

Firewall Learning Mode (FLM)

Christoph Strauss - 2021-04-27 - HiSecOS

This lesson describes how to use the Firewall Learning Mode on HiSecOS devices as of v04.0.00

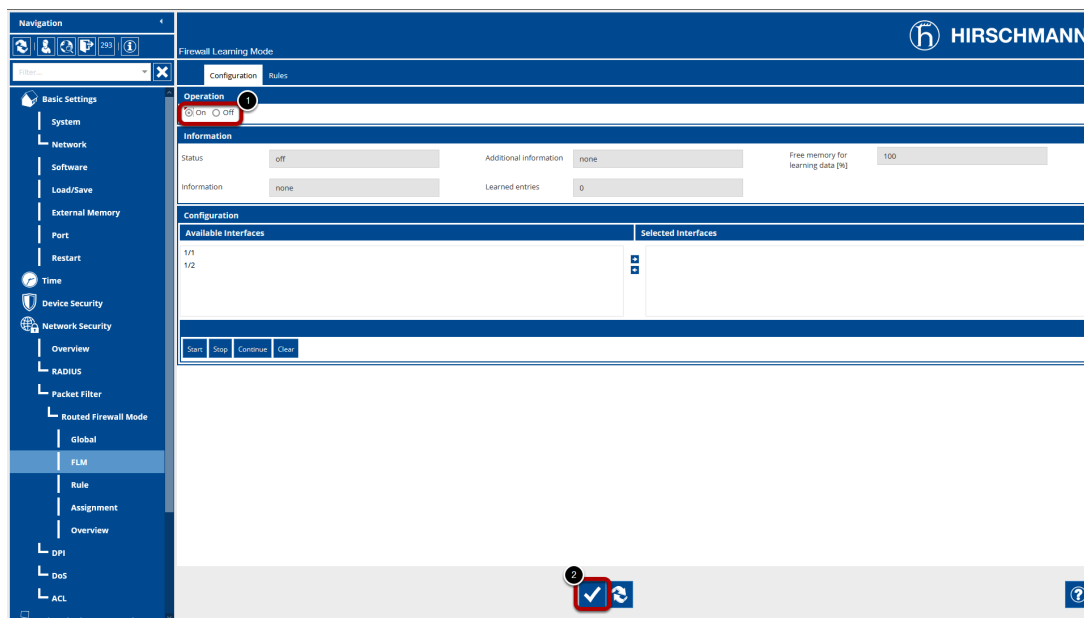
Limitations:

- Router Interfaces only (L3 FW)
- Max. 4 Interfaces selectable (min. 2)

Prerequisites:

- EAGLE operates in router mode
- Two or more router interfaces on physical or logical interfaces are configured

Enable FLM



Navigate to the FLM dialog (Network Security - Packet Filter - Routed Firewall Mode - FLM)

1. Set in the Operation frame the radio button to 'On'
2. Click the set button at the bottom of the page to write the change to the device

Select Interfaces

Firewall Learning Mode

Configuration Rules

Operation

On Off

Information

Status off Additional information none Free memory for learning data [%] 100

Information none Learned entries 0

Configuration

Available Interfaces

1/1

1

2

Add Selected

Start Stop Continue Clear

✓ ↺ ?

Select at least two interfaces from the available interfaces by highlighting them and press the arrow key to the right.

1. Highlight entries of the available interfaces (you can use SHIFT or CTRL key to select multiple)
2. Press the arrow key to move the interfaces in the selected column

Start Learning

Firewall Learning Mode

Configuration Rules

Operation

On Off

Information

Status learning Additional information none Free memory for learning data [%] 100

Information normal Learned entries 0

Configuration

Available Interfaces

Selected Interfaces

1/1

1/2

Start Stop Continue Clear

Press the 'Start' button to start the learning phase.

The status will change to learning.

Generate some traffic over the firewall and reload the page.

The learned entries counter will increase.

Stop Learning

Firewall Learning Mode

Configuration Rules

Operation

On Off

Information

Status: stopped-data-present Additional information: none Free memory for learning data [%]: 100

Information: normal Learned entries: 5

Configuration

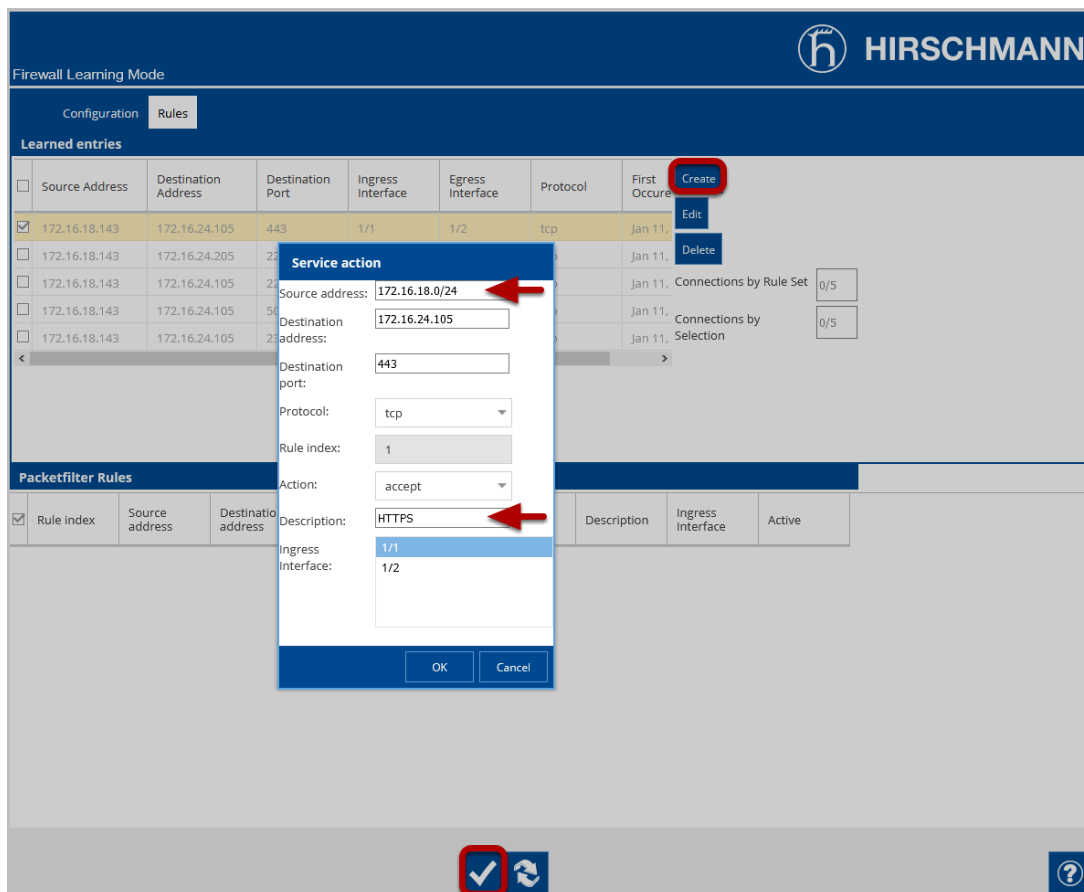
Available Interfaces Selected Interfaces

1/1
1/2

Start Stop Continue Clear

1. Reload the page and check the 'learned entries' counter
2. Stop the learning by pressing the 'Stop' button - the status will change to 'stopped-data-present'
3. Change to the rules tab to review the learned firewall rules

FLM - Rules Tab



On the FLM Rules Tab you see the learned entries as well as the configured packet filter rules.

Highlight one of the learned entries and click the 'Create' button on the right to create a filter rule.

In the pop-up window you can modify the rule and add a description before creating the rule.

Repeat these steps until all wanted traffic is covered by a rule then click the write button at the bottom of the page.

Packet Filter Rules

Packet Filter Rule												
Rule index	Description	Source address	Destination address	Protocol	Source port	Destination port	Parameters	Action	Log	Trap	DPI profile index	Active
1	HTTPS [FLM]	172.16.18.0/24	172.16.24.105	tcp	any	443	none	accept	☐	☐	0	☒
2	SSH [FLM]	172.16.18.143	172.16.24.0/24	tcp	any	22	none	accept	☐	☐	0	☒
3	TELNET [FLM]	172.16.18.143	172.16.24.0/24	tcp	any	23	none	accept	☐	☐	0	☒
4	MODBUS [FLM]	172.16.18.143	172.16.24.105	tcp	any	502	none	accept	☐	☐	0	☒

Navigate to Network Security - Packet Filter - Routed Firewall Mode - Rules to check the created rules.

As you can see the rules are already activated.

Packet Filter Assignment

Packet Filter Assignment												
Information												
Assignments 4												
Uncommitted changes present												
Description	Rule index	Interface	Direction	Priority	Active							
HTTPS [FLM]	1	1/1	ingress	1	☒							
SSH [FLM]	2	1/1	ingress	1	☒							
TELNET [FLM]	3	1/1	ingress	1	☒							
☒ MODBUS [FLM]	4	1/1	ingress	1	☒							

Navigate to Network Security - Packet Filter - Routed Firewall Mode - Assignment to check the interface assignment of the rules.

The FLM created rules needs to be set active in the interface assignment.

1. Check the Active flag for each entry
2. Click the write button
3. Uncommitted changes are present
4. Click on the little arrow next to the "hamburger" button and select 'Commit'

Note: Commit changes will activate the configured packet filter rules and flush the firewall state table. Existing connections needs to be re-established.