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

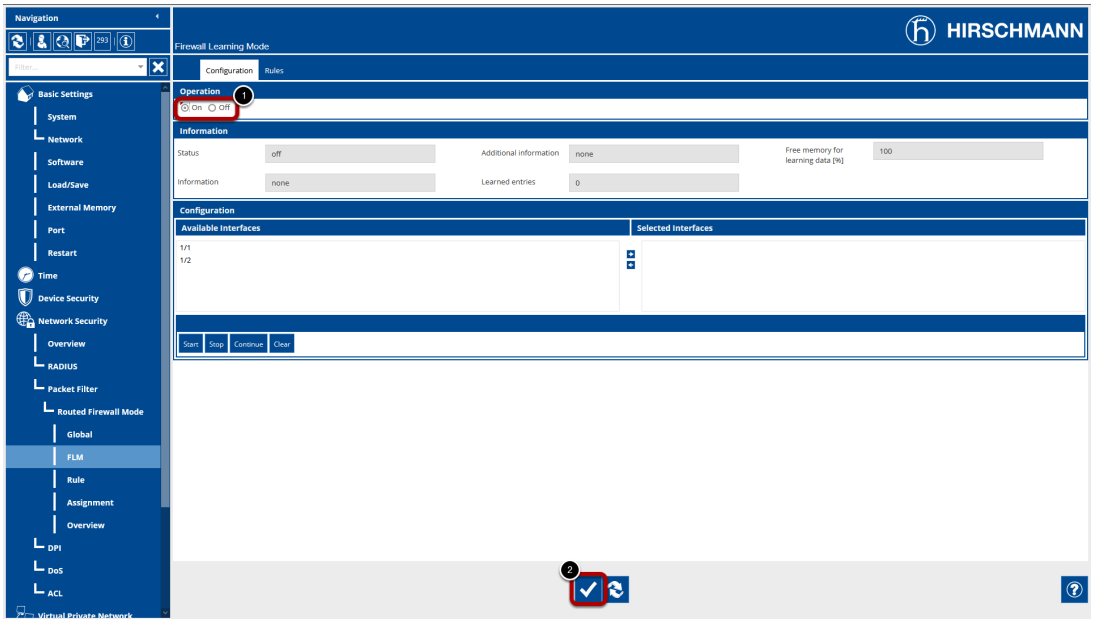
Einschränkungen:

- 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

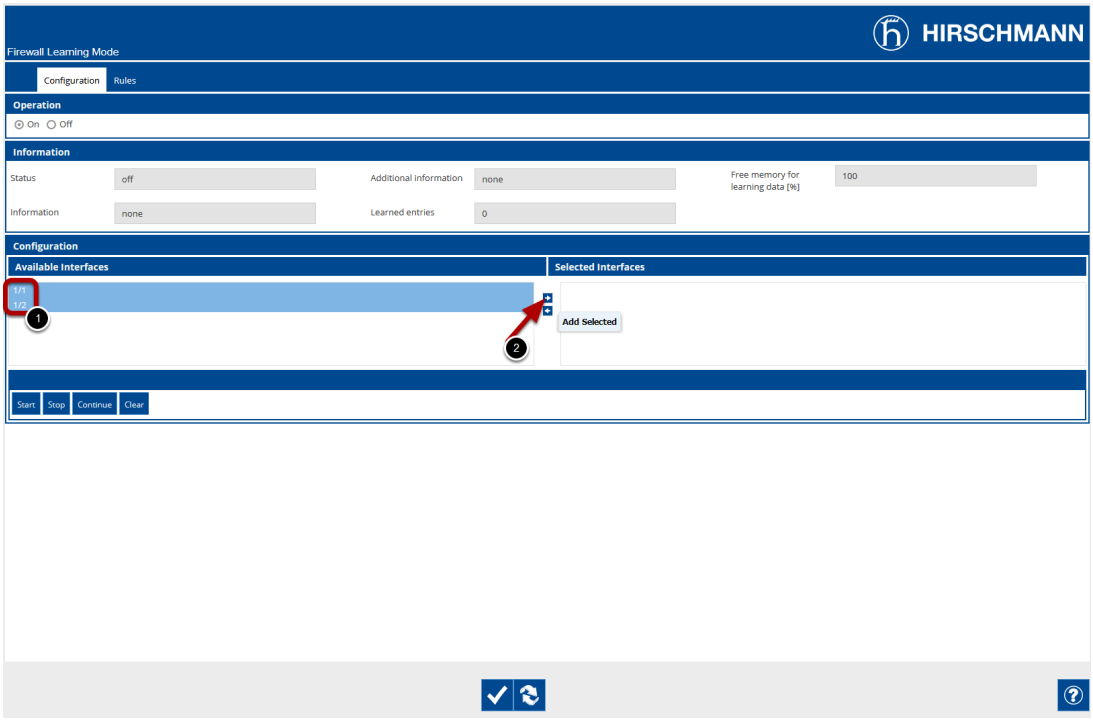


Navigieren Sie zum FLM-Dialog (Network Security - Packet Filter - Routed Firewall Mode - FLM)

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

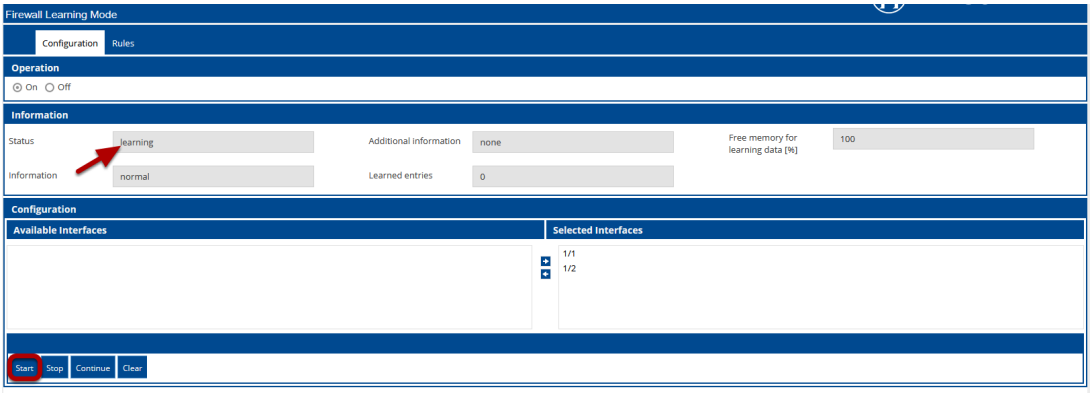
Interfaces auswählen



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

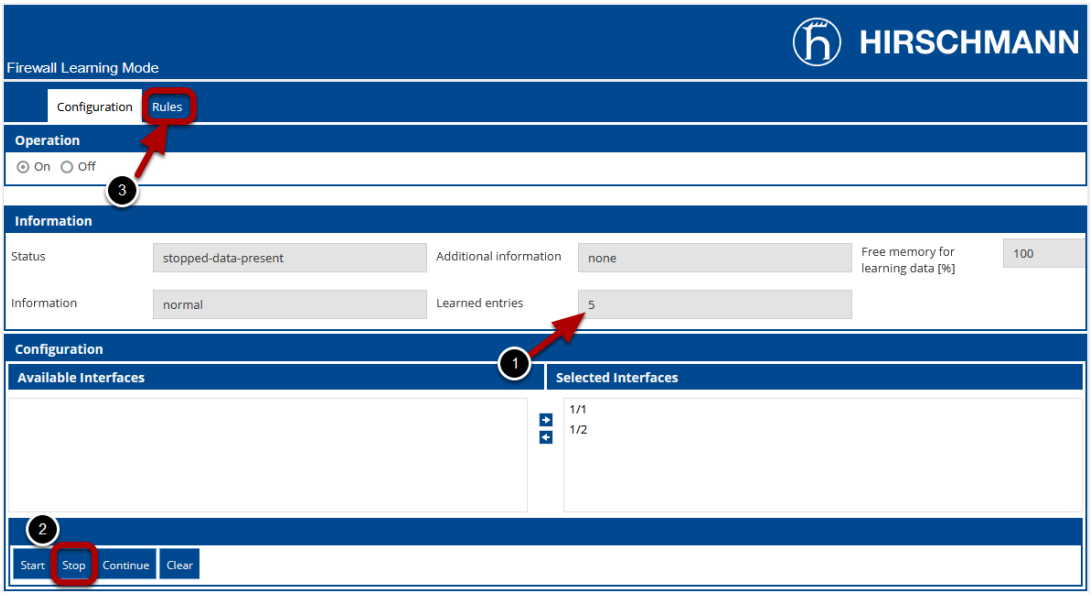
1. Markieren Sie die Einträge der Available Interfaces (Sie können mit UMSCHALT oder STRG mehrere auswählen)
2. Drücken Sie die Pfeiltaste, um die Interfaces in die Selected Interfaces Spalte zu verschieben

Start learning



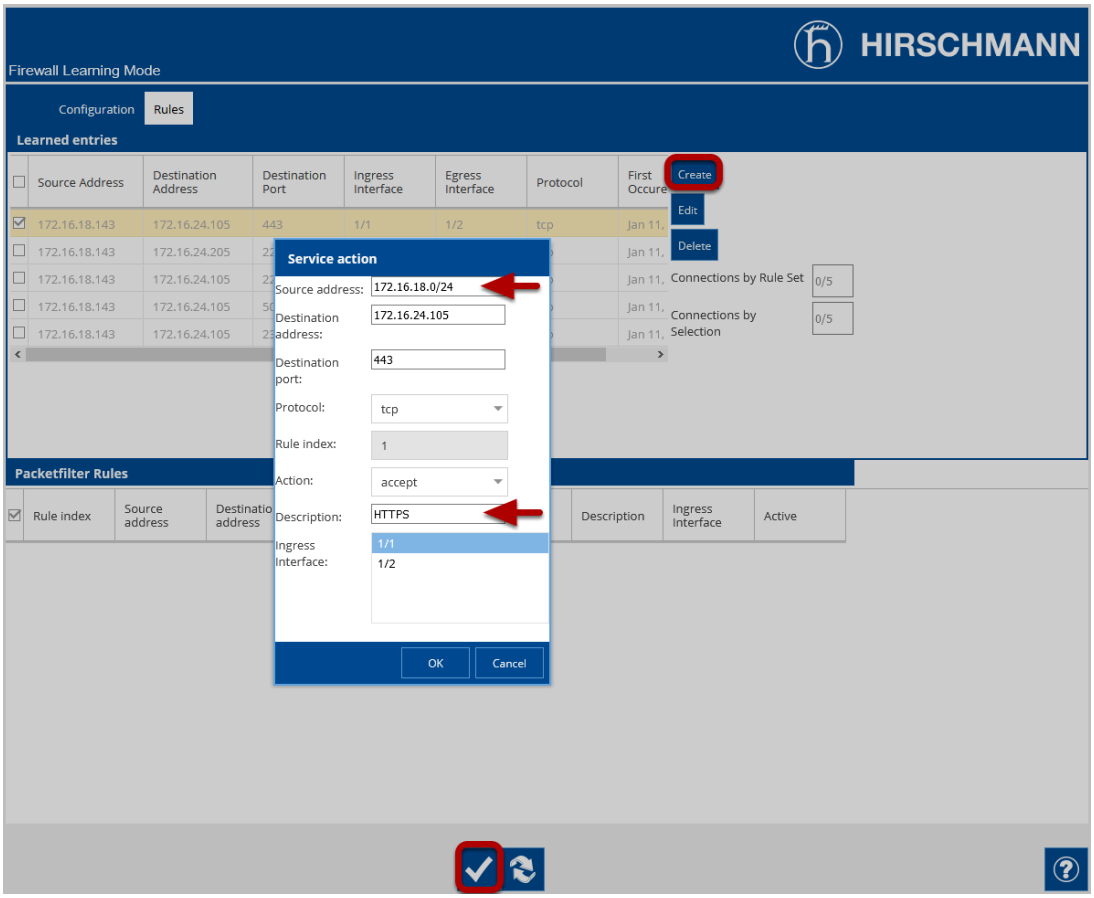
Drücken Sie die 'Start'-Taste, um die Lernphase zu starten.
Der Status ändert sich in 'learning'
Generieren Sie Datenverkehr über die Firewall und laden Sie die Seite neu.
Der Zähler für gelernte Einträge wird erhöht.

Stop Learning



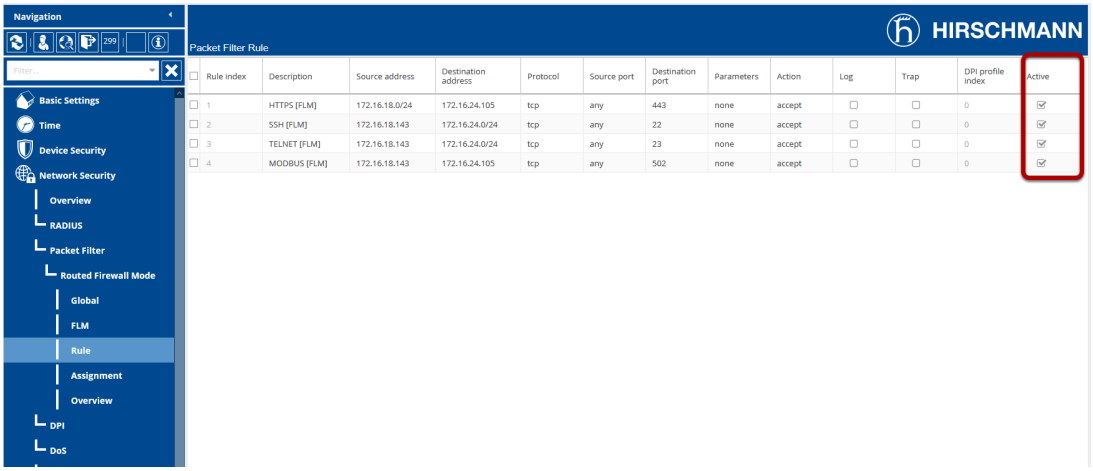
1. Laden Sie die Seite neu und überprüfen Sie den Zähler "Gelernte Einträge"
2. Stoppen Sie das Lernen durch Drücken der Taste 'Stop' - der Status ändert sich in 'stopped-data-present'
3. Wechseln Sie auf den Tab Rules' um die erlernten Firewall-Regeln zu überprüfen

FLM - Rules Tab



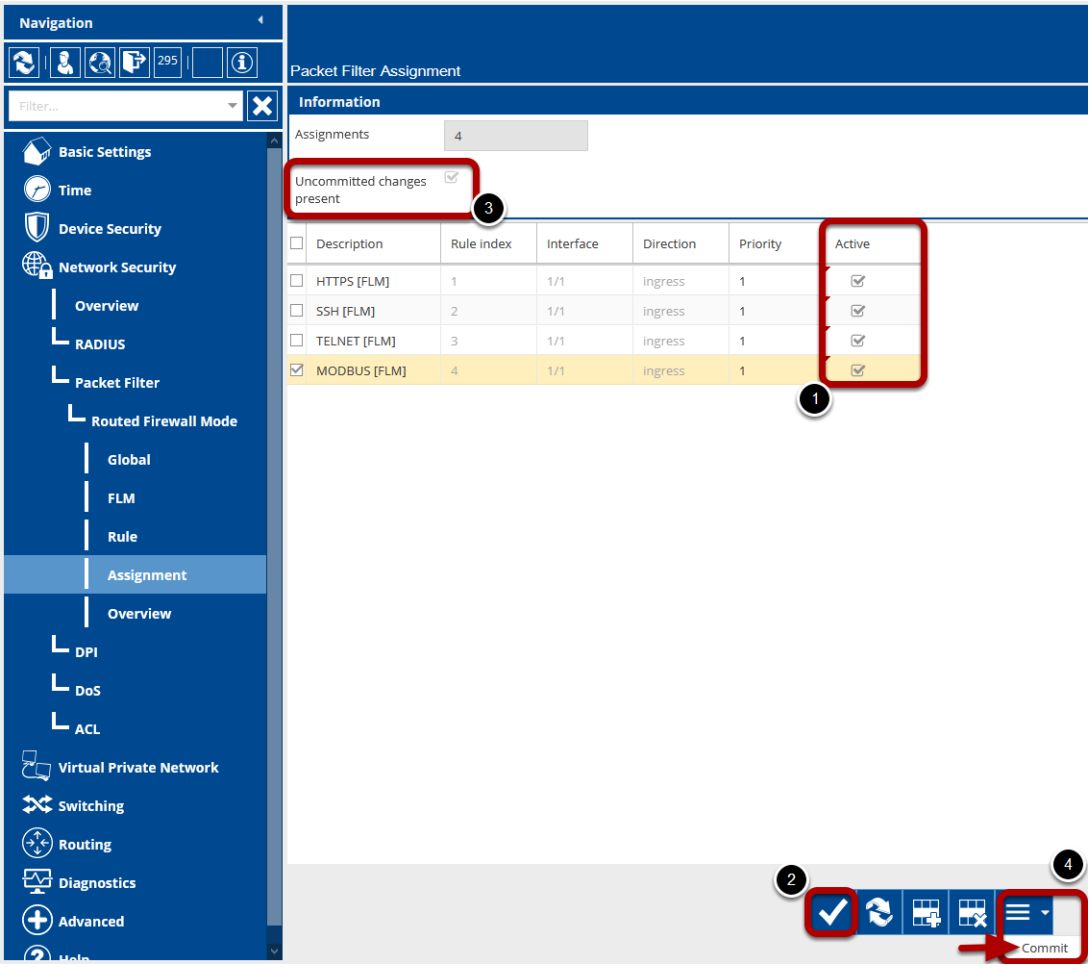
Auf der Registerkarte FLM-Regeln sehen Sie die gelernten Einträge sowie die konfigurierten Paketfilterregeln.
Markieren Sie einen der gelernten Einträge und klicken Sie rechts auf die Schaltfläche "Create" um eine Filterregel zu erstellen.
Im Popup-Fenster können Sie die Regel ändern und eine Beschreibung 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



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



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.