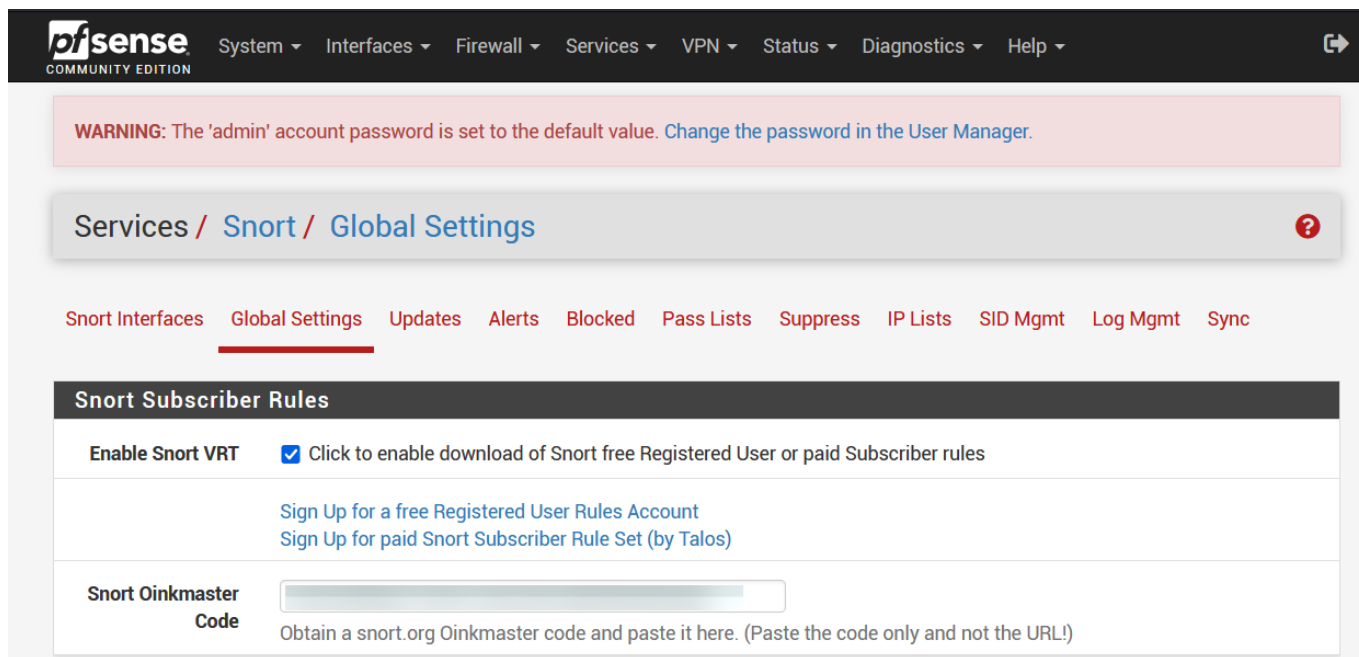


Security: pfSense IDS/IPS Snort

źródło: <https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html>

1. Konfiguracja kodu OinkCode



The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb trail is "Services / Snort / Global Settings". A horizontal menu contains links: Snort Interfaces, Global Settings (which is underlined), Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The main content area is titled "Snort Subscriber Rules". It contains two sections: "Enable Snort VRT" with a checked checkbox and a link to "Click to enable download of Snort free Registered User or paid Subscriber rules", and "Snort Oinkmaster Code" with a text input field and a note: "Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)"

2. Wymuszenie aktualizacji zasad

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

⌂

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / **Snort** / Updates ?

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	80dd7fbe61809a22627b2e70c9183e07	Monday, 02-Jun-25 13:24:43 CEST
Snort GPLv2 Community Rules	d183d5bf5becd6dc8ad3404ce1db62db	Monday, 02-Jun-25 13:24:43 CEST
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update	Jun-02 2025 13:24	Result: Success
Update Rules	✓ Update Rules	⬇ Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

[📄 View Log](#)[🗑 Clear Log](#)

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size	1 KiB
---------------------	-------

3. Dodanie interfejsu do monitorowania SNORT

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Snort / WAN1 - Interface Settings

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

WAN1 Settings

General Settings

Enable

☒ Enable interface

Interface

WAN2 (hn2)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN2

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

4. Włączenie zasad community GPLv2

Services / Snort / Interface Settings / WAN2 - Categories ?

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN2 Settings **WAN2 Categories** WAN2 Rules WAN2 Variables WAN2 Preprocs WAN2 IP Rep WAN2 Logs

Automatic Flowbit Resolution

Resolve Flowbits ☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☐ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets (Categories) Snort will load at startup

 - Category is auto-enabled by SID Mgmt conf files
 - Category is auto-disabled by SID Mgmt conf files

Select All Unselect All  Save

Enable **Ruleset: Snort GPLv2 Community Rules**

☒ [Snort GPLv2 Community Rules \(Talos certified\)](#)

5. Dodanie zasady żeby ping był reportowany

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / **Snort** / Interface Settings / WAN2 - Rules 

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN2 Settings WAN2 Categories **WAN2 Rules** WAN2 Variables WAN2 Preprocs WAN2 IP Rep WAN2 Logs

Available Rule Categories

Category Selection: 
Select the rule category to view and manage.

Defined Custom Rules

```
alert icmp any any -> any any (msg:"ICMP Ping Detected"; itype:8; sid:1000001; rev:1;)
alert icmp any any -> any any (msg:"ICMP Echo Reply Detected"; itype:0; sid:1000002; rev:1;)
```

 Save  Cancel  Clear

6. Test Ping

pfSense

COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

➔

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Snort / Alerts

?

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

WAN2 (hn2) ▾

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

11 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-06-02 13:32:48		0	ICMP		172.16.32.123 		172.16.32.1 		1:1000001 	ICMP Ping Detected
2025-06-02 13:32:43		0	ICMP		172.16.32.123 		172.16.32.1 		1:1000001 	ICMP Ping Detected
2025-06-02 13:32:38		0	ICMP		172.16.32.123 		172.16.32.1 		1:1000001 	ICMP Ping Detected
2025-06-02 13:32:33		0	ICMP		172.16.32.123 		172.16.32.1 		1:1000001 	ICMP Ping Detected

From:

<https://wiki.ostrowski.net.pl/> - **Kacper's Wiki**

Permanent link:

https://wiki.ostrowski.net.pl/doku.php?id=notatki:security_ips_snort&rev=1748863999

Last update: **2025/06/02 13:33**