Implementasi IDS di Mikrotik

By
Antonius Duty Susilo
dutymlg@gmail.com



Profile

- Antonius Duty Susilo
- Trainer And Consultant Mikrotik
- Instructor Cisco Academy and Oracle Academy (Oracle WDP)
- Ph.D Student In UTEM Malaysia (Universiti Teknikal Malaysia Melaka)
- Guest Lecturer in Polinema (Politeknik Negeri Malang), STIKI (Sekolah Tinggi Informatika dan Komputer Indonesia Malang, STMIK Pradnya Paramita Malang

MikroTik

WWW.POWERPOINTIFY.COM

IDS (Intrusion Detection System)

intrusion Detection System (**IDS**) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

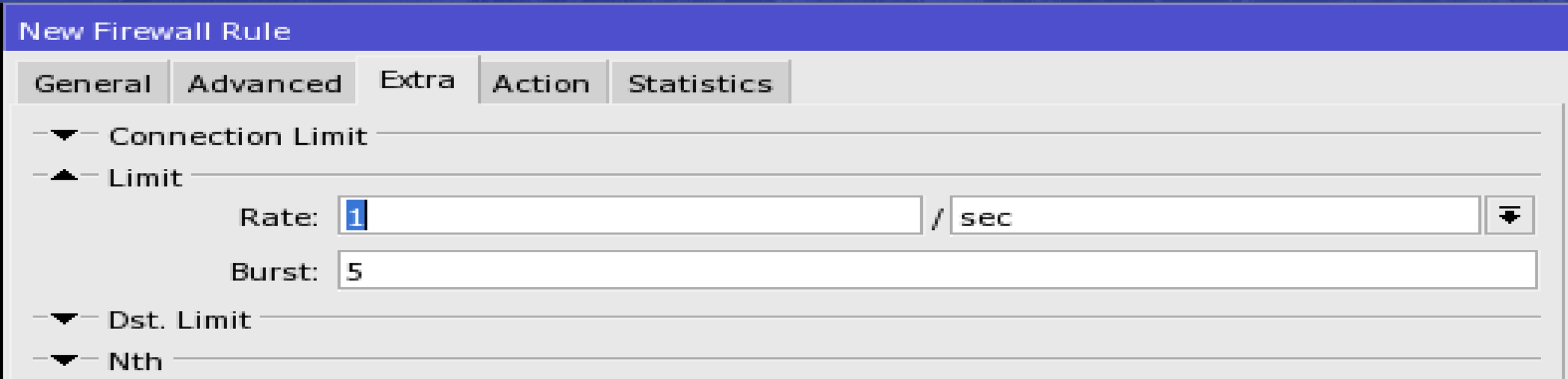


Jenis intrusion (penyusupan)

- Ada 5 jenis utama
  - Ping flood
  - Port scan
  - Serangan DoS
  - Serangan DDoS
  - Akses yang tidak dikenal ke router
- Di mikrotik, Chain yang digunakan adalah input atau output

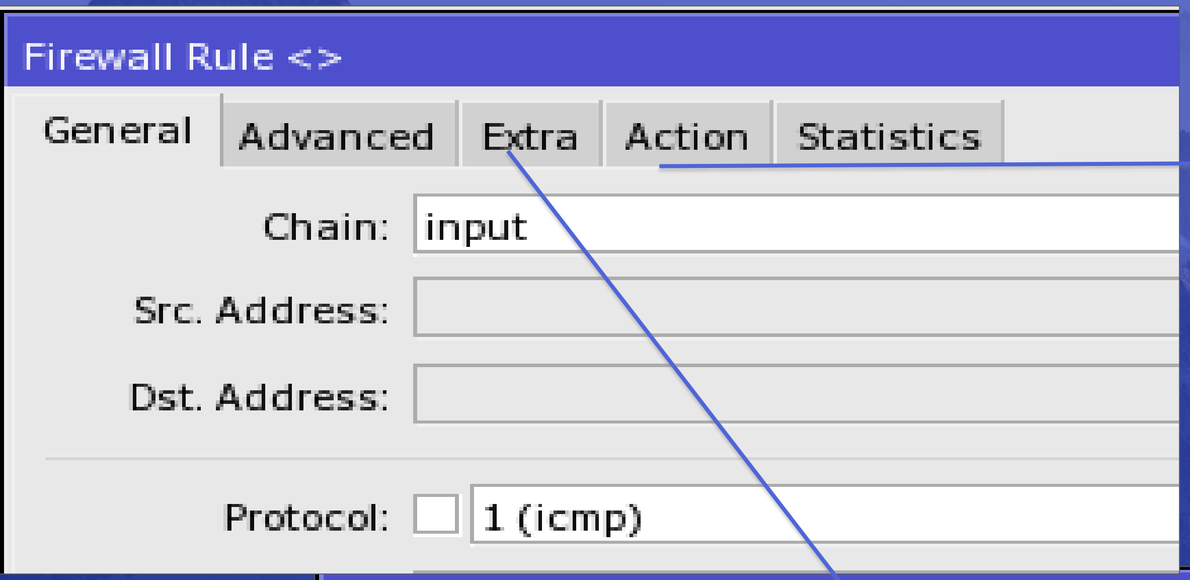
Ping Flood

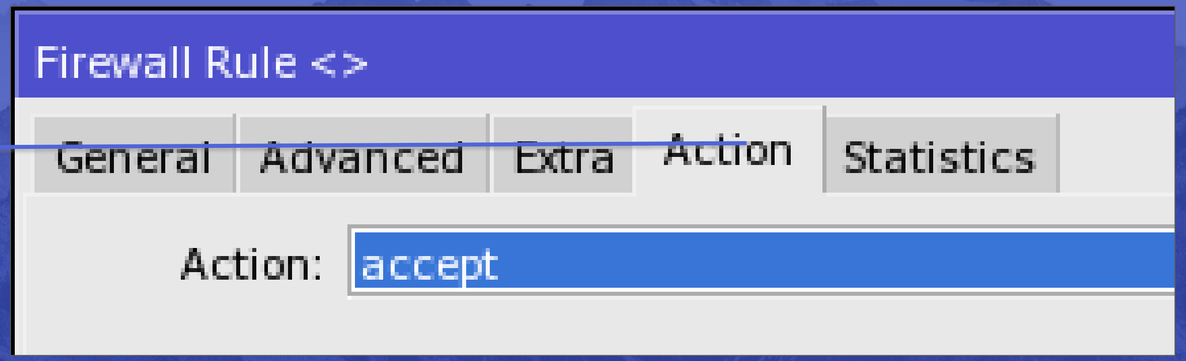
- ***Ping Flood*** atau "Banjir Ping" adalah sebuah serangan DDOS yang membuat target menjadi down. Ping flood bisa dikirim dalam jumlah yang sangat banyak sehingga membuat target menjadi error bahkan sampai rusak.
- Menggunakan new firewall rule ---extra ----limit
- Menggunakan action “log”

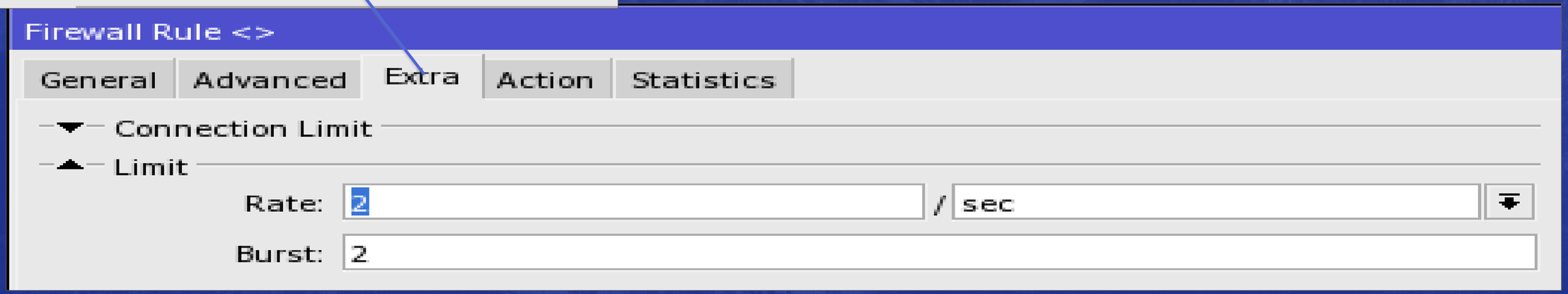


Limit (for ping-flood)

Contoh membuat sebuah rule untuk membatasi protocol icmp sampai 2 paket / detik

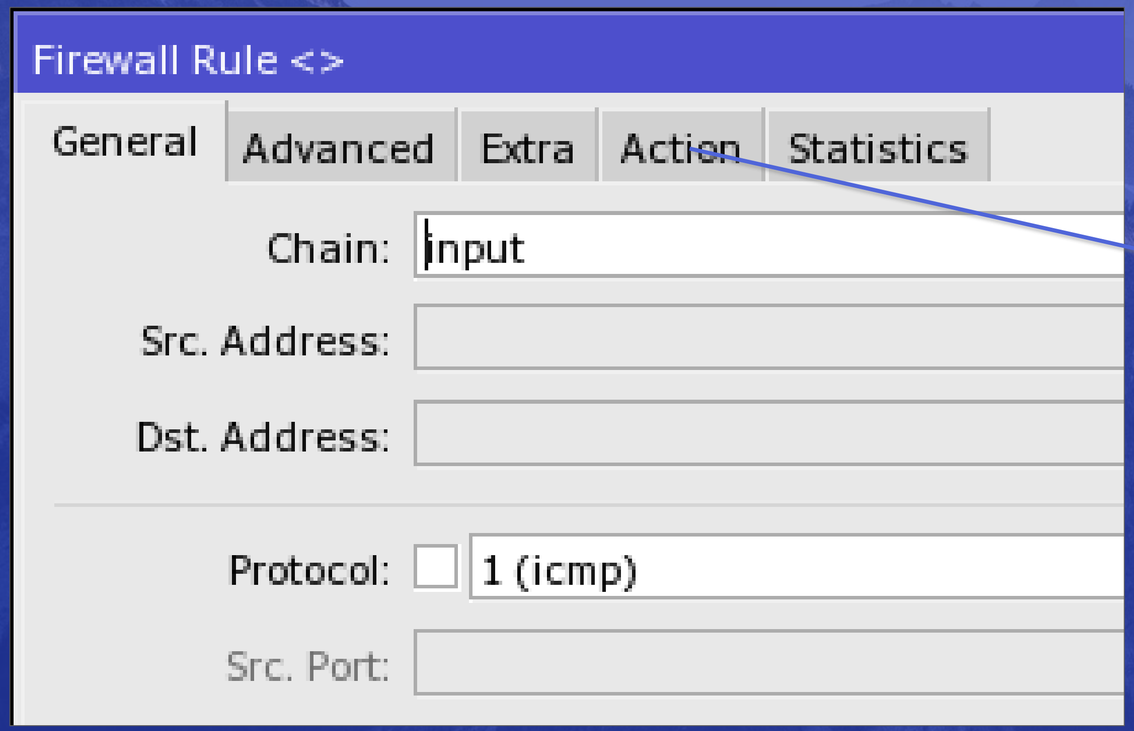


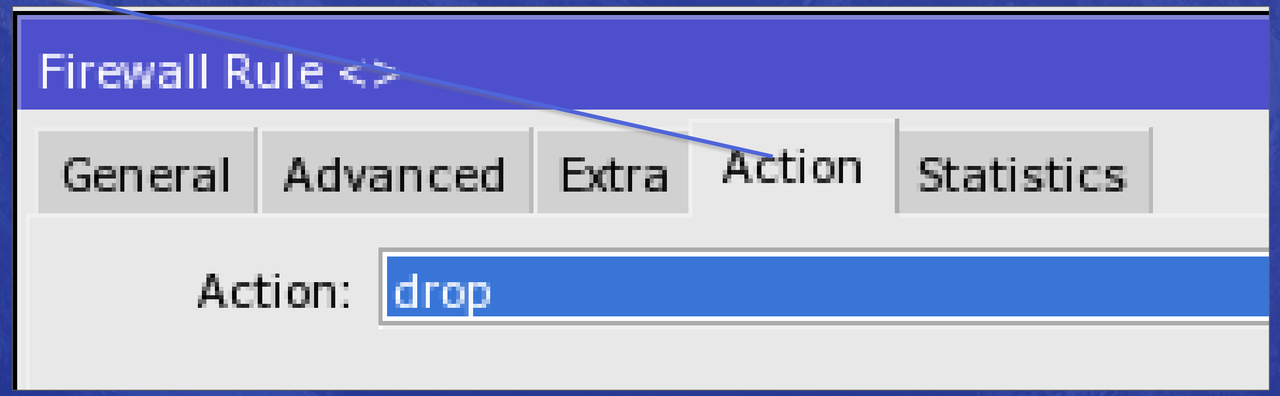




Limit (for ping-flood)

- Membuat rule lagi untuk membatasi lebih dari 2
- Make another rule to block other than those traffic before (2 pps burstable to 2 other pps)





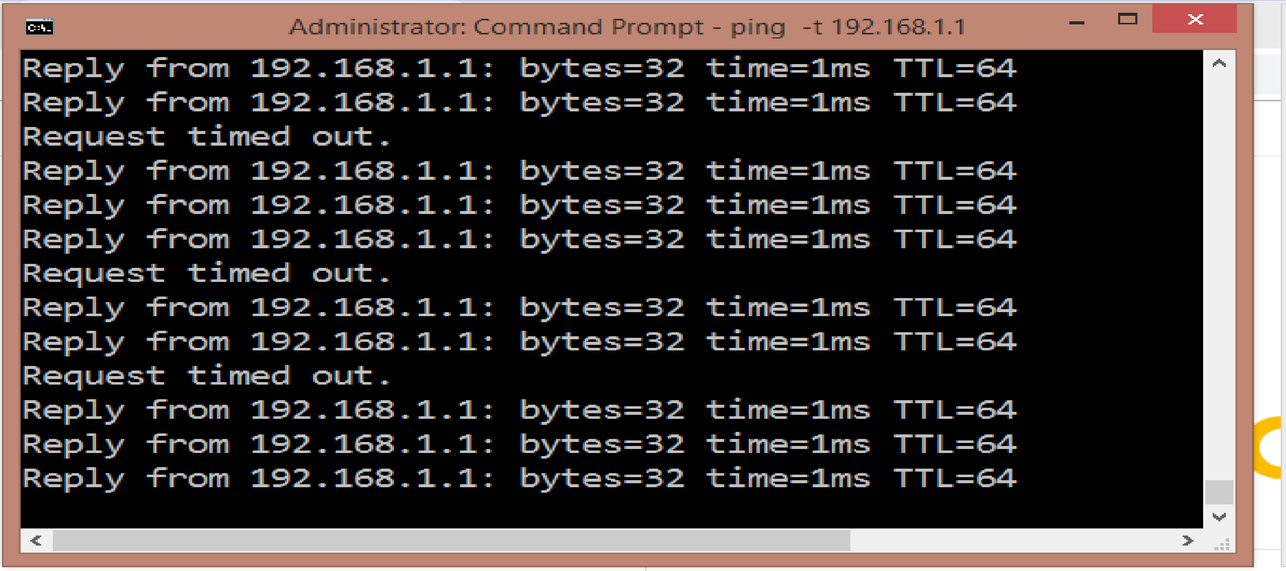
Limit (for ping-flood)

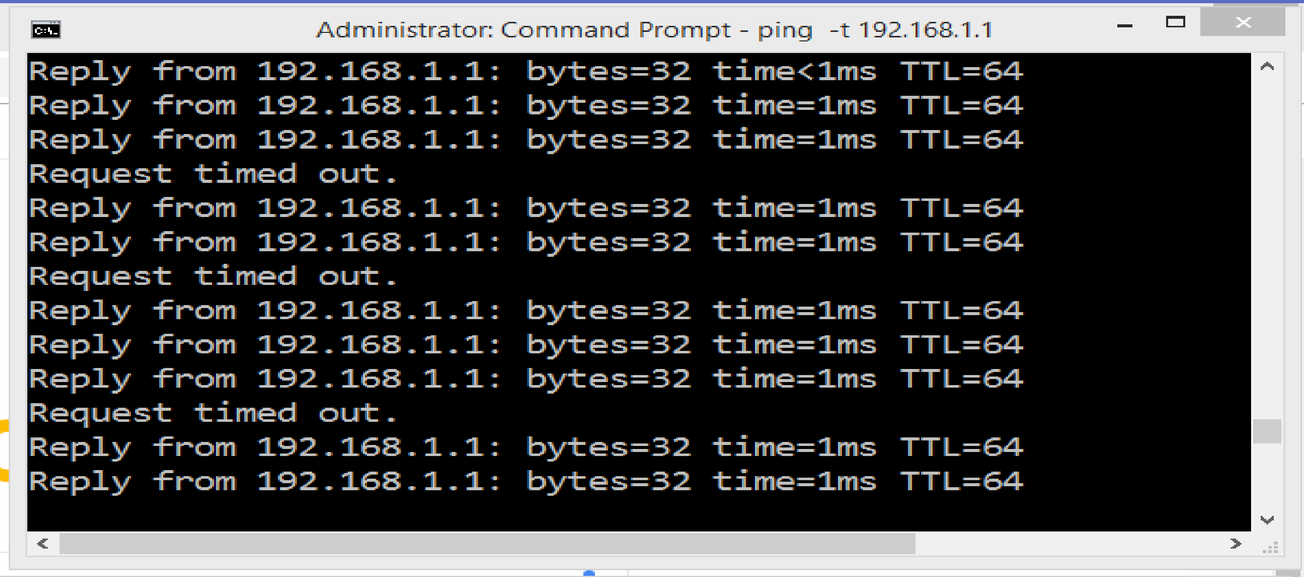
- Hasil ping

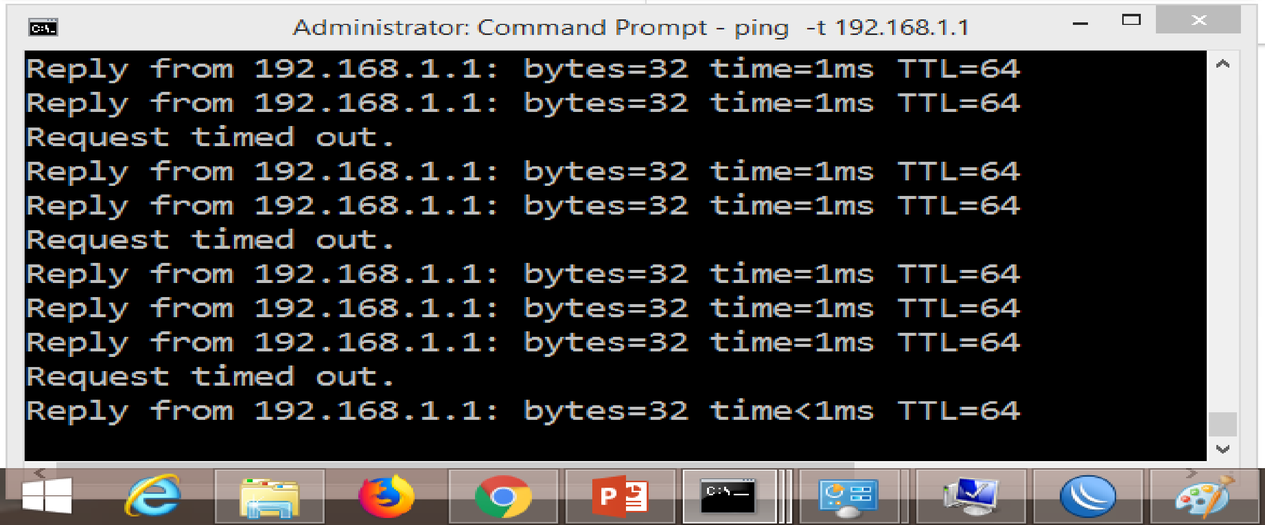
#		Action	Chain	Dst. Address	Protocol	In. Inter...	Out. Int...	Bytes	Packets	
0		acc...	input		1 (icmp)			26.3 KiB	448	
1		drop	input		1 (icmp)			4680 B	78	

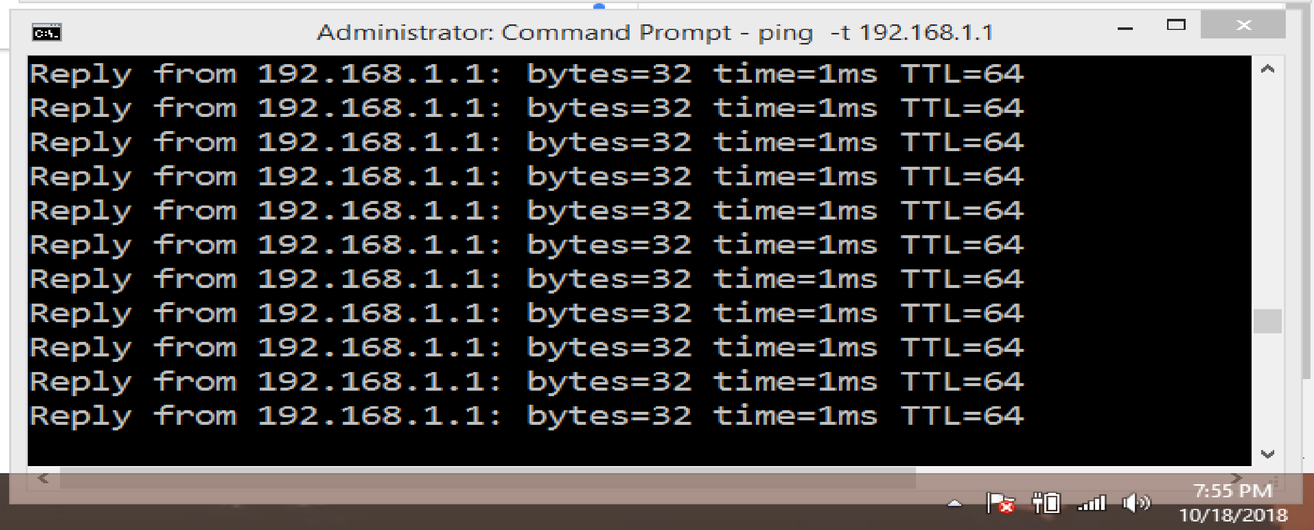
Limit (for ping-flood)

- **Hasil ping**









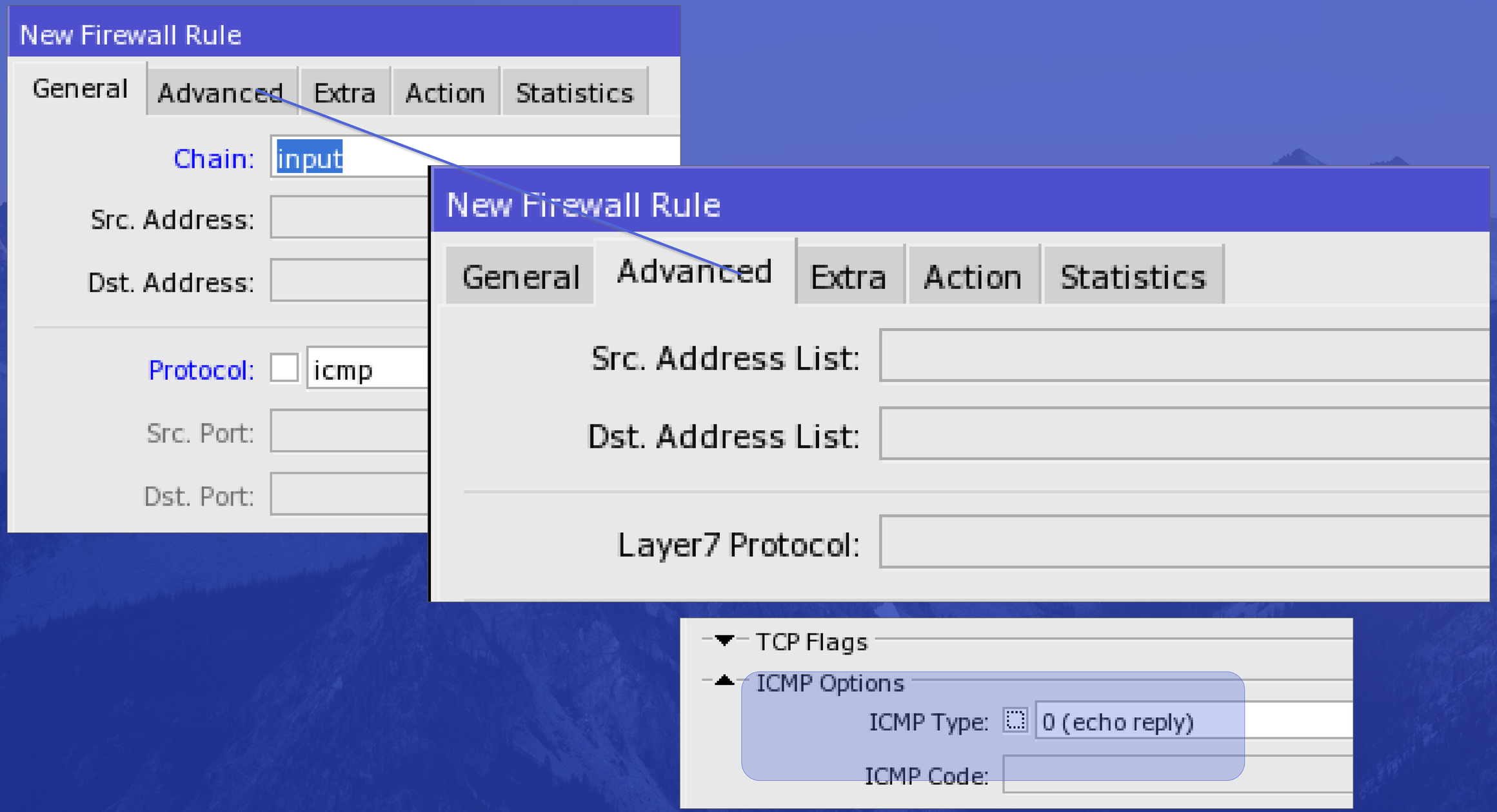
Tipe ICMP Message

- Format messages ICMp terdiri dari type dan code, sebagai contoh Message ping 0:0 atau type 0 dan code 0, yang berarti echo reply, dan Message ping 8:0 atau type 8 dan code 0, yang berarti echo request.
- Tipe icmp message yang digunakan adalah
  - PING - messages 0:0 dan 8:0
  - TRACEROUTE – messages 11:0 dan 3:3
  - Path MTU discovery – message 3:4
- Tipe yang lain harus di blok atau dibuang

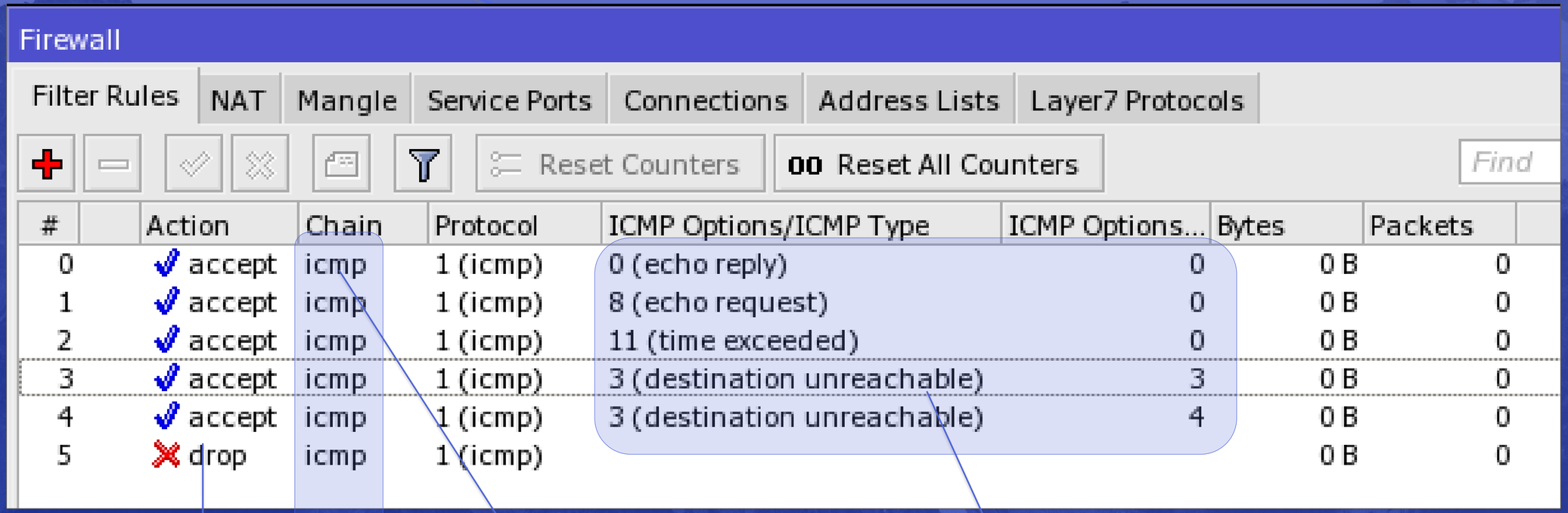
Type dan Code Message ICMP

Type	Code	Status	Description
0 – Echo Reply[5]:14	0		Echo reply (used to ping)
1 and 2		unassigned	*Reserved*
3 – Destination Unreachable[5]:4	0		Destination network unreachable
	1		Destination host unreachable
	2		Destination protocol unreachable
	3		Destination port unreachable
	4		Fragmentation required, and DF flag set
	5		Source route failed
	6		Destination network unknown
	7		Destination host unknown
	8		Source host isolated
	9		Network administratively prohibited
	10		Host administratively prohibited
	11		Network unreachable for ToS
	12		Host unreachable for ToS
	13		Communication administratively prohibited
	14		Host Precedence Violation
	15		Precedence cutoff in effect
4 – Source Quench	0	deprecated	Source quench (congestion control)
5 – Redirect Message	0		Redirect Datagram for the Network
	1		Redirect Datagram for the Host
	2		Redirect Datagram for the ToS & network
	3		Redirect Datagram for the ToS & host
6		deprecated	Alternate Host Address
7		unassigned	*Reserved*
8 – Echo Request	0		Echo request (used to ping)
9 – Router Advertisement	0		Router Advertisement
10 – Router Solicitation	0		Router discovery/selection/solicitation
11 – Time Exceeded[5]:6	0		TTL expired in transit
	1		Fragment reassembly time exceeded

Contoh aturan ICMP



ICMP Flood



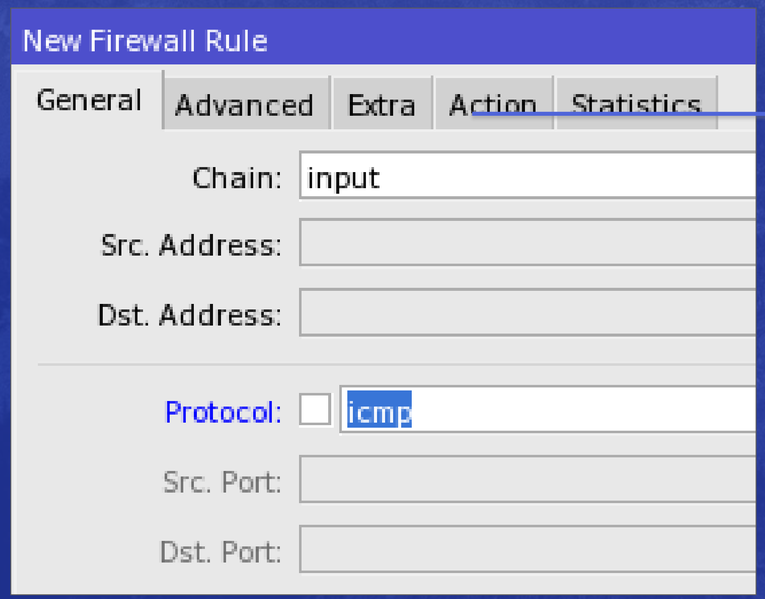
DROP other ICMP type and code

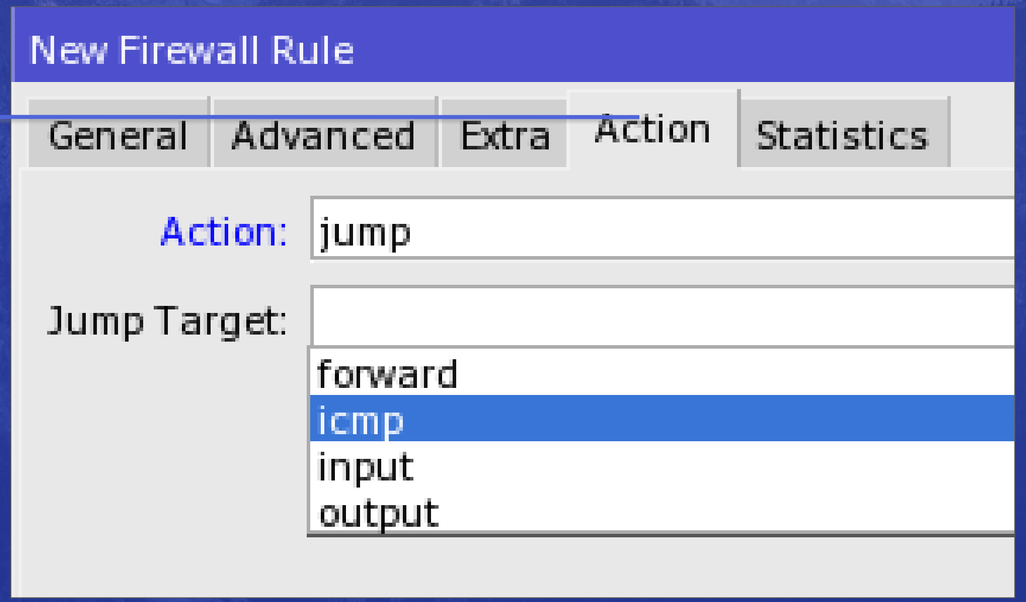
New Firewall CHAIN

ACCEPT all ICMP Type and Code defined earlier

ICMP Flood

- Arahkan semua ICMP paket ke chain icmp
  1. Buat chain input dengan action jump
  2. Tempatkan sesuai urutan
  3. Buat an action “jump” rule dengan chain Forward
  4. Tempatkan sesuai urutan





Port knocking

- Port Knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu

- Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule knocking yang diterapkan, maka secara dinamis firewall akan memberikan akses ke port yang sudah diblock.

Gambaran Port Knocking





1.Koneksi ke TCP port 1234

2.Router akan menghandle beberapa saat koneksi tersebut

3.Koneksi ke TCP-4321

4.Router akan mengidentifikasi apakah IP yang digunakan sama dengan koneksi yang pertama (TCP-1234)

5.Jika sama IP yang digunakan dan waktu tidak melebihi limit yang diberikan maka diijinkan mengakses router.

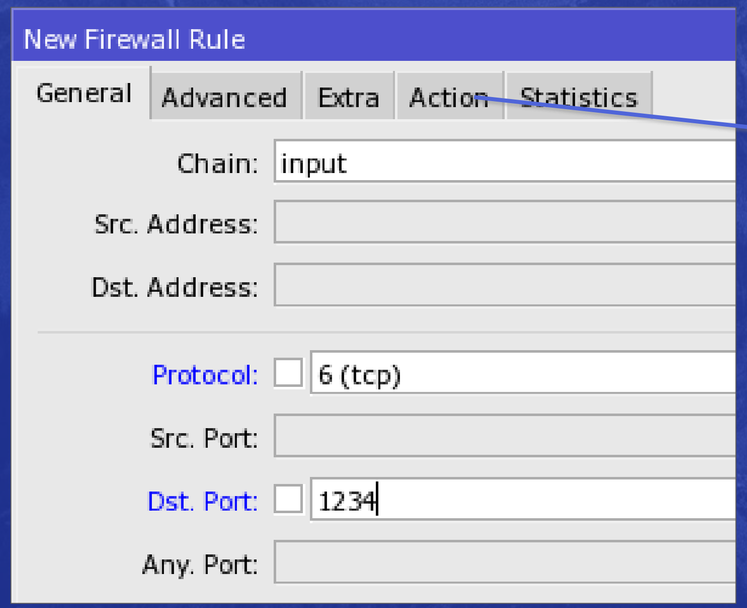
Knocking Port
TCP 1234
TCP 4321

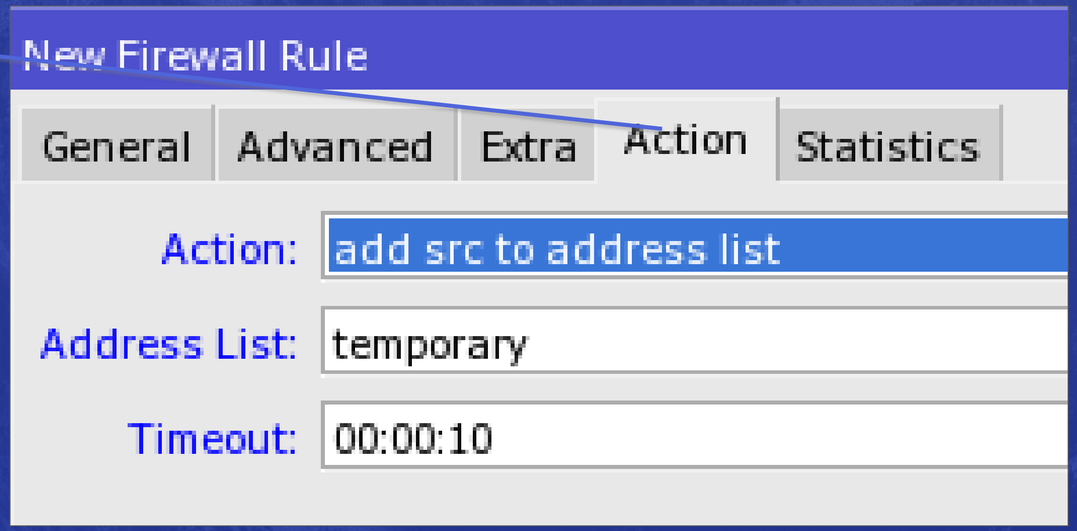
Tahapan Port knocking di mikrotik

- Menggunakan input chain
- Menangkap koneksi yang pertama (port 1234) dan masukkan ke address-list temporary (sementara) selama beberapa detik (berarti diberi waktu beberapa detik untuk membuka koneksi kedua)
- Menangkap koneksi yang kedua (port 4321) dan membandingkan dengan koneksi pertama
- Jika ip sudah sesuai yang digunakan maka dapat mengakses router
  Jika tidak sesuai akan didrop

Port Knocking

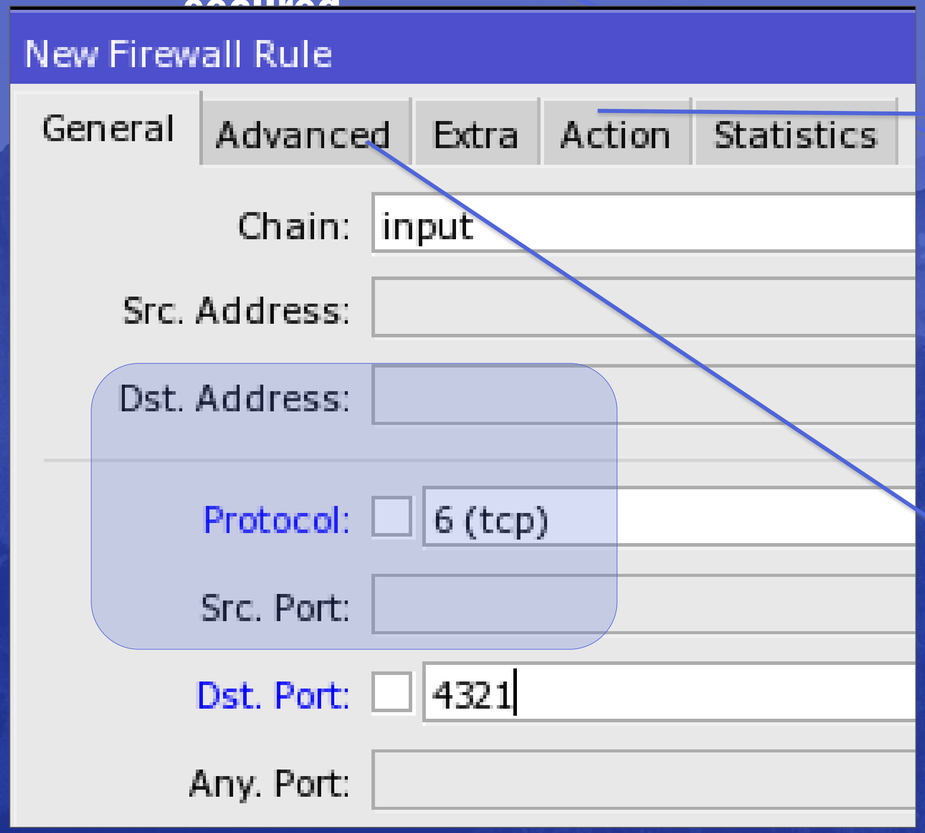
- Menangkap koneksi tcp(1234) dan dimasukkan ke add src to address list selama 10 detik

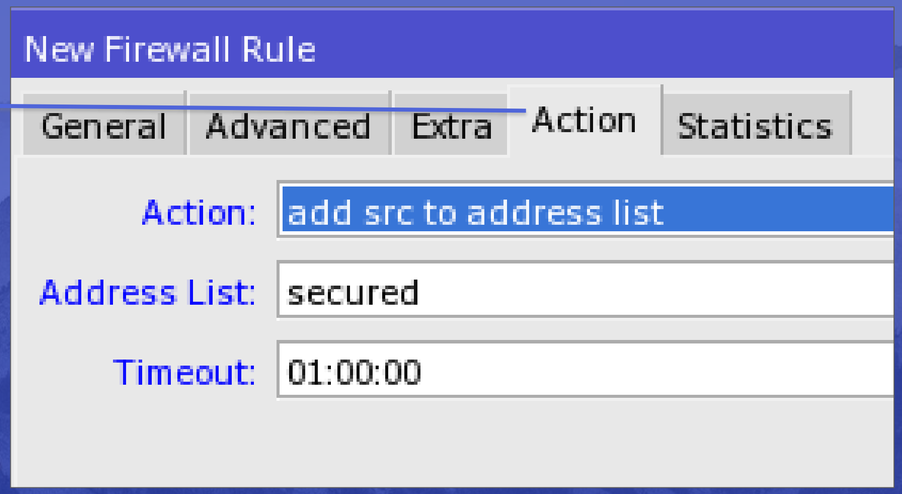


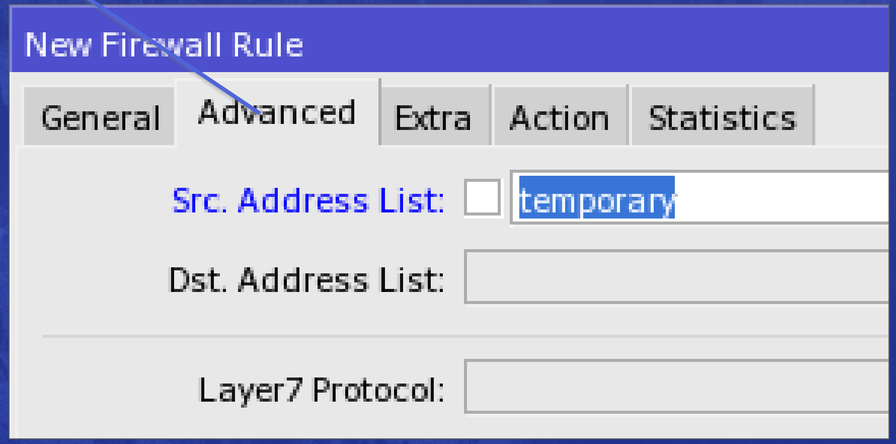


Port Knocking

- **Menangkap tcp(4321) dan dibandingkan dengan src address list . Kalau sesuai maka diberi nama address list secured**

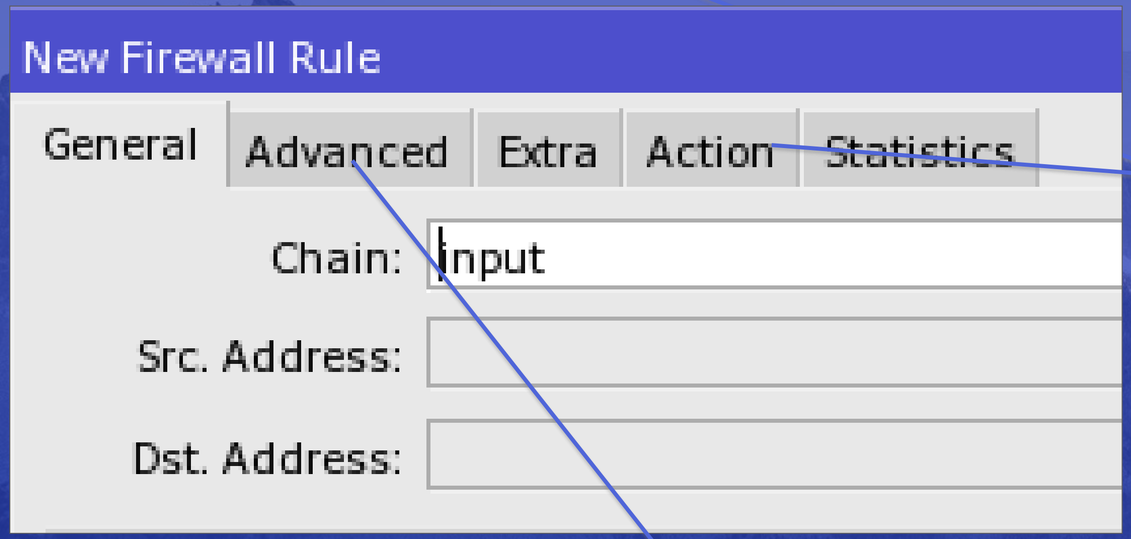


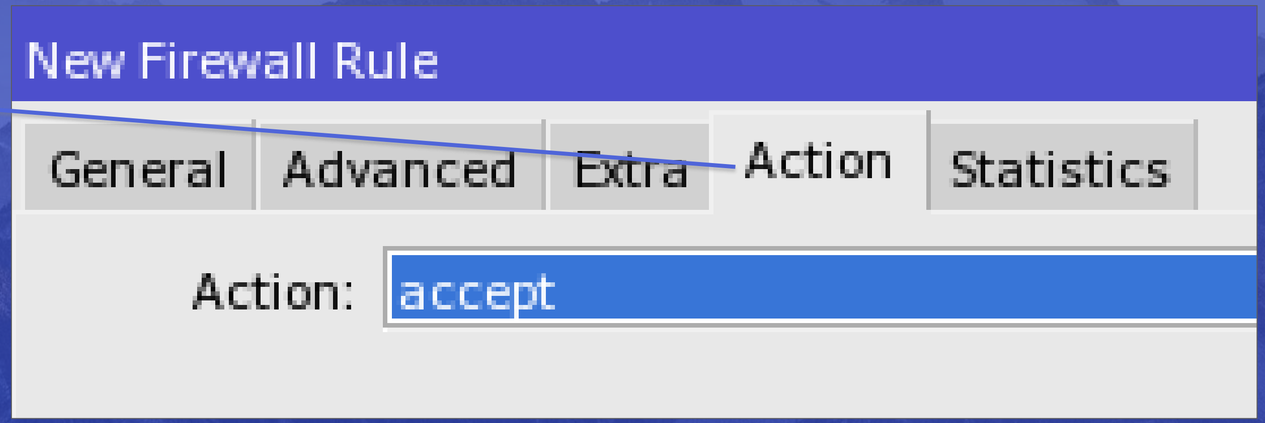


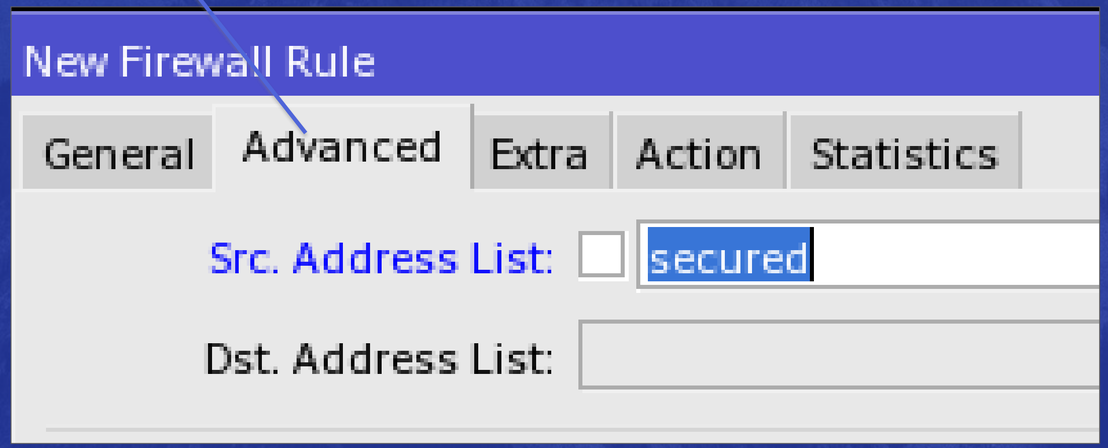


Port Knocking

- **Jika sudah sesuai maka akan accept**







Port Knocking

- **Drop semua trafik**

Firewall

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

Reset Counters | Reset All Counters | Find | input

#	Action	Chain	Proto...	Src. Port	Dst. Port	Bytes	Packets
6	add src to address list	input	6 (tcp)		1234	0 B	0
7	add src to address list	input	6 (tcp)		4321	0 B	0
8	accept	input				0 B	0
9	drop	input				15.0 KiB	177

Test port knoking

- **Sebelum Knoking**

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

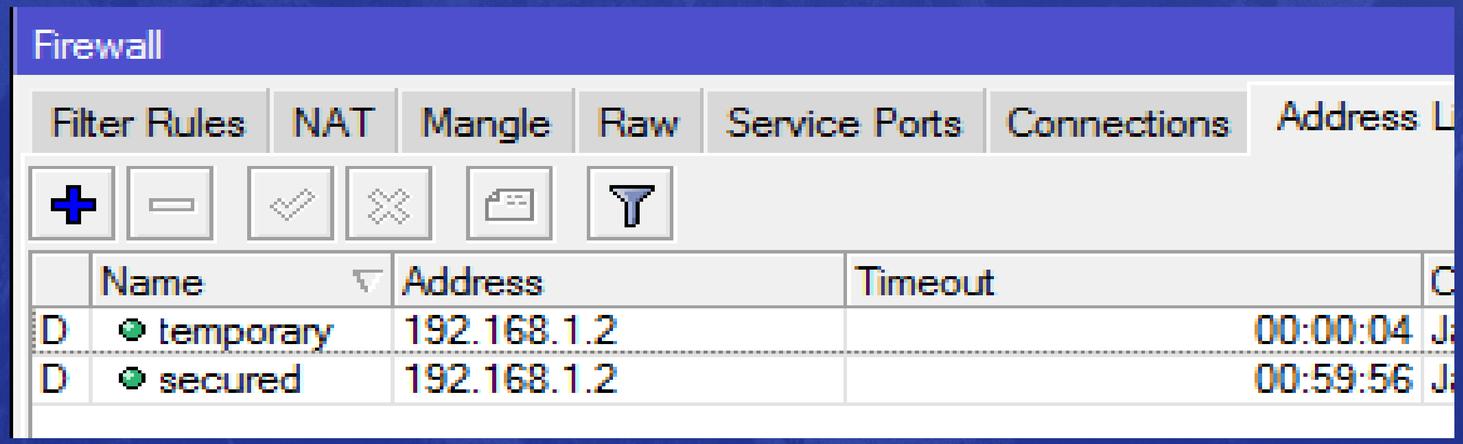
Test port knoking

- **Melakukan Knoking**

```
F:\MUM\tool\tools>knock 192.168.1.1 1234

F:\MUM\tool\tools>knock 192.168.1.1 4321
```

- **Setelah melakukan knoking IP akan masuk di addresslist**



Test port knoking

- Setelah melakukan knoking, mencoba ping kembali ke IP Router

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Port Scan

- Prot scan adalah metode intrusion yang melakukan scan port lebih dari 1 port yang bertujuan melihat port yang terbuka
- Ada 2 jenis port yaitu :

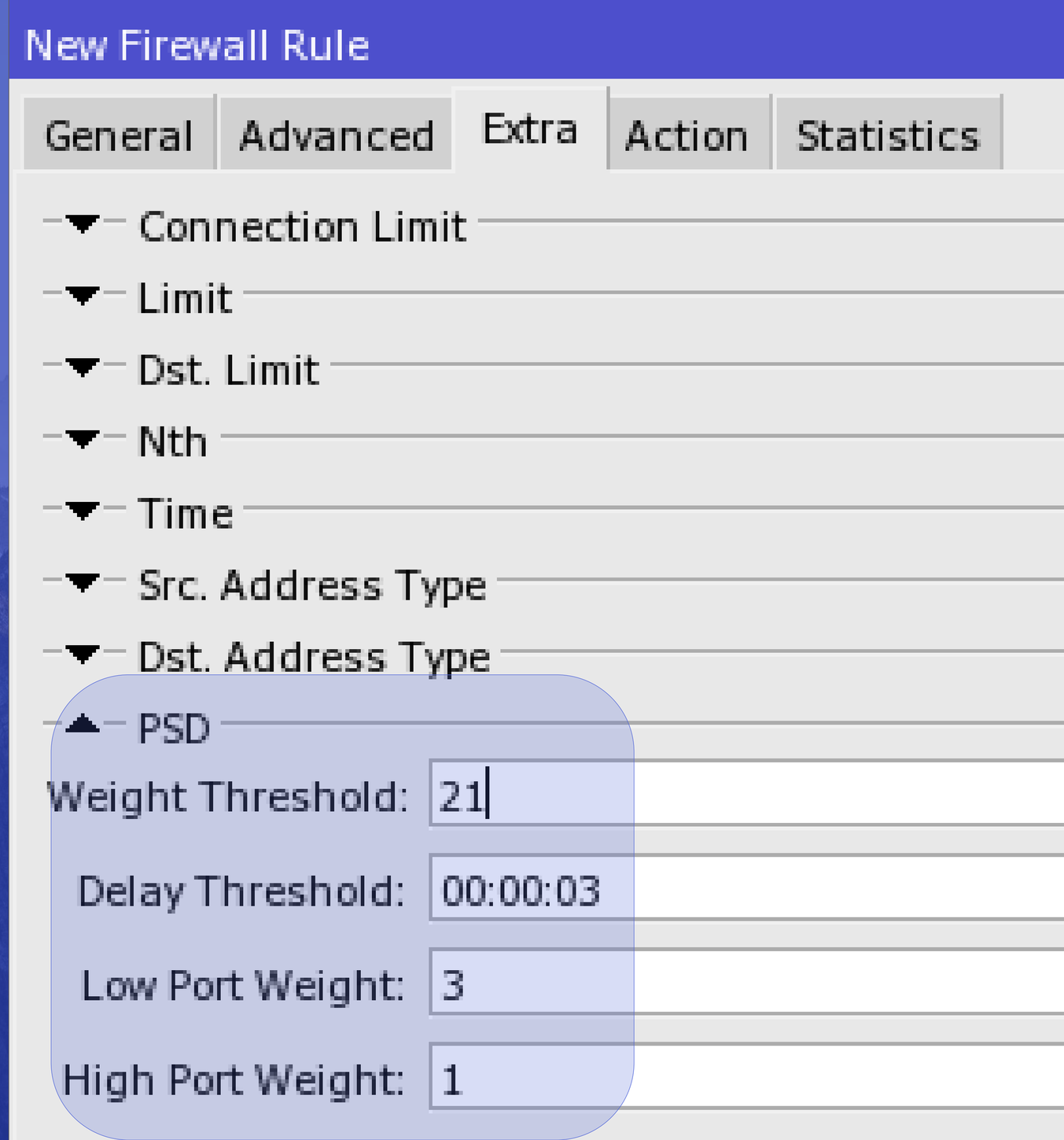
  Low port (or well-know-port) biasanya port yang dikenal dan umum di gunakan .

  Port ini antara 0 – 1023

  High port yaitu port antara 1024 - 65535

Port Scan Detect

- MikroTik dapat mendeteksi port mengguankan option psd
- PSD hanya untuk protocol
- Low ports
  - From 0 to 1023
- High ports
  - From 1024 to 65535



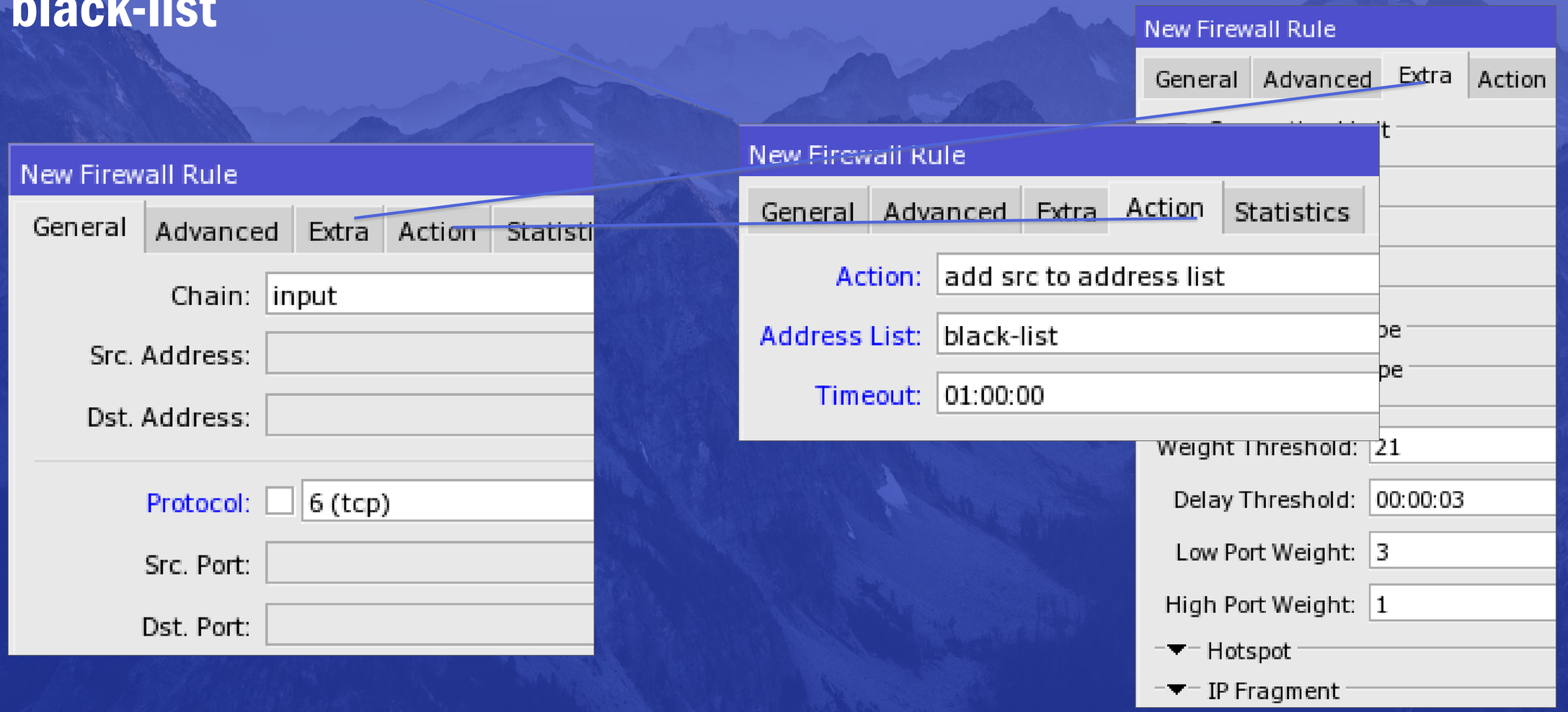
Mendeteksi Port Scan

Langkah –langkah untuk mendeteksi scan port menggunakan chain input

- Tangkap koneksi yang mencoba scan port dan letakkan pada src address black-list
- Drop koneksi dari src address black-list

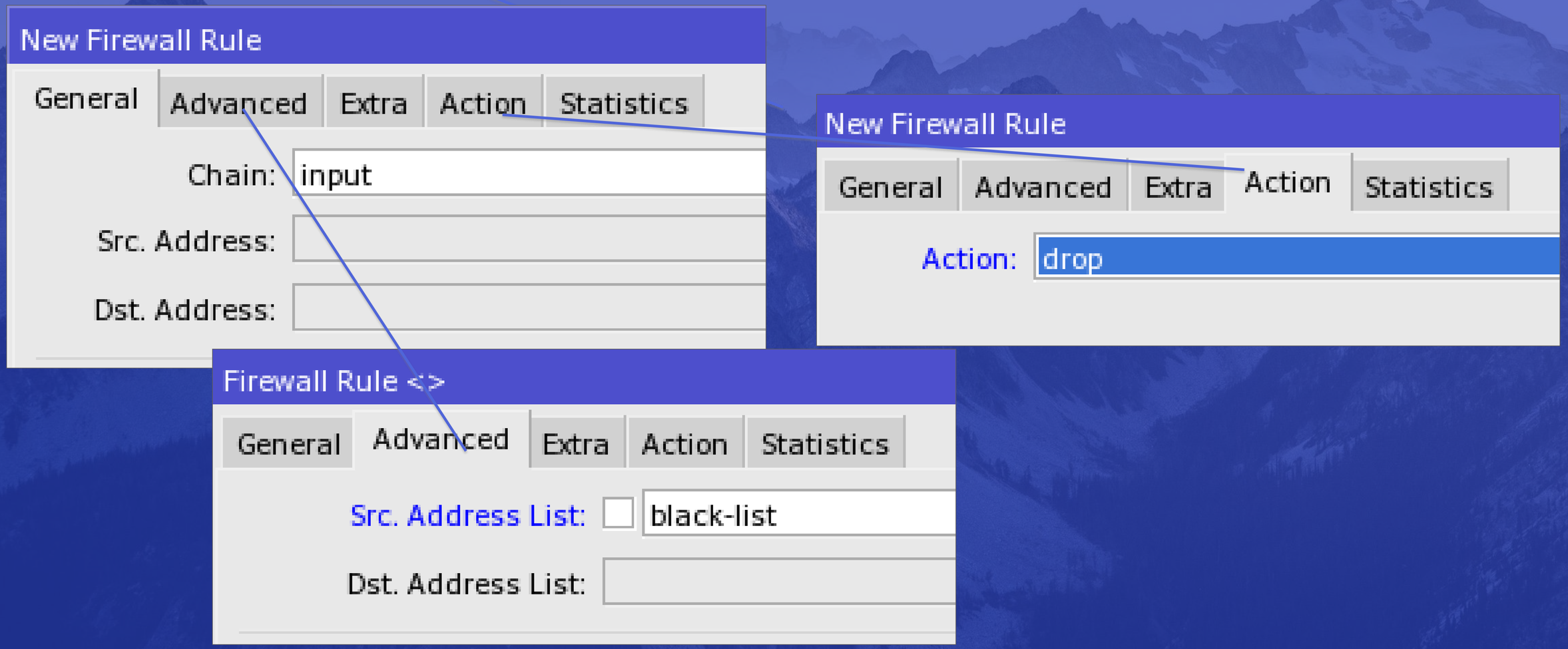
Port Scan Detect

- Tangkap koneksi yang mencoba scan port dan letakkan pada src address black-list



Port Scan

- **Drop koneksi pada src-address black-list**



MikroTik

Terima Kasih