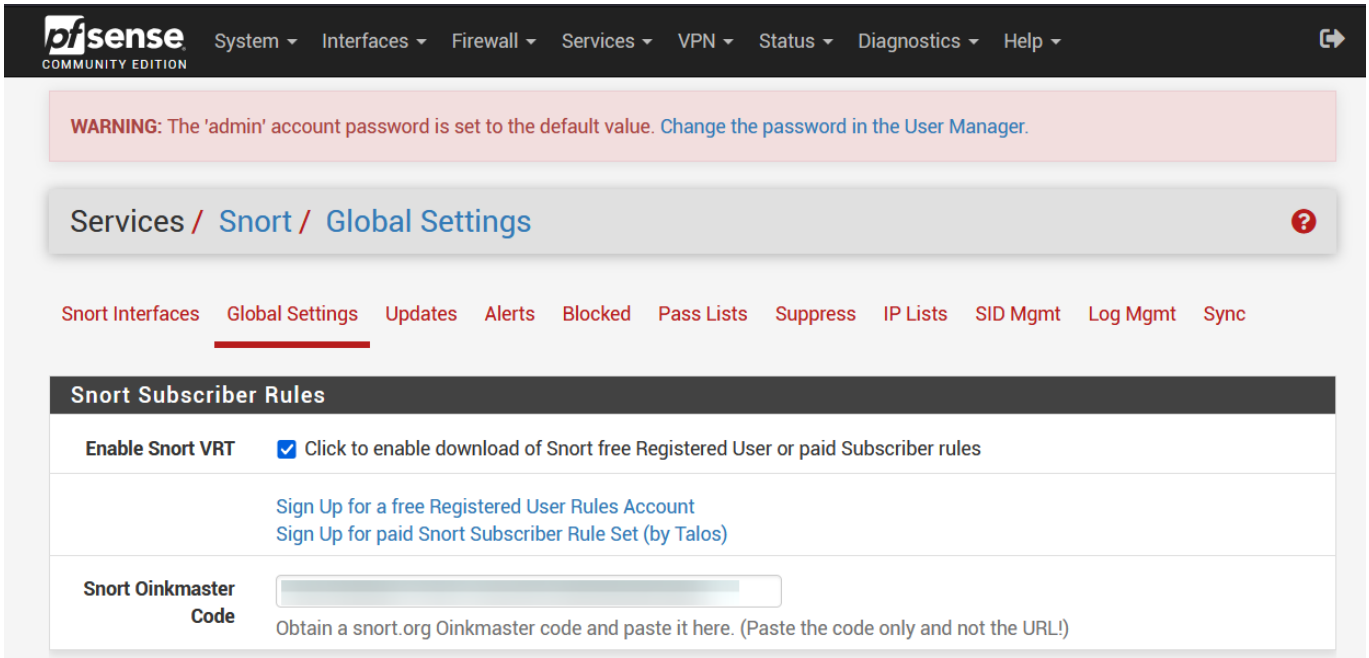
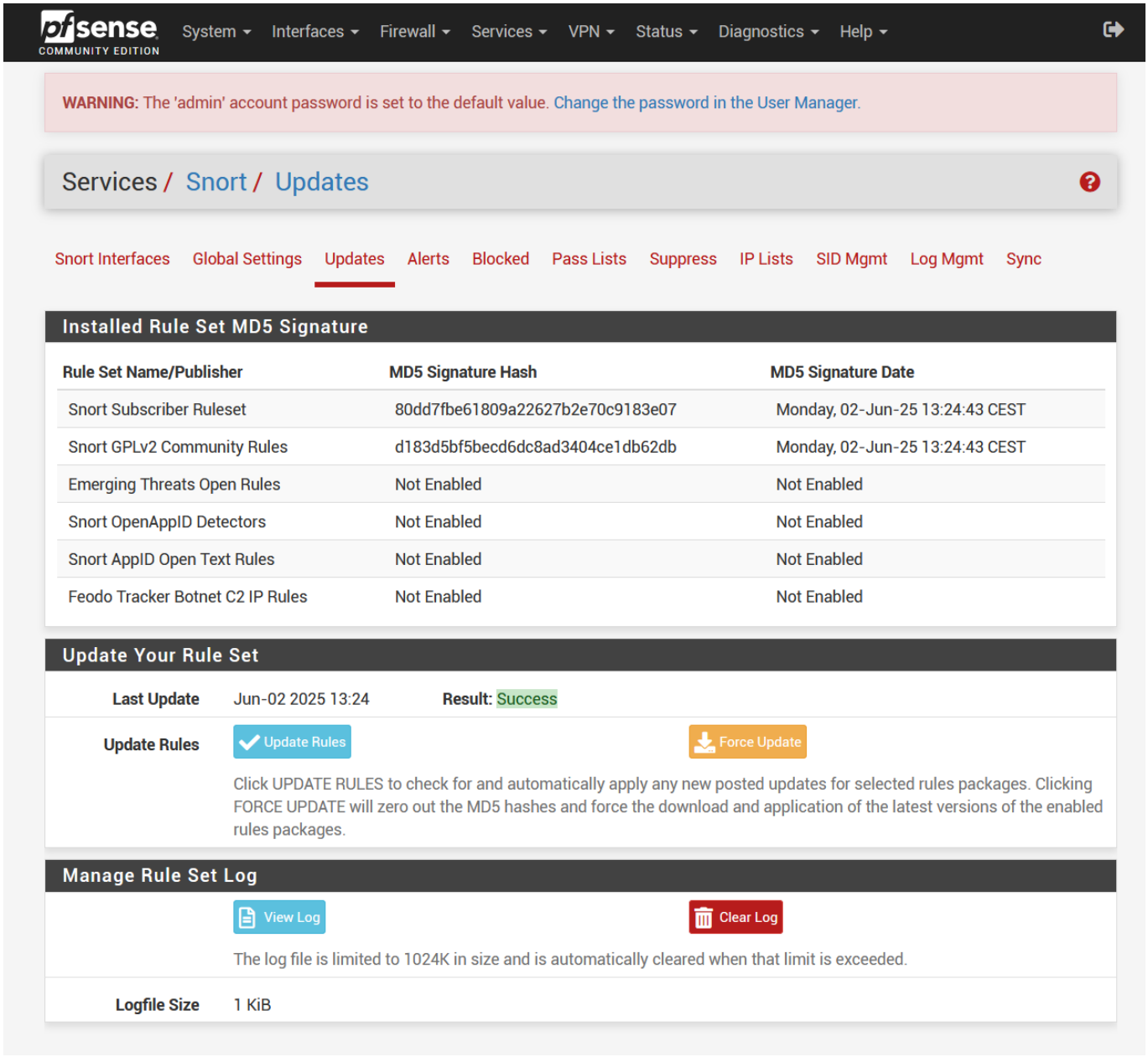
Security: pfSense IDS/IPS Snort

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

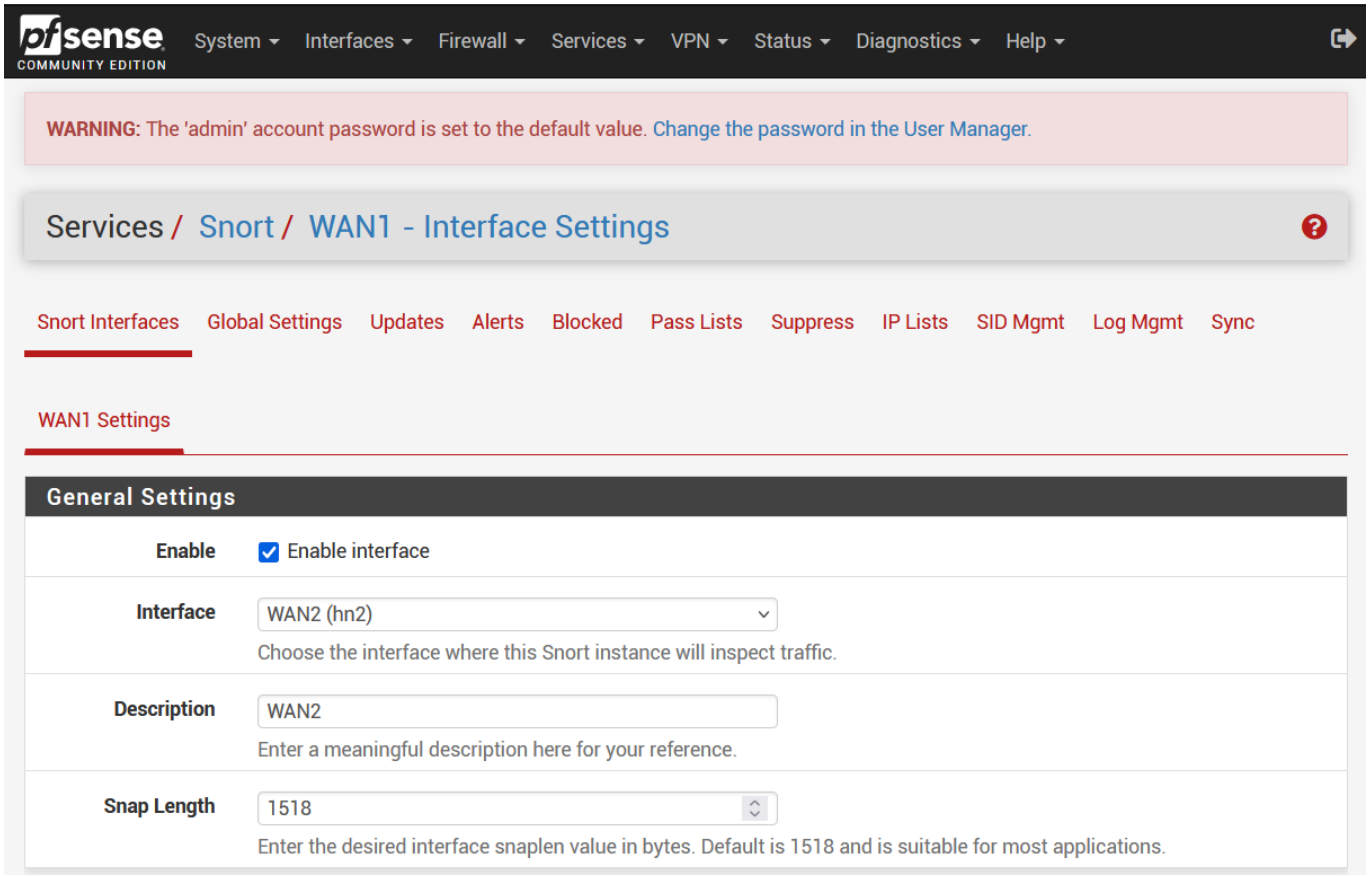
1. Konfiguracja kodu OinkCode



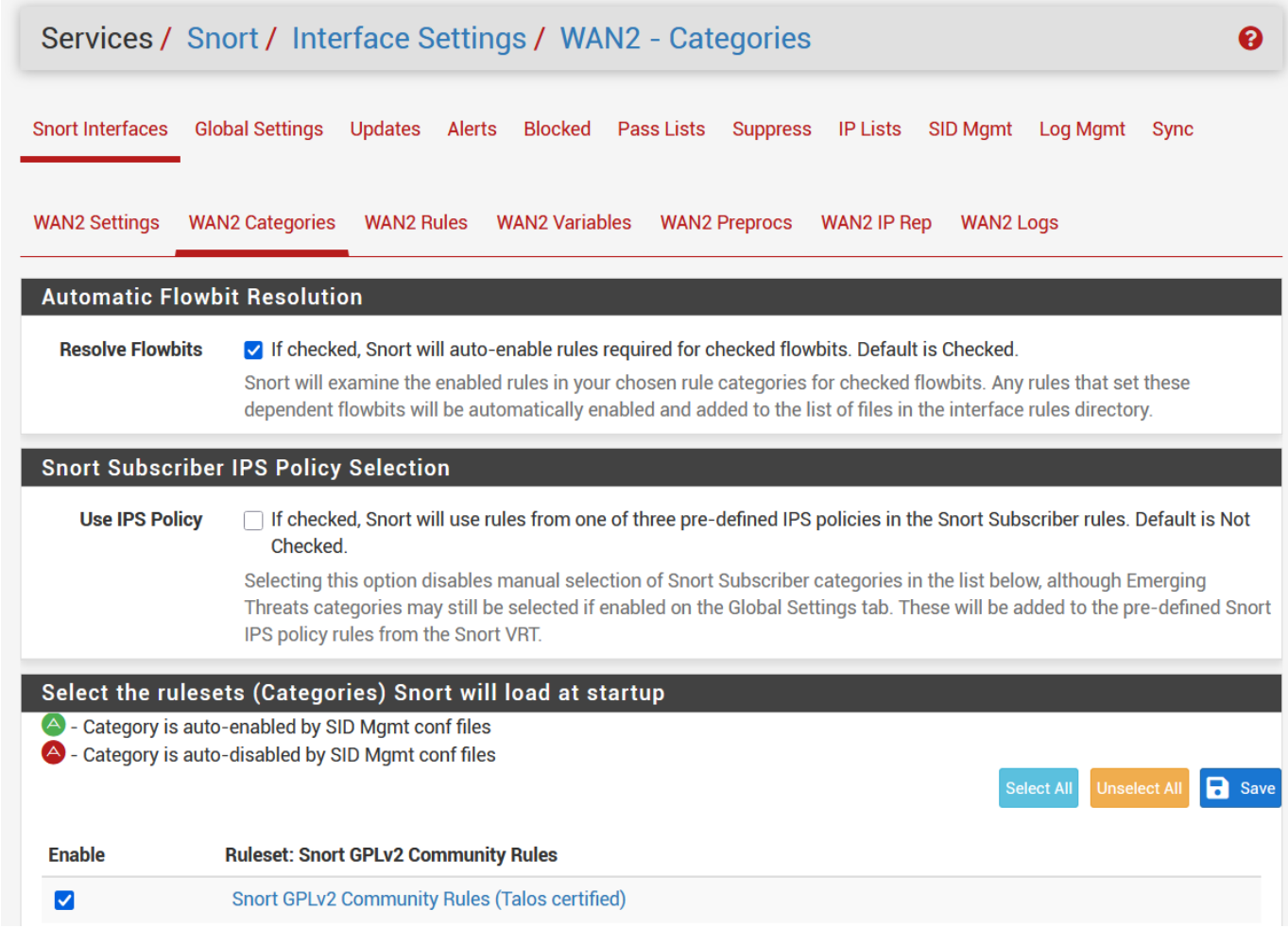
2. Wymuszenie aktualizacji zasad



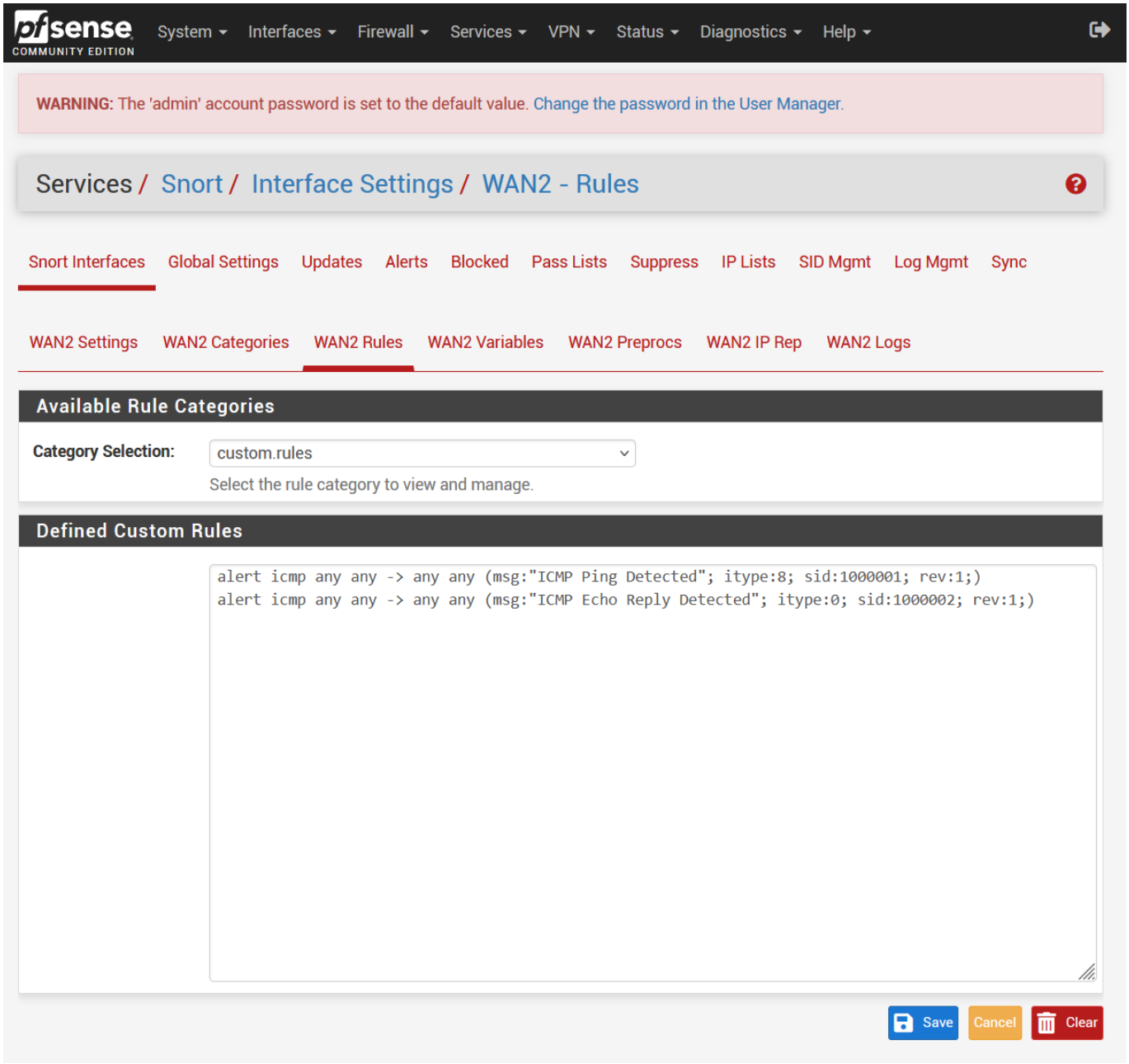
3. Dodanie interfejsu do monitorowania SNORT



4. Włączenie zasad community GPLv2



5. Dodanie zasady żeby ping był reportowany


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 / 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:
custom.rules
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