# IMPLEMENTING
# NETWORK SECURITY

with MikroTik RouterOS

# IP FIREWALL

## ADVANCED and EXTRA CONDITIONS


@uxville tycoonux

+639175910742

uxville.unabia@inquirinity.com


# UXVILLE G. UNABIA


*Inquirinity Corporation - Philippines*


MikroTik Certified Trainer

MikroTik Academy Coordinator

MikroTik Academy Trainer

MTCNA | MTCRE | MTCUME | MTCTCE | MTCWE

CCSI | CCNP | CCNA | MCT | MCSA | FCT | NSE4
UBWS | HCDA | CSSA | PCE | VMTSP

INQUIRINITY CORPORATION

Davao City, Philippines

ICT certification-based training center

MikroTik Academy – Inquirinity Computer Academy

Reseller of ICT products – MikroTik & others

Partnered for a start-up WISP

System and Network consultation

# OBJECTIVES

- To list built-in MikroTik IP Firewall capabilities in implementing network security
- A primer on MTCTCE certification
- To look beyond network connectivity - build and maintain secure networks

# NEED FOR GRANULAR POLICIES

## IP FIREWALL

General conditions form the basic firewall rules and are certainly significant however will be inefficient or at worst inapplicable on scenarios that would need to consider non-contiguous networks, unknown ports, content, time, connection rate - just to name a few

# ADVANCED CONDITIONS

## IP FIREWALL

- Src. Address List
- Dst. Address List
- Layer 7 protocol
- Content
- Connection Bytes
- Connection Rate
- Packet size
- TCP Flags
- ICMP Options

# SRC/DST ADDRESS LIST

## ADVANCED CONDITIONS

Allow or block multiple non-contiguous IP address or networks without using multiple firewall rules

Addresses could be entered statically or acquired dynamically and either remain in disk permanently or removed after a specific timeout

# SRC/DST ADDRESS LIST
## ADVANCED CONDITIONS

**Network Security Use Cases:**

- BOGON filtering
- Port Knocking
- Whitelisting
- Blacklisting

# LAYER 7 PROTOCOL

## ADVANCED CONDITIONS

L7 matcher collects the first 10 packets of a connection or the first 2KB of a connection and searches for the pattern in the collected data.

L7 matcher is very resource intensive and can’t identify protocols in SSL tunnels

# LAYER 7 PROTOCOL

## ADVANCED CONDITIONS

**Network Security Use Cases:**

- File type filtering
- Malware patterns

Check for some Made for MikroTik solutions/plugins

# TLS-HOST

## ADVANCED CONDITIONS

"Allows to match HTTPS traffic based on TLS SNI hostname. Accepts GLOB syntax for wildcard matching.

Matcher will not be able to match hostname if TLS handshake frame is fragmented into multiple TCP segments (packets)"

# TLS-HOST

## ADVANCED CONDITIONS

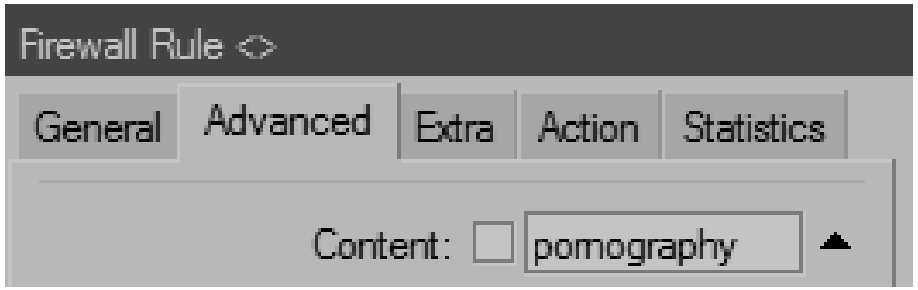
**Network Security Use Cases:**

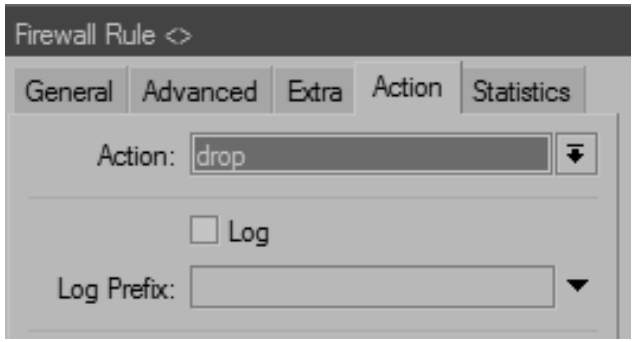
- Block HTTPS (malicious) websites

# CONTENT

## ADVANCED CONDITIONS

Match packets that contain specified text




Will not work on encrypted or fragmented packet

# CONTENT

## ADVANCED CONDITIONS

**Network Security Use Cases:**

- Will form part as a solution in dealing with Brute Force attacks

# CONNECTION BYTES

## ADVANCED CONDITIONS

Matches packets if only a given amount of bytes has been transferred through the particular connection – upload and download

# CONNECTION RATE

## ADVANCED CONDITIONS

"A firewall matcher that allows to capture traffic based on present speed of the connection.

Works only with TCP and UDP traffic. You need to specify protocol to activate these options"

# CONNECTION BYTES/RATE

## ADVANCED CONDITIONS

**Network Security Use Cases:**

- Although implementation is more towards traffic prioritization, it could be a significant part of establishing baselines, it turn forms basis for any network monitoring activities

# PACKET SIZE

## ADVANCED CONDITIONS

Matches packets of specified size or size range in bytes

Integer value from 0 to 65535

# PACKET SIZE
## ADVANCED CONDITIONS

**Network Security Use Cases:**

- Prevent ICMP Attacks – ICMP tunnelling (injecting arbitrary data into an echo packet)

# TCP FLAGS

## ADVANCED CONDITIONS

Matches specified TCP flags

- ack - acknowledging data
- cwr - congestion window reduced
- ece - ECN-echo flag
- fin - close conneciton
- psh - push function

# TCP FLAGS

## ADVANCED CONDITIONS

Matches specified TCP flags

- rst - drop connection
- syn - new connection
- urg - urgent data

# TCP FLAGS

## ADVANCED CONDITIONS

**Network Security Use Cases:**

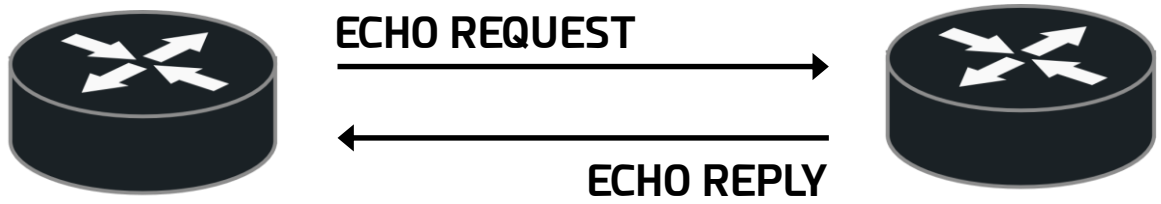
- Various combinations of TCP flags can indicated port scanner activity

# ICMP OPTIONS

## ADVANCED CONDITIONS

Matches ICMP **type:code** fields

- Type 0 - Echo reply
- Type 3 - Destination Unreachable
- Type 8 - Echo
- Type 11 - Time Exceeded



# ICMP OPTIONS

## ADVANCED CONDITIONS

Matches ICMP **type:code** fields

- Code 0 - Echo reply
- Code 3 - Destination Unreachable
- Code 4 - Source Quench

# ICMP OPTIONS
## ADVANCED CONDITIONS

**Network Security Use Cases:**

- Allow typical ICMP messages

  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

# EXTRA CONDITIONS

## IP FIREWALL

Connection Limit

Limit

Dst. Limit

Time

Src/Dst address type

PSD

# CONNECTION LIMIT

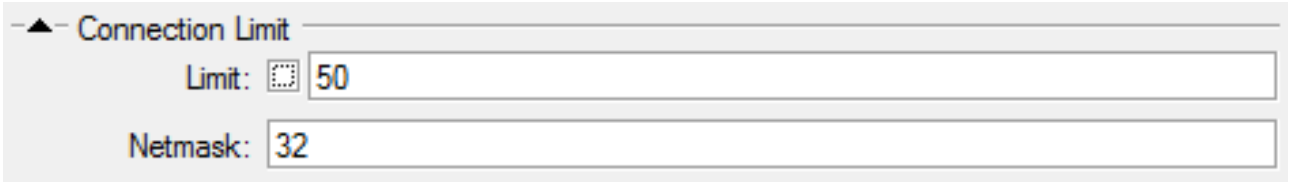
## EXTRA CONDITIONS

"Matches connections per address or address block up to and including the given value

Should be used together with connection-state=new and/or with tcp-flags=syn because this matcher is very resource intensive"

# CONNECTION LIMIT

## EXTRA CONDITIONS




Match until the connection limit of 50 is reached per /32 IP address of network in the src-address

# LIMIT

## EXTRA CONDITIONS

Matches packets up to a limited rate

Rule using this matcher will match until this limit is reached.

Parameters are the following:

| | |
|---|---|
| Rate | Burst |
| Time | Mode |

# LIMIT

## EXTRA CONDITIONS


Match until an average rate of 100 packets per minute is reached, not counting the 5 burst packets

# DST-LIMIT

## EXTRA CONDITIONS

Matches packets until a given rate is exceeded. Rate is defined as packets per time interval.

As opposed to the limit matcher, every flow has it's own limit.

Flow is defined by mode parameter

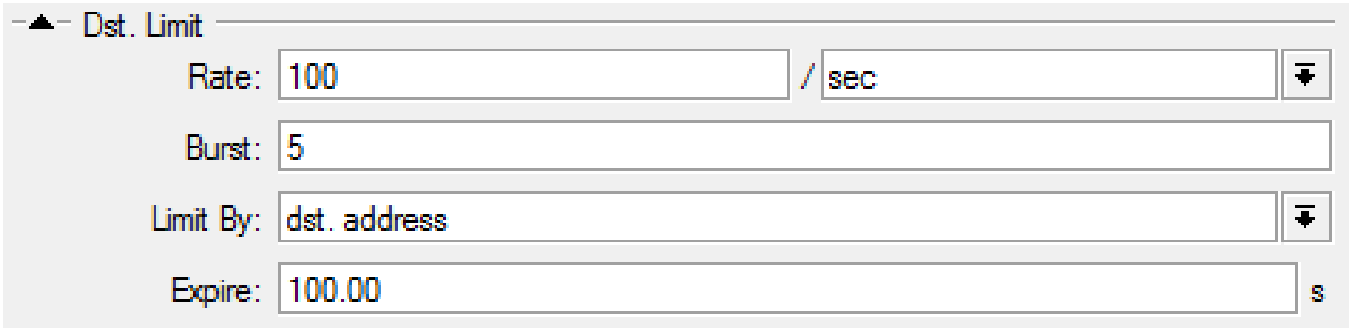
# DST-LIMIT
## EXTRA CONDITIONS

Parameters are the following:

- Rate
- Time
- Burst
- Limit By
- Expire

# DST-LIMIT

## EXTRA CONDITIONS




For every flow by dst. address, match until an average rate of 100 packets per second is reached, not counting the 5 burst packets.

For every 100 seconds, flow with no packets will be allowed to be deleted

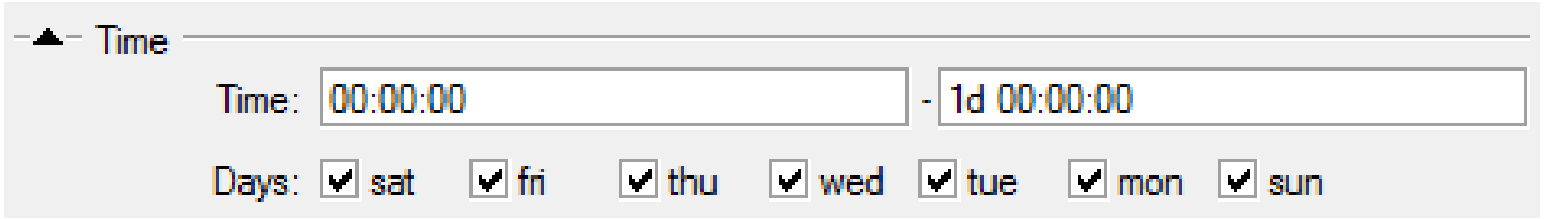
# CONNECTION LIMIT / LIMIT / DST-LIMIT

## EXTRA CONDITIONS

**Network Security Use Cases:**

- DDoS Detection and Blocking
- Dealing with Brute Force attacks

# TIME
## EXTRA CONDITIONS




Allows to create a filter based on the packets arrival time and date or for locally generated packets, departure time and date

# TIME

## EXTRA CONDITIONS

**Network Security Use Cases:**

- Time-based access rules

# SRC/DST ADDRESS TYPE

## EXTRA CONDITIONS


Matches the source/destination address type

| | |
|---|---|
| **unicast** | IP address used for point to point transmission |
| **local** | IP address assigned to one of router's interfaces |
| **broadcast** | Packet is sent to all devices in subnet |
| **multicast** | Packet is forward to defined group of devices |

# SRC/DST ADDRESS TYPE
## EXTRA CONDITIONS

**Network Security Use Cases:**

- DDoS attacks use the special broadcast address – Block any packets (outside your network) directed to the broadcast address and Block outgoing packets (from your network) destined for the broadcast address

# PSD
## EXTRA CONDITIONS


**WeightThreshold** Total weight of the latest TCP/UDP scans

**DelayThreshold** Delay for the packets with different destination ports coming from the same host to be treated as possible port scan sequence

**LowPortWeight** Weight of the packets with privileged (<=1024) destination port

**HighPortWeight** Weight of the packet with non-privileged destination port

# PSD

## EXTRA CONDITIONS

**Network Security Use Cases:**

- Drop Port Scanners

Implement PSD in the input chain (to protect from) and forward chain (local port scanners)

# NOTABLE MUM PRESENTATIONS

**Layer 7 Protocol**

https://mum.mikrotik.com//presentations/US18/presentation_5365_1524221989.pdf

**TLS-HOST**

https://mum.mikrotik.com/presentations/CR18/presentation_5701_1532535774.pdf

# NOTABLE MUM PRESENTATIONS

**Brute Force – Content, Address List**

https://mum.mikrotik.com//presentations/ID16/presentation_3549_1476685233.pdf

**IDS – Limit, Port Knocking, PSD**

https://mum.mikrotik.com/presentations/ID18/presentation_5640_1540365379.pdf

# NOTABLE MUM PRESENTATIONS

**DoS – TCP Flags, Connection-Limit**

https://mum.mikrotik.com//presentations/CY15/Denial_of_Service_Attack.pdf

IMPLEMENTING
NETWORK SECURITY
WITH **MIKROTIK** ROUTEROS
IP FIREWALL ADVANCED
AND EXTRA CONDITIONS

## Resources:

https://wiki.mikrotik.com

https://mum.mikrotik.com

https://forum.mikrotik.com

IMPLEMENTING
NETWORK SECURITY
WITH **MIKROTIK** ROUTEROS
IP FIREWALL ADVANCED
AND EXTRA CONDITIONS

# THANK **YOU**