



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



IDS (Intrusion Detection System)

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



- 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”

New Firewall Rule

General Advanced Extra Action Statistics

Connection Limit

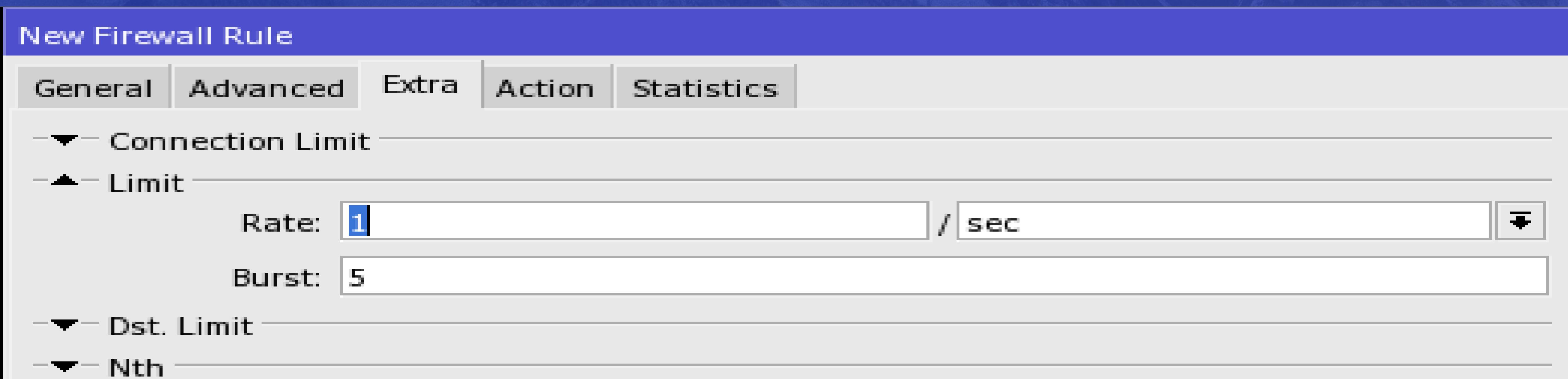
Limit

Rate: / sec

Burst:

Dst. Limit

Nth



Limit (for ping-flood)

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

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: 1 (icmp)

Firewall Rule <>

General Advanced Extra Action Statistics

Action: accept

Firewall Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Rate: 2 / sec

Burst: 2

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)

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: Input

Src. Address:

Dst. Address:

Protocol: 1 (icmp)

Src. Port:

Firewall Rule <>

General Advanced Extra Action Statistics

Action: drop

Limit (for ping-flood)

- Hasil ping

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

Limit (for ping-flood)

- # • Hasil ping

```
Administrator: Command Prompt - ping -t 192.168.1.1

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Request timed out.
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
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Request timed out.
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
```

```
Administrator: Command Prompt - ping -t 192.168.1.1

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
Request timed out.

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Request timed out.

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
Request timed out.

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

```
Administrator: Command Prompt - ping -t 192.168.1.1

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Request timed out.
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
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

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
	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)
	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
	0		TTL expired in transit
11 – Time Exceeded ^{[5]:6}	1		Fragment reassembly time exceeded



Contoh aturan ICMP

New Firewall Rule

General Advanced Extra Action Statistics

Chain: **input**

Src. Address:

Dst. Address:

Protocol: **icmp**

Src. Port:

Dst. Port:

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

TCP Flags:

ICMP Options:

ICMP Type: **0 (echo reply)**

ICMP Code:

ICMP Flood

Firewall

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

+ - ✓ ✎ 🔍 Reset Counters **00 Reset All Counters** Find

#	Action	Chain	Protocol	ICMP Options/ICMP Type	ICMP Options...	Bytes	Packets
0	✓ accept	icmp	1 (icmp)	0 (echo reply)	0	0 B	0
1	✓ accept	icmp	1 (icmp)	8 (echo request)	0	0 B	0
2	✓ accept	icmp	1 (icmp)	11 (time exceeded)	0	0 B	0
3	✓ accept	icmp	1 (icmp)	3 (destination unreachable)	3	0 B	0
4	✓ accept	icmp	1 (icmp)	3 (destination unreachable)	4	0 B	0
5	✗ drop	icmp	1 (icmp)			0 B	0

New Firewall CHAIN

DROP other ICMP type
and code

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

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Chain: <input type="text" value="input"/>				
Src. Address:				
Dst. Address:				
Protocol: <input checked="" type="checkbox"/> icmp				
Src. Port:				
Dst. Port:				

New Firewall Rule

General	Advanced	Extra	Action	Statistics
			Action: jump	
			Jump Target:	
			forward	
			icmp	
			input	
			output	

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.

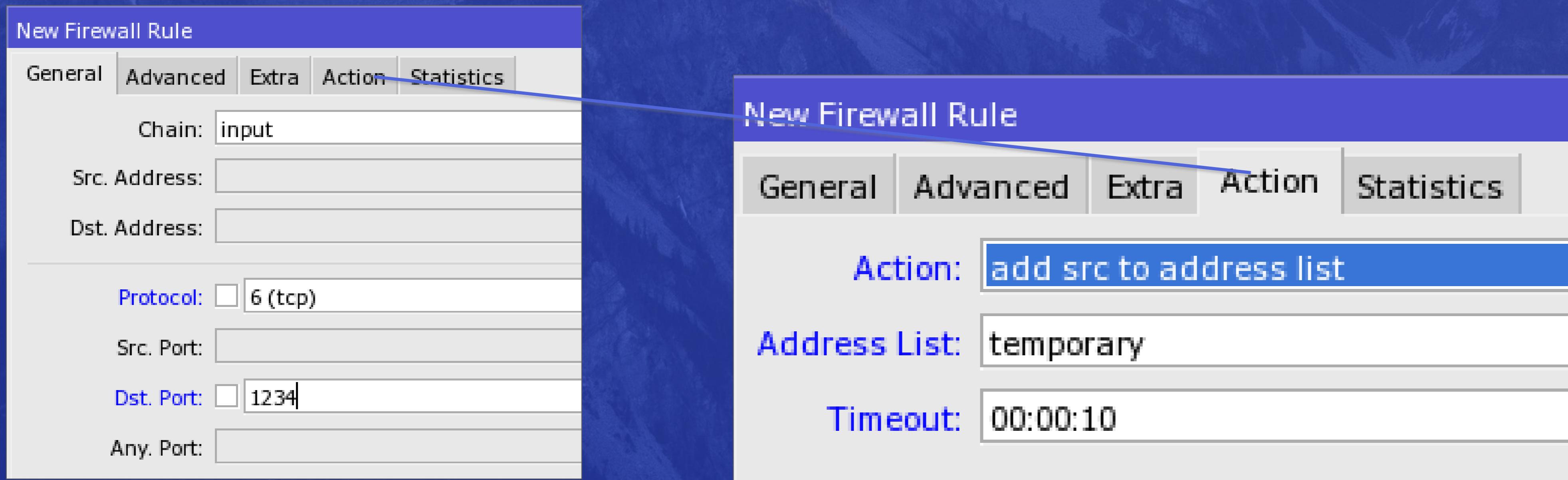
Knocking Port
TCP 1234
TCP 4321

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



The image shows two overlapping windows of the Winbox interface on a MikroTik device, illustrating the configuration of two firewall rules for a port knocking sequence.

Left Window (Top): New Firewall Rule - General Tab

- Chain:** input
- Protocol:** 6 (tcp)
- Src. Port:**
- Dst. Port:** 1234
- Any. Port:**

Right Window (Bottom): New Firewall Rule - Action Tab

- Action:** **add src to address list**
- Address List:** temporary
- Timeout:** 00:00:10

Port Knocking

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

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Chain: input				
Src. Address:				
Dst. Address:				
Protocol: <input type="checkbox"/> 6 (tcp)				
Src. Port:				
Dst. Port: <input type="checkbox"/> 4321				
Any. Port:				

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Action: <input type="checkbox"/> add src to address list				
Address List: secured				
Timeout: 01:00:00				

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Src. Address List: <input type="checkbox"/> temporary				
Dst. Address List:				
Layer7 Protocol:				

Port Knocking

- Jika sudah sesuai maka akan accept

New Firewall Rule

General Advanced Extra Action Statistics

Chain: Input

Src. Address:

Dst. Address:

New Firewall Rule

General Advanced Extra Action Statistics

Action: accept

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List: secured

Dst. Address List:

Port Knocking

- Drop semua trafik

Firewall

Filter Rules									NAT	Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols	
#		Action		Chain	Proto...	Src. Port	Dst. Port	Bytes							
6	<input type="checkbox"/>	add src to address list		input	6 (tcp)		1234	0 B							0
7	<input type="checkbox"/>	add src to address list		input	6 (tcp)		4321	0 B							0
8	<input checked="" type="checkbox"/>	accept		input				0 B							0
9	<input type="checkbox"/>	drop		input				15.0 KiB							177

Test port knocking

- Sebelum Knocking

```
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),
```

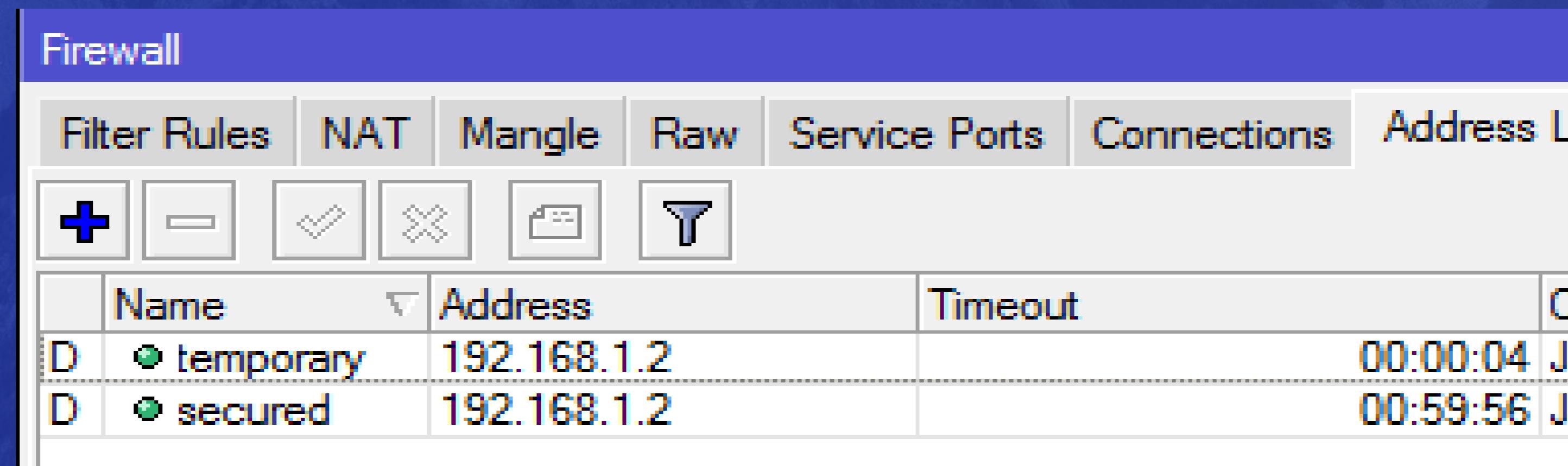
Test port knocking

- Melakukan Knocking

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

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

- Setelah melakukan knocking IP akan masuk di addresslist



	Name	Address	Timeout	Comment
D	● temporary	192.168.1.2	00:00:04	Just now
D	● secured	192.168.1.2	00:59:56	Just now

Test port knocking

- Setelah melakukan knocking, 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
```

```
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 mendekripsi port menggunakan option psd
- PSD hanya untuk protocol
- Low ports
 - From 0 to 1023
- High ports
 - From 1024 to 65535

New Firewall Rule

General Advanced Extra Action Statistics

▼ Connection Limit

▼ Limit

▼ Dst. Limit

▼ Nth

▼ Time

▼ Src. Address Type

▼ Dst. Address Type

▲ PSD

Weight Threshold: 21

Delay Threshold: 00:00:03

Low Port Weight: 3

High Port Weight: 1

This screenshot shows the configuration of a new firewall rule in the Winbox interface. The 'PSD' (Port Scan Detection) section is currently selected, indicated by a blue rounded rectangle around its input fields. The 'Weight Threshold' is set to 21, which is highlighted with a blue border. The 'Delay Threshold' is set to 00:00:03. The 'Low Port Weight' is set to 3 and the 'High Port Weight' is set to 1. Other tabs like General, Advanced, Extra, Action, and Statistics are also visible at the top of the window.

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

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Chain: input				
Src. Address:				
Dst. Address:				
Protocol:	<input type="checkbox"/>	6 (tcp)		
Src. Port:				
Dst. Port:				

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Action: add src to address list				
Address List: black-list				
Timeout: 01:00:00				
Weight Threshold: 21				
Delay Threshold: 00:00:03				
Low Port Weight: 3				
High Port Weight: 1				
Hotspot				
IP Fragment				

- Drop koneksi pada src-address black-list

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

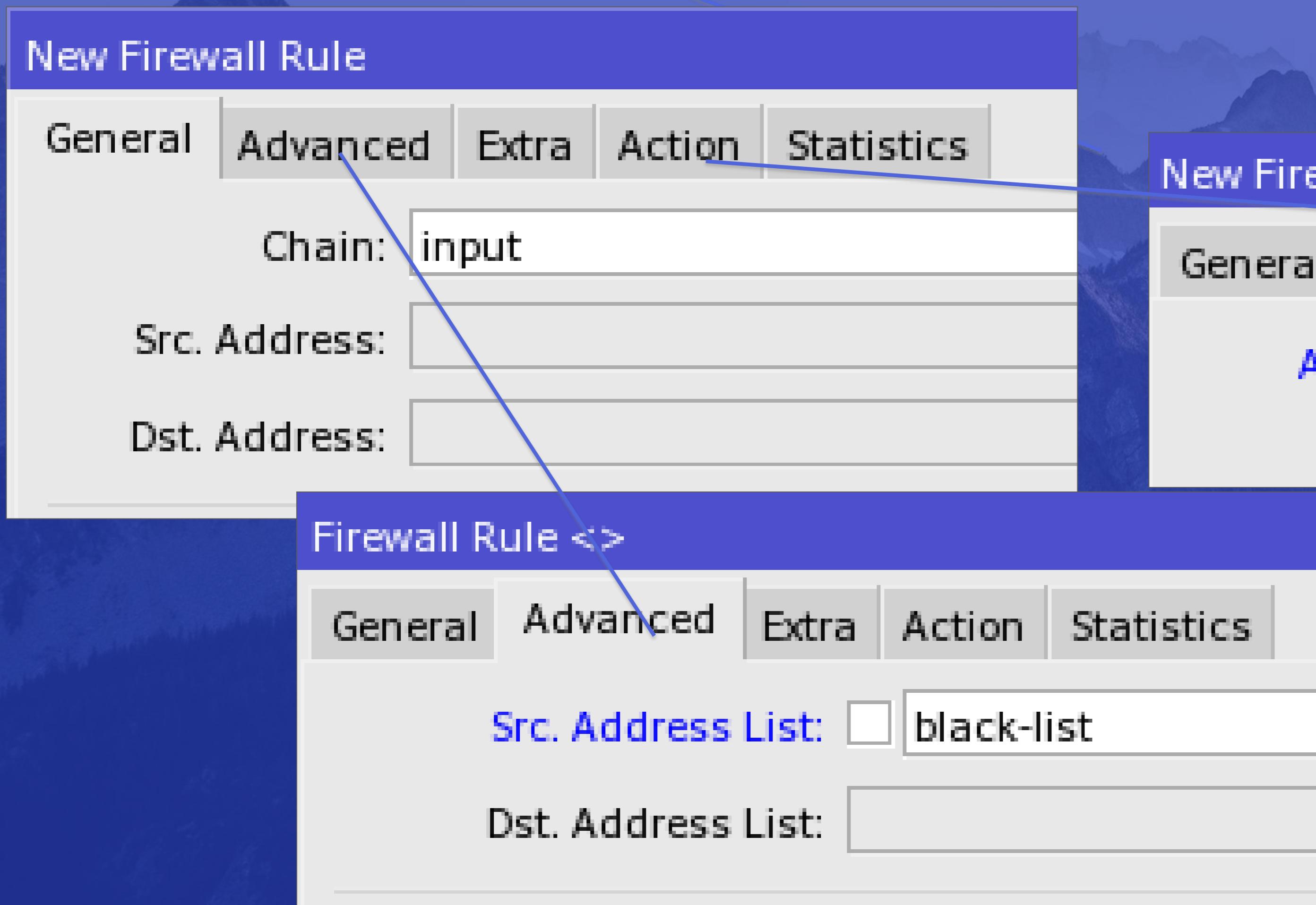
Dst. Address:

Firewall Rule <>

General Advanced Extra Action Statistics

Src. Address List: black-list

Dst. Address List:



New Firewall Rule

General Advanced Extra Action Statistics

Action: drop



Terima Kasih