

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

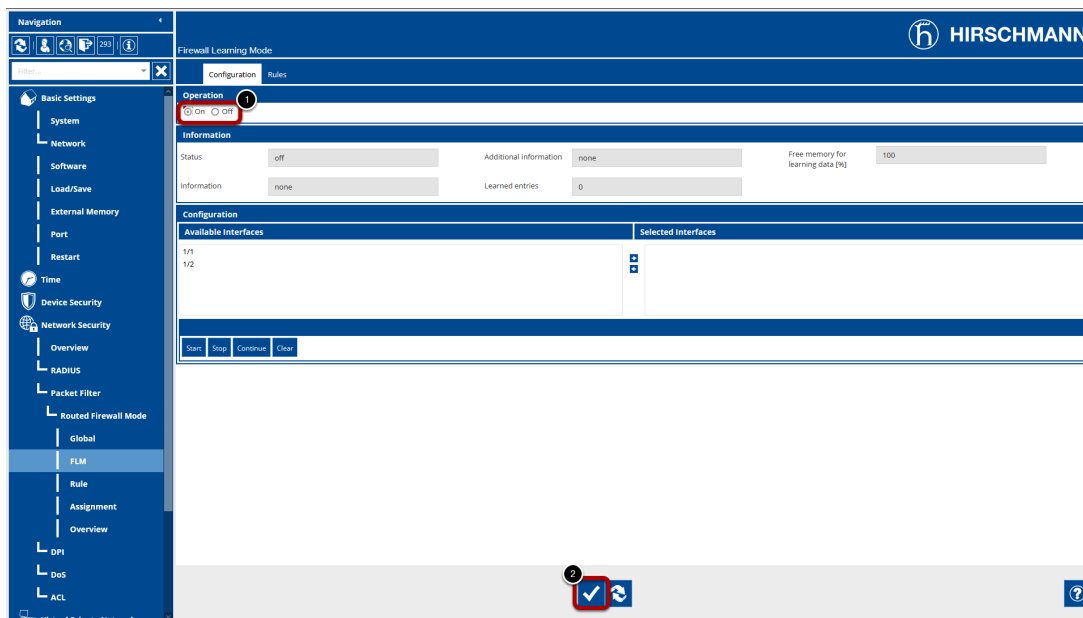
Limitations:

- 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

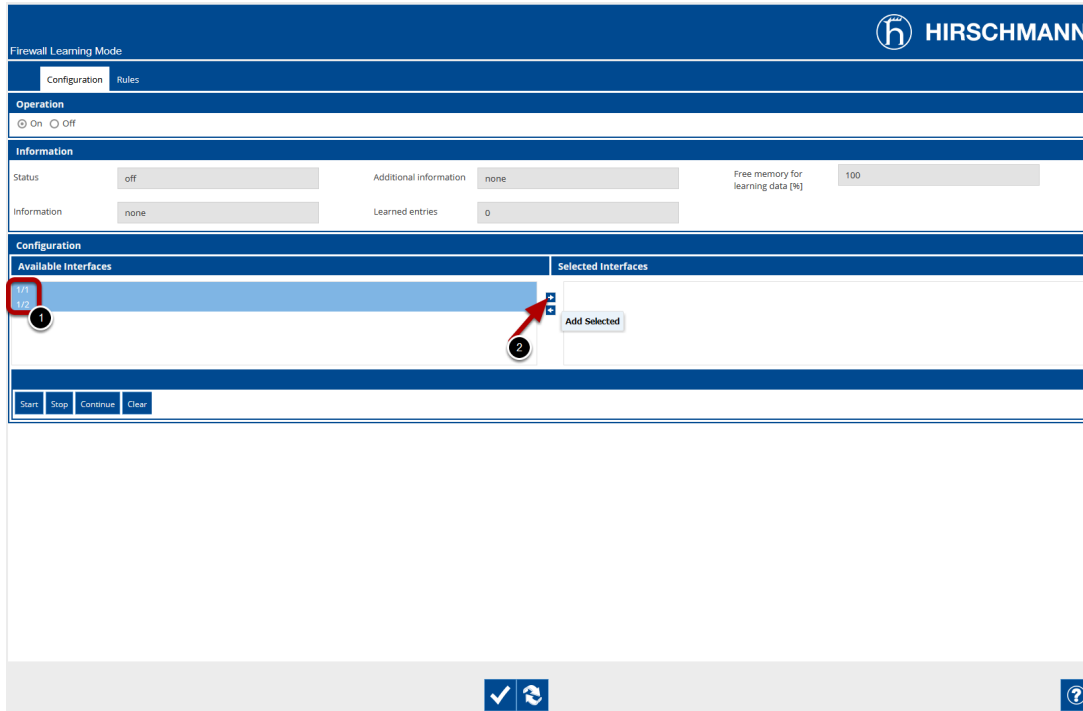
Enable FLM



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

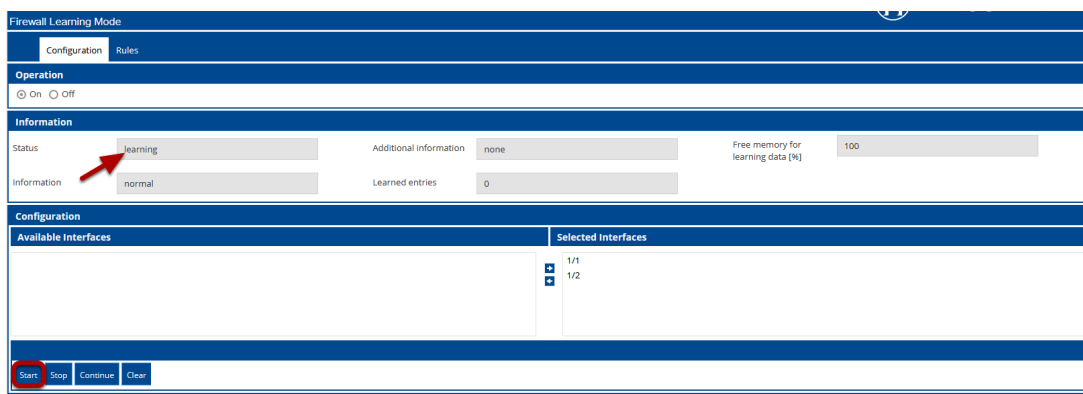
Select Interfaces



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 bar displays the Hirschmann logo and the text "HIRSCHMANN". Below this, the "Firewall Learning Mode" section contains two tabs: "Configuration" and "Rules". The "Rules" tab is selected and circled in red. A red arrow points from the "Rules" tab to the "Learned entries" counter in the "Information" section, which shows a value of 5. Another red arrow points from the "Learned entries" counter to the "Stop" button in the "Configuration" section, which is also circled in red. A third red arrow points from the "Stop" button to the "On" radio button in the "Operation" section. The "Information" section shows the status as "stopped-data-present", "Additional information" as "none", and "Free memory for learning data [%]" as "100". The "Configuration" section shows "Available Interfaces" and "Selected Interfaces". The "Selected Interfaces" section shows two interfaces: "1/1" and "1/2".

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 and a 'Rules' sub-tab. 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 above the table. One entry is selected, and a 'Service action' dialog box is open over it. This dialog box has 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), Description (HTTPS), and Ingress interface (1/2). Red arrows point to the source address and description fields. At the bottom of the dialog are 'OK' and 'Cancel' buttons. Below the 'Learned entries' table is the 'Packetfilter Rules' section, which has a table with columns for Rule index, Source address, Destination address, Description, Ingress Interface, and Active. 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).

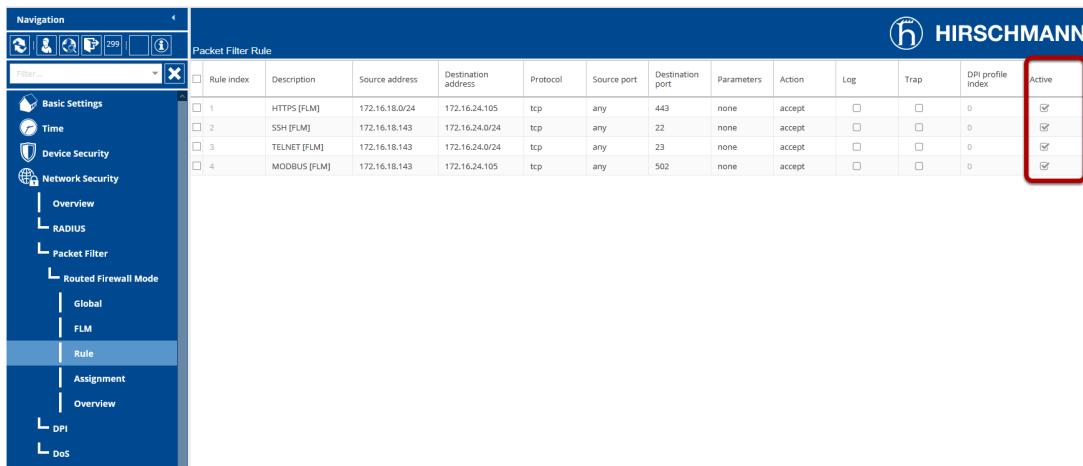
On the FLM Rules Tab you see the learned entries as well as the configured packet filter rules.

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.

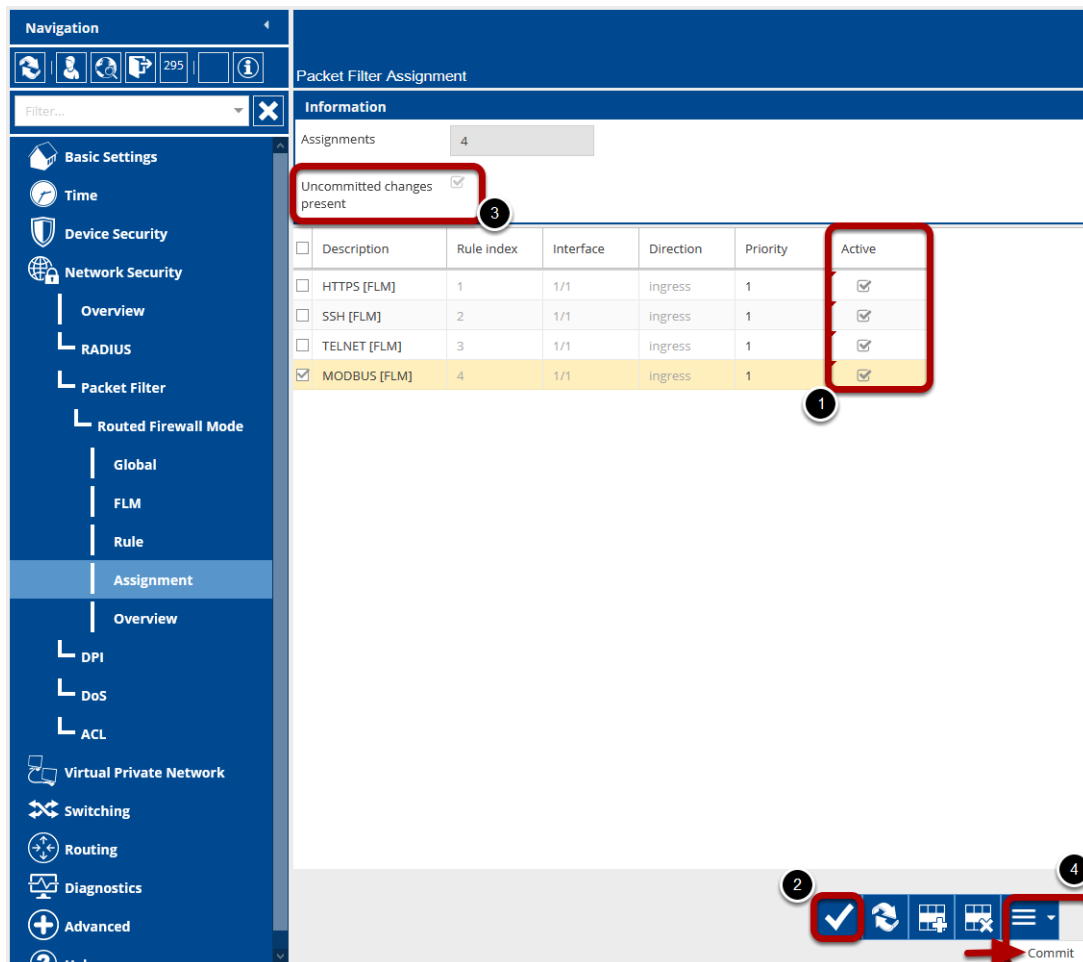
Packet Filter Rules



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.