

知识库 > Products > HiSecOS > Firewall Learning Mode (FLM)

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

Navi	gation ·	(h) HIRSCHMANN
		Frevail Learning Mode
Filter.	. 👻 🗙	Configuration Rules
	Basic Settings	Operation D
	System	Son Odi
	L Network	Information
	Software	Status off Additional information none Here mending to 100 Here mending to 100 Here mending to 100 Here mending target and the starting data (b)
	Load/Save	Information none Learned entries 0
	External Memory	Configuration
	Port	Available Interfaces Selected Interfaces
	Restart	
0	Time	
Ū	Device Security	
	Network Security	
	Overview	Sant Sop Consue Clear
	Packet Filter	
	L Routed Firewall Mode	
	Global	
	FLM	
	Rule	
	Assignment	
	Overview	
		<b>9</b>

# 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

#### Enable FLM

## Select Interfaces

					(h) HIRSCHMANN
Firewall Learning N	/ode				
Configuratio	Rules				
Operation					
⊙ On ⊖ Off					
Information					
Status	off	Additional information	none	Free memory for 1 learning data [%]	00
Information	none	Learned entries	0		
Configuration					
Available Interfa	:es		Selected Interfaces		
1/1 1/2			2		
			Add Selected		
			2		
Start Stop Cont	inue Clear				
			<ul> <li>✓ S</li> </ul>		•

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

- 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	Additional information none	Free memory for 100 learning data (%)
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 Mod	e			<b>(h</b> )	HIRSCHM	IANN
Configuration	Rules					
Operation						
⊙ On ⊖ Off						
Information						
Status	stopped-data-present	Additional information	none		Free memory for learning data [96]	100
Information	normal	Learned entries	5			
Configuration						
Available Interfaces		Sel	lected Interfaces			
		•	1/1 1/2			
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 'stoppeddata-present'
- 3. Change to the rules tab to review the learned firewall rules

FLM - Rules Tab

										<b>)</b>	HIRSCHMANN
Firewall Learning Mo	ode										
Configuration	Rules										
Learned entries											
Source Address	Destination Address	Destination Port	Ingress Interface	Egress Interface	Proto	col	First Occure	Create			
172.16.18.143	172.16.24.105	443	1/1	1/2	tcp		Jan 11,	Edit			
172.16.18.143	172.16.24.205	<sup>22</sup> Service ac	tion		>		Jan 11,	Delete	,		
172.16.18.143	172.16.24.105	22 Source addres	ss: 172.16.18.0	/24	-		Jan 11,	Connections by	Rule Set	0/5	
172.16.18.143	172.16.24.105	50 Destination	172.16.24.1	.05	>		Jan 11,	Connections by	[	0/5	
172.16.18.143	172.16.24.105	23address:	442		2		Jan 11,	Selection	L		
		Destination port:	443								
		Protocol:	tcp	-							
		Rule index:	1								
Packetfilter Rules		Action:	accept	-							
Rule index Sol	urce Destin dress addres	atio S Description:	HTTPS	-	- 1	Descrip	otion	Ingress Interface	Active		
		Ingress	1/1								
		Interface:	1/2								
				K Cance							
											(?)
Packetfilter Rules       ✓     Rule index       So       add	urce Destin dress addres	Protocol: Rule index: Action: bescription: Ingress Interface:	tcp 1 accept HTTPS 1/1 1/2	K Cance		Descrip	ation	Ingress Interface	Active		

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

Navigation	1	Τ											æ		
24	🔇 🗗 299   🕕 🛈	Pa	icket Filter Ri	Je									<u></u> р) н	IRSCH	MANN
Filter	~ X		Rule index	Description	Source address	Destination address	Protocol	Source port	Destination port	Parameters	Action	Log	Trap	DPI profile index	Active
🔗 Basi	: Settings	^	1	HTTPS (FLM)	172.16.18.0/24	172.16.24.105	tcp	any	443	none	accept	0		0	
🕝 Time			2	SSH [FLM]	172.16.18.143	172.16.24.0/24	tcp	any	22	none	accept			0	8
Devi	ce Security		3	TELNET [FLM]	172.16.18.143	172.16.24.0/24	tcp	any	23	none	accept			0	
æ			4	MODBUS [FLM]	172.16.18.143	172.16.24.105	tcp	any	502	none	accept			0	
	kerview KolUS Routed Firewall Mode Global FLM Rule														
	Assignment														
	Overview														
	<u>ข</u>														
L Do	os														

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

Navigation 4											
S   🖁 🚱 📭 295   🗊	Packet Filter Assignm	nent									
Filter	Information										
	Assignments	4									
Basic Settings											
C Time	present 3										
Device Security	Description	Rule index	Interface	Direction	Priority	Active					
Network Security	HTTPS [FLM]	1	1/1	ingress	1						
Overview	SSH [FLM]	2	1/1	ingress	1						
	TELNET [FLM]	3	1/1	ingress	1	™					
Packet Filter	MODBUS [FLM]	4	1/1	ingress	1						
L Routed Firewall Mode											
Global											
FLM											
Rule											
Assignment											
Overview											
L <sub>DoS</sub>											
Virtual Private Network											
Switching											
Routing							4				
Diagnostics					2						
Advanced											

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 reestablished.