

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

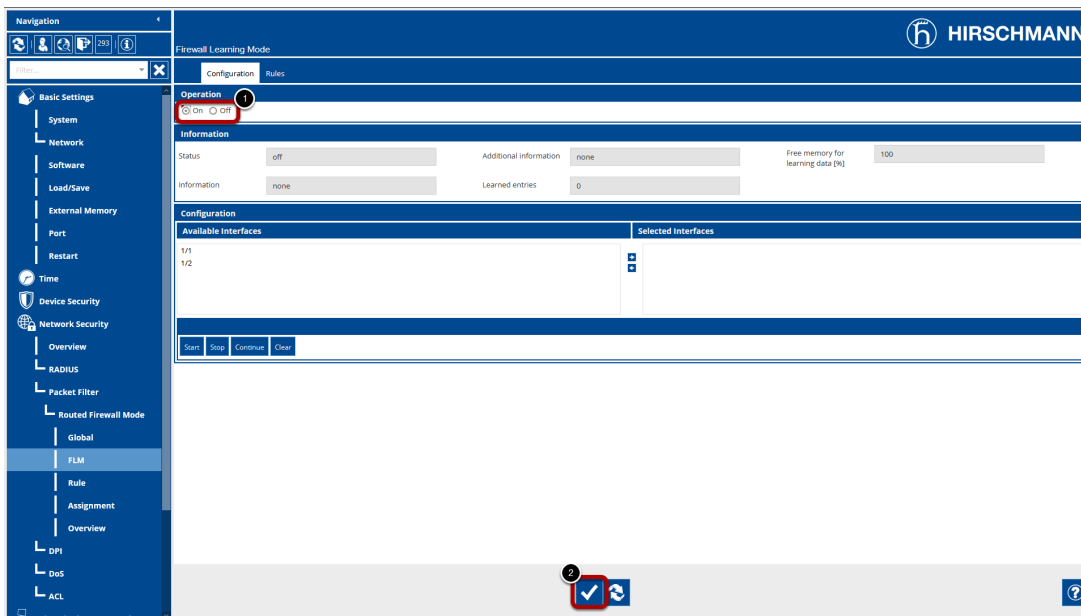
Limitations:

- 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

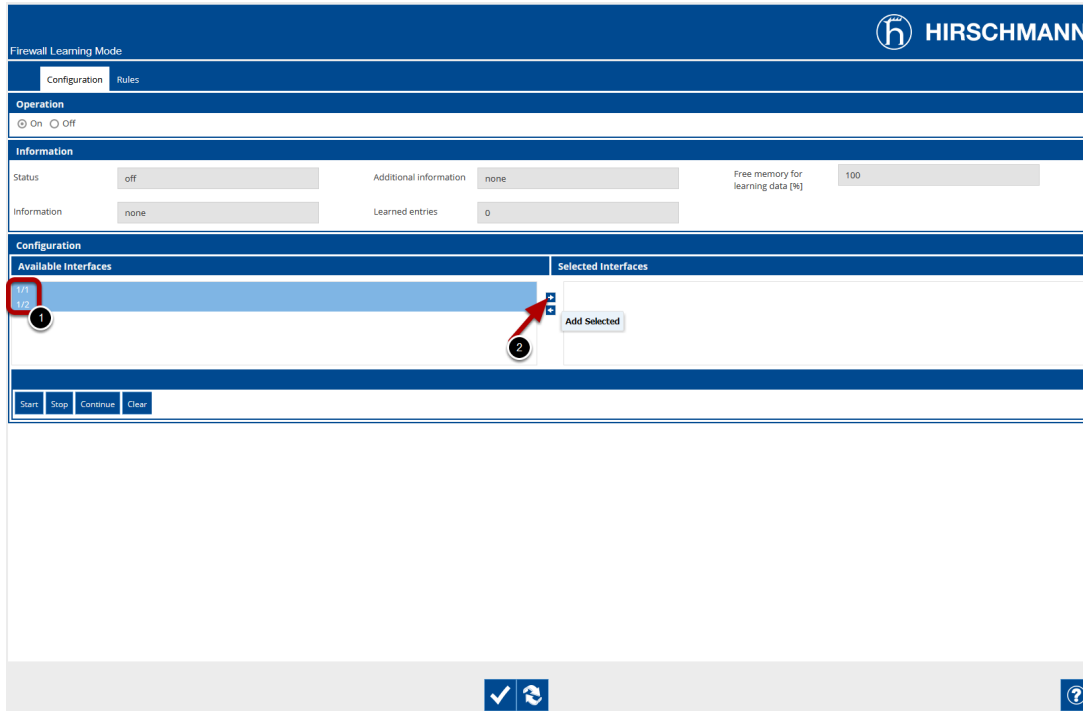
Enable FLM



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

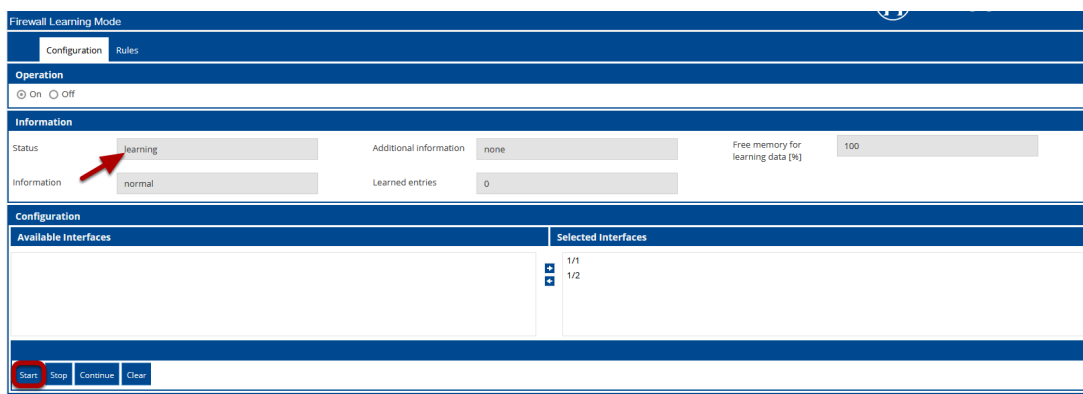
Select Interfaces



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



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

The screenshot shows the Hirschmann Firewall Learning Mode (FLM) interface. The top navigation bar has 'Configuration' and 'Rules' tabs, with 'Rules' selected. The 'Operation' section has 'On' selected. The 'Information' section shows 'Status: stopped-data-present', 'Additional information: none', 'Free memory for learning data [%]: 100', 'Information: normal', and 'Learned entries: 5'. The 'Configuration' section shows 'Available Interfaces' and 'Selected Interfaces'. The 'Stop' button is circled in red, and a red arrow points to the 'Learned entries' counter.

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

The screenshot shows the Hirschmann Firewall Learning Mode interface. At the top, there is a 'Configuration' tab with a sub-tab for 'Rules'. Below this, there are two main sections: 'Learned entries' and 'Packetfilter Rules'. The 'Learned entries' section contains a table with columns for Source Address, Destination Address, Destination Port, Ingress Interface, Egress Interface, Protocol, and First Occurrence. A 'Create' button is circled in red in the top right of this section. A 'Service action' dialog box is open, showing fields for Source address (172.16.18.0/24), Destination address (172.16.24.105), Destination port (443), Protocol (tcp), Rule index (1), Action (accept), and Description (HTTPS). A 'Create' button is also visible in the top right of the dialog box. At the bottom of the interface, there is a 'Write' button (a checkmark in a red box) and a 'Refresh' button (a circular arrow icon).

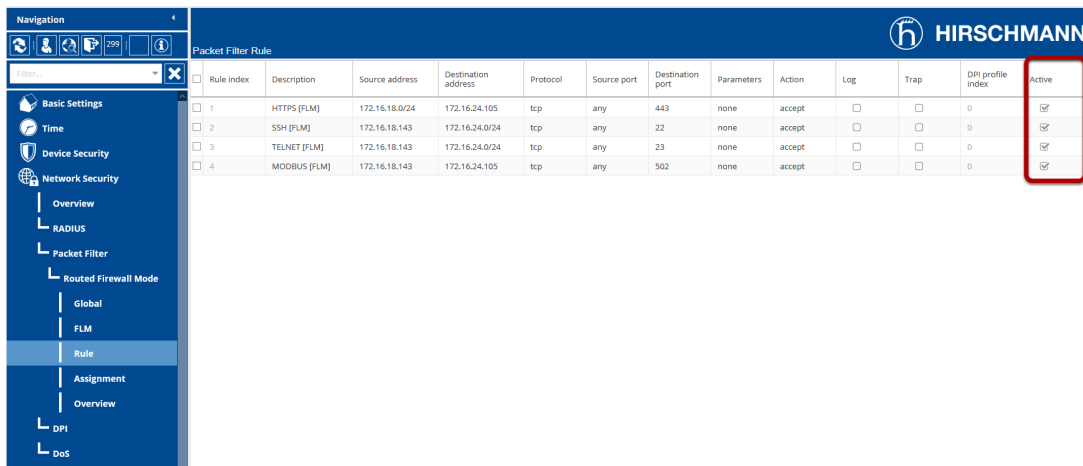
On the FLM Rules Tab you see the learned entries as well as the configured packet filter rules.

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.

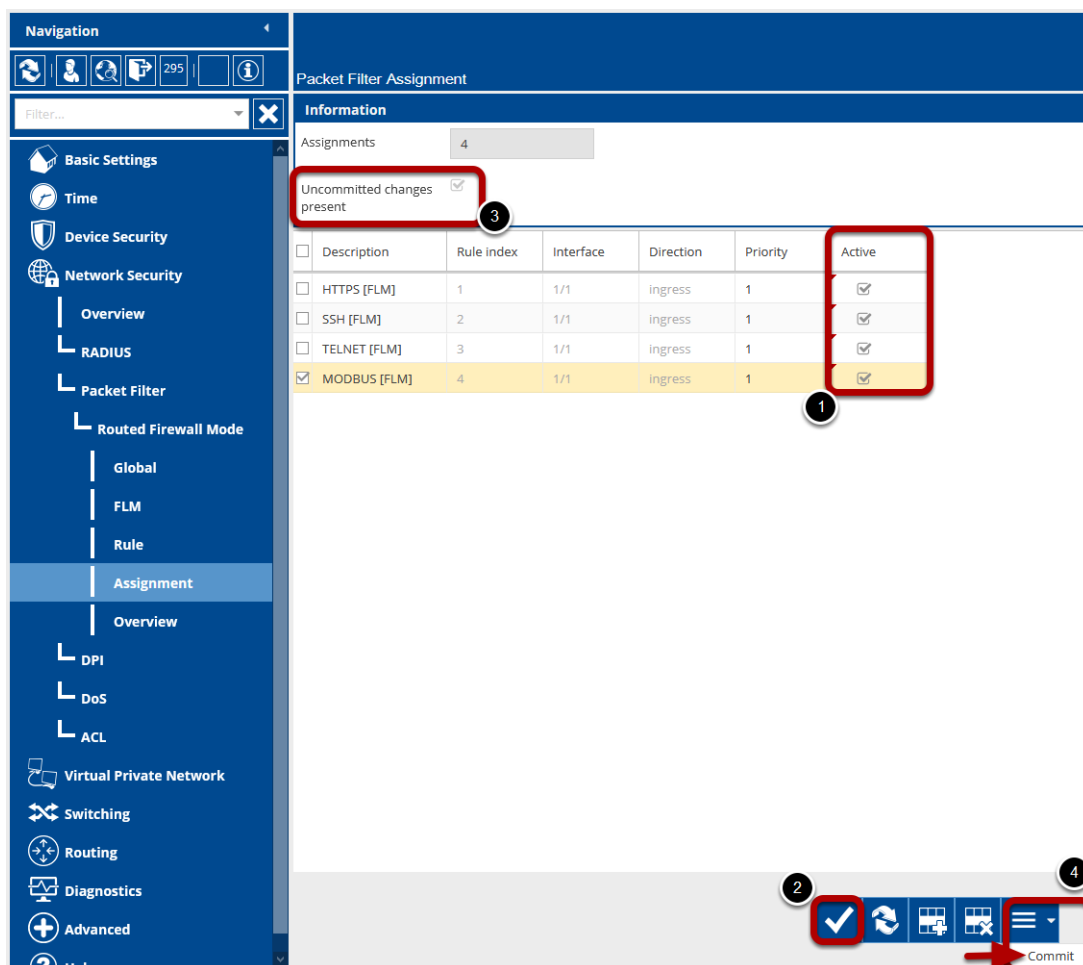
Packet Filter Rules



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



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.