

Practice Managing Internet Connection Campus Network Area (CAN) **With Firewall & Address List** **MikroTik Router**

By Juniar Sinaga

Jakarta

MUM Indonesia, April 2011



Speaker Profile

- Studied Pasca Sarjana major of MIS, STMIK Nusa Mandiri, Jakarta.
- Have been working on campus Bina Sarana Informatika (BSI) since 2004.
- Lecturer in Computer Technic on BSI.
- IT Support & Maintenance on BSI.
- Using MikroTik Router OS since June 2010.



juniar_sinaga@yahoo.com

CAN (Campus Area Network) Concept

“Computer network made up of an interconnection of local area networks (LAN's) within a limited geographical area”.

- Terdiri dari interkoneksi jaringan area lokal (LAN) dalam wilayah geografis yang terbatas.
- Pengembangan jaringan LAN yang mencakup satu kampus yang lebih luas dan terintegrasi.

CAN (Campus Network) Concept

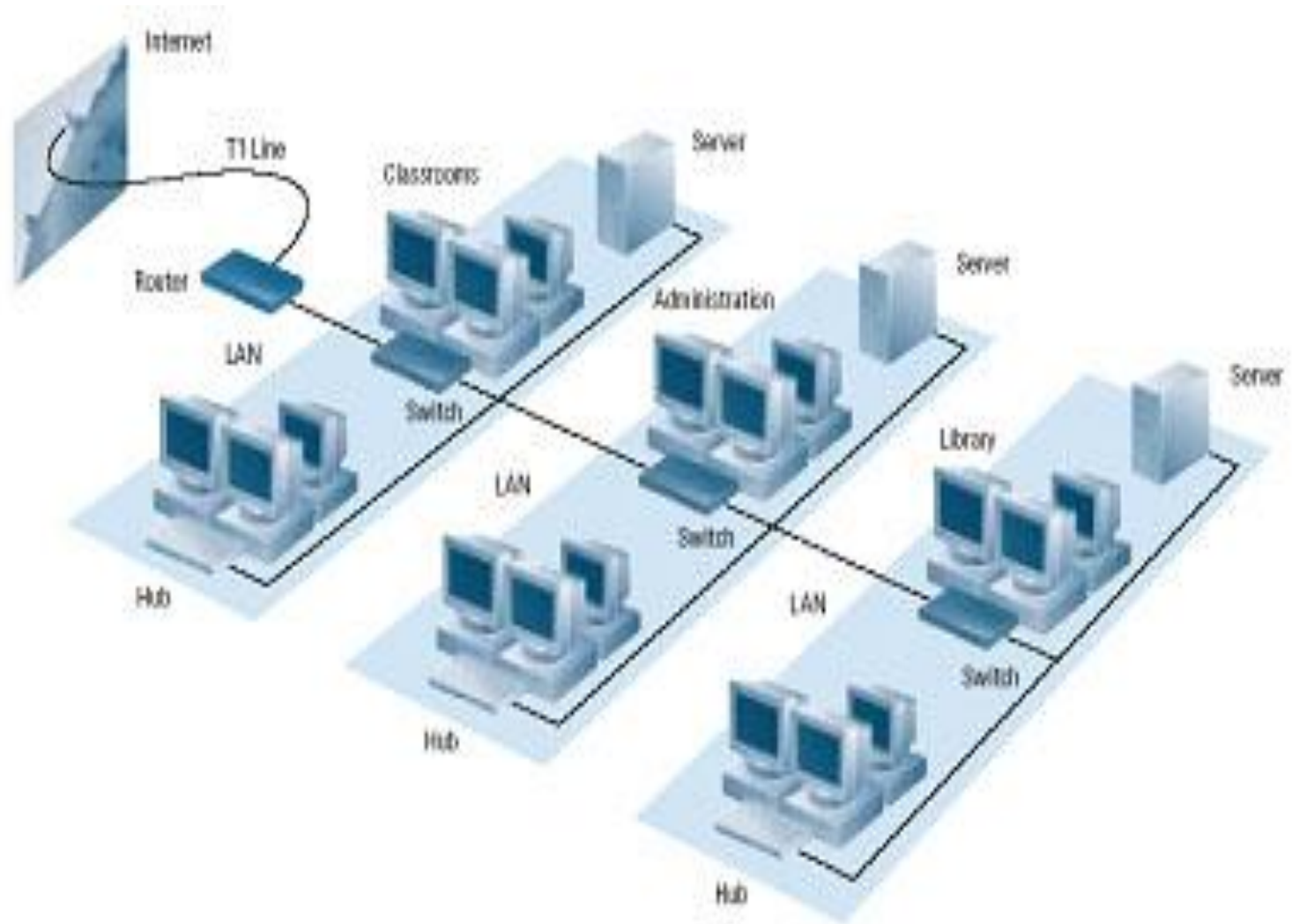
Universitas atau kampus yang berbasis networking dan memungkinkan untuk menghubungkan beberapa bangunan kampus seperti:

- Departemen / fakultas akademik.
- Perpustakaan (Library).
- Laboratorium (Lab).
- Branch (Cabang Kampus).

Characteristics of CAN

- Devices interconnected.
- Sharing of resources.
- Remote access connection.
- Hotspot area.
- Ect.

Infrastructure Of CAN



Problem On Network Area Campus

- Troubled for maintenance.
- Free access for illegal site (porn ,sex, ect).
- Free streaming and downloading illegal video.
- Hacking the router.

How to Solve ?

Manage internet connection using *Firewall* *for:*

- Drop illegal traffic.
- Restrict access to the network services.
- Protect local traffic.
- Limit access to the router with WB.

Targets

- Controlling Internet Traffic:
 - ✓ Streaming and downloading.
 - ✓ Social networking.
- Reducing internet bandwidth.
- Increasing router performance.
- “INSAN (Internet Sehat Dan Aman) Goes To Campus”.
- Supporting “Cloud Computing” technology.



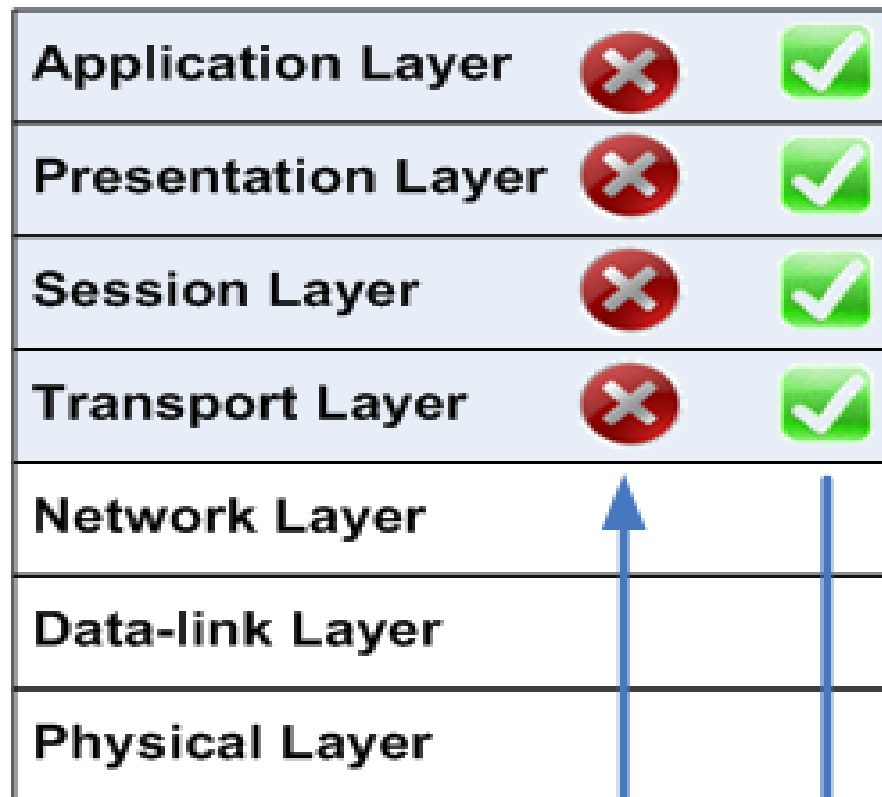
Which firewall will be used?

MikroTik Firewall & Address List

- ❖ Easy to manage system.
- ✓ *Just 2 Action, enjoy your rule.*
- ❖ Fully optimizes your network usage.
- ✓ *Use stateful firewall.*

Stateful firewall

Stateful Firewall



Lalu lintas akan disaring pada banyak level berdasarkan peraturan packet filtering, session, atau aplikasi,

Lalu lintas yang tidak lolos penyaringan akan diblok pada level Network Layer

—Lalu lintas yang datang—

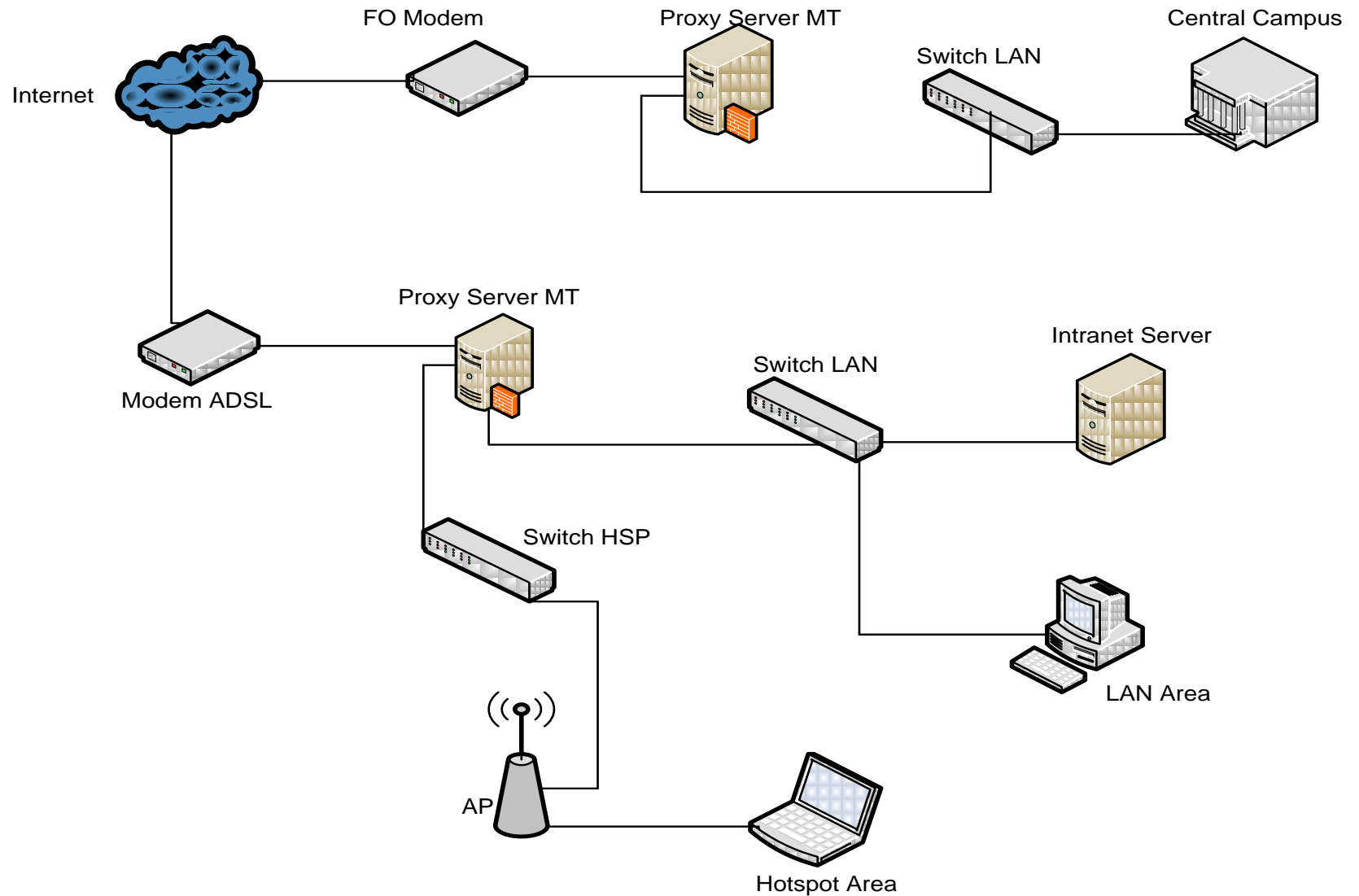
—Lalu lintas yang diizinkan—

Address Lists

“Address lists was introduced to assign multiple IP addresses/ranges to the same firewall rule, in this way reducing the total number of firewall rules and increasing router performance”

“Address diperkenalkan untuk menetapkan beberapa alamat IP /range IP untuk aturan firewall yang sama, mengurangi banyaknya rule pada firewall, sehingga meningkatkan kinerja router”.

Basic Network Topology



CAN (Campus Area Network)

Skenario IP Address

- Modem IP : (118.96.x.y)
- LAN IP : 172.16.x.0/22
- HSP IP : 10.10.y.0/24

Drop/Block site with Firewall MT using content.

❖ *Just 2 Action...*

- 1. Create Mangle.*
- 2. Drop / block with Firewall filter .*

Mangle create for drop YT

Mangle Rule <> [X]

General | **Advanced** | Extra | Action | Statistics

Chain: ▼

Src. Address: ▼

Dst. Address: ▼

Protocol: ▼

Src. Port: ▼

Dst. Port: ▼

Any. Port: ▼

P2P: ▼

In. Interface: ▼

Out. Interface: ▼

Packet Mark: ▼

Connection Mark: ▼

Routing Mark: ▼

Connection Type: ▼

Connection State: ▼

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Block With Content

Mangle Rule <> [X]

General Advanced Extra Action Statistics

Src. Address List: [] ▼

Dst. Address List: [] ▼

Layer7 Protocol: [] ▼

Content: ☐ youtube.com ▲

Connection Bytes: [] ▼

Src. MAC Address: [] ▼

Out. Bridge Port: [] ▼

In. Bridge Port: [] ▼

Ingress Priority: [] ▼

DSCP (TOS): [] ▼

TCP MSS: [] ▼

Packet Size: [] ▼

Random: [] ▼

▼ TCP Flags

▼ ICMP Options

IPv4 Options: [] ▼

disabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Action in mangle

Mangle Rule <> [X]

General Advanced Extra **Action** Statistics

Action: [v]

Address List: [v]

Timeout: [v]

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

disabled

Filter rule for block YT

Firewall Rule <> [X]

General | **Advanced** | Extra | Action | Statistics

Chain: ▼

Src. Address: ▼

Dst. Address: ▼

Protocol: ▼

Src. Port: ▼

Dst. Port: ▼

Any. Port: ▼

P2P: ▼

In. Interface: ▼

Out. Interface: ▼

Packet Mark: ▼

Connection Mark: ▼

Routing Mark: ▼

Connection Type: ▼

Connection State: ▼

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Destination address list

Firewall Rule <>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List: ☐ youtube

Layer7 Protocol:

Content:

Connection Bytes:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

Ingress Priority:

DSCP (TOS):

TCP MSS:

Packet Size:

Random:

▼ TCP Flags

▼ ICMP Options

IPv4 Options:

OK

Cancel

Apply

Disable

Comment

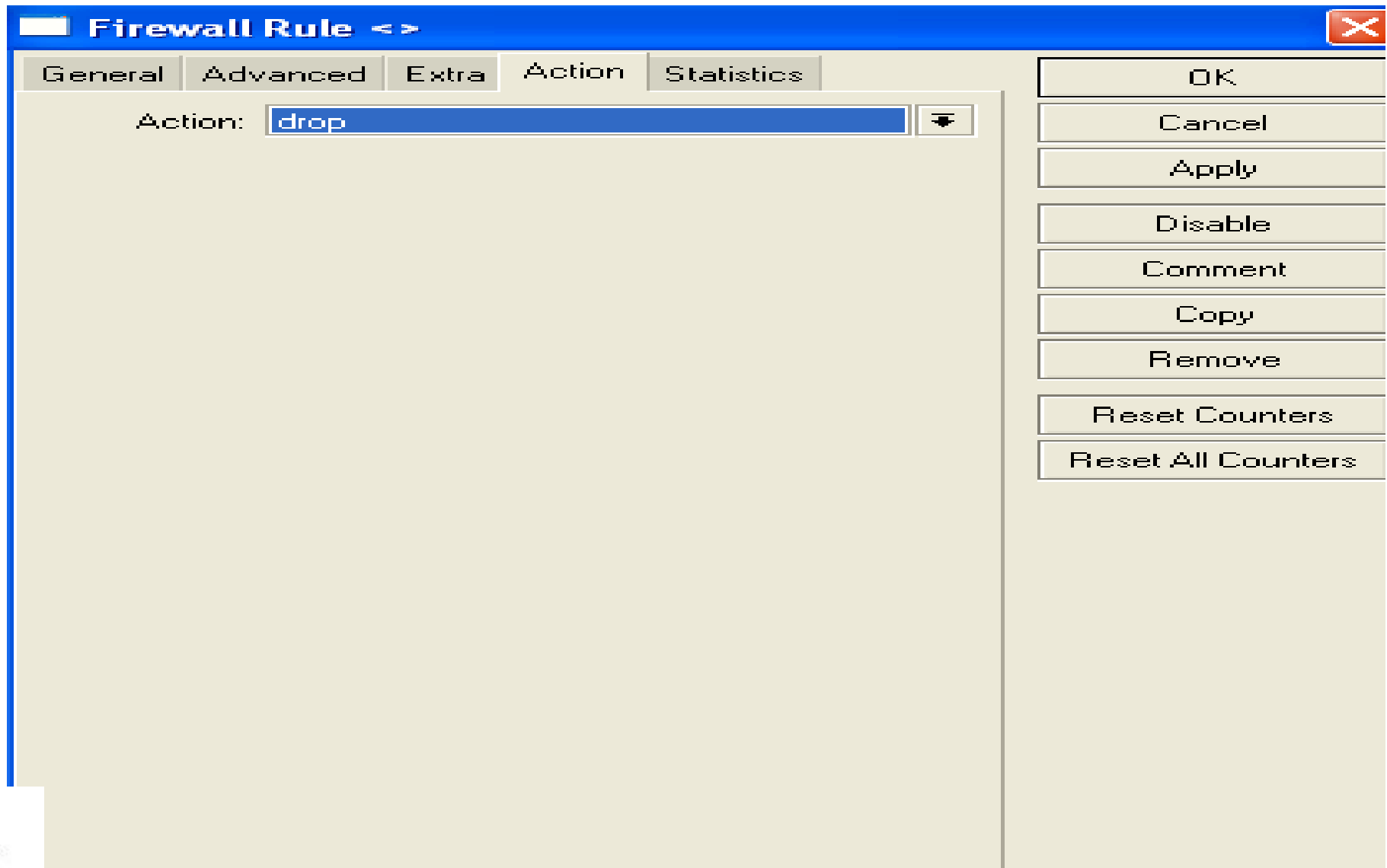
Copy

Remove

Reset Counters

Reset All Counters

Action to drop youtube



Firewall Rule <>

General Advanced Extra **Action** Statistics

Action:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Output Firewall filt rule

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
17	<input checked="" type="checkbox"/> add dst to address list	forward			6 (tcp)				
::: Limit BW D/W zip									
18	<input checked="" type="checkbox"/> add dst to address list	forward			6 (tcp)				
::: Limit BW D/W avi									
19	<input checked="" type="checkbox"/> add dst to address list	forward			6 (tcp)				
::: Limit BW D/W flv									
20	<input checked="" type="checkbox"/> add dst to address list	forward			6 (tcp)				
::: Port scanners to list									
22	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: NMAP FIN Stealth scan									
24	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: SYN/FIN scan									
26	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: SYN/RST scan									
27	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: FIN/PSH/URG scan									
28	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: ALL/ALL scan									
29	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: NMAP NULL scan									
30	<input checked="" type="checkbox"/> add src to address list	input			6 (tcp)				
::: Drop YT									
0	<input checked="" type="checkbox"/> drop	forward							
::: Blok All P2P									
2	<input checked="" type="checkbox"/> drop	forward							
::: Block Porn With Layer 7									
3	<input checked="" type="checkbox"/> drop	forward							
::: Blok SSH									
4	<input checked="" type="checkbox"/> drop	input			6 (tcp)		22	ether2	
::: Blok FTP									

0 items (1 selected)

Drop/Block Acces WB With Address List

❖ *Just 2 Action...*

- 1. Create Address list for block .*
- 2. Drop with Firewall filter .*

Address List

Firewall

Filter Rules NAT Mangle Service Ports Connections **Address Lists** Layer7 Protocols

Find all

Name	Address
Allow Access WB For IT	
allow access winbox	172.16.72.111-172.16.72.113
Allow Access WB For ADM	
allow access winbox	172.16.72.2
Deny Access WB For Ruang Kerja	
deny access winbox	172.16.72.3-172.16.72.30
Deny Access WB For Kelas	
deny access winbox	172.16.72.31-172.16.72.50
Deny Access WB For Wacah	
deny access winbox	172.16.72.114-172.16.72.119
Deny Access WB For DHCP	
deny access winbox	172.16.72.120-172.16.72.249
D downloads	172.16.72.111
D downloads	172.16.72.46
D downloads	125.160.18.58
Drop Internet Global Yang Tidak Digunakan	
drop internet	172.16.72.220-172.16.72.249
Drop Internet DHCP	
drop internet	172.16.72.119-172.16.72.219
Drop Internet DHCP1	
drop internet	172.16.73.0/24
Drop Internet DHCP2	
drop internet	172.16.74.0/24
Drop Internet DHCP3	
drop internet	172.16.75.0/24
drop internet	172.16.72.25
Drop Internet IP R.Dosen Yang Tidak Digunakan	
drop internet	172.16.72.25-172.16.72.30
Drop Internet Kelas Ujian	
drop internet ujian	172.16.72.31-172.16.72.50

17 items (1 selected)

Create firewall filter for drop WB

Firewall Rule <> [X]

General | **Advanced** | Extra | Action | Statistics

Chain: ▼

Src. Address: ▼

Dst. Address: ▼

Protocol: ▼

Src. Port: ▼

Dst. Port: ▼

Any. Port: ▼

P2P: ▼

In. Interface: ▼

Out. Interface: ▼

Packet Mark: ▼

Connection Mark: ▼

Routing Mark: ▼

Connection Type: ▼

Connection State: ▼

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Address list “deny access winbox”

Firewall Rule <>

General Advanced Extra Action Statistics

Src. Address List: ▼ ▲

Dst. Address List: ▼

Layer7 Protocol: ▼

Content: ▼

Connection Bytes: ▼

Src. MAC Address: ▼

Out. Bridge Port: ▼

In. Bridge Port: ▼

Ingress Priority: ▼

DSCP (TOS): ▼

TCP MSS: ▼

Packet Size: ▼

Random: ▼

▼ TCP Flags

▼ ICMP Options

IPv4 Options: ▼

OK

Cancel

Apply

Disable

Comment

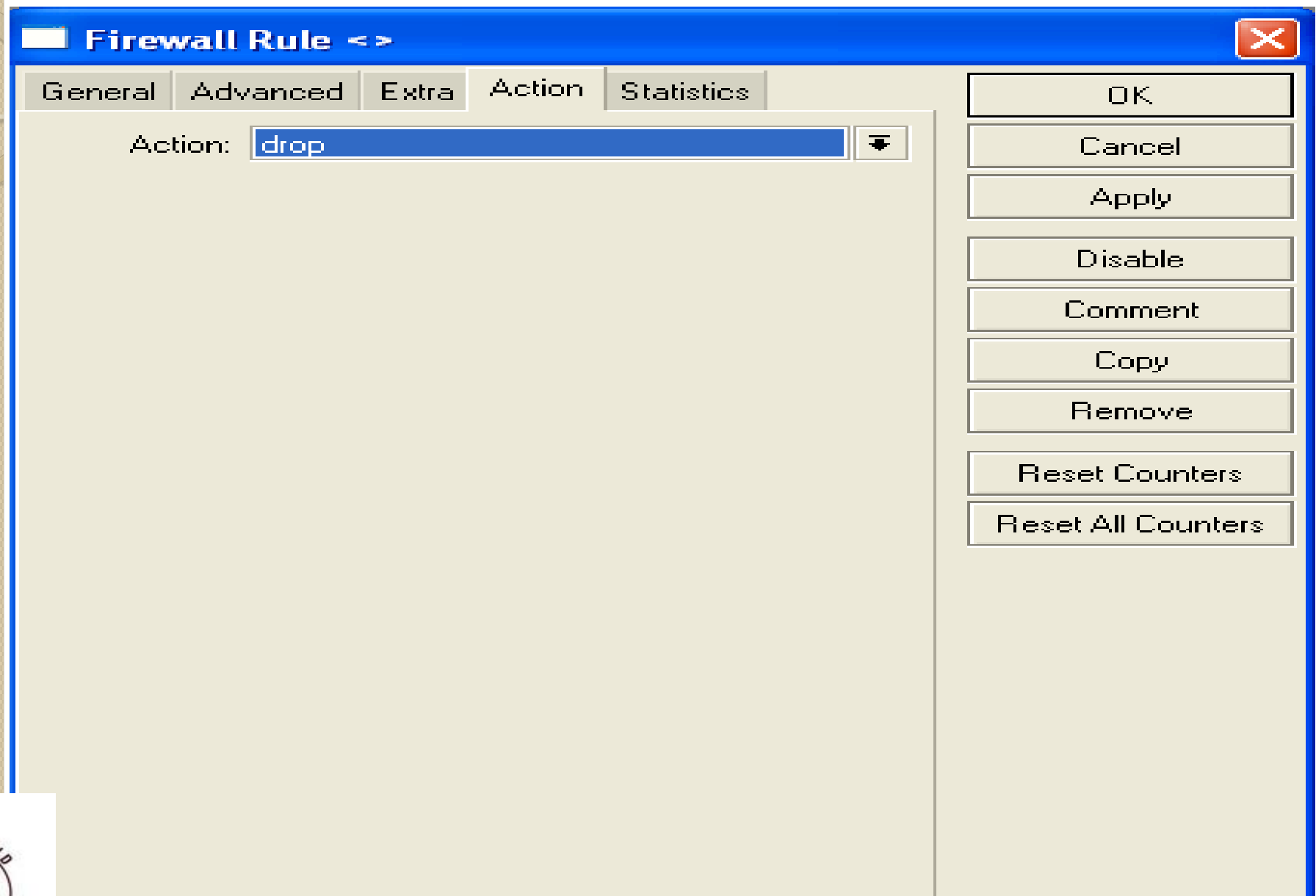
Copy

Remove

Reset Counters

Reset All Counters

Drop access WB with firewall filt



Drop access WB from HSP

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

Find all

Name	Address
Allow Access WB For IT	
allow access winbox	172.16.72.111-172.16.72.113
Allow Access WB For ADM	
allow access winbox	172.16.72.2
Deny Access WB For Ruang Kerja	
deny access winbox	172.16.72.3-172.16.72.30
Deny Access WB For Kelas	
deny access winbox	172.16.72.31-172.16.72.50
Deny Access WB For Wacth	
deny access winbox	172.16.72.114-172.16.72.119
Deny Access WB For DHCP	
deny access winbox	172.16.72.120-172.16.72.249
Deny Access WB For HSP	
deny access winbox	10.10.1.0/24
Drop Internet Global Yang Tidak Digunakan	
drop internet	172.16.72.220-172.16.72.249
Drop Internet DHCP	
drop internet	172.16.72.119-172.16.72.219
Drop Internet DHCP1	
drop internet	172.16.73.0/24
Drop Internet DHCP2	
drop internet	172.16.74.0/24
Drop Internet DHCP3	
drop internet	172.16.75.0/24
drop internet	172.16.72.25
Drop Internet IP R.Dosen Yang Tidak Digunakan	
drop internet	172.16.72.25-172.16.72.30
Drop Internet Kelas Ujian	
drop internet ujian	172.16.72.31-172.16.72.50

15 items (1 selected)

Conclusion

Mikrotik Firewall & address list, easy setup and configure.

- ✓ MT Firewall is easy, simple, and practice to drop /block site (Just 2 Action, enjoy your blocking).
- ✓ MT Firewall easy to protect router from ext and int network.
- ✓ Another technic to block site with MT using WebProxy.

Reference

- <http://www.mikrotik.com/testdocs/ros/3.0/refman3.0.pdf>
- http://wiki.mikrotik.com/wiki/Dmitry_on_firewalling
- http://en.wikipedia.org/wiki/Green_computing
- http://en.wikipedia.org/wiki/Computer_network#Campus_network