PENILAIAN HARIAN
PRAKTIK KONFIGURASI MIKROTIK – MTCNA
Firewall Filter: Blokir Akses Client Tertentu & Blokir Website

Kompetensi Keahlian	: Teknik Jaringan Komputer dan Telekomunikasi (TJKT)
Kelas / Semester	: XI TJKT dan XII TJKT
Mata Pelajaran	: Administrasi Infrastruktur Jaringan (Konsentrasi TJKT)
Materi Pokok	: Firewall Mikrotik – Address List, Filter Rule (Blokir Client & Website)
Media Praktik	: Simulator GNS3 (Topologi: Cloud/NAT – Router Mikrotik – Switch – 2 Client Webterm)
Alokasi Waktu	: 4 x 35 menit (140 menit) — 1 kali pertemuan
Sifat Tugas	: Individu (praktik mandiri di topologi GNS3 masing-masing)
Pengumpulan Tugas	: File laporan format .docx, dikirim ke email yusufburhani06@gmail.com

A. Kompetensi Dasar dan Tujuan Pembelajaran

Setelah melaksanakan praktik ini, siswa diharapkan mampu:

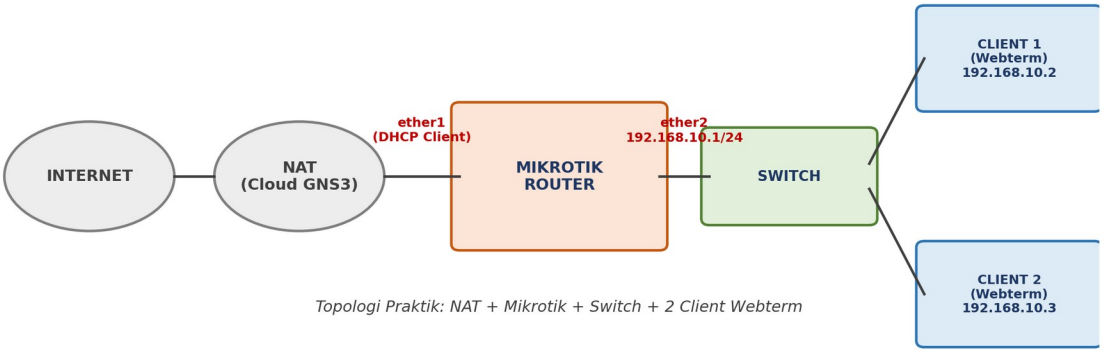
1. Membangun dan mengonfigurasi topologi dasar Mikrotik (NAT, IP Address, DHCP) pada simulator GNS3.
2. Menjelaskan konsep dan cara kerja firewall filter pada Mikrotik (chain input, forward, output).
3. Membuat address-list untuk mengelompokkan client yang akan diblokir aksesnya ke internet.
4. Membuat rule firewall filter untuk memblokir akses internet client tertentu berdasarkan IP Address.
5. Memblokir akses ke website/situs tertentu menggunakan metode address-list pada firewall filter.
6. Menguji dan menganalisis hasil konfigurasi firewall yang telah dibuat.
7. Mendokumentasikan seluruh proses konfigurasi dalam bentuk laporan praktik yang sistematis.

B. Alat dan Bahan

- Laptop/PC dengan aplikasi GNS3 dan GNS3 VM (atau GNS3 versi lokal) yang sudah terinstal.
- Image RouterOS Mikrotik (CHR/x86) yang telah ditambahkan ke GNS3.
- Node NAT (Cloud/NAT GNS3) sebagai penyedia akses internet ke luar.
- Node Client berupa VPCS atau Webterm (browser) sebagai perangkat pengguna.
- Koneksi internet aktif pada komputer praktik (untuk NAT dan pengujian akses website).
- Aplikasi Winbox (opsional) atau terminal console Mikrotik pada GNS3.
- Microsoft Word (atau aplikasi sejenis) untuk menyusun laporan hasil praktik.

C. Topologi Jaringan

Topologi yang digunakan pada praktik ini terdiri dari NAT (sumber internet), 1 Router Mikrotik, 1 Switch, dan 2 Client Webterm, dengan susunan sebagai berikut:



Topologi Praktik: NAT + Mikrotik + Switch + 2 Client Webterm

Kedua client terhubung ke Mikrotik melalui 1 switch pada ether2, sehingga berada pada satu subnet yang sama (192.168.10.0/24). Dengan adanya 2 client ini, hasil blokir client tertentu dapat dibandingkan secara langsung: client yang diblokir tidak bisa akses internet, sedangkan client yang tidak diblokir tetap normal.

Gunakan skema pengalamatan IP berikut ini (silakan sesuaikan dengan hasil DHCP dari NAT GNS3 jika berbeda, catat IP yang sebenarnya didapat di laporan):

Perangkat	Interface	IP Address	Keterangan
Mikrotik	ether1	DHCP Client (ke NAT)	Koneksi ke internet
Mikrotik	ether2	192.168.10.1/24	Gateway untuk client (via switch)
Client 1 Webterm	eth0	192.168.10.2/24 (DHCP dari Mikrotik)	Client yang akan diblokir
Client 2 Webterm	eth0	192.168.10.3/24 (DHCP dari Mikrotik)	Client pembanding (tetap normal)

D. Dasar Teori Singkat

1. Firewall Filter

Firewall filter pada Mikrotik bekerja berdasarkan chain (jalur lalu lintas paket data):

- input: paket yang ditujukan ke router itu sendiri.
- forward: paket yang melewati router (misalnya dari client menuju internet).
- output: paket yang berasal dari router menuju luar.

Untuk memblokir akses internet client, rule dipasang pada chain forward karena traffic client menuju internet melewati router.

2. Address List

Address-list adalah kumpulan/daftar IP Address yang diberi nama tertentu, sehingga satu rule firewall dapat diterapkan ke banyak IP sekaligus, dan lebih mudah dikelola dibanding menuliskan IP satu per satu di setiap rule. Address-list dapat berisi IP client (untuk memblokir client tertentu, seperti pada Tahap 3) maupun IP address dari sebuah website (untuk memblokir akses ke website tertentu, seperti pada Tahap 4).

3. Memblokir Website dengan Address List

Setiap website pada dasarnya diakses melalui sebuah IP Address server. Dengan mencari tahu IP Address dari sebuah domain (misalnya menggunakan perintah ping dari Mikrotik), IP tersebut dapat dimasukkan ke dalam address-list,

kemudian dibuatkan rule firewall filter pada chain forward dengan parameter dst-address-list untuk memblokir seluruh trafik menuju IP tersebut. Perlu diperhatikan bahwa sebagian website besar menggunakan lebih dari satu server (CDN) dengan beberapa IP Address berbeda, sehingga mungkin perlu menambahkan lebih dari satu IP ke dalam address-list agar blokir lebih maksimal.

E. Langkah Kerja

Tahap 1 – Persiapan Topologi (± 15 menit)

8. Buka aplikasi GNS3, lalu buka project topologi Mikrotik (NAT + Mikrotik + Switch + 2 Client Webterm) yang sudah tersedia.
9. Jalankan (start) semua node pada topologi: NAT, Router Mikrotik, Switch, Client 1 Webterm, dan Client 2 Webterm.
10. Buka console Mikrotik melalui klik kanan node Mikrotik → Console.

Tahap 2 – Konfigurasi Dasar Mikrotik (± 25 menit)

Ketikkan perintah berikut pada terminal Mikrotik satu per satu:

```
# Mengaktifkan DHCP Client pada ether1 (arah NAT/internet)
/ip dhcp-client add interface=ether1 disabled=no

# Memberi IP address statis pada ether2 (arah client)
/ip address add address=192.168.10.1/24 interface=ether2

# Mengaktifkan NAT (masquerade) agar client bisa akses internet
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

# Mengaktifkan DHCP Server untuk client pada ether2
/ip pool add name=pool-client ranges=192.168.10.2-192.168.10.100
/ip dhcp-server add interface=ether2 address-pool=pool-client disabled=no
/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-
server=192.168.10.1
```

Pada Client 1 Webterm dan Client 2 Webterm, atur network interface agar menggunakan DHCP (obtain IP automatically), kemudian buka browser pada kedua client dan pastikan keduanya bisa mengakses internet (misalnya membuka google.com) sebelum melanjutkan ke tahap blokir. Catat IP yang didapat masing-masing client (seharusnya 192.168.10.2 dan 192.168.10.3).

Tahap 3 – Studi Kasus 1: Blokir Akses Client Tertentu (± 40 menit)

Skenario: dari 2 client yang tersedia, hanya SATU client sesuai penugasan pada Tabel F (192.168.10.2 atau 192.168.10.3) yang akan diblokir aksesnya ke internet, sedangkan client yang satunya harus tetap bisa mengakses internet secara normal. Skenario ini membuktikan bahwa rule firewall yang dibuat benar-benar menyasar client tertentu saja, bukan memblokir seluruh jaringan. Pada contoh perintah di bawah ini digunakan Client 1 (192.168.10.2); jika client yang ditugaskan kepada kalian adalah Client 2, ganti IP address pada perintah menjadi 192.168.10.3.

11. Buat address-list untuk menampung IP client yang akan diblokir:

```
/ip firewall address-list add list=Client_Blokir address=192.168.10.2/32
comment="Client yang diblokir aksesnya"
```

12. Buat rule firewall filter pada chain forward untuk memblokir client tersebut:

```
/ip firewall filter add chain=forward src-address-list=Client_Blokir action=drop \
  comment="Blokir akses internet untuk client tertentu" place-before=0
```

13. Pastikan rule berada pada urutan paling atas (di atas rule accept/masquerade lain) menggunakan perintah:

```
/ip firewall filter print
```

14. Uji dari client yang diblokir: coba akses browser ke situs mana saja. Pastikan akses gagal (timeout/tidak bisa terhubung).
15. Uji dari client yang TIDAK diblokir: coba akses browser ke situs mana saja. Pastikan akses tetap berhasil normal (karena IP-nya tidak masuk address-list Client_Blokir).

16. Ambil screenshot hasil pengujian pada kedua client (yang diblokir gagal, yang tidak diblokir normal) sebagai bukti perbandingan pada laporan.
17. Nonaktifkan sementara rule blokir (disable, jangan dihapus) untuk membandingkan kondisi sebelum dan sesudah, lalu uji kembali akses internet dari client yang tadi diblokir, dan ambil screenshot-nya.

```
/ip firewall filter disable [find comment="Blokir akses internet untuk client
tertentu"]
```

Tahap 4 – Studi Kasus 2: Blokir Website Tertentu (± 40 menit)

Skenario: seluruh client pada jaringan tetap bisa mengakses internet secara umum, namun tidak boleh membuka website tertentu menggunakan address-list. Website yang wajib diblokir SAMA untuk seluruh siswa (kelas XI dan XII), yaitu: facebook.com.

18. Nonaktifkan (disable) rule Client_Blokir dari Tahap 3 terlebih dahulu, agar kedua client (Client 1 dan Client 2) sama-sama bisa akses internet normal sebelum menguji blokir website.
19. Cari tahu IP Address dari website facebook.com menggunakan perintah ping pada terminal Mikrotik:

```
/ping facebook.com count=3
```

20. Catat IP Address yang muncul pada hasil ping tersebut. Ulangi ping beberapa kali (2–3 kali) untuk melihat apakah IP yang muncul selalu sama atau berbeda-beda (indikasi website menggunakan CDN dengan banyak server).
21. Tambahkan IP Address hasil ping ke dalam address-list khusus untuk website yang diblokir:

```
/ip firewall address-list add list=Web_Blokir address=<IP_hasil_ping_1>
comment="Website diblokir - facebook.com"
/ip firewall address-list add list=Web_Blokir address=<IP_hasil_ping_2>
comment="Website diblokir - facebook.com"
```

22. Buat rule firewall filter pada chain forward untuk memblokir seluruh trafik menuju address-list tersebut:

```
/ip firewall filter add chain=forward dst-address-list=Web_Blokir action=drop \
  comment="Blokir akses ke website tertentu (address-list)"
```

23. Uji akses ke facebook.com dari browser kedua client (Client 1 dan Client 2). Catat hasilnya (berhasil diblokir atau tidak) — pada tahap ini kedua client seharusnya sama-sama terblokir karena rule diterapkan pada chain forward untuk semua trafik, bukan berdasarkan client tertentu.
24. Jika facebook.com masih bisa diakses, kemungkinan IP yang didapat dari ping belum mencakup seluruh server (CDN) yang digunakan website tersebut. Lakukan ping/tracert ulang beberapa kali, lalu tambahkan IP baru yang ditemukan ke dalam address-list Web_Blokir, dan uji kembali.
25. Uji akses ke website lain (misalnya google.com) untuk memastikan internet kedua client tetap berjalan normal dan hanya facebook.com saja yang terblokir.
26. Ambil screenshot untuk seluruh kondisi (isi address-list Web_Blokir, rule firewall filter, akses facebook.com yang gagal, dan akses website lain tetap normal) pada kedua client.

F. Penugasan (Wajib Dikerjakan Setiap Siswa)

Untuk Tahap 4 (blokir website), seluruh siswa WAJIB mengerjakan target yang sama, yaitu memblokir akses ke facebook.com menggunakan metode address-list — tidak dibedakan per nomor absen.

Sedangkan untuk Tahap 3 (blokir client tertentu), agar hasil pekerjaan tiap siswa tetap bisa dibandingkan satu sama lain namun tidak sama persis, client yang diblokir ditentukan berdasarkan nomor absen kalian, dengan ketentuan berikut:

Sisa Bagi (Absen ÷ 2)	Client yang Diblokir Total di Tahap 3
0 (absen genap)	Client 1 (192.168.10.2) — Client 2 tetap normal
1 (absen ganjil)	Client 2 (192.168.10.3) — Client 1 tetap normal

Contoh: siswa dengan nomor absen 12 (genap) → wajib memblokir Client 1 pada Tahap 3. Siswa dengan nomor absen 7 (ganjil) → wajib memblokir Client 2 pada Tahap 3.

Setiap siswa WAJIB menyelesaikan seluruh langkah kerja pada Tahap 1 sampai Tahap 4 di atas: Tahap 3 dengan client sesuai pembagian tabel di atas, dan Tahap 4 dengan target website facebook.com untuk semua siswa.

G. Sistematika Laporan Praktik

Susun laporan hasil praktik dalam file Microsoft Word (.docx) dengan sistematika berikut:

27. Cover / Halaman Judul — berisi judul praktik, nama, kelas, dan tanggal praktik.
28. Tujuan Praktik — tuliskan ulang tujuan pembelajaran pada bagian A.
29. Topologi Jaringan — screenshot topologi GNS3 beserta keterangan IP Address yang digunakan (sesuai hasil praktik, bukan hanya contoh).
30. Langkah Konfigurasi — seluruh perintah/command yang dijalankan pada Mikrotik, disertai screenshot terminal untuk setiap tahap (konfigurasi dasar, blokir client dengan address-list, blokir website dengan address-list).
31. Hasil Pengujian — screenshot browser kedua Client Webterm yang menunjukkan: (a) akses internet normal pada kedua client sebelum diblokir, (b) akses gagal pada client yang diblokir sedangkan client satunya tetap normal (Tahap 3), (c) akses website tertentu gagal pada kedua client setelah diblokir (Tahap 4), (d) akses ke website lain tetap normal pada kedua client.
32. Analisis — jelaskan dengan kalimat sendiri bagaimana address-list bekerja pada rule firewall filter, mengapa src-address-list digunakan untuk blokir client sedangkan dst-address-list digunakan untuk blokir website, dan mengapa blokir website berbasis IP kadang perlu lebih dari satu alamat IP (kaitkan dengan konsep CDN).
33. Kesimpulan — ringkasan hasil praktik yang telah dilakukan.

H. Ketentuan Pengumpulan Tugas

- Laporan dikumpulkan dalam format file .docx (bukan .pdf/.jpg).
- Format nama file: Kelas_NamaLengkap_TugasFirewallMikrotik.docx (contoh: XITJKT1_AhmadFauzan_TugasFirewallMikrotik.docx).
- Laporan dikirim melalui email ke: yusufburhani06@gmail.com
- Subjek email: Tugas Firewall Mikrotik – [Kelas] – [Nama Lengkap]
- Tugas dikumpulkan paling lambat sesuai batas waktu yang disampaikan guru pengampu.
- Pastikan seluruh screenshot pada laporan jelas terbaca (tidak buram/terpotong).

I. Rubrik Penilaian

Aspek Penilaian	Bobot	Keterangan
Konfigurasi dasar Mikrotik (IP, DHCP, NAT) berjalan benar	20%	Kedua client mendapat IP dan bisa akses internet sebelum tahap blokir
Blokir akses client tertentu berhasil (Tahap 3)	25%	Address-list dan rule filter benar; hanya 1 client terblokir, client lain tetap normal (terbukti dari screenshot)
Blokir website facebook.com berhasil (Tahap 4)	25%	Address-list Web_Blokir dan rule dst-address-list berhasil memblokir facebook.com pada kedua client
Kelengkapan dan kejelasan dokumentasi (screenshot & command)	15%	Semua tahap terdokumentasi dengan screenshot yang relevan
Analisis dan kesimpulan	15%	Penjelasan logis, menggunakan bahasa sendiri, sesuai hasil praktik

Selamat mengerjakan. Kerjakan secara mandiri, jujur, dan teliti dalam setiap tahap konfigurasi.