

Firewall Learning Mode (FLM)

Christoph Strauss - 2021-04-27 - HiSecOS

In dieser Lektion wird beschrieben, wie Sie den Firewall-Learning-Mode auf HiSecOS-Geräten ab Version 04.0.00 verwenden

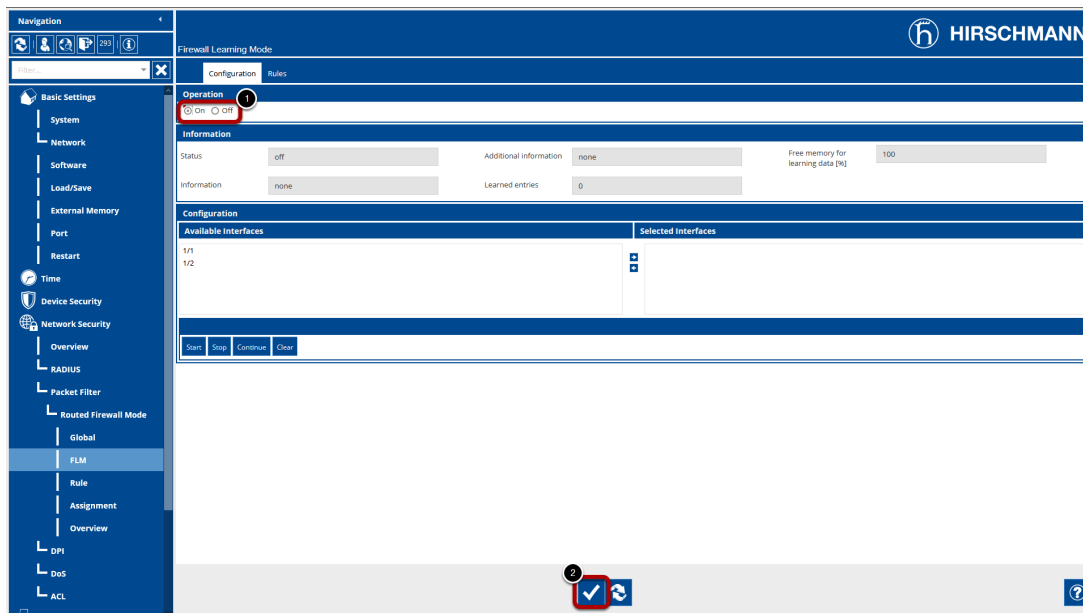
Einschränkungen:

- Nur Router-Schnittstellen (L3 FW)
- Max. 4 Interfaces wählbar (min. 2)

Voraussetzungen:

- EAGLE arbeitet im Router-Modus
- Es sind zwei oder mehr Router-Schnittstellen an physischen oder logischen Schnittstellen konfiguriert

FLM aktivieren

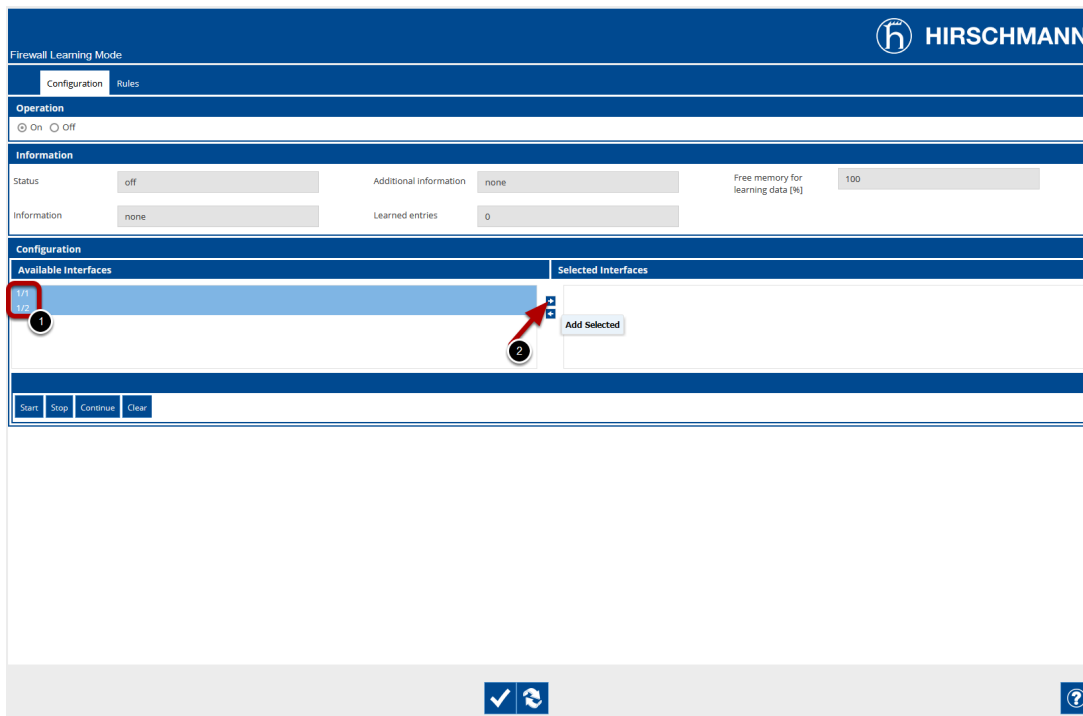


Navigieren Sie zum FLM-Dialog (Network Security - Packet Filter - Routed Firewall Mode - FLM)

1. Stellen Sie im Frame 'Operation' das Optionsfeld auf "On"

2. Klicken Sie unten auf der Seite auf die Schaltfläche "Write", um die Änderung auf das Gerät zu schreiben

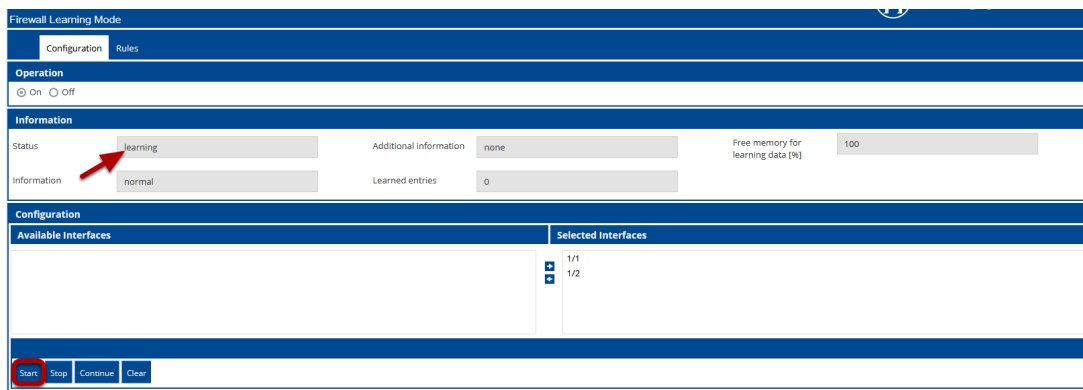
Interfaces auswählen



Wählen Sie mindestens zwei Interfaces aus den Available Interfaces aus, indem Sie sie markieren und drücken Sie die Pfeiltaste nach rechts.

1. Markieren Sie die Einträge der Available Interfaces (Sie können mit UMSCHALT oder STRG mehrere auswählen)
2. Drücken Sie die Pfeiltaste, um die Interfaces in die Selected Interfaces Spalte zu verschieben

Start learning



Drücken Sie die 'Start'-Taste, um die Lernphase zu starten.

Der Status ändert sich in 'learning'

Generieren Sie Datenverkehr über die Firewall und laden Sie die Seite neu.

Der Zähler für gelernte Einträge wird erhöht.

Stop Learning

The screenshot shows the Hirschmann Firewall Learning Mode interface. The top navigation bar includes 'Configuration' and 'Rules' tabs. The 'Rules' tab is active. The 'Operation' section has 'On' selected. The 'Information' section displays 'Status: stopped-data-present', 'Additional information: none', 'Free memory for learning data [%]: 100', and 'Information: normal'. The 'Learned entries' counter shows '5'. The 'Configuration' section has 'Available Interfaces' and 'Selected Interfaces' (1/1, 1/2). The 'Start' button is circled in red, and the 'Stop' button is also circled in red. Red arrows point to the 'Rules' tab and the 'Learned entries' counter.

1. Laden Sie die Seite neu und überprüfen Sie den Zähler "Gelernte Einträge"
2. Stoppen Sie das Lernen durch Drücken der Taste 'Stop' - der Status ändert sich in 'stopped-data-present'
3. Wechseln Sie auf den Tab 'Rules' um die erlernten Firewall-Regeln zu überprüfen

FLM - Rules Tab

Firewall Learning Mode

HIRSCHMANN

Configuration Rules

Learned entries

<input type="checkbox"/>	Source Address	Destination Address	Destination Port	Ingress Interface	Egress Interface	Protocol	First Occurrence	Actions
<input checked="" type="checkbox"/>	172.16.18.143	172.16.24.105	443	1/1	1/2	tcp	Jan 11, 2024	Create, Edit, Delete
<input type="checkbox"/>	172.16.18.143	172.16.24.205	25				Jan 11, 2024	
<input type="checkbox"/>	172.16.18.143	172.16.24.105	25				Jan 11, 2024	
<input type="checkbox"/>	172.16.18.143	172.16.24.105	53				Jan 11, 2024	
<input type="checkbox"/>	172.16.18.143	172.16.24.105	25				Jan 11, 2024	

Service action

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

Ingress interface: 1/1, 1/2

Packetfilter Rules

<input checked="" type="checkbox"/>	Rule index	Source address	Destination address	Description	Ingress Interface	Active
<input checked="" type="checkbox"/>	1			HTTPS	1/1, 1/2	

OK Cancel

✓ ↺ ?

Auf der Registerkarte FLM-Regeln sehen Sie die gelernten Einträge sowie die konfigurierten Paketfilterregeln.

Markieren Sie einen der gelernten Einträge und klicken Sie rechts auf die Schaltfläche "Create" um eine Filterregel zu erstellen.

Im Popup-Fenster können Sie die Regel ändern und eine Beschreibung hinzufügen bevor Sie die Regel erstellen.

Wiederholen Sie diese Schritte, bis der gesamte gewünschte Datenverkehr von einer Regel abgedeckt ist, und klicken Sie dann auf die Schaltfläche "Write" unten auf der Seite.

Packet Filter Rules

Rule index	Description	Source address	Destination address	Protocol	Source port	Destination port	Parameters	Action	Log	Trap	DPI profile index	Active
<input type="checkbox"/>	HTTPS [FLM]	172.16.18.0/24	172.16.24.105	tcp	any	443	none	accept	<input type="checkbox"/>	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SSH [FLM]	172.16.18.143	172.16.24.0/24	tcp	any	22	none	accept	<input type="checkbox"/>	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	TELNET [FLM]	172.16.18.143	172.16.24.0/24	tcp	any	23	none	accept	<input type="checkbox"/>	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MODBUS [FLM]	172.16.18.143	172.16.24.105	tcp	any	502	none	accept	<input type="checkbox"/>	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>

Navigieren Sie zu 'Network Security - Packet Filter - Routed Firewall Mode - Rules' um die erstellten Regeln zu überprüfen. Wie Sie sehen, sind die Regeln bereits aktiviert.

Packet Filter Assignment

Description	Rule index	Interface	Direction	Priority	Active
<input type="checkbox"/> HTTPS [FLM]	1	1/1	ingress	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> SSH [FLM]	2	1/1	ingress	1	<input checked="" type="checkbox"/>
<input type="checkbox"/> TELNET [FLM]	3	1/1	ingress	1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> MODBUS [FLM]	4	1/1	ingress	1	<input checked="" type="checkbox"/>

Commit

Navigieren Sie zu 'Network Security - Packet Filter - Routed Firewall Mode - Assignment' um die Interface-Zuweisung der Regeln zu überprüfen. Die

von FLM erstellten Regeln müssen in der Interface-Zuweisung noch aktiviert werden.

1. Aktivieren Sie das Flag 'aktive' für jeden Eintrag
2. Klicken Sie auf die Schaltfläche 'Write'
3. Uncommitted changes are present wird im Infomation-Frame angezeigt
4. Klicken Sie auf den kleinen Pfeil neben der "Hamburger"-Schaltfläche und wählen Sie 'Commit'

Hinweis: Durch 'Commit' werden die konfigurierten Paketfilterregeln aktiviert und die Firewall-State-Tabelle gelöscht. Bestehende Verbindungen müssen neu aufgebaut werden.