

## LAMPIRAN

## L7 Protocols - Regexp “streaming”



## L7 Protocols - Regexp “drop-porn”



## L7 Protocols - Regexp “sosmed-drop”



## Firewall Filter “drop-porn” & “sosmed-drop” Blocking

```

3   ;;; block porn by keywords
   chain=forward action=drop layer7-protocol=drop-porn

4   ;;; social media drop
   chain=forward action=drop layer7-protocol=sosmed-drop

```

## Firewall Filter Protocol TCP & ICMP

```

6   ;;; TCP dan ICMP ltel
   chain=input action=drop protocol=tcp in-interface=ltel dst-port=20,21,22,23,8291

7   chain=input action=accept connection-state=established protocol=icmp in-interface=ltel

8   chain=input action=drop protocol=icmp in-interface=ltel

9   ;;; TCP dan ICMP ether2
   chain=input action=accept src-address-list=admin in-interface=ether2

10  chain=input action=add-src-to-address-list protocol=tcp src-address-list=jaringan lokal
    address-list=akses ilegal address-list-timeout=0s in-interface=ether2
    dst-port=20,21,22,23,8291

11  chain=input action=drop protocol=tcp src-address-list=jaringan lokal in-interface=ether2
    dst-port=20,21,22,23,8291

12  chain=input action=accept connection-state=established protocol=icmp in-interface=ether2

13  chain=input action=add-src-to-address-list protocol=icmp src-address-list=jaringan lokal
    address-list=ping ilegal address-list-timeout=0s in-interface=ether2

14  chain=input action=drop protocol=icmp src-address-list=jaringan lokal in-interface=ether2

15  ;;; TCP dan ICMP wlan1
   chain=input action=add-src-to-address-list protocol=tcp src-address-list=wireless lokal
    address-list=akses ilegal address-list-timeout=0s in-interface=wlan1
    dst-port=20,21,22,23,8291

16  chain=input action=drop protocol=tcp src-address-list=wireless lokal in-interface=wlan1
    dst-port=20,21,22,23,8291

17  chain=input action=accept connection-state=established protocol=icmp in-interface=wlan1

18  chain=input action=add-src-to-address-list protocol=icmp src-address-list=wireless lokal
    address-list=ping ilegal address-list-timeout=0s in-interface=wlan1

19  chain=input action=drop protocol=icmp src-address-list=wireless lokal in-interface=wlan1

```

## Script List “sosmed-allow” &amp; “sosmed-drop”

```
[admin@MikroTik] > /system script print
Flags: I - invalid
 0  name="sosmed-allow" owner="admin"
    policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api
    last-started=jun/23/2014 11:08:45 run-count=5
    source=/ip firewall filter set [find comment="social media drop"] disabled=yes

 1  name="sosmed-drop" owner="admin"
    policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api
    last-started=jun/23/2014 13:00:00 run-count=7
    source=/ip firewall filter set [find comment="social media drop"] disabled=no
[admin@MikroTik] >
```

## Scheduler List “sosmed-allow” &amp; “sosmed-drop” Running

```
[admin@MikroTik] > /system scheduler print
Flags: X - disabled
#  NAME          START-DATE  START-TIME  INTERVAL  ON-EVENT          RUN-COUNT
0  sunday        jun/22/2014 00:00:00  1w        sosmed-allow      0
1  weekdays...   jun/22/2014 08:00:00  1d        sosmed-drop       0
2  weekdays...   jun/22/2014 12:00:00  1d        sosmed-allow      0
3  weekdays...   jun/22/2014 17:00:00  1d        sosmed-allow      0
4  weekdays...   jun/22/2014 13:00:00  1d        sosmed-drop       0
[admin@MikroTik] >
```

## Address List Firewall

```
Terminal
[admin@MikroTik] > /ip firewall address-list print
Flags: X - disabled, D - dynamic
#  LIST          ADDRESS          TIMEOUT
0  jaringan lokal 192.168.88.0/24
1  wireless lokal 10.5.50.0/24
2  admin          192.168.88.2
```

## Firewall Mangle Rule

```

Terminal
[admin@MikroTik] > /ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
0   ;;; BROWSING LOKAL
    chain=prerouting action=mark-connection new-connection-mark=http.IIX.con
    passthrough=yes protocol=tcp src-address-list=wireless lokal
    dst-address-list=nice dst-port=80,443,3128,8080,182 connection-bytes=0-131072

1   chain=prerouting action=mark-packet new-packet-mark=http.IIX passthrough=yes
    connection-mark=http.IIX.con

2   ;;; BROWSING LOKAL LAN
    chain=prerouting action=mark-connection new-connection-mark=http.IIX.con.lan
    passthrough=yes protocol=tcp src-address-list=jaringan lokal
    dst-address-list=nice dst-port=80,443,3128,8080,182 connection-bytes=0-131072

3   chain=prerouting action=mark-packet new-packet-mark=http.IIX.lan
    passthrough=yes connection-mark=http.IIX.con.lan

4   ;;; BROWSING INTERNASIONAL
    chain=prerouting action=mark-connection new-connection-mark=http.IX.con
    passthrough=yes protocol=tcp src-address-list=wireless lokal
    dst-address-list=!nice dst-port=80,443,3128,8080,182
    connection-bytes=0-131072

5   chain=prerouting action=mark-packet new-packet-mark=http.IX passthrough=yes
    connection-mark=http.IX.con

6   ;;; BROWSING INTERNASIONAL LAN
    chain=prerouting action=mark-connection new-connection-mark=http.IX.con.lan
    passthrough=yes protocol=tcp src-address-list=jaringan lokal
    dst-address-list=!nice dst-port=80,443,3128,8080,182
    connection-bytes=0-131072

7   chain=prerouting action=mark-packet new-packet-mark=http.IX.lan passthrough=ye>
    connection-mark=http.IX.con.lan

8   ;;; Download LOKAL
    chain=prerouting action=mark-connection new-connection-mark=dl.IIX.con
    passthrough=yes protocol=tcp src-address-list=wireless lokal
    dst-address-list=nice connection-bytes=131072-4294967295

9   chain=prerouting action=mark-packet new-packet-mark=dl.IIX passthrough=yes
    connection-mark=dl.IIX.con

```

## Lanjutan Firewall Mangle Rule

```
10  ;;; Download LOKAL LAN
    chain=prerouting action=mark-connection new-connection-mark=dl.IIX.con.lan
    passthrough=yes protocol=tcp src-address-list=jaringan lokal
    dst-address-list=nice connection-bytes=131072-4294967295

11  chain=prerouting action=mark-packet new-packet-mark=dl.IIX.lan passthrough=yes
    connection-mark=dl.IIX.con.lan

12  ;;; Download INT
    chain=prerouting action=mark-connection new-connection-mark=dl.IX.con
    passthrough=yes protocol=tcp src-address-list=wireless lokal
    dst-address-list=!nice connection-bytes=131072-4294967295

13  chain=prerouting action=mark-packet new-packet-mark=dl.IX passthrough=yes
    connection-mark=dl.IX.con

14  ;;; Download INT LAN
    chain=prerouting action=mark-connection new-connection-mark=dl.IX.con.lan
    passthrough=yes protocol=tcp src-address-list=jaringan lokal
    dst-address-list=!nice connection-bytes=131072-4294967295

15  chain=prerouting action=mark-packet new-packet-mark=dl.IX.lan passthrough=yes
    connection-mark=dl.IX.con.lan

16  ;;; STREAMING
    chain=prerouting action=mark-connection new-connection-mark=str.con
    passthrough=yes src-address-list=wireless lokal layer7-protocol=streaming

17  chain=prerouting action=mark-packet new-packet-mark=str passthrough=yes
    connection-mark=str.con

18  ;;; STREAMING LAN
    chain=prerouting action=mark-connection new-connection-mark=str.con.lan
    passthrough=yes src-address-list=jaringan lokal layer7-protocol=streaming

19  chain=prerouting action=mark-packet new-packet-mark=str.lan passthrough=yes
    connection-mark=str.con.lan
```

## Queue Tree List

```

Terminal
..          Move up one level
/command    Use command at the base level
Using nice.rsc from www.mikrotik.co.id, 22 June 2014 18:14:14 WIB, 1481 lines.
[admin@MikroTik] > /queue print
bad command name print (line 1 column 8)
[admin@MikroTik] > /queue tree print
Flags: X - disabled, I - invalid
0  name="BOLT LTE" parent=global packet-mark="" limit-at=0 queue=default priority=8
   max-limit=5M burst-limit=0 burst-threshold=0 burst-time=0s

1  name="HTTP LOKAL" parent=WIFI packet-mark=http.IIX limit-at=200k queue=default
   priority=8 max-limit=3M burst-limit=0 burst-threshold=0 burst-time=0s

2  name="HTTP INT" parent=WIFI packet-mark=http.IX limit-at=200k queue=default priority=8
   max-limit=3M burst-limit=0 burst-threshold=0 burst-time=0s

3  name="DOWNLOAD LOKAL" parent=WIFI packet-mark=d1.IIX limit-at=350k queue=default
   priority=8 max-limit=4M burst-limit=0 burst-threshold=0 burst-time=0s

4  name="DOWNLOAD INT" parent=WIFI packet-mark=d1.IX limit-at=350k queue=default
   priority=8 max-limit=4M burst-limit=0 burst-threshold=0 burst-time=0s

5  name="STREAMING" parent=WIFI packet-mark=str limit-at=300k queue=default priority=8
   max-limit=3M burst-limit=0 burst-threshold=0 burst-time=0s

6  name="WIFI" parent=BOLT LTE packet-mark="" limit-at=1500k queue=default priority=8
   max-limit=4M burst-limit=0 burst-threshold=0 burst-time=0s

7  name="LAN" parent=BOLT LTE packet-mark="" limit-at=3M queue=default priority=8
   max-limit=4M burst-limit=0 burst-threshold=0 burst-time=0s

8  name="DL IX LAN" parent=LAN packet-mark=d1.IX.lan limit-at=700k queue=default
   priority=8 max-limit=4M burst-limit=0 burst-threshold=0 burst-time=0s

9  name="DL IIX LAN" parent=LAN packet-mark=d1.IIX.lan limit-at=700k queue=default
   priority=8 max-limit=4M burst-limit=0 burst-threshold=0 burst-time=0s

10 name="HTTP IX LAN" parent=LAN packet-mark=http.IX.lan limit-at=500k queue=default
   priority=8 max-limit=3M burst-limit=0 burst-threshold=0 burst-time=0s

11 name="HTTP IIX LAN" parent=LAN packet-mark=http.IIX.lan limit-at=500k queue=default
   priority=8 max-limit=3M burst-limit=0 burst-threshold=0 burst-time=0s

12 name="STREAMING LAN" parent=LAN packet-mark=str.lan limit-at=500k queue=default
   priority=8 max-limit=3M burst-limit=0 burst-threshold=0 burst-time=0s
[admin@MikroTik] >

```