


Trong pfSense, mục Services / Suricata / WAN - Interface Settings

Alert and Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Suricata alert.
IPS Mode	<div>Legacy Mode</div> <p>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</p> <p>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</p>
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is Checked.
Which IP to Block	<div>BOTH</div> <p>Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.</p>
Block On DROP Only	<input checked="" type="checkbox"/> Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.
IP Pass List	<div>default</div> <div> View List</div> <p>Choose the Pass List you want this interface to use. Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.</p> <p>The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.</p>
Enable Passlist Debugging Log	<input type="checkbox"/> Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata_em052736/passlist_debug.log. Default is Not Checked.
Performance and Detection Engine Settings	

Hình 3. 35. Bật chế độ IPS

Trong Services / Suricata / Interface Settings / WAN - Rules

Services / Suricata / Alerts

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

Alert Log View Settings

Instance to View

(WAN) WAN

Choose which instance alerts you want to inspect.

Save or Remove Logs

Download

Clear

All alert log files for selected interface will be downloaded

Clear the currently active Alerts log file

Save Settings

Save

Refresh

Default is ON

250

Number of alerts to display. Default is 250

Alert Log View Filter

+

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/21/2024 03:31:19	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:18	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:17	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:16	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:15	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack

Hình 3. 39. Log phát hiện tấn công

Services / Suricata / Interface Settings / WAN - Rules

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

WAN Settings

WAN Categories

WAN Rules

WAN Flow/Stream

WAN App Parsers

WAN Variables

WAN IP Rep

Available Rule Categories

Category

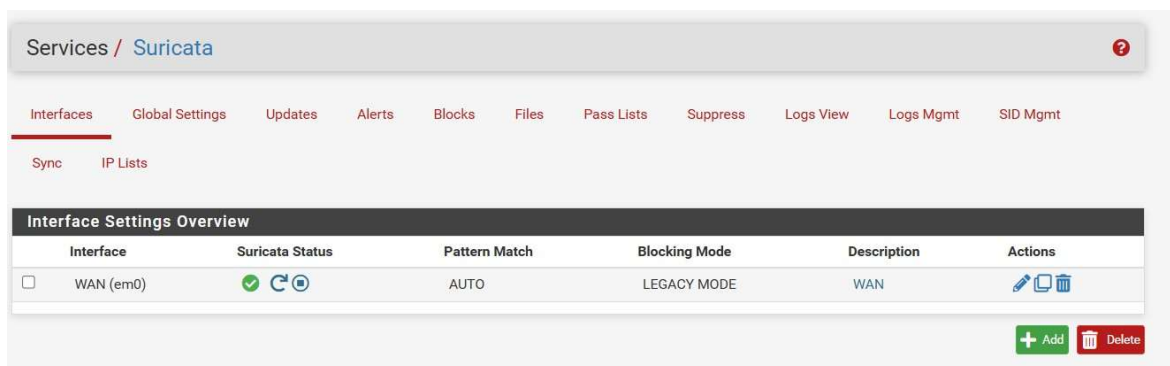
custom.rules

Select the rule category to view and manage.

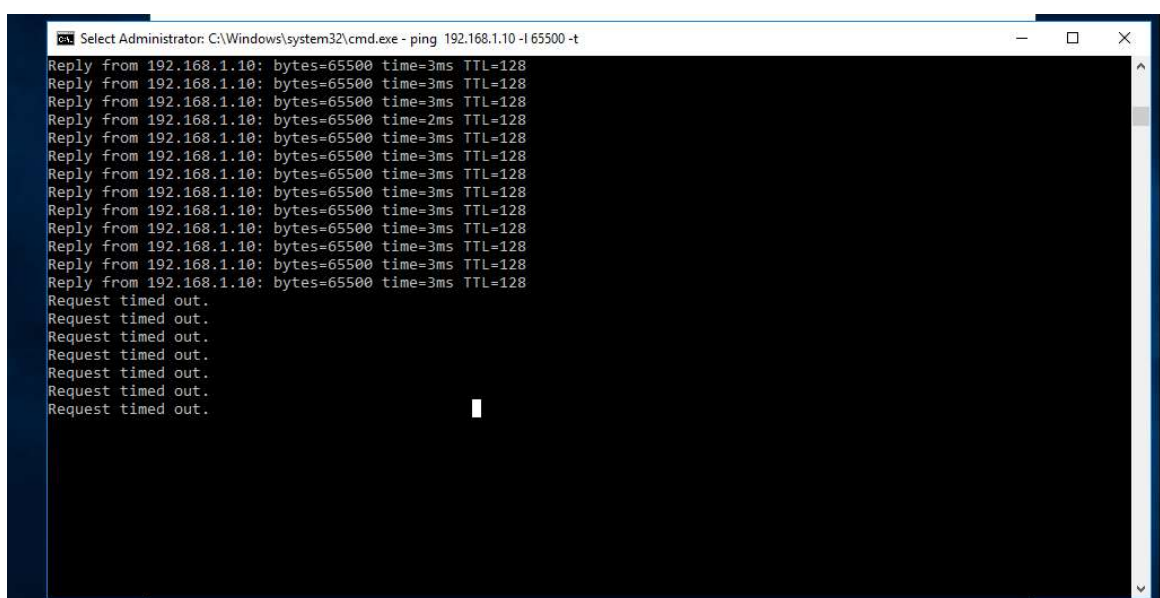
Defined Custom Rules

```
drop icmp 192.168.182.0/24 any -> any any (msg:"attack"; dsize: >10000; sid:3; rev:2;)
```

Hình 3. 40. Sửa rule alert → drop để chặn các gói tấn công



Hình 3. 41. Reset và đảm bảo rule đã được kích hoạt



Hình 3. 42. Lệnh tấn công xuất hiện gói bị drop

Services / Suricata / Alerts

InterfacesGlobal SettingsUpdatesAlertsBlocksFilesPass ListsSuppressLogs ViewLogs MgmtSID Mgmt

SyncIP Lists

Alert Log View Settings

Instance to View

(WAN) WAN

Choose which instance alerts you want to inspect.

Save or Remove Logs

Download

All alert log files for selected interface will be downloaded

Clear

Clear the currently active Alerts log file

Save Settings

Save

Save auto-refresh and view settings

☒ Refresh

Default is ON

250

Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/21/2024 03:37:17		3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:37:17		3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:37:16		3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:37:16		3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack

Hình 3. 43. Log drop

Services / Suricata / Blocked Hosts

InterfacesGlobal SettingsUpdatesAlertsBlocksFilesPass ListsSuppressLogs ViewLogs MgmtSID Mgmt

SyncIP Lists

Blocked Hosts Log View Settings

Save or Remove Hosts

Download

All blocked hosts will be saved

Clear

All blocked hosts will be cleared

Save Settings

Save

Save auto-refresh and view settings

☒ Refresh

Default is ON

500

Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Suricata

Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.

Blocked IP	Block Date/Time	Block Alert Description	Block Rule GID:SID	Remove Block
192.168.182.173	11/21/2024 03:36:47	attack	1:3	

1 host IP address is currently being blocked.

Hình 3. 44. Xuất hiện ip bị block trong Services / Suricata / Blocked Hosts