) dari paket-paket untuk suatu aplikasi tertentu, dengan menggunakan satu atau lebih aturan pada firewall/router.
- Prinsipnya setiap aplikasi berbasis TCP akan menggunakan salah satu port yang tersedia, dan firewall membelokkan paket yang menuju ke port layanan tertentu, ke arah port dari proxy yang bersesuaian

Cara Kerja Transparent Proxy ...

- Sebagai Contoh : Pada saat klient membuka hubungan HTTP (port 80) dengan suatu web server, firewall pada router yang menerima segera mengenali bahwa ada paket data yang berasal dari klien dengan nomor port 80.
- Misal kita juga mempunyai satu HTTP proxy server yang berjalan pada port 3130.
- Pada Firewall router kita buat satu aturan yang menyatakan bahwa setiap paket yang datang dari jaringan lokal menuju ke port 80 harus dibelokkan ke arah alamat HTTP proxy server port 3130. Akibatnya, semua permintaan web dari pengguna akan masuk dan diwakili oleh HTTP proxy server diatas.

Cara Kerja Transparent Proxy ...



/sbin/iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3130

Management User's Authentication

Konsep

- Membatasi akses internet menggunakan username dan password setiap kali ingin mengakses internet,
- Jika username dan password yang dimasukkan benar, maka client tersebut bisa mengakses internet,
- Jika username dan password yang dimasukkan salah, maka client tersebut tidak bisa mengakses internet.

Management Waktu Akses Internet

- Akses internet hanya bisa dilakukan pada waktu-waktu tertentu
- Waktu akses internet berdasarkan hari-hari dan jam-jam tertentu
- Keuntungan: mengoptimalkan penggunaan bandwidth

Management Bandwidth

- *Bandwith* adalah kecepatan transmisi dalam sistem komunikasi data, dihitung dalam satuan bit / detik (bps - bit per second).
- Management bandwidth pada proxy dapat dilakukan pada penggunaan bandwidth pada network atau masing-masing client.
- Management bandwidth yang baik akan mengoptimalkan client untuk akses ke jaringan internet

Installasi dan Konfigurasi Squid Proxy Server

Squid Proxy-Server

- Squid merupakan software proxy yang sekarang ini banyak digunakan
- Squid sudah termasuk di dalam distro Debian DNU/Linux
- Instalasi pada Debian digunakan perintah berikut:
  - $ apt-get install squid

Konfigurasi Dasar

- Edit file /etc/squid/squid.conf
- http_port → menentukan squid akan berjalan di port berapa atau akan berjalan di Ip berapa dan port berapa
  - Contoh :
  - http_port 192.168.0.1:8080 (jalan di IP 192.168.0.1 di port 8080)
  - http_port 8080 (jalan di sembarang IP di port 8080)

Cache_Peer

- Cache_peer adalah metode squid dalam melakukan hirarki akses, squid memungkinkan dirinya untuk bekerjasama dengan mesin proxy yang lain
- Cache_peer sangat berguna bagi mesin yang tidak punya koneksi langsung ke internet tapi bisa mengakses ke suatu proxy yang terhubung ke internet (mesin yang punya akses ke internet disebut dengan parent)
- Cache_peer
  - cache_peer **proxy.eepis-its.edu** parent **3128** 3130
  - Proxy.eepis-its.edu adalah mesin parent yang membuka port pada 3128

Loging

- Sangat diperlukan untuk menganalisa dan memonitor kejadian pada squid
- cache_access_log : melihat URL akses ke proxy
  - cache_access_log /var/log/squid/access.log
- cache_log : melihat kejadian pada squid tergantung dari nilai debug_options
  - cache_log /var/log/squid/cache.log
- Harus dipastikan bahwa file tersebut adalah writable oleh squid

Access Filtering menggunakan ACL

- ACL : access control list
  - Format umum :
    - acl aclname acltype string1 …
    - acl aclname acltype "file" …
  - Acl bisa menggunakan string yang ada pada file konfigurasi dan juga bisa menggunakan file eksternal
  - Aclname adalah nama yang diberikan untuk acl tersebut
  - Squid akan membatasi akses berdasarkan nama aclnya

TIPE ACL

TIPE ACL	ARGUMEN	KETERANGAN
src	alm_ip/netmask … alm_ip1-alm_ip2	Asal alamat IP klien Rentang alamat IP
dst	alm_ip/netmask …	Tujuan alamat IP URL
myip	alm_ip/netmask …	Socket alamat IP local
srcdomain	nama_domain …	Asal domain klien
dstdomain	nama_domain …	Tujuan domain URL
scrdom_regex	[-i] xxx …	Pernyataan untuk asal klien
dstdom_regex	[-i] xxx …	Pernyataan untuk tujuan server
time	[hari] [h1:m1-h2:m2]	Singkatan nama hari: S-Sunday, M-Monday, T-Tuesday, W-Wednesday, H-Thursday, F-Friday A-Saturday

Tipe Acl .....

`url_regex`	`[-i] ^http:// …`	Pernyataan nama URL lengkap
`urlpath_regex`	`[-i] \.gif$ …`	Pernyataan path padaURL
`port`	`port …` `port1-port2`	Nomor port Rentang nomor port
`myport`	`port …`	Port socket TCP local
`proto`	`protocol …`	Nama protokol yang dikendalikan (HTTP, FTP, dll)
`method`	`metode …`	Nama metode yang dikendalikan (GET, POST, dll)
`browser`	`[-i] regexp`	Pernyataan untuk pola pencocokan pada header permintaan
`ident`	`username …`	Daftar username

Tipe Acl.....

ident_regex	[-i] pola	Pernyataan untuk username
src_as	Angka …	Angka system autonomi asal klien
dst_as	angka …	Angka system autonomi tujuan server
proxy_auth	username …	Autentikasi username melalui proses eksternal
proxy_auth_regex	[-i] pattern …	Autentikasi username melalui proses eksternal
Snmp_community	string ….	Nama komunitas untuk membatasi agen SNMP
maxconn	jumlah	Jumlah maksimum koneksi HTTP untuk satu alamat IP
req_mime_type	tipe_mime1 …	Pernyataan berdasarkan tipe MIME yang diminta klien

ACL Type untuk waktu

- acl aclname time [day-abbrevs] [h1:m1-h2:m2]
  - S - Sunday
  - M - Monday
  - T - Tuesday
  - W - Wednesday
  - H - Thursday
  - F - Friday
  - A – Saturday
- h1:m1 dan h2:m2 adalah jam dan menit, h1:m1 adalah start waktu dan h2:m2 adalah waktu selesai
- Contoh : acl yang melambangkan hari senin sampai jumat jam 9 pagi sampai jam 10 pagi adalah :
  - acl waktuku MTWHF 09:00-10:00

Membatasi akses

- Menggunakan **http_access**
- Format
  - http_access (allow | deny) (!) aclname aclname …
  - http_access akan match jika acl acl yang tergabung mempunyai nilai yang memenuhi
- Squid akan menganggap semua akses akan di deny (menggunakan http_access deny all) di baris-baris akhir setelah acl
- Agar kita bisa memperbolehkan user yang sesuai dengan acl mengakses ke proxy, maka tempatkanlah http_access yang berkaitan dengan acl kita di tempat sebelum http_access deny all

Contoh membatasi Akses

- acl lab_A src 10.126.10.1/255.255.255.255
- acl lab_B src 10.126.11.1/255.255.255.255
- acl lab_C src 10.126.13.0/255.255.255.0

Di bagian http_access :

http_access allow lab_A

http_access allow lab_B waktuku

http_access deny all (sudah ada)

Dengan demikian acl yang boleh mengakses adalah Lab_A dan lab_B, lab_C tidak karena tidak disebutkan pada http_access

Web Filtering

- Menggunakan acl dstdom_regex
- Gunakan options –i untuk menjadikannya CASE-INSENSITIVE (huruf besar huruf kecil sama saja)

- Untuk memfilter website www.detik.com
  - acl web_terlarang url_regex –i www.detik.com
  - acl web_terlarang url_regex –i www.jerapah.com

Implementasi Web Filtering

- acl web_terlarang dstdom_regex –i www.detik.com
- acl web_terlarang dstdom_regex –i www.jerapah.com

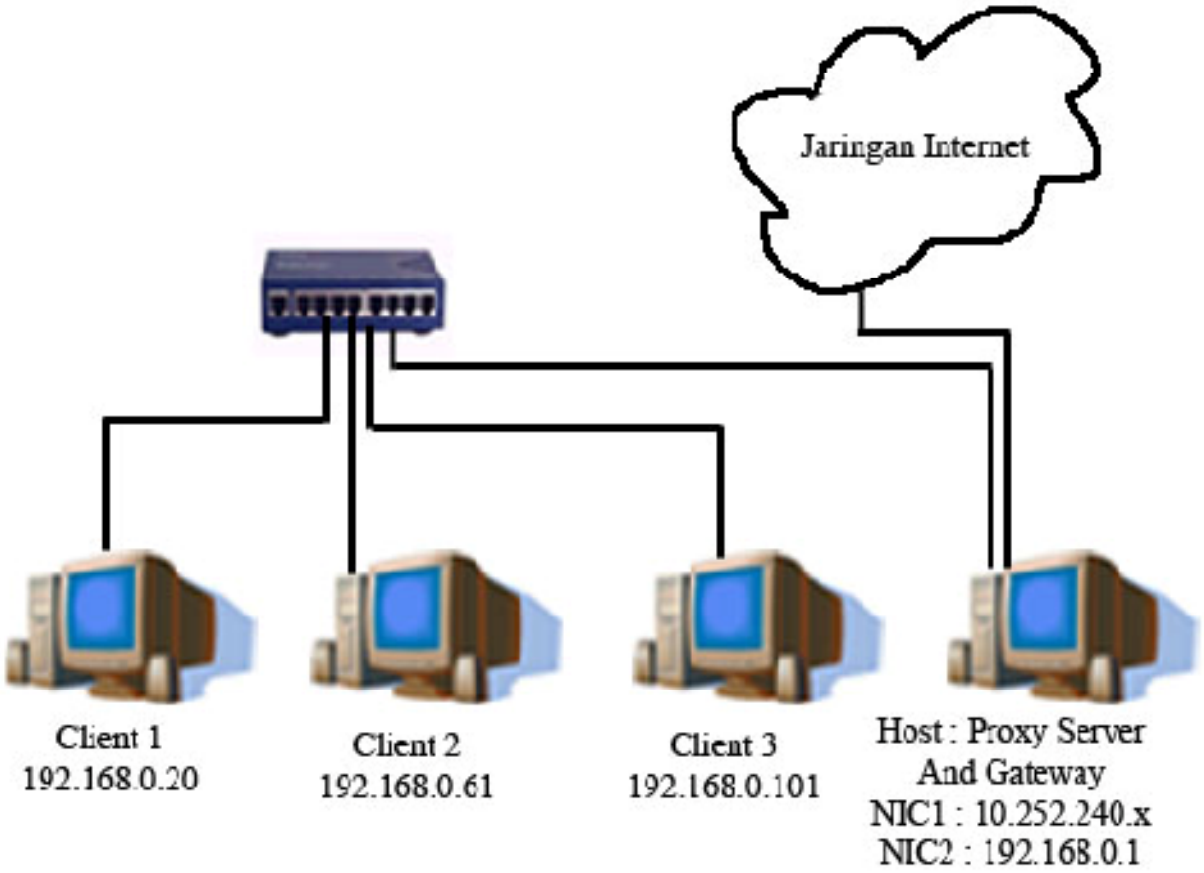
- http_access deny web_terlarang
- http_access allow LabA LabB
- http_access deny all

Management Bandwidth

Opsi-Opsi yang digunakan adalah

- menentukan jumlah aturan yang dipakai
  - delay_pool pool
- Menentukan kelas masing-masing pool
  - delay_class pool kelas
- Menentukan parameter masing-masing pool sesuai kelas yang digunakan
  - delay_parameters pool parameter
- Menentukan hak akses penggunaan bandwidth
  - delay_access pool allow | deny [!]nama_acl

Studi Kasus


Jaringan Internet
Client 1
192.168.0.20
Client 2
192.168.0.61
Client 3
192.168.0.101
Host : Proxy Server
And Gateway
NIC1 : 10.252.240.x
NIC2 : 192.168.0.1

- Port yang digunakan 8080 yang melewati IP 192.168.0.1
- Cache_peer proxy.eepis-its.edu
- Client1 akses pada hari Senin – Jum'at 24 jam
- Client 2 akses pada jam kerje Senin – Jum'at 08:00-18:00
- Client 3 akses pada hari sabtu dan minggu 24 jam
- Beberapa situs-situs terlarang diblok

Konfigurasi Port

- Squid berjalan pada IP 192.168.0.1 dan port 8080
  - http_port 192.168.0.1:8080
- Cache_peer
  - cache_peer proxy.eepis-its.edu parent 443 0
- Karena untuk mengakses proxy.eepis-its.edu harus menggunakan authentikasi maka saya perlu menambahkan :
  - login=share@student.eepis-its.edu:share
    - share@student.eepis-its.edu=username
    - share = password

Konfigurasi ACL

- Authentikasi
  - acl butuhpasswd proxy_auth REQUIRED
- Filter situs secara eksternal
  - acl domainterlarang dstdomain “/etc/squid/domain-terlarang.txt”
  - acl kataterlarang url_regex -i "/etc/squid/kata-terlarang.txt"
  - acl ipterlarang dst "/etc/squid/ip-terlarang.txt“
  - acl nonterlarang url_regex -i "/etc/squid/non-terlarang.txt“
- Filter IP yang boleh akses internet
  - acl lan src 192.168.0.2-192.168.0.254/255.255.255.255
  - acl client1 src 192.168.0.20/255.255.255.255
  - acl client2 src 192.168.0.61/255.255.255.255
  - acl client3 src 192.168.0.101/255.255.255.255

Konfigurasi Acl ....

- Filter file yang di download (optional)
  - acl download url_regex -i ftp \.exe$ \.mp3$ \.mp4$ \.tar.gz$ \.gz$ \.tar.bz2$ \.rpm$ \.zip$ \.rar$
  - acl download url_regex -i \.avi$ \.mpg$ \.mpeg$ \.rm$ \.iso$ \.wav$ \.mov$ \.dat$ \.mpe$ \.mid$
  - acl download url_regex -i \.midi$ \.rmi$ \.wma$ \.wmv$ \.ogg$ \.ogm$ \.m1v$ \.mp2$ \.wax$
  - acl download url_regex -i \.m3u$ \.asx$ \.wpl$ \.wmx$ \.dvr-ms$ \.snd$ \.au$ \.aif$ \.asf$ \.m2v$
  - acl download url_regex -i \.m2p$ \.ts$ \.tp$ \.trp$ \.div$ \.divx$ \.mod$ \.vob$ \.aob$ \.dts$
  - acl download url_regex -i \.ac3$ \.cda$ \.vro$ \.deb$
- Filter waktu akses internet
  - acl hari time M T W H F
  - acl jam_kerja time M T W H F 08:00-18:00
  - acl sabtuminggu time A S

Konfigurasi http_access

- Aturan akses situs-situs terlarang
  - http_access deny domainterlarang
  - http_access deny kataterlarang
  - http_access deny ipterlarang
  - http_access allow nonterlarang
- Aturan user yang bisa akses internet
  - http_access deny lan
  - http_access deny client1 !hari
  - http_access deny client2 !jam_kerja
  - http_access deny client3 !sabtuminggu
  - http_access allow manager
  - http_access allow localhost
  - http_access deny !Safe_ports
  - http_access deny CONNECT !SSL_ports

- Aturan penggunaan autentikasi user
  - http_access allow butuhpasswd
- Aturan yang terakhir ini adalah untuk membatasi selain user yang telah didefinisikan di atas tidak bisa mengakses dan diakses
  - http_access deny all

Konfigurasi Akhir

- Setelah konfigurasi selesai, simpan file konfigurasi
  - Stop squid lalu jalankan perintah /usr/bin/squid –z untuk membuat direktori cache
  - Buat file domain-terlarang.txt, kata-terlarang.txt, ip-terlarang.txt, non-terlarang.txt pada direktori /etc/squid
    - cd /etc/squid
    - touch domain-terlarang.txt kata-terlarang.txt ip-terlarang.txt non-terlarang.txt
  - Masukkan nama domain, kata-kata serta ip yang akan diblok pada masing-masing file.
- Jalankan squid
  - /etc/init.d/squid start