



# IDS IMPLEMENTATION WITH MIKROTIK

BY: ANTONIUS DUTY SUSILO

MUM (MIKROTIK USER MEETING)

VIETNAM

2017

# PROFILE

- Antonius Duty Susilo
- Email [dutymlg@gmail.com](mailto: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](http://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 become 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](http://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](http://www.ypt.or.id))



# 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



The background features a light gray gradient with several realistic water droplets of varying sizes scattered in the corners. The droplets have highlights and shadows, giving them a three-dimensional appearance. The text is centered in the middle of the page.

# 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”

New Firewall Rule

General Advanced Extra Action Statistics

▼ Connection Limit

▲ Limit

Rate:  /

Burst:

▼ Dst. Limit

▼ Nth



# LIMIT (FOR PING-FLOOD)

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

The image shows a screenshot of the Mikrotik WinBox Firewall Rule configuration interface. The main window is titled "Firewall Rule <>" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "General" tab is active, showing the following fields:

- Chain: input
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol:  1 (icmp)

Below the "General" tab, the "Limit" section is expanded, showing the following settings:

- Connection Limit: (empty)
- Limit: (empty)
- Rate: 2 / sec
- Burst: 2

Two smaller, semi-transparent windows are overlaid on the main window. The top one is also titled "Firewall Rule <>" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "Action" tab is active, showing the "Action: accept" field. The bottom one is also titled "Firewall Rule <>" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "Action" tab is active, showing the "Action: accept" field. A blue arrow points from the "Action" tab of the top window to the "Action" tab of the bottom window.

# LIMIT (FOR PING-FLOOD)

- 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)

- TRY TO PING SEVERAL TIMES (MORE THAN 2)

#	Action	Chain	Protocol	In. Int...	Out. In...	Bytes	Packets
0	✓ acc...	input	1 (icmp)			22.8 KiB	278
1	✗ drop	input	1 (icmp)			10.0 KiB	122

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

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

- 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

+ - ✓ ✗ [Filter Icon] 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

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

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

Action: jump

Jump Target:

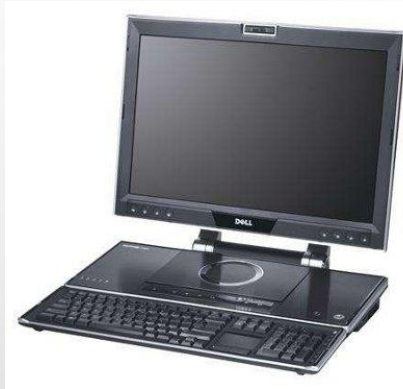
- forward
- icmp
- input
- output



# 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 1<sup>st</sup> attempt and 2<sup>nd</sup>, 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

The image shows two overlapping screenshots of the Mikrotik WinBox Firewall Rule configuration interface. The background window is the 'New Firewall Rule' dialog, with the 'General' tab selected. The 'Chain' is set to 'input'. The 'Protocol' is set to '6 (tcp)' and the 'Dst. Port' is set to '1234'. The 'Action' tab is highlighted with a blue arrow pointing to a second, smaller screenshot of the same dialog. This smaller screenshot shows the 'Action' tab selected, with the 'Action' set to 'add src to address list', the 'Address List' set to 'temporary', and the 'Timeout' set to '00:00:10'.

Field	Value
Chain	input
Src. Address	
Dst. Address	
Protocol	<input type="checkbox"/> 6 (tcp)
Src. Port	
Dst. Port	<input type="checkbox"/> 1234
Any. Port	

Field	Value
Action	add src to address list
Address List	temporary
Timeout	00:00:10

# PORT KNOCKING

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

The image displays three screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to configure a port knocking rule.

**Top-Left Screenshot (General Tab):**

- Chain: input
- Src. Address: [Empty]
- Dst. Address: [Empty]

**Bottom-Left Screenshot (Advanced Tab):**

- Protocol:  6 (tcp)
- Src. Port: [Empty]
- Dst. Port:  4321
- Any. Port: [Empty]

**Right Screenshot (Action Tab):**

- Action: add src to address list
- Address List: secured
- Timeout: 01:00:00

A blue arrow points from the Action tab of the top-left window to the Action tab of the right window, indicating the configuration flow.

# PORT KNOCKING

- ALLOW ACCESS FROM SRC-ADDRESS-LIST SECURED

The image displays three screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to create a rule for port knocking.

**Top Left Screenshot:** Shows the "New Firewall Rule" dialog box with the "General" tab selected. The "Chain" field is set to "input". The "Src. Address" and "Dst. Address" fields are empty.

**Top Right Screenshot:** Shows the "New Firewall Rule" dialog box with the "Action" tab selected. The "Action" field is set to "accept".

**Bottom Screenshot:** Shows the "New Firewall Rule" dialog box with the "Advanced" tab selected. The "Src. Address List" checkbox is checked, and the "secured" address list is selected. The "Dst. Address List" field is empty.

Blue arrows indicate the sequence of configuration steps: from the "Chain" field in the General tab to the "Action" field in the Action tab, and then to the "Src. Address List" field in the Advanced tab.

# PORT KNOCKING

- DROP ANOTHER TRAFFIC
- ALL THE RULE VIEW

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📄 🔍 Reset Counters 00 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

At the end, DROP ALL

C:\WINDOWS\system32\cmd.exe - p admin@00:0C:42:5E:5C:6A (46\_

```
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.
```

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
  -U, --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>
```



The image shows a Windows desktop environment with three overlapping windows:

- Top-left window:** A command prompt window titled "C:\WINDOWS\system32\cmd.exe - p" showing the output of a network test. It displays five "Request timed out." messages followed by five "Reply from 192.168.46.254: bytes=" messages.
- Bottom-left window:** A command prompt window titled "C:\WINDOWS\system32\cmd.exe" showing the help text for the 'knock' utility. The help text includes options: `--udp` (make all ports hits use), `--verbose` (be verbose), `--version` (display version), and `--help` (this help). An example command is shown: `knock myserver.example.com 123:tcp 45`. Below the help text, the user has entered `knock 192.168.46.254 1234` and `knock 192.168.46.254 4321`.
- Right window:** A Mikrotik WinBox window titled "admin@00:0C:42:5E:5C:6A (46\_H" showing the Firewall configuration page. The "Filter Rules" tab is selected. A table lists a rule named "secured" with address "192.168.46.1".

Name	Address
D secured	192.168.46.1

# PORT KNOCKING

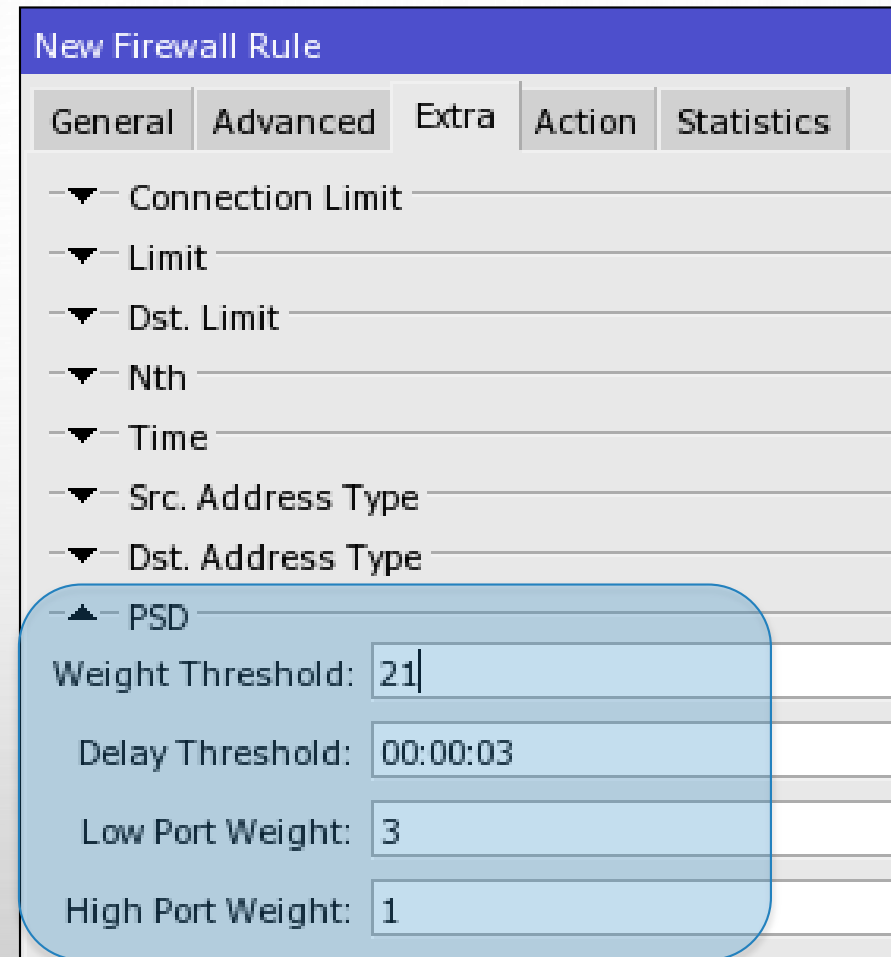
- TRY TO CHANGE THE PORT
- MAKE IT A SEQUENCE OF 3 PORTS OR MORE
  - USE TEMPORARY-X AS THE TEMPORARY LIST FOR MORE THAN 2 PORTS USED

# 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



The screenshot shows the 'New Firewall Rule' configuration window in Mikrotik WinBox. The 'Advanced' tab is selected, and the 'PSD' (Port Scan Detect) option is expanded. The settings for PSD are as follows:

Setting	Value
Weight Threshold	21
Delay Threshold	00:00:03
Low Port Weight	3
High Port Weight	1

# 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

The image displays three overlapping screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to create a rule that drops connections from a source address black-list.

**Top-Left Screenshot (New Firewall Rule - General Tab):** Shows the initial configuration with Chain: input, Src. Address, and Dst. Address fields.

**Top-Right Screenshot (New Firewall Rule - Action Tab):** Shows the Action tab where the Action is set to drop.

**Bottom Screenshot (Firewall Rule - Advanced Tab):** Shows the Advanced tab where the Src. Address List is set to black-list.

Blue arrows indicate the sequence of configuration steps: from the General tab to the Action tab, and then to the Advanced tab.

# PORT SCAN DETECT

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol:  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

New Firewall Rule

General Advanced Extra Action

Connection Limit

Weight Threshold: 21

Delay Threshold: 00:00:03

Low Port Weight: 3

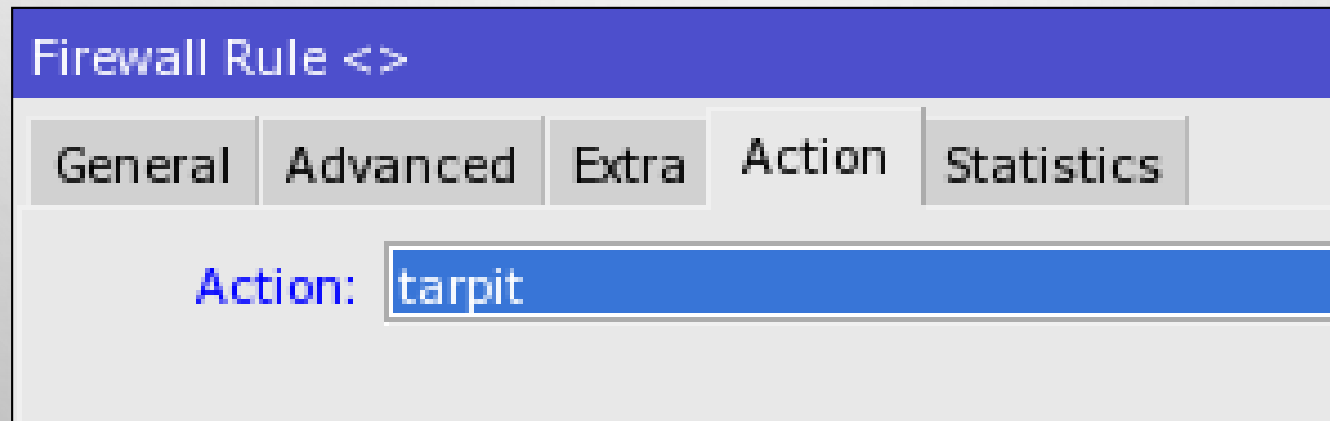
High Port Weight: 1

Hotspot

IP Fragment

# 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

**New Firewall Rule**

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

Chain: input

Src. Address:

Dst. Address:

Protocol:  6 (tcp)

Src. Port:

**New Firewall Rule**

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

Action: add src to address list

Address List: black-list

Timeout: 01:00:00

**New Firewall Rule**

General | Advanced | **Extra** | Action | Statist

▲ Connection Limit

Limit:  8

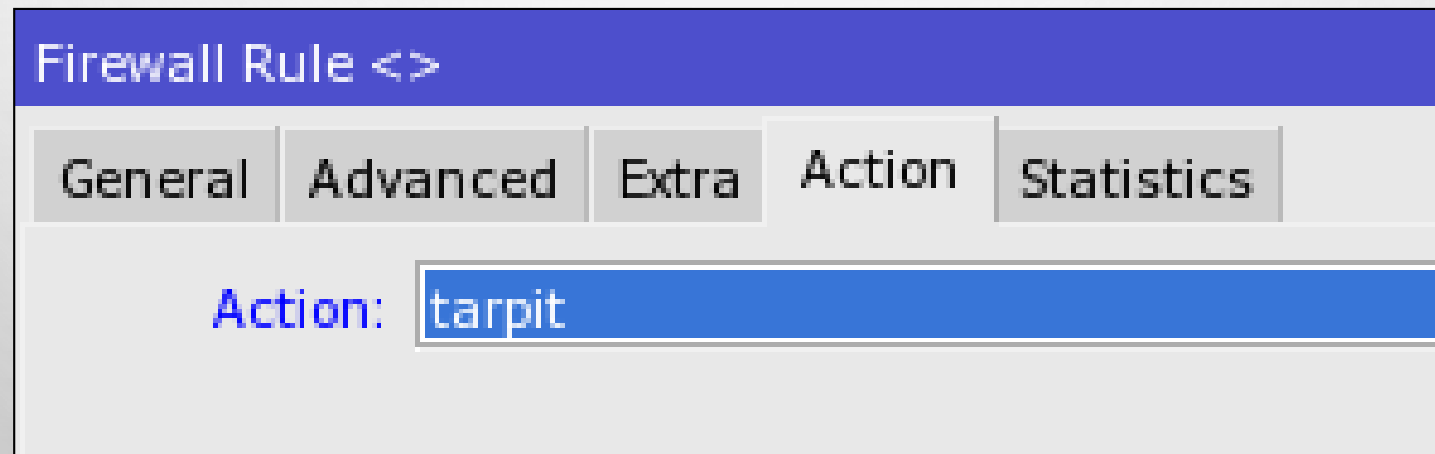
Netmask: 32

▼ Limit

▼ Dst. Limit

# 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

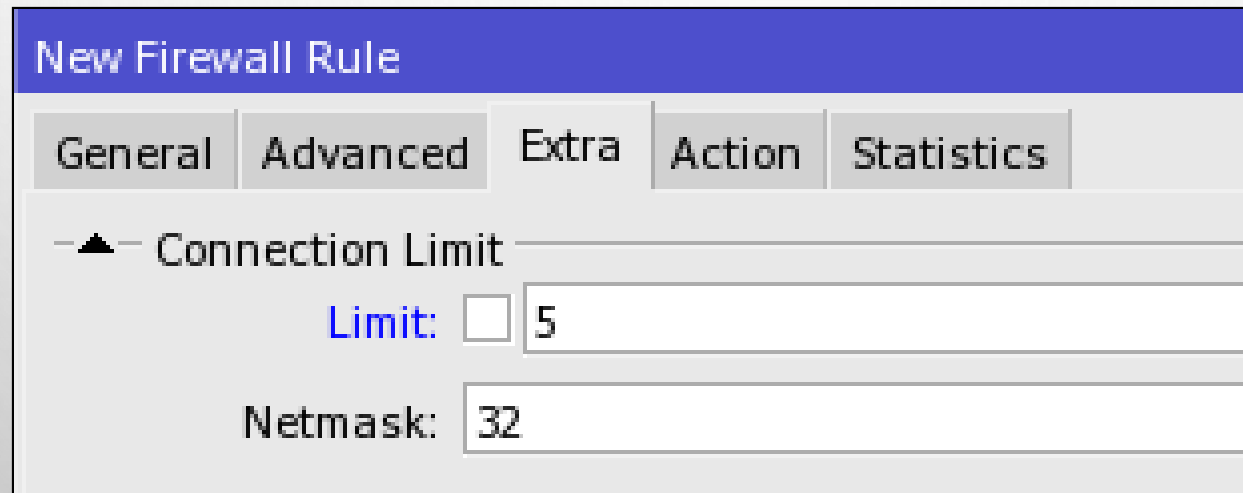


# CONNECTION LIMIT

- 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



The screenshot shows a configuration window titled "New Firewall Rule" with a blue header. Below the header are five tabs: "General", "Advanced", "Extra", "Action", and "Statistics". The "Advanced" tab is selected. Under the "Advanced" tab, there is a section for "Connection Limit" with a small upward-pointing triangle icon to its left. This section contains two input fields: "Limit:" with a value of "5" and "Netmask:" with a value of "32".

# 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

The image displays three overlapping windows from Mikrotik WinBox illustrating the configuration of a firewall rule to tarpit connections from a black-listed source address.

- New Firewall Rule (Top Left):** Shows the 'Advanced' tab selected. The 'Chain' is set to 'input'. The 'Src. Address' and 'Dst. Address' fields are empty.
- Firewall Rule <> (Top Right):** Shows the 'Action' tab selected. The 'Action' is set to 'tarpit'.
- Firewall Rule <> (Bottom):** Shows the 'Advanced' tab selected. The 'Src. Address List' checkbox is checked, and the list is named 'black-list'. The 'Dst. Address List' field is empty.

Blue arrows indicate the flow of configuration: from the 'Advanced' tab in the 'New Firewall Rule' window to the 'Advanced' tab in the 'Firewall Rule <>' window, and from the 'Action' tab in the 'New Firewall Rule' window to the 'Action' tab in the 'Firewall Rule <>' window.

# 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

The image displays three overlapping screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to create a connection limit rule.

**Top-Left Screenshot (General Tab):** Shows the 'Chain' field set to 'input'. The 'Src. Address' and 'Dst. Address' fields are empty.

**Top-Right Screenshot (Action Tab):** Shows the 'Action' field set to 'add src to address list', the 'Address List' field set to 'black-list', and the 'Timeout' field set to '01:00:00'.

**Bottom Screenshot (Extra Tab):** Shows the 'Connection Limit' section expanded, with the 'Limit' field set to '5' and the 'Netmask' field set to '32'.

# 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

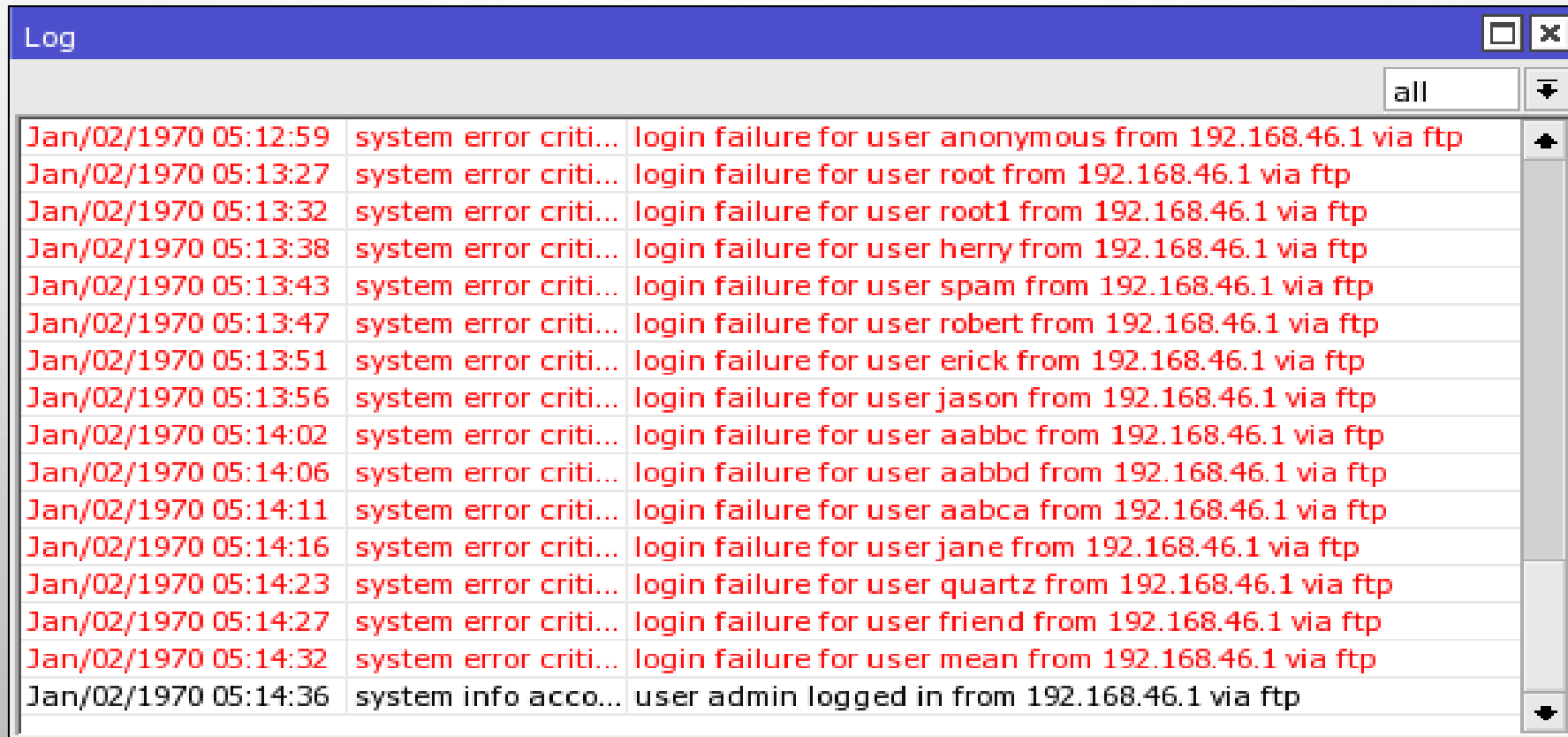
# DDOS ATTACKS

- 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

Connection Tracking	
TCP Syn Sent Timeout:	<input type="text" value="00:00:05"/>
TCP Syn Received Timeout:	<input type="text" value="00:00:05"/>
TCP Established Timeout:	<input type="text" value="1d 00:00:00"/>
TCP Fin Wait Timeout:	<input type="text" value="00:00:10"/>
TCP Close Wait Timeout:	<input type="text" value="00:00:10"/>
TCP Last Ack Timeout:	<input type="text" value="00:00:10"/>
TCP Time Wait:	<input type="text" value="00:00:10"/>
TCP Close:	<input type="text" value="00:00:10"/>
UDP Timeout:	<input type="text" value="00:00:10"/>
UDP Stream Timeout:	<input type="text" value="00:03:00"/>
ICMP Timeout:	<input type="text" value="00:00:10"/>
Generic Timeout:	<input type="text" value="00:10:00"/>

# 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

The image displays three screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to configure a destination limit rule.

**Top-Left Screenshot (General Tab):**

- Chain:
- Src. Address:
- Dst. Address:
- Protocol:  6 (tcp)

**Bottom-Left Screenshot (General Tab):**

- Content:  530 Login incorrect

**Right Screenshot (Advanced Tab):**

- Connection Limit:
- Limit:  /
- Burst:
- Limit By:
- Expire:

# 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

The image shows a screenshot of the Mikrotik WinBox Firewall Rule configuration interface. The main window is titled "New Firewall Rule" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "Advanced" tab is selected. The "Chain" field is set to "output". The "Src. Address:" and "Dst. Address:" fields are empty. The "Protocol:" field is set to "6 (tcp)". A blue arrow points from the "Advanced" tab in the main window to the "Advanced" tab in a smaller, overlapping window. This smaller window also has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "Action:" field is set to "drop". The "Content:" field is set to "530 Login incorrect". The "Src. Address List:" and "Dst. Address List:" fields are empty. The "Layer7 Protocol:" field is empty.

The image features a light gray gradient background with several realistic water droplets of various sizes scattered in the corners. The droplets have highlights and shadows, giving them a three-dimensional appearance. In the center of the page, the words "THANK YOU" are written in a bold, black, sans-serif font.

**THANK YOU**