IDS IMPLEMENTATION WITH MIKROTIK

BY: ANTONIUS DUTY SUSILO

MUM (MIKROTIK USER MEETING)

VIETNAM

2017

PROFILE

- Antonius Duty Susilo
- Email dutymlg@gmail.com
- Master degree of Information Technology in ITB (Institute Teknologi Bandung) Indonesia
- Teacher in SMK Telkom Malang and Lecturer in University
- Trainer Mikrotik (belajarmikrotik.com) and Consultant Mikrotik
- Cisco Networking Academy Program and Oracle Academy Instructor and Oracle WDP (Workforce Development Program) Instructor

SMK TELKOM MALANG

SMK TELKOM Malang was founded in 1992 to became the first Vocational High School in Indonesia to organize the Vocational Education in Telecommunication Engineering specializing in informatics engineering program (www.smktelkom-mlg.sch.id)

SMK Telkom Malang is under the auspices of Telkom Education Foundation or Yayasan Pendidikan Telkom (YPT) Bandung (www.ypt.or.id)

Telkom Schools

SMK Telkom Malang

SMK TELKOM MALANG

The Study Program :

Computer and Networks Engineering
Students will be able to create Computer Technicians and Network Engineer

Software Engineering
Students will be educated in software development and programming

Principal : Drs. Hendy Adriyanto

INTRUSION DETECTION SYSTEM

SECURING ROUTER

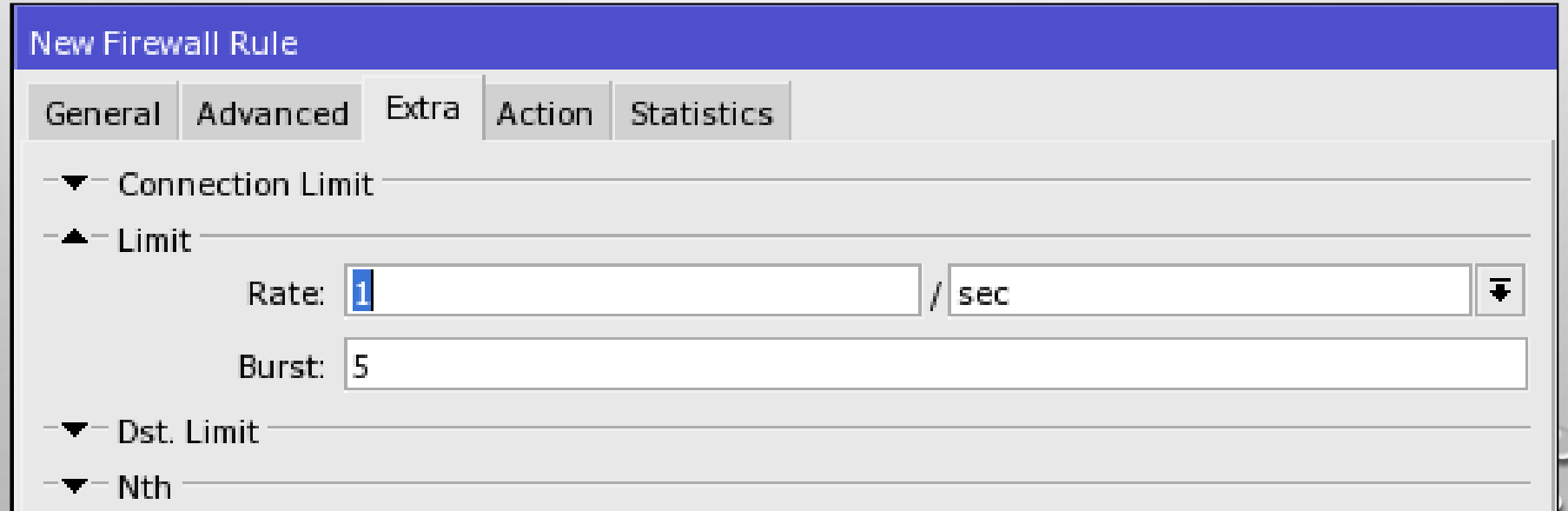
- THE MAIN IDEA TO SECURED THE ROUTER IS BY MINIMIZING THE INTRUSION
- SECURITY MEANS COMPLEXITY

NETWORK INTRUSION TYPES

- NETWORK INTRUSION IS A SERIOUS SECURITY RISK THAT COULD RESULT IN NOT ONLY THE TEMPORAL DENIAL, BUT ALSO IN TOTAL REFUSAL OF NETWORK SERVICE
- WE CAN POINT OUT 5 MAJOR NETWORK INTRUSION TYPES:
  - PING FLOOD
  - PORT SCAN
  - DOS ATTACK
  - DDOS ATTACK
  - UNAUTHORIZED ACCESS TO THE ROUTER
- ALL IDS IS IMPLEMENTED IN INPUT OR OUTPUT CHAIN

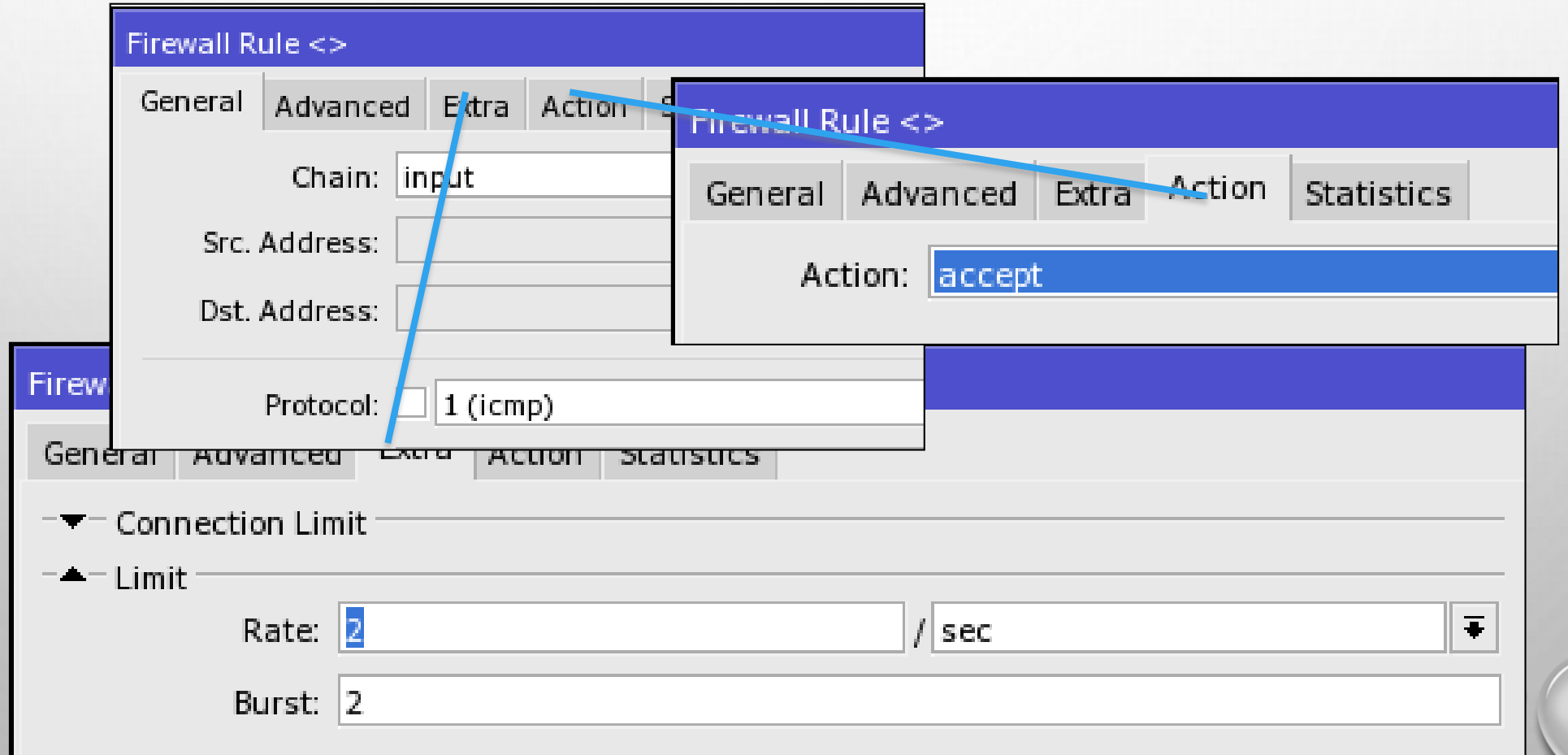
PING FLOOD

- PING FLOOD USUALLY CONSIST FROM VOLUMES OF RANDOM ICMP MESSAGES
- WITH “LIMIT” CONDITION IT IS POSSIBLE TO BOUND THE RULE MATCH RATE TO A GIVEN LIMIT
- THIS CONDITION IS OFTEN USED WITH ACTION “LOG”



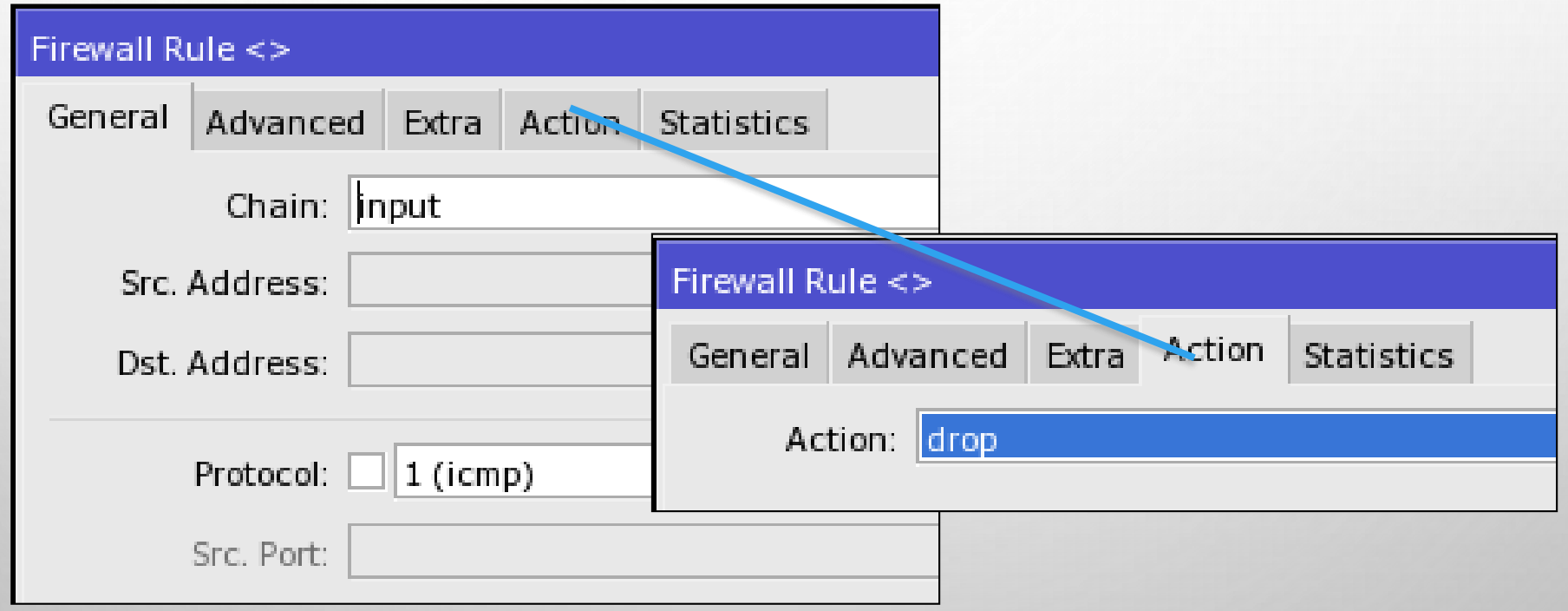
LIMIT (FOR PING-FLOOD)

- MAKE A RULE TO LIMIT ICMP PROTOCOL TO 2 PACKET / SECOND AND BURSTABLE TO 2 OTHER PACKET



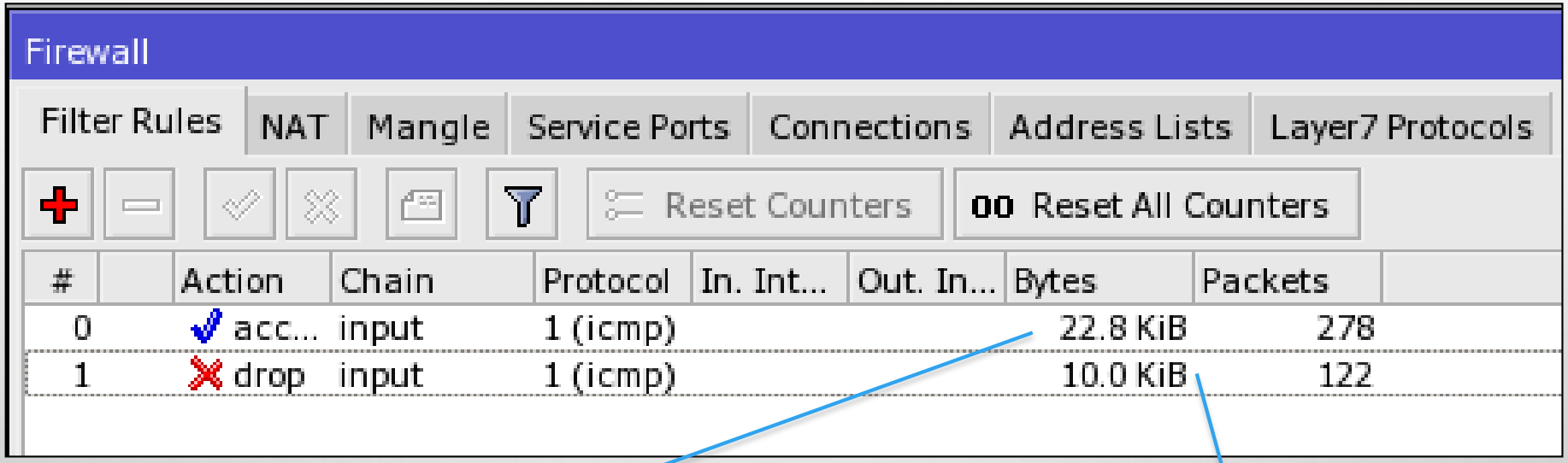
LIMIT (FOR PING-FLOOD)

- MAKE ANOTHER RULE TO BLOCK OTHER THAN THOSE TRAFFIC BEFORE (2 PPS BURSTABLE TO 2 OTHER PPS)



LIMIT (FOR PING-FLOOD)

- TRY TO PING SEVERAL TIMES (MORE THAN 2)



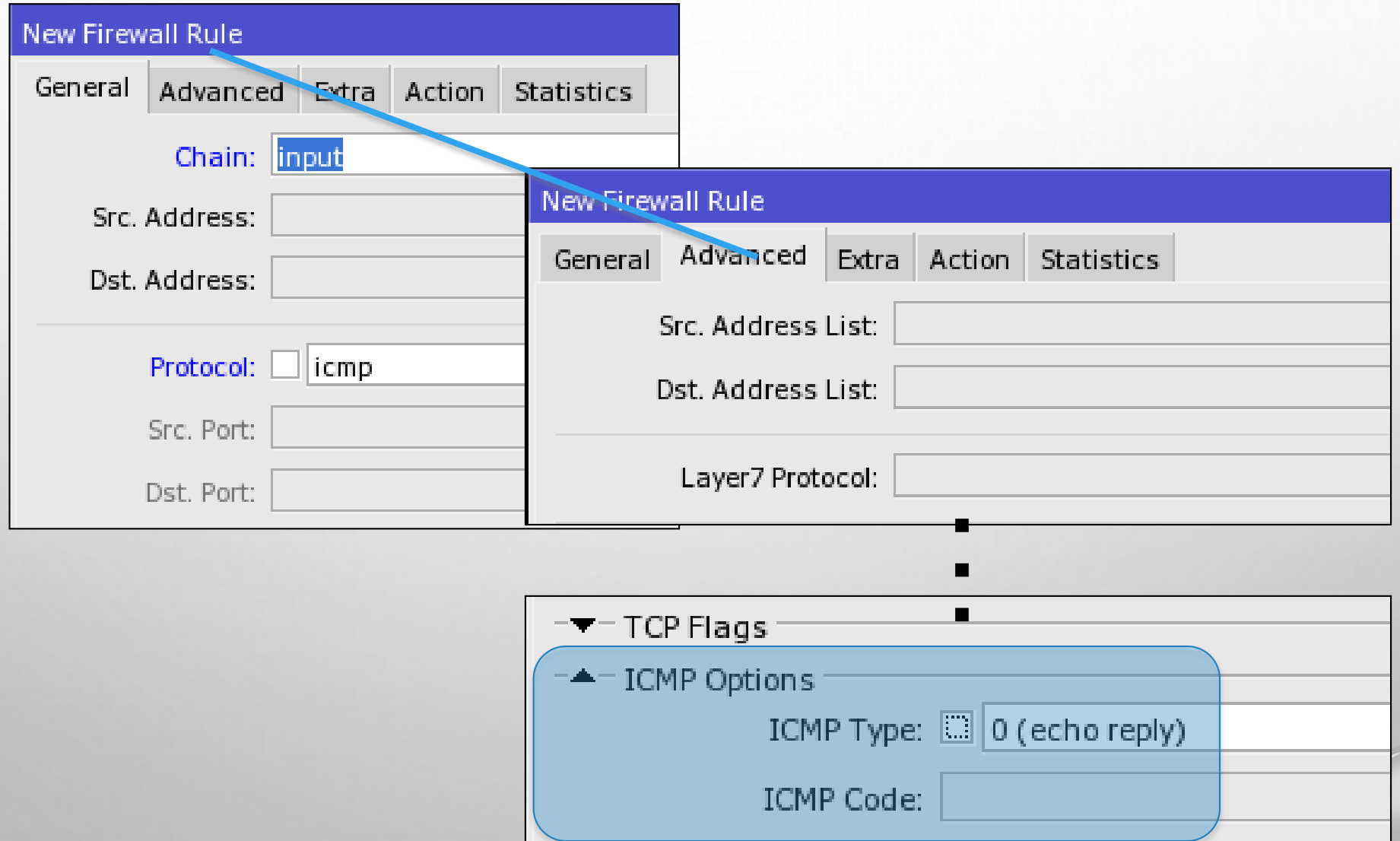
Accept Counter (if less than or equal to 2 pps)

Drop counter (more than 2 pps or 4 pps)

ICMP MESSAGE TYPES

- TYPICAL IP ROUTER USES ONLY FIVE TYPES OF ICMP MESSAGES (TYPE:CODE)
  - FOR PING - MESSAGES 0:0 AND 8:0
  - FOR TRACEROUTE – MESSAGES 11:0 AND 3:3
  - FOR PATH MTU DISCOVERY – MESSAGE 3:4
- OTHER TYPES OF ICMP MESSAGES SHOULD BE BLOCKED

ICMP MESSAGE RULE EXAMPLE



ICMP FLOOD

- MAKE THE NEW CHAIN – ICMP
  - ACCEPT 5 NECESSARY ICMP MESSAGES
  - SET MATCH RATE TO 3 PPS WITH 5 PACKET BURST POSSIBILITY
  - DROP ALL OTHER ICMP PACKETS

ICMP FLOOD

New Firewall CHAIN

Firewall

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

Reset Counters | Reset All Counters | Find

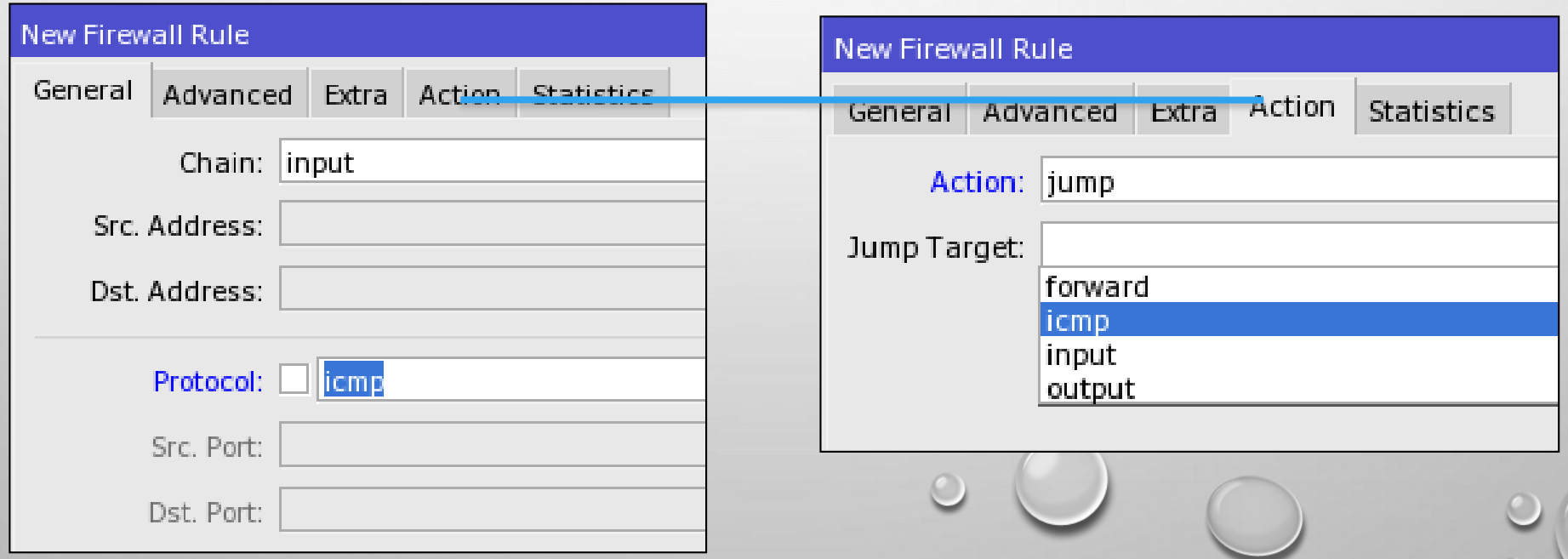
#	Action	Chain	Protocol	ICMP Options/ICMP Type	ICMP Options...	Bytes	Packets
0	accept	icmp	1 (icmp)	0 (echo reply)	0	0 B	0
1	accept	icmp	1 (icmp)	8 (echo request)	0	0 B	0
2	accept	icmp	1 (icmp)	11 (time exceeded)	0	0 B	0
3	accept	icmp	1 (icmp)	3 (destination unreachable)	3	0 B	0
4	accept	icmp	1 (icmp)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

DROP other ICMP type and code

ACCEPT all ICMP Type and Code defined earlier

ICMP FLOOD

- MOVE ALL ICMP PACKETS TO ICMP CHAIN
  - CREATE AN ACTION “JUMP” RULE IN THE CHAIN INPUT
  - PLACE IT ACCORDINGLY
  - CREATE AN ACTION “JUMP” RULE IN THE CHAIN FORWARD
  - PLACE IT ACCORDINGLY



PORT KNOCKING

- PORT KNOCKING IS A METHOD OF EXTERNALLY OPENING PORTS ON A FIREWALL BY GENERATING A CONNECTION ATTEMPT ON A SET OF PRE-SPECIFIC CLOSED PORT
- THE PRIMARY PURPOSE OF PORT KNOCKING IS TO PREVENT AN ATTACKER FROM CONNECTING TO AN OPEN PORT AND GET A BRUTE-FORCE ON THE USERNAME/PASSWORD
- THE PORT "KNOCK" ITSELF IS SIMILAR TO A SECRET HANDSHAKE AND CAN CONSIST OF ANY NUMBER OF TCP, UDP, OR EVEN SOMETIMES ICMP AND OTHER PROTOCOL PACKETS TO NUMBERED PORTS ON THE DESTINATION MACHINE

PORT KNOCKING SCHEME

1. Send a connection to TCP-1234
2. The router store requester IP for an amount of time
3. Send a connection to TCP-4321
4. The router checked if the IP is the same IP with the first connection (TCP-1234)
5. If the IP is the same and the time between 1st attempt and 2nd, then the requester IP will be allowed to access the router

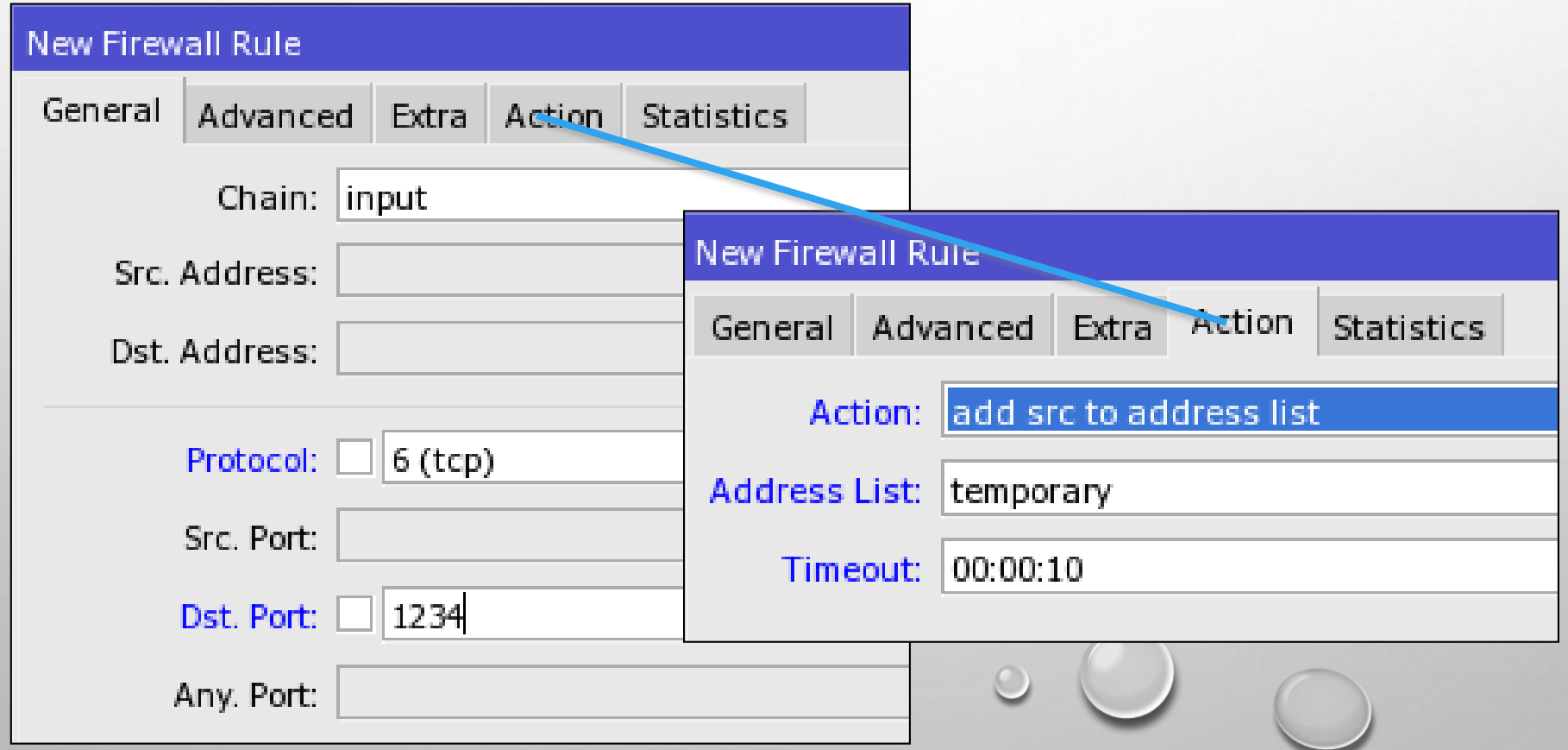
Knocking Port
TCP 1234
TCP 4321

PORT KNOCKING IN MIKROTIK

- THE STEP OF APPLYING PORT KNOCKING IN MIKROTIK (EVERYTHING IS APPLIED IN INPUT CHAIN)
  - TRAP A CONNECTION TO TCP PORT 1234 AND PUT THE SRC-ADDRESS TO AN ADDRESS-LIST TEMPORARY FOR 10S
  - TRAP A CONNECTION TO TCP PORT 4321 AND CHECKED WHETHER THE SRC-ADDRESS IS ALREADY AT ADDRESS-LIST TEMPORARY. IF SO PUT THE SRC-ADDRESS TO AN ADDRESS-LIST SECURED
  - ALLOW ACCESS FROM SRC-ADDRESS-LIST SECURED
  - DROP OTHER CONNECTION

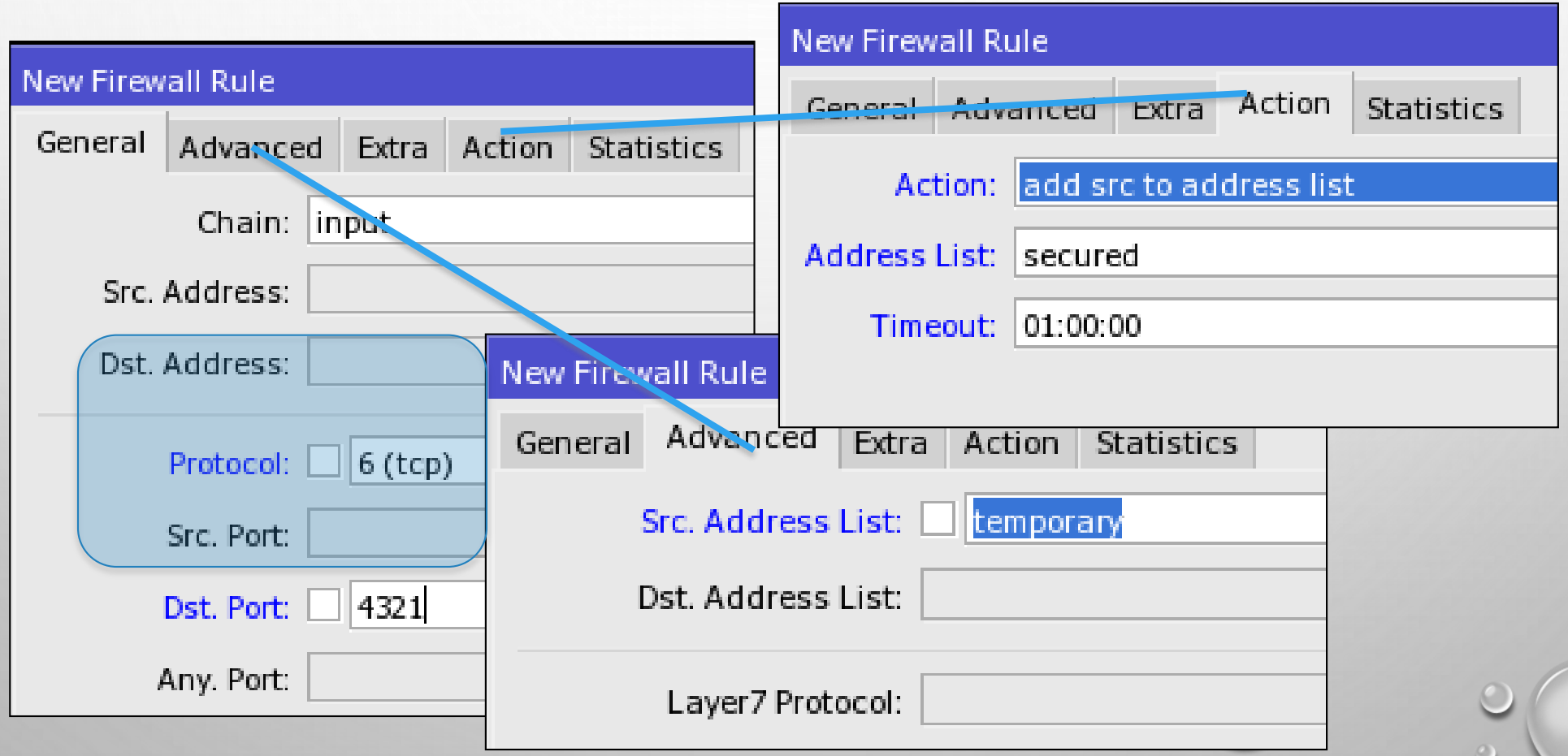
PORT KNOCKING

- TRAP TCP(1234) AND PUT THE SOURCE ADDRESS TO ADDRESS-LIST TEMPORARY FOR 10 SECONDS



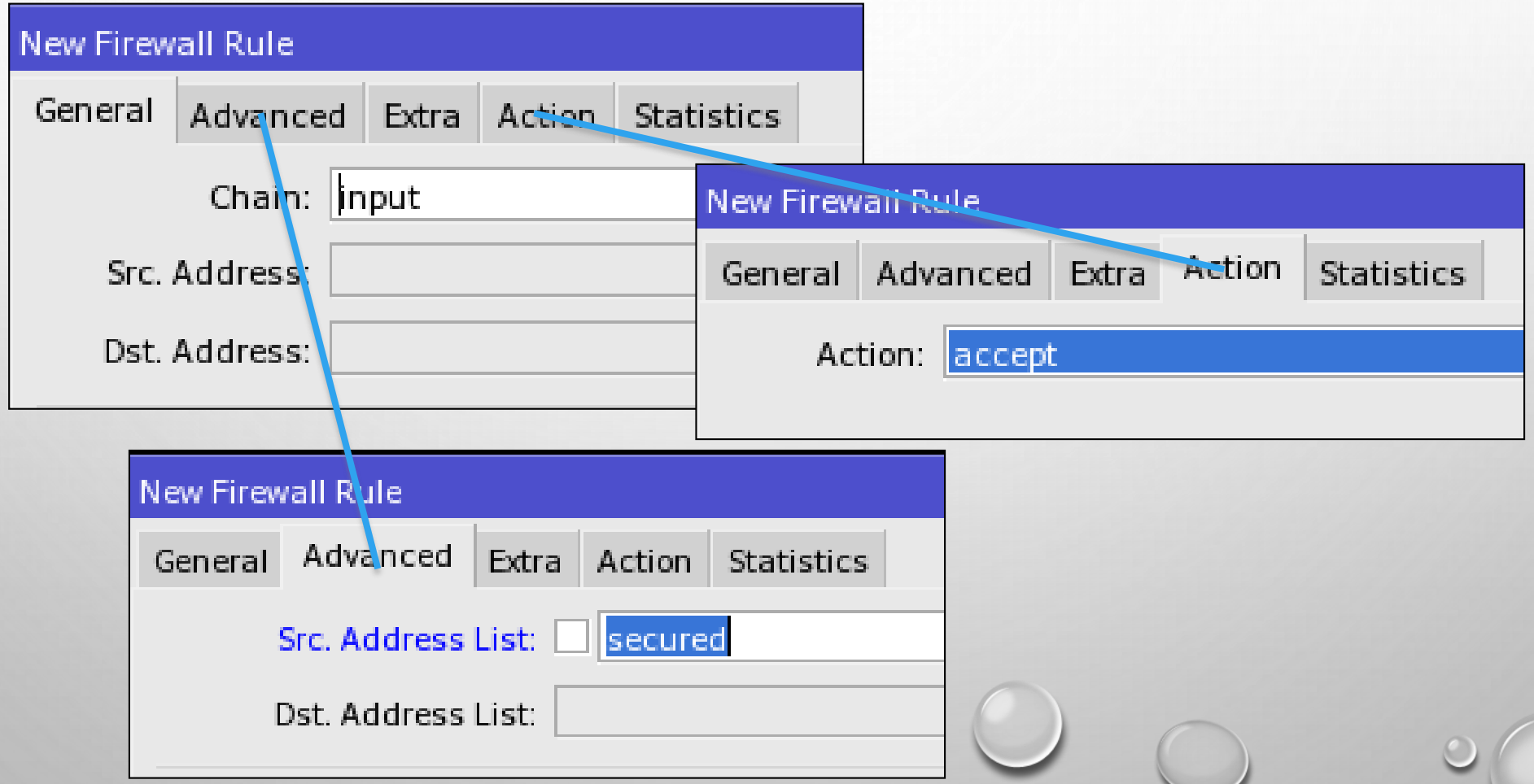
PORT KNOCKING

- TRAP TCP(4321) AND SRC-ADDRESS IS IN TEMPORARY. PUT IT TO ADDRESS-LIST SECURED



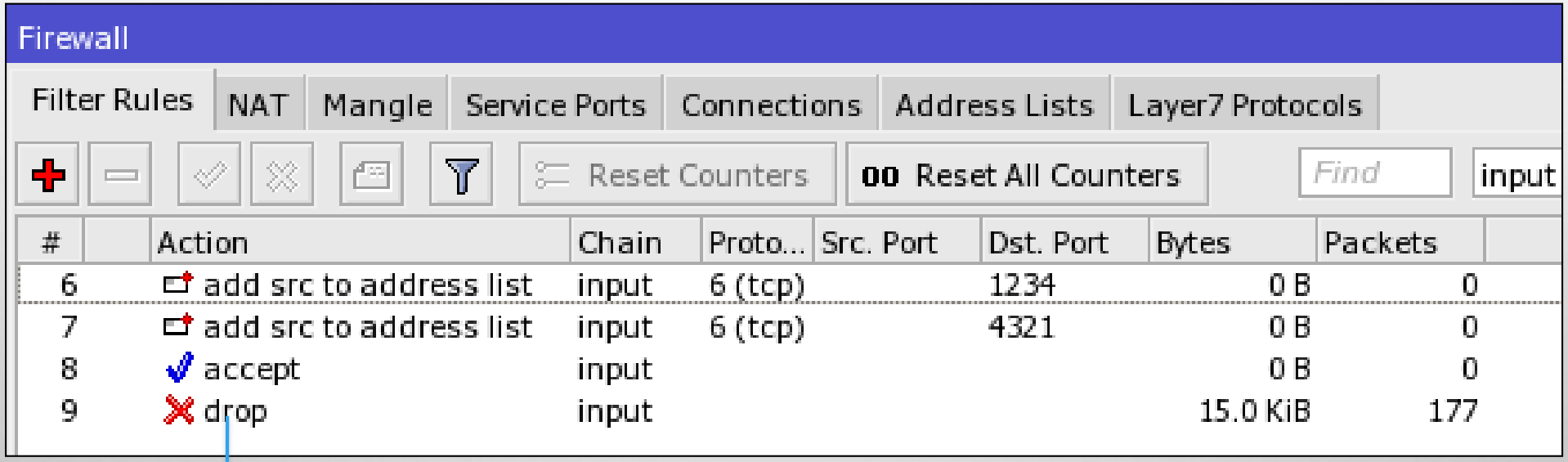
PORT KNOCKING

- ALLOW ACCESS FROM SRC-ADDRESS-LIST SECURED



PORT KNOCKING

- DROP ANOTHER TRAFFIC
- ALL THE RULE VIEW



#	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

At the end, DROP ALL

C:\WINDOWS\system32\cmd.exe - p

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

admin@00:0C:42:5E:5C:6A (46_

Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS

Firewall

Filter Rules | NAT | Mangle | Service

	Name	Address
D	temporary	192.168.46.1

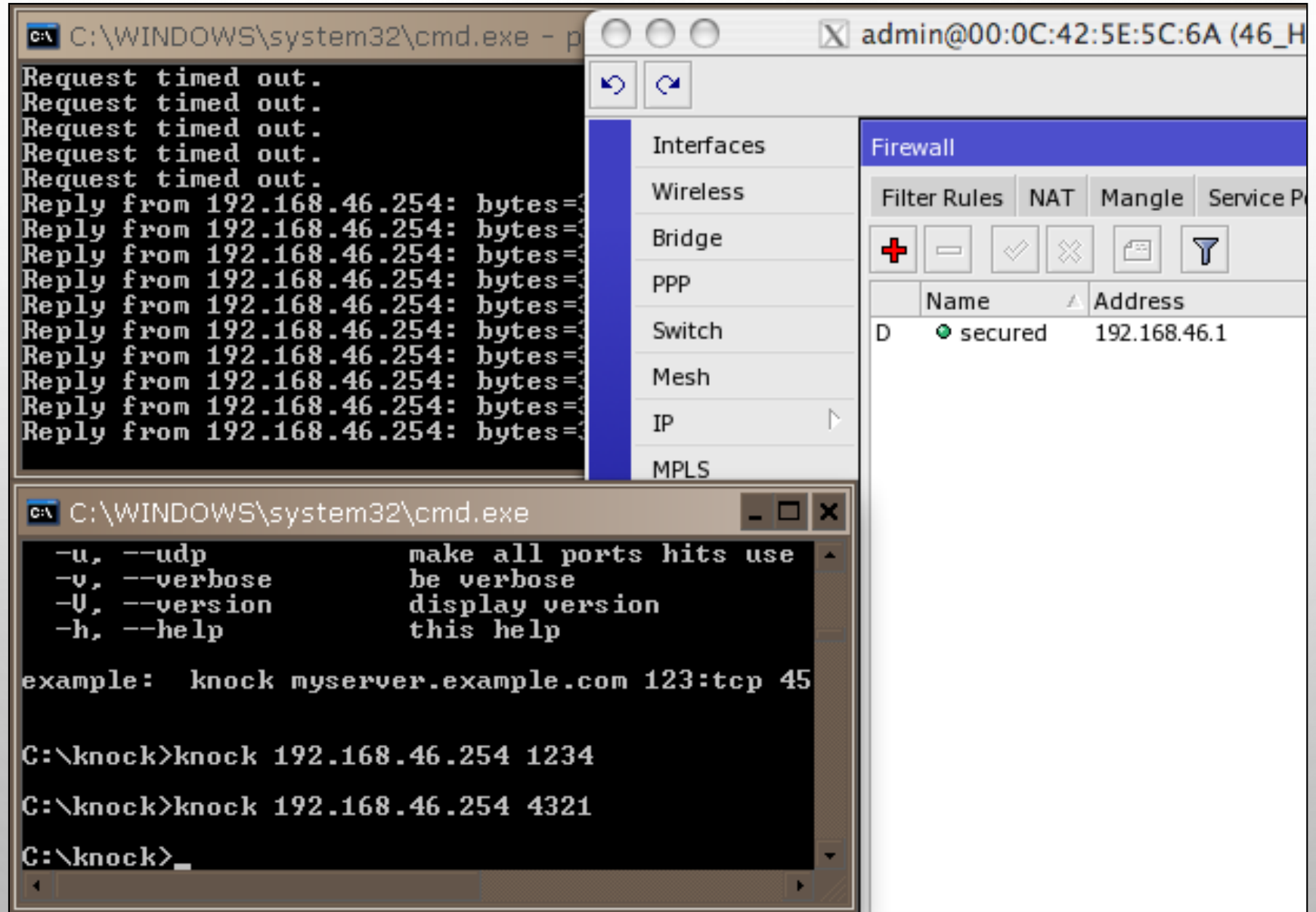
C:\WINDOWS\system32\cmd.exe

```
usage: knock [options] <host> <port[:proto]> [p
options:
  -u, --udp             make all ports hits use
  -v, --verbose         be verbose
  -V, --version         display version
  -h, --help            this help

example:  knock myserver.example.com 123:tcp 45


C:\knock>knock 192.168.46.254 1234

C:\knock>
```


C:\WINDOWS\system32\cmd.exe - p
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.46.254: bytes=
admin@00:0C:42:5E:5C:6A (46_H
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Firewall
Filter Rules
NAT
Mangle
Name
Address
D
secured
192.168.46.1
C:\WINDOWS\system32\cmd.exe
-u, --udp make all ports hits use
-v, --verbose be verbose
-V, --version display version
-h, --help this help
example: knock myserver.example.com 123:tcp 45
C:\knock>knock 192.168.46.254 1234
C:\knock>knock 192.168.46.254 4321
C:\knock>

PORT KNOCKING

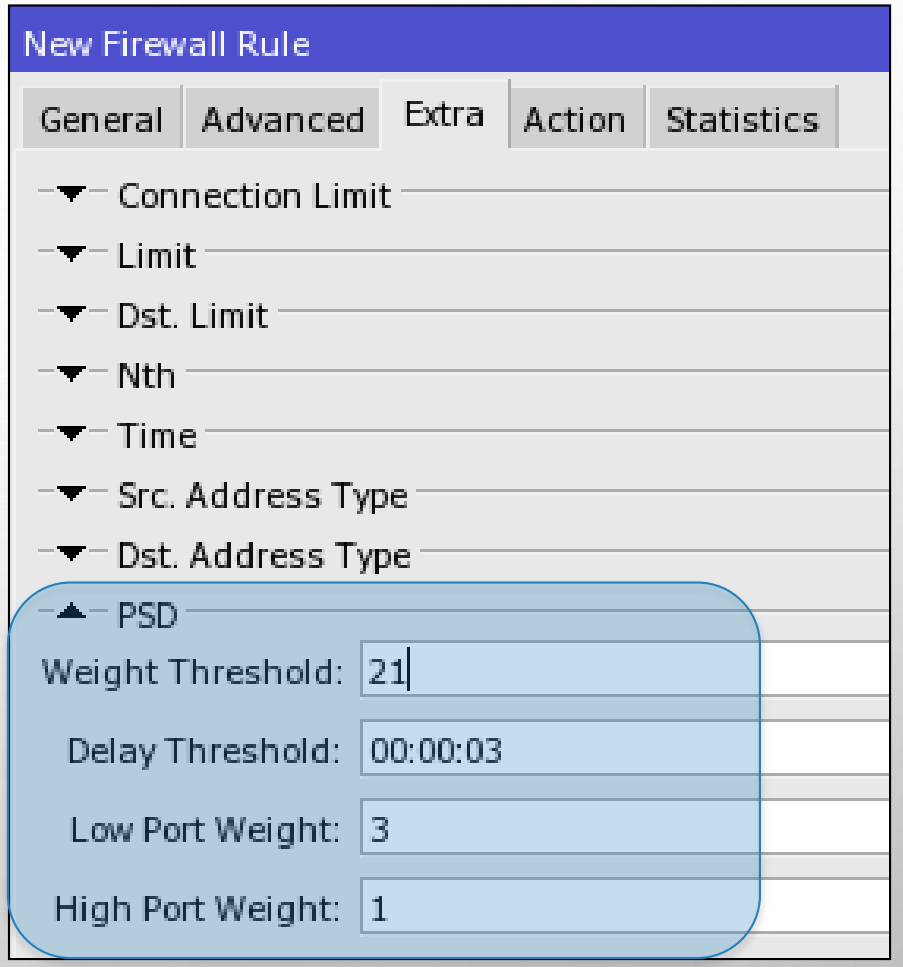
- TRY TO CHANGE THE PORT
- MAKE IT A SEQUENCE OF 3 PORTS OR MORE
  - USE TEMPORARY-X AS THE TEMPORARY LIST FOR MORE THAN 2 PORTS USED

PORT SCAN

- PORT SCAN IS A METHOD OF INTRUSION WHERE THE OUTSIDER WILL SCAN THE ROUTER'S PORT TO FIND ONE OR MORE OPEN PORT THAT THEY CAN USE TO PENETRATE THE ROUTER
- THERE ARE 2 KIND OF PORT, WHICH ARE :
  - LOW PORT (OR WELL-KNOW-PORT) WHICH USUALLY USE BY MANY PROGRAMS TO IDENTIFY THEMSELVES. THIS PORT RANGE IS FROM 0 – 1023
  - HIGH PORT WHICH ARE USED RARELY AS AN APPLICATION. THE PORT RANGE IS FROM 1024 - 65535

PORT SCAN DETECT

- MIKROTIK CAN DETECT PORT SCAN BY PSD OPTION IN ADVANCED TAB AT THE FIREWALL
- PSD IS POSSIBLE ONLY FOR TCP PROTOCOL
- LOW PORTS
  - FROM 0 TO 1023
- HIGH PORTS
  - FROM 1024 TO 65535

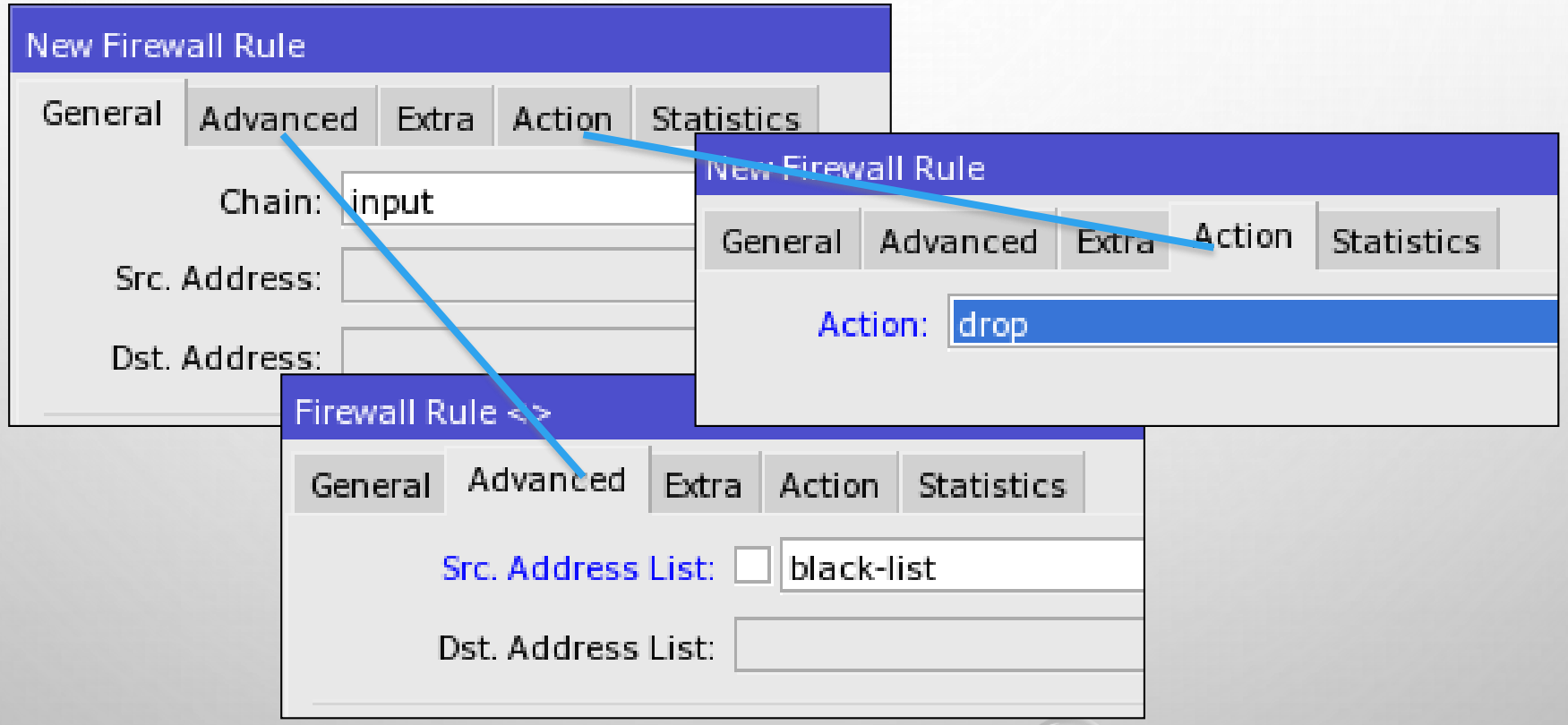


PORT SCAN DETECT STEP-BY-STEP

- THE STEP OF APPLYING PSD IN MIKROTIK (EVERYTHING IS APPLIED IN INPUT CHAIN)
  - DROP A CONNECTION FROM SRC-ADDRESS BLACK-LIST
  - TRAP A CONNECTION THAT TRY TO DO A PSD AND PUT THE SRC-ADDRESS TO ADDRESS-LIST BLACK-LIST
  - NOTE : DO NOT CHANGE THE ORDER OF THE RULES ABOVE

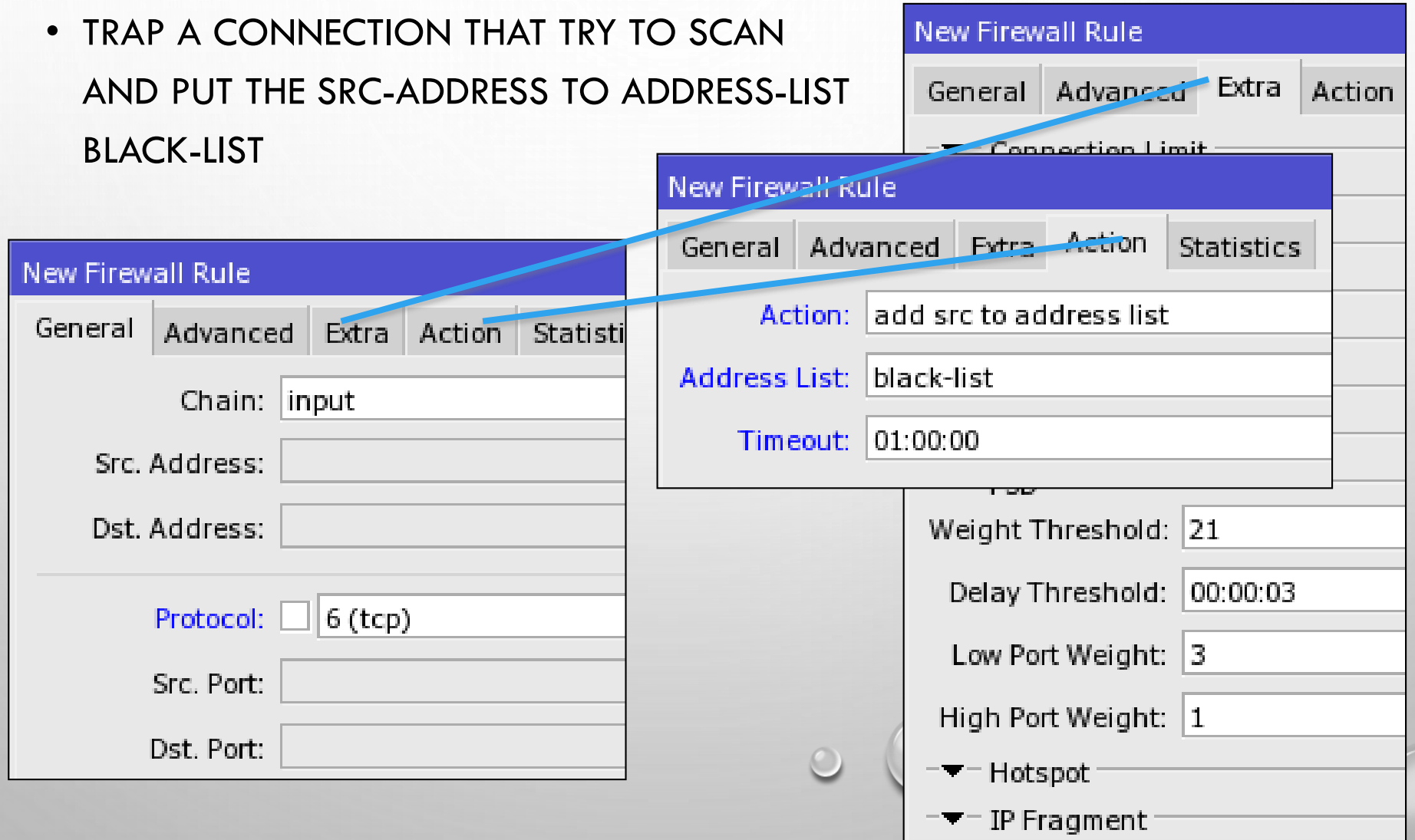
PORT SCAN

- DROP A CONNECTION FROM SRC-ADDRESS BLACK-LIST



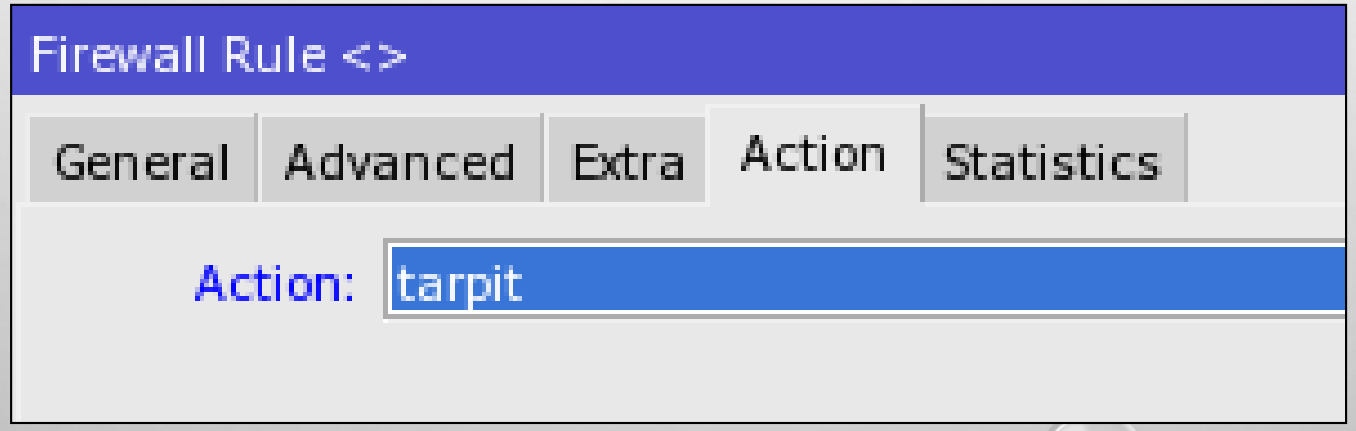
PORT SCAN DETECT

- TRAP A CONNECTION THAT TRY TO SCAN AND PUT THE SRC-ADDRESS TO ADDRESS-LIST BLACK-LIST



PORT SCAN DETECT

- TRY TO CHANGE THE OPTIONS (LOW PORT WEIGHT, HIGH PORT WEIGHT, AND WEIGHT THRESHOLD)
- INSTEAD OF USING DROP AT THE FIRST RULE, YOU CAN ALSO USE TARPIT (TCP TRAFFIC ONLY). FIGURED OUT THE DIFFERENCE



DOS ATTACKS

- MAIN TARGET FOR DOS ATTACKS IS CONSUMPTION OF RESOURCES, SUCH AS CPU TIME OR BANDWIDTH, SO THE STANDARD SERVICES WILL GET DENIAL OF SERVICE (DOS)
- USUALLY ROUTER IS FLOODED WITH TCP/SYN (CONNECTION REQUEST) PACKETS. CAUSING THE SERVER TO RESPOND WITH A TCP/SYN-ACK PACKET, AND WAITING FOR A TCP/ACK PACKET.
- MOSTLY DOS ATTACKERS ARE VIRUS INFECTED CUSTOMERS

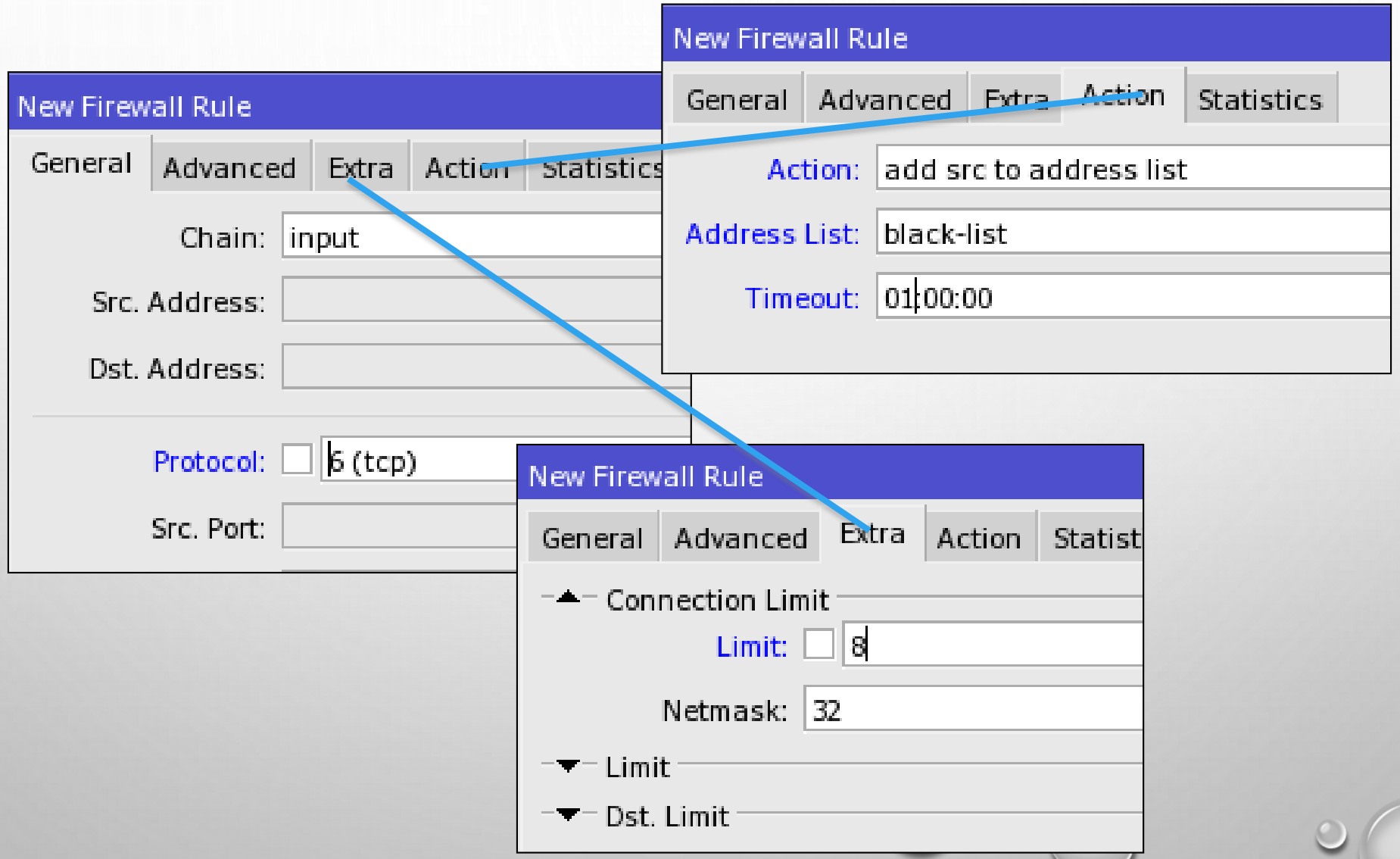
SYN FLOOD

U	10.17.0.1:57403	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.3:40103	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.3:40104	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.4:56080	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.4:56081	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.5:39813	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.5:39814	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.6:42043	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.6:42044	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.8:52842	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.8:52843	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.10:4...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.10:4...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.11:5...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.11:5...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.12:3...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.12:3...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.13:5...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.13:5...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.14:4...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.14:4...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.16:4...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.16:4...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.17:5...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.17:5...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.18:6...	1.1.1.111:80	6 (tcp)		(none)		syn sent
U	10.17.0.18:6...	1.1.1.111:80	6 (tcp)		(none)		syn sent

DOS ATTACK PROTECTION

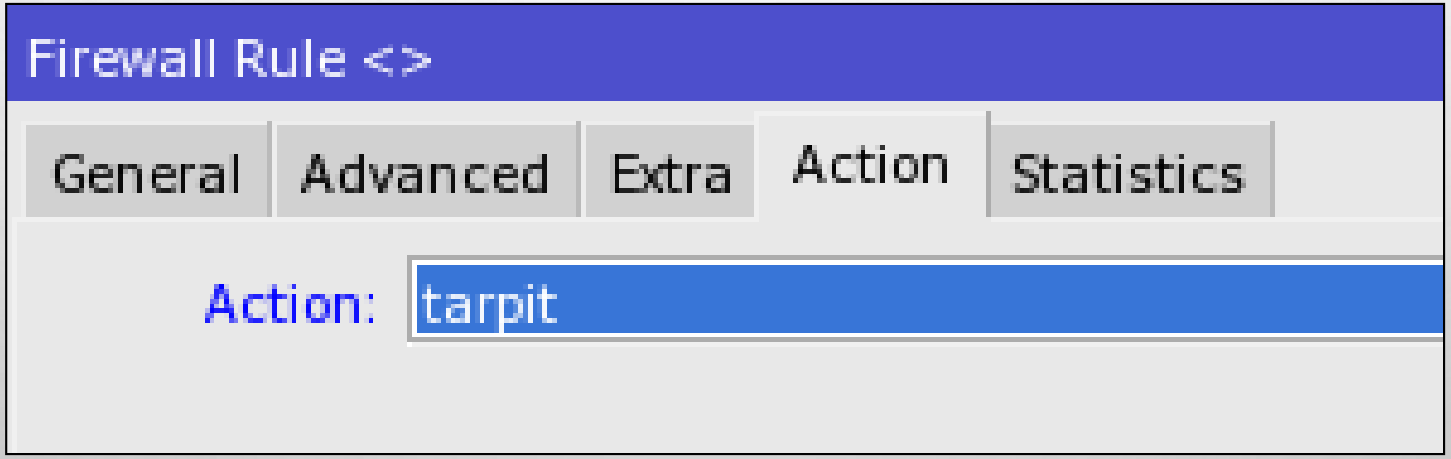
- ALL IP'S WITH MORE THAN 10 CONNECTIONS TO THE ROUTER SHOULD BE CONSIDERED AS DOS ATTACKERS
- WITH EVERY DROPPED TCP CONNECTION WE WILL ALLOW ATTACKER TO CREATE NEW CONNECTION
- WE SHOULD IMPLEMENT DOS PROTECTION INTO 2 STEPS:
  - DETECTION - CREATING A LIST OF DOS ATTACKERS ON THE BASIS OF CONNECTION-LIMIT
  - SUPPRESSION – APPLYING RESTRICTIONS TO THE DETECTED DOS ATTACKERS

DOS ATTACK DETECTION



DOS ATTACK SUPPRESSION

- TO STOP THE ATTACKER FROM CREATING NEW CONNECTIONS, WE WILL USE ACTION “TARPIT”
- WE MUST PLACE THIS RULE BEFORE THE DETECTION RULE OR ELSE ADDRESS-LIST ENTRY WILL REWRITE ALL THE TIME

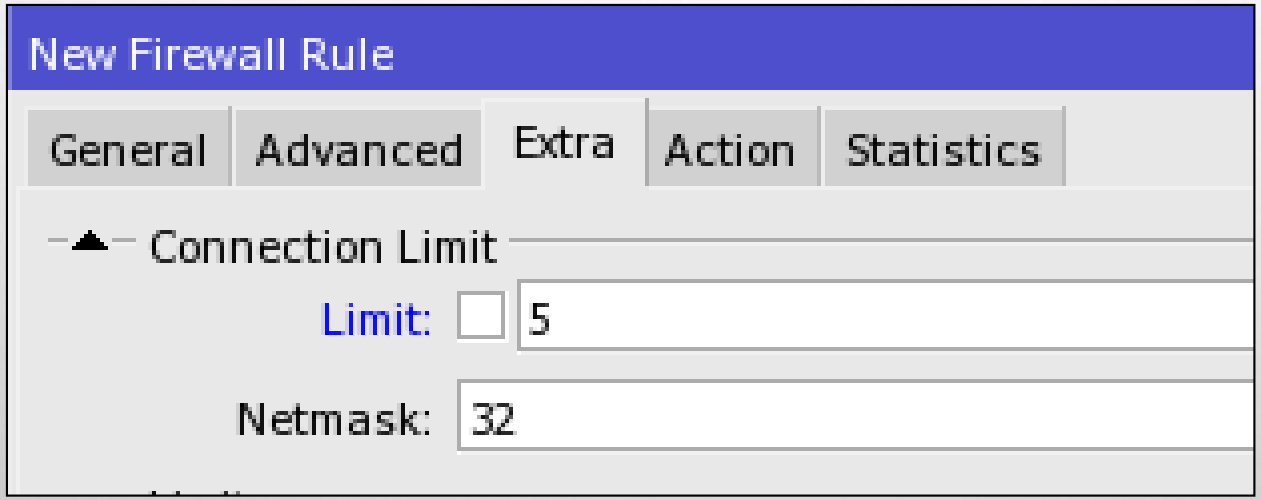


CONNECTION LIMIT

- CONNECTION LIMIT LIMITS THE PACKET PER SECOND (PPS) RATE ON A PER DESTINATION IP OR PER DESTINATION PORT BASE
- AS OPPOSED TO THE LIMIT MATCH, EVERY DESTINATION IP ADDRESS / DESTINATION PORT HAS IT'S OWN LIMIT
- CONNECTION LIMIT ONLY EFFECT THE TCP TRAFFIC

CONNECTION LIMIT

- LIMIT THE NUMBER OF ACTIVE CONNECTIONS TO 5 PER SINGLE IP ADDRESS FOR TELNET SESSION TO THE ROUTER
- THINK ABOUT THE VARIOUS EFFECTS OF THE RULE ABOVE



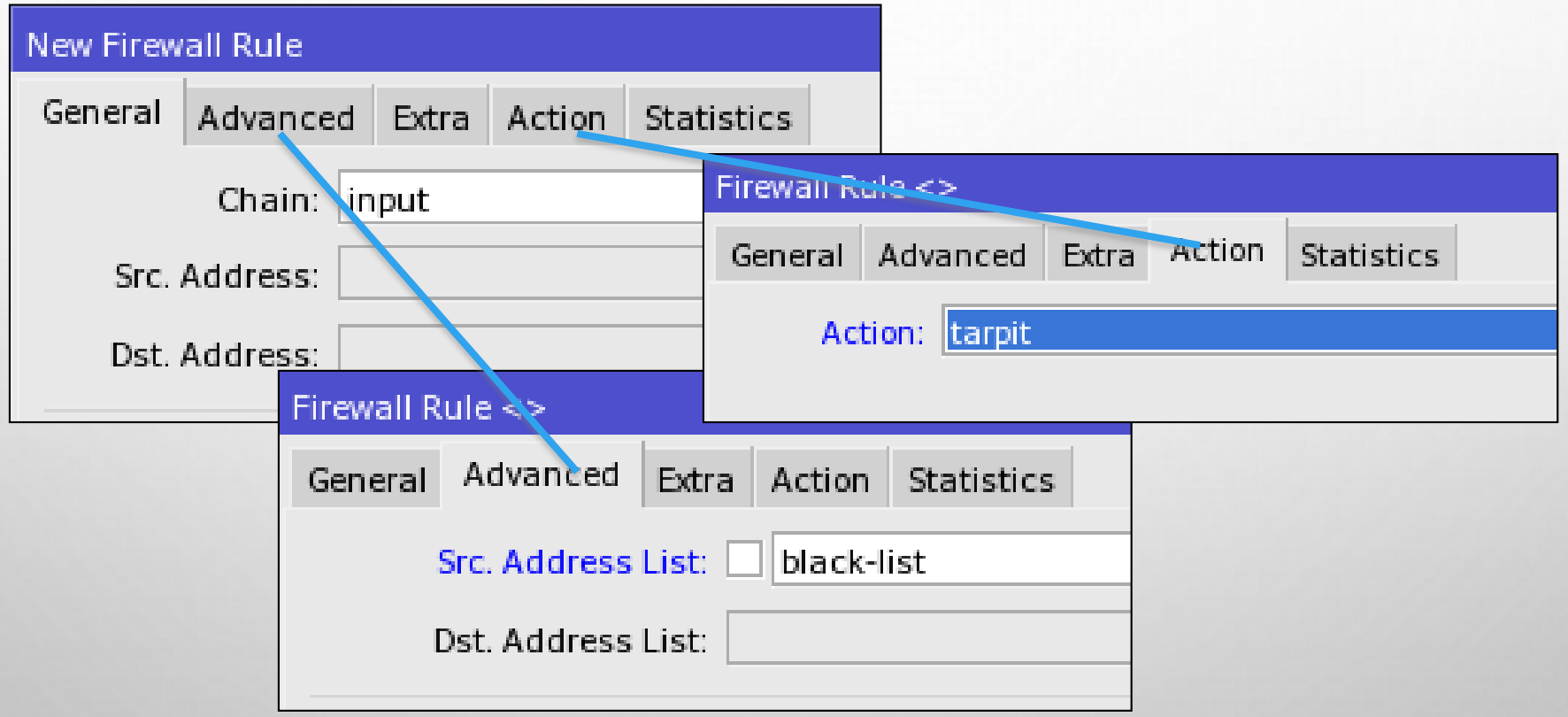
CONNECTION LIMIT

- THE STEP OF MAINTAINING DOS ATTACK IN MIKROTIK (EVERYTHING IS APPLIED IN INPUT CHAIN)
  - TARPIT A CONNECTION FROM SRC-ADDRESS BLACK-LIST
  - CREATE A RULE TO ALLOW ONLY 5 SIMULTANEOUS CONNECTION FROM A /32 IP, OTHERWISE ADD THE SRC-ADDRESS TO A BLACK-LIST ADDRESS-LIST

  - NOTE : TARPIT AND CONNECTION-LIMIT ONLY VALID FOR TCP PACKET

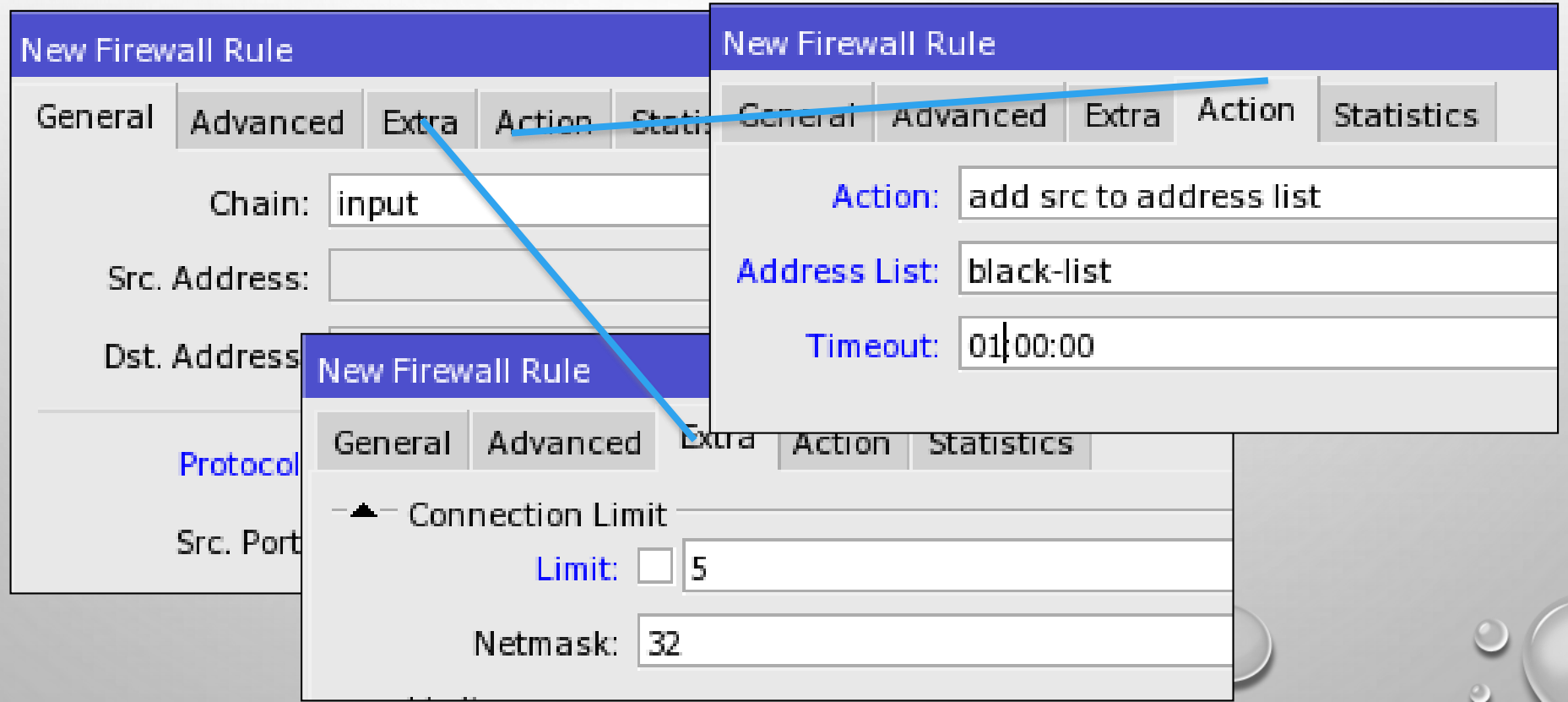
CONNECTION LIMIT

- TARPIT A CONNECTION WITH SRC-ADDRESS BLACK-LIST



CONNECTION LIMIT

- CREATE A RULE TO ALLOW ONLY 5 SIMULTANEOUS CONNECTION FROM A /32 IP, OTHERWISE ADD THE SRC-ADDRESS TO A BLACK-LIST ADDRESS-LIST

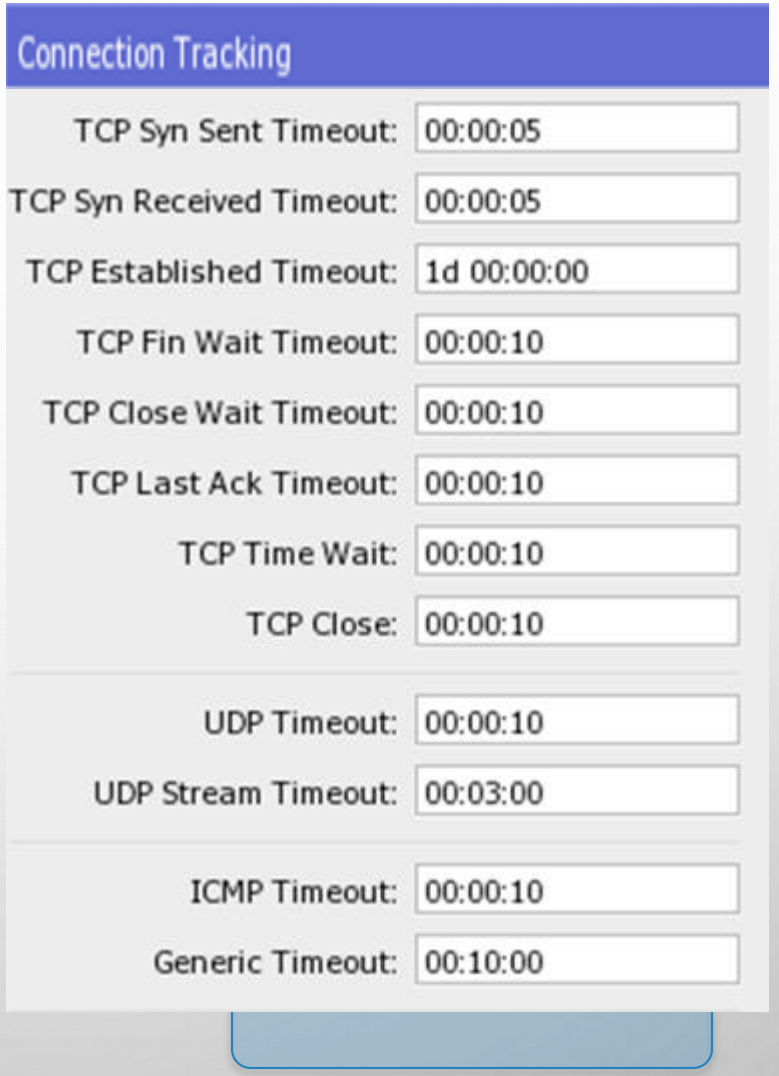


CONNECTION LIMIT

- TRY TO MAKE A TELNET OR WEB ACCESS CONNECTION TO YOUR ROUTER AS MUCH AS POSSIBLE
- SEE WHAT IS HAPPENED
  - IT WILL SHOW UP DIFFERENCES ON THE 6TH TELNET/WEB SESSION

DDOS ATTACKS

- A DISTRIBUTED DENIAL OF SERVICE ATTACK IS VERY SIMILAR TO DOS ATTACK ONLY IT OCCURS FROM MULTIPLE COMPROMISED SYSTEMS
- ONLY THING THAT COULD HELP IS “TCPSYN COOKIE” OPTION IN CONNTRACK SYSTEM



BRUTE FORCE ATTACK

- BRUTE FORCE IS AN ATTEMPT TO CONNECTING TO A ROUTER WITH RANDOM USERNAME/PASSWORD

Log

all

Jan/02/1970 05:12:59	system error criti...	login failure for user anonymous from 192.168.46.1 via ftp
Jan/02/1970 05:13:27	system error criti...	login failure for user root from 192.168.46.1 via ftp
Jan/02/1970 05:13:32	system error criti...	login failure for user root1 from 192.168.46.1 via ftp
Jan/02/1970 05:13:38	system error criti...	login failure for user herry from 192.168.46.1 via ftp
Jan/02/1970 05:13:43	system error criti...	login failure for user spam from 192.168.46.1 via ftp
Jan/02/1970 05:13:47	system error criti...	login failure for user robert from 192.168.46.1 via ftp
Jan/02/1970 05:13:51	system error criti...	login failure for user erick from 192.168.46.1 via ftp
Jan/02/1970 05:13:56	system error criti...	login failure for user jason from 192.168.46.1 via ftp
Jan/02/1970 05:14:02	system error criti...	login failure for user aabbc from 192.168.46.1 via ftp
Jan/02/1970 05:14:06	system error criti...	login failure for user aabbd from 192.168.46.1 via ftp
Jan/02/1970 05:14:11	system error criti...	login failure for user aabca from 192.168.46.1 via ftp
Jan/02/1970 05:14:16	system error criti...	login failure for user jane from 192.168.46.1 via ftp
Jan/02/1970 05:14:23	system error criti...	login failure for user quartz from 192.168.46.1 via ftp
Jan/02/1970 05:14:27	system error criti...	login failure for user friend from 192.168.46.1 via ftp
Jan/02/1970 05:14:32	system error criti...	login failure for user mean from 192.168.46.1 via ftp
Jan/02/1970 05:14:36	system info acco...	user admin logged in from 192.168.46.1 via ftp

BRUTE FORCE DETECTION

- THE IDEA TO DETECT BRUTE FORCE IS BY DETECTING AN UNSUCCESSFULLY LOGIN ATTEMPT FROM THE OUTSIDER
- WE CAN DETECT AN UNSUCCESSFULLY LOGIN ATTEMPT BY CHECKING THE RESPONSE FROM ROUTER TO OUTSIDER
- FOR FTP CONNECTION, ALL UNSUCCESSFULLY LOGIN ATTEMPT WILL RETURN TO OUTSIDER WITH A TEXT CONTAINS “530 LOGIN INCORRECT”

BRUTE FORCE DETECTION

- BRUTE FORCE ATTEMPTS ALWAYS GENERATED BY A MACHINE, THUS IT WILL REPEATED SIMULTANEOUSLY
- UNSUCCESSFUL LOGIN FOR ONE OR TWO TIMES CANNOT CONSIDER TO BE A BRUTE FORCE ATTEMPT

DETECTING A BRUTE FORCE

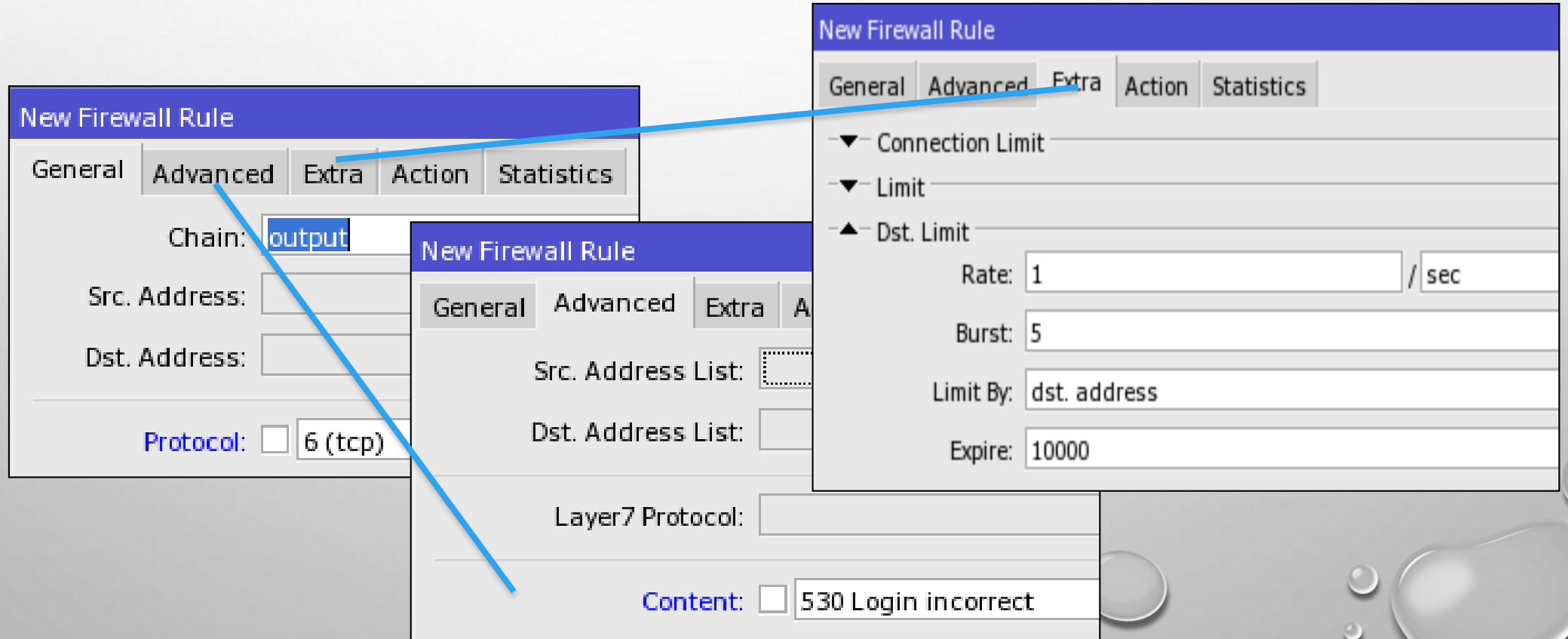
- THE STEP TO DETECTING A BRUTE FORCE ATTACK IN MIKROTIK (CREATED IN OUTPUT-CHAIN)
  - ADD A RULE TO ALLOW AN UNSUCCESSFUL ATTEMPT WITH 1 CONNECTION PER MINUTE (BURST IT TO 5 CONNECTION) BASED ON DESTINATION-ADDRESS
  - ADD A RULE TO PUT A DESTINATION-ADDRESS THAT HAS MORE THAN 1 CONNECTION PER MINUTE (HAS BEEN KICKED-OUT FROM THE RULE BEFORE) INTO AN ADDRESS-LIST NAMED BLACKLIST

DROP THE BRUTE FORCE IP

- THE STEP TO BLOCKING A BRUTE FORCE ATTACK IN MIKROTIK (AFTER THE BRUTE FORCER IP HAS BEEN REVEALED)
  - IN INPUT CHAIN, ADD A RULE TO DROP PACKET FROM SRC-ADDRESS BLACKLIST

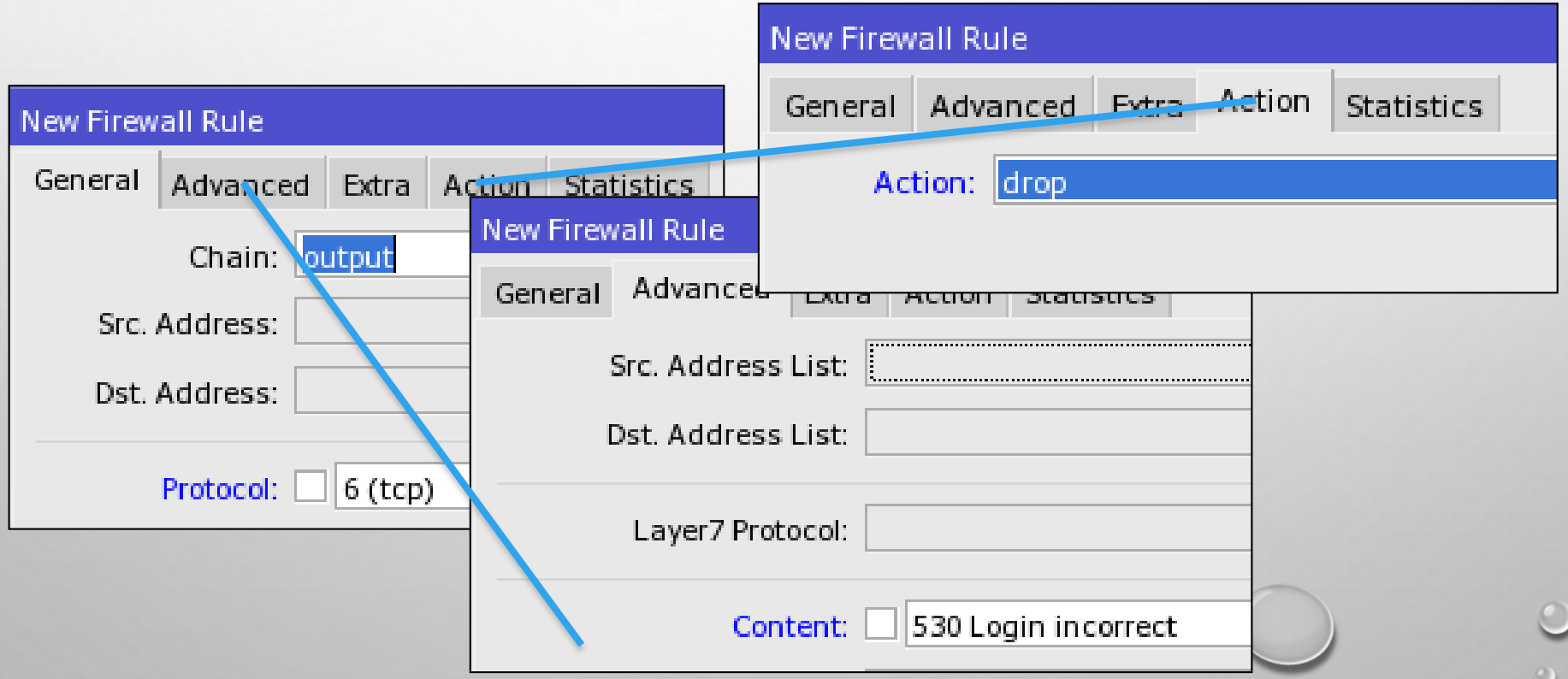
DESTINATION LIMIT

- ADD A RULE TO ACCEPT AN UNSUCCESSFUL ATTEMPT WITH 1 CONNECTION PER MINUTE (BURST IT TO 5 CONNECTION) BASED ON DESTINATION-ADDRESS



DESTINATION LIMIT

- ADD A RULE TO PUT A DESTINATION-ADDRESS THAT HAS MORE THAN 1 CONNECTION PER MINUTE (HAS BEEN KICKED-OUT FROM THE RULE BEFORE) INTO AN ADDRESS-LIST NAMED BLACKLIST



THANK YOU