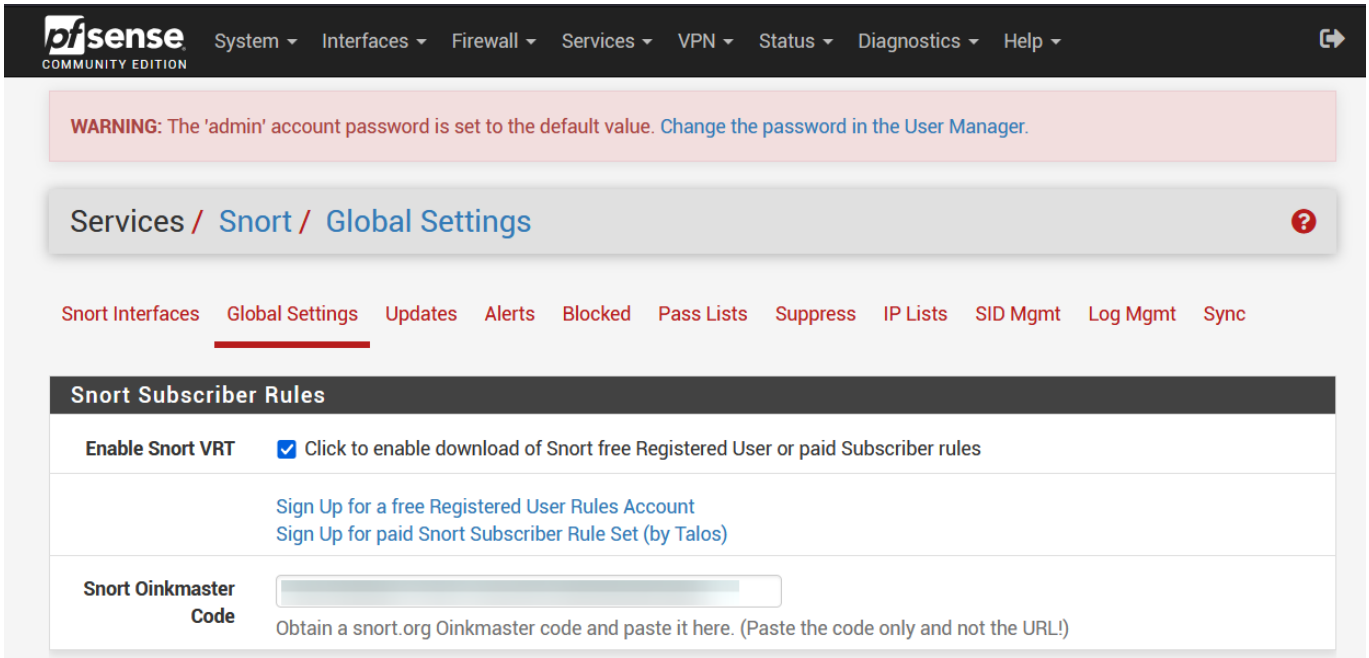
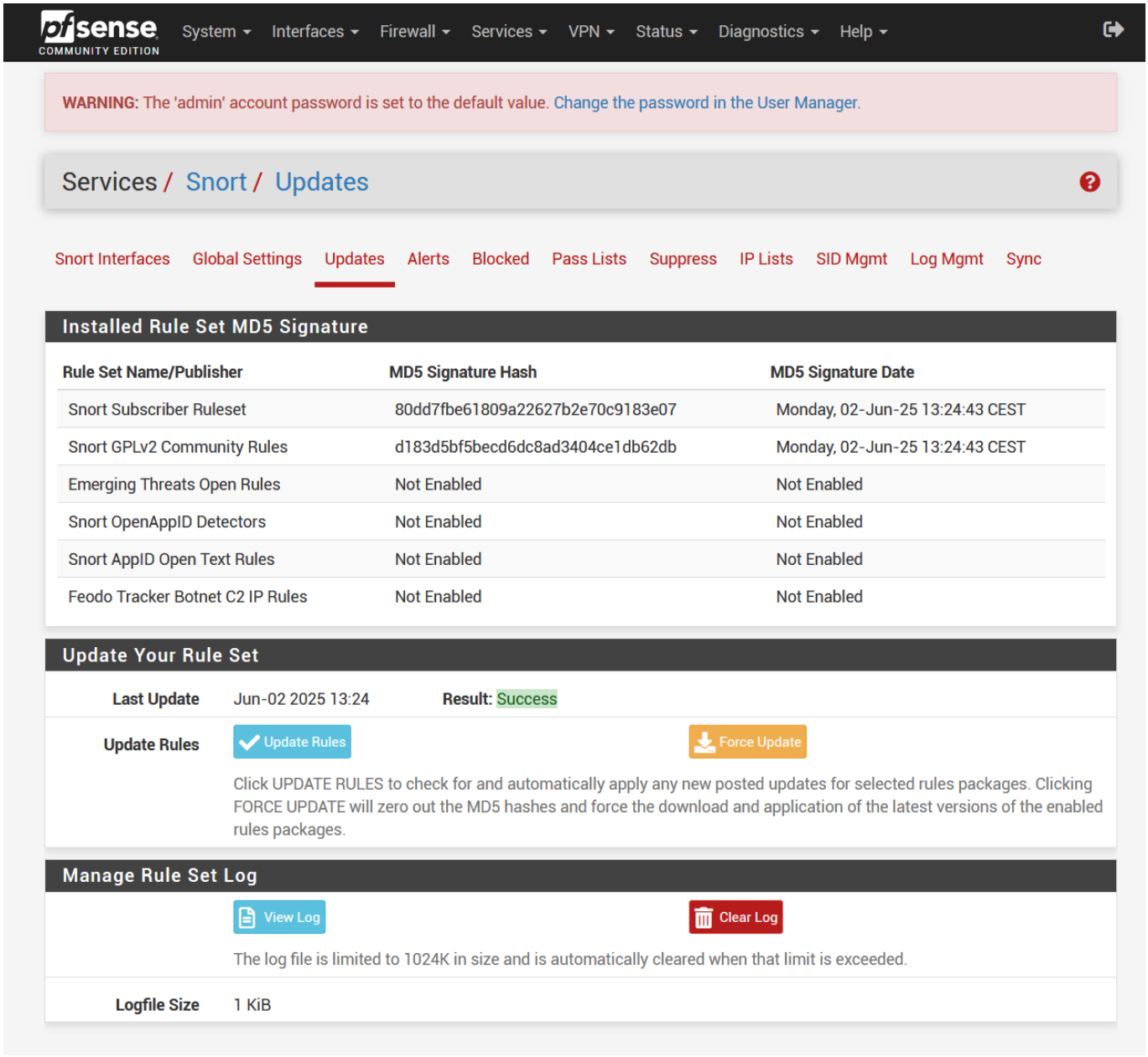
Security: pfSense IDS/IPS Snort

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

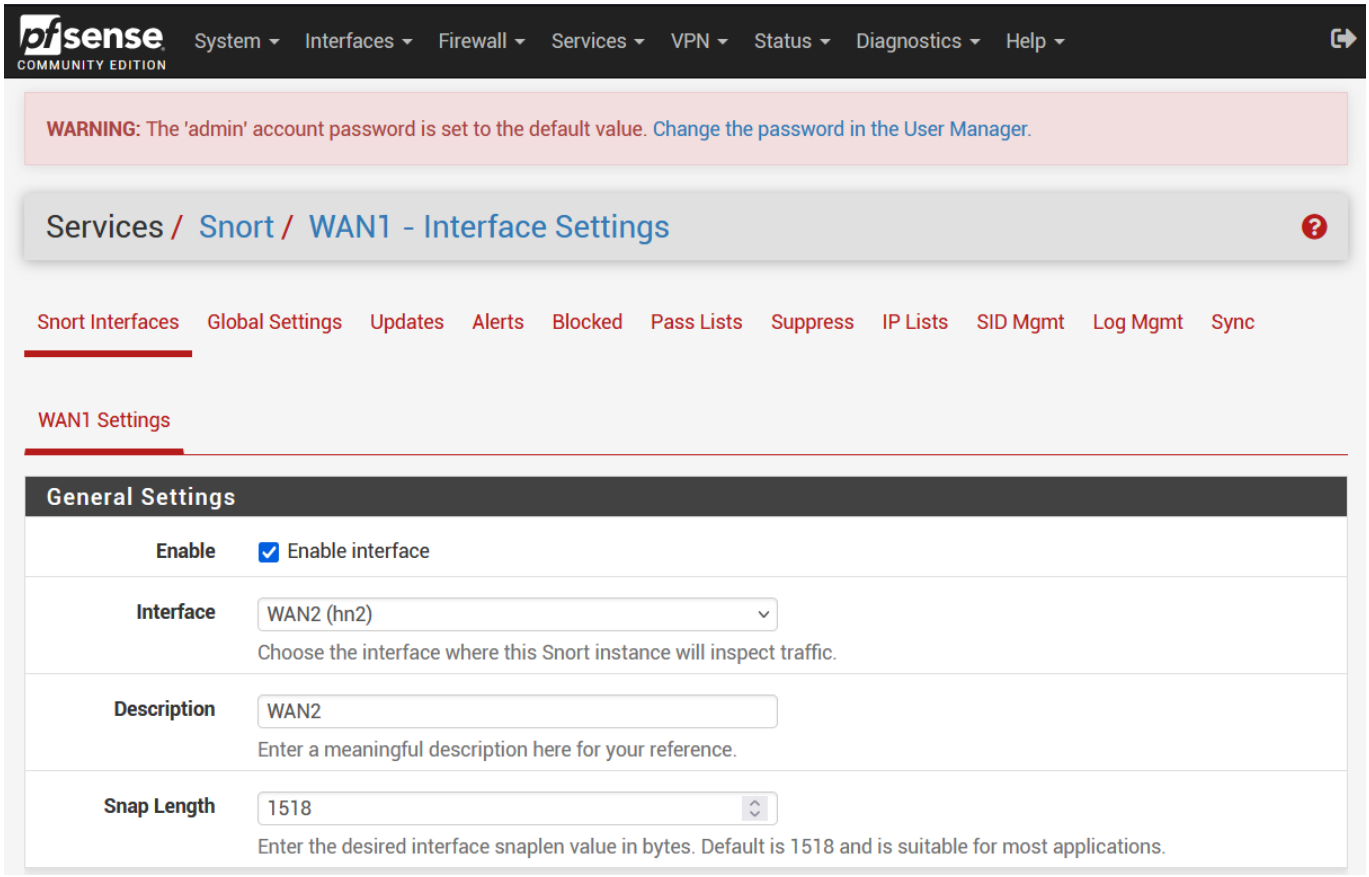
1. Konfiguracja kodu OinkCode



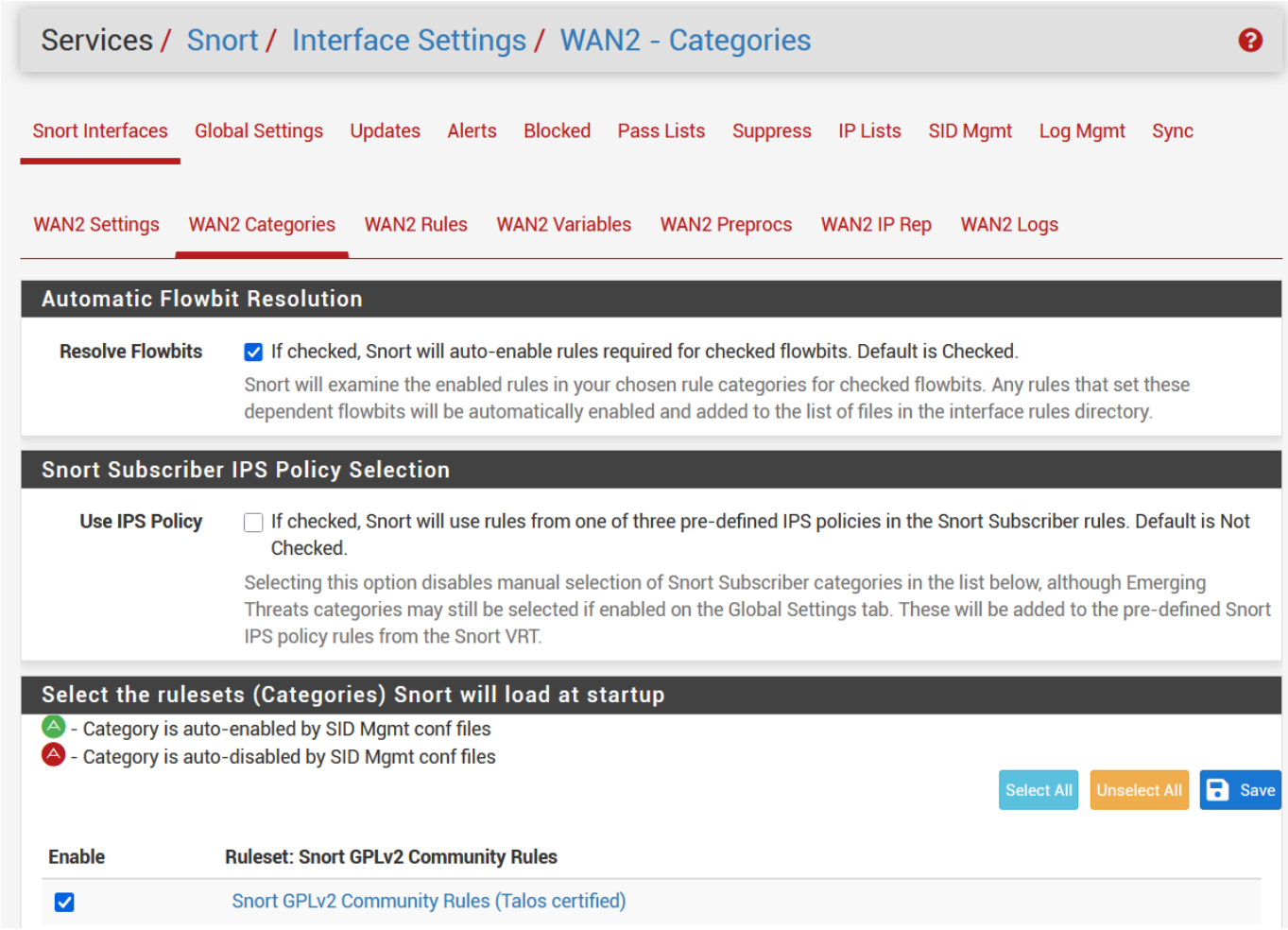
2. Wymuszenie aktualizacji zasad



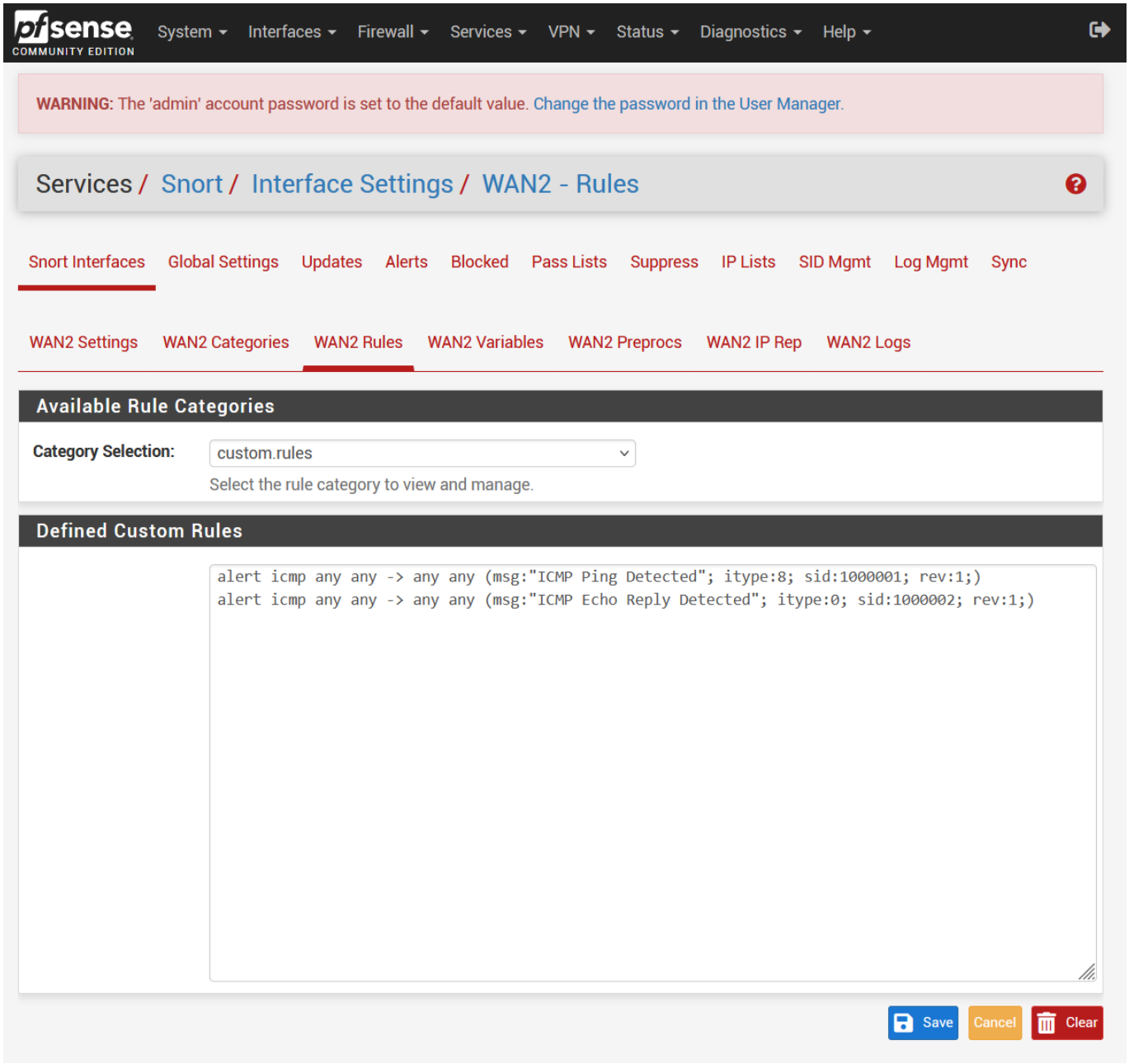
3. Dodanie interfejsu do monitorowania SNORT



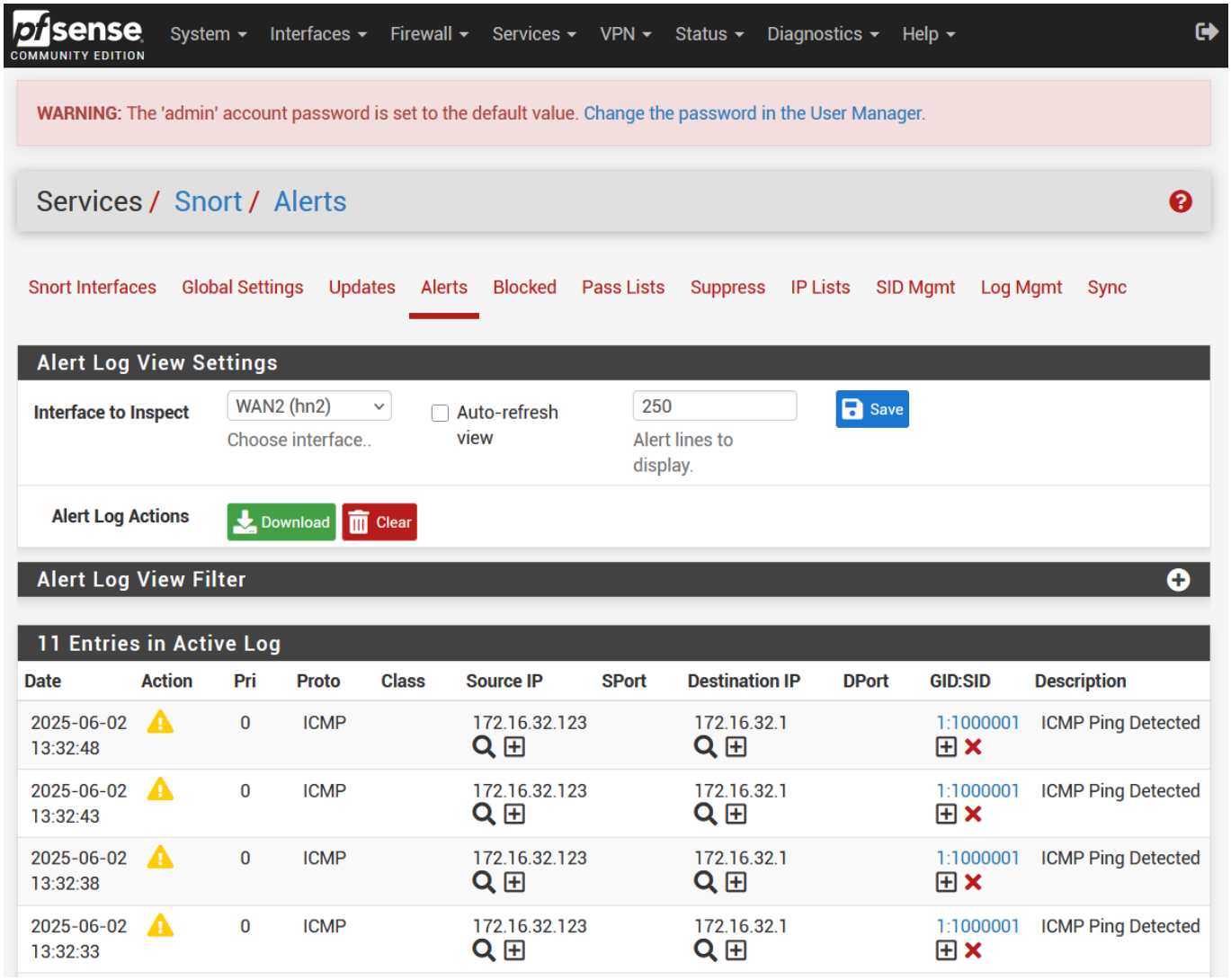
4. Włączenie zasad community GPLv2



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



7. Dodanie innych reguł

reguły dodane w custom.rules:

```
# BLOCK ICMP PING (Echo Request)
drop icmp any any -> any any (msg:"BLOCKED: ICMP Ping Detected"; itype:8;
sid:1000001; rev:1;)

# BLOCK NMAP Stealth Scan (SYN)
drop tcp any any -> any any (flags:S; msg:"BLOCKED: Nmap Stealth SYN Scan";
sid:1000002; rev:1;)

# BLOCK Null Scan
drop tcp any any -> any any (flags:0; msg:"BLOCKED: Null Scan Detected";
sid:1000003; rev:1;)

# BLOCK Xmas Scan
drop tcp any any -> any any (flags:FPU; msg:"BLOCKED: Xmas Scan Detected";
sid:1000004; rev:1;)
```

```
# BLOCK Shellcode-like Payloads
drop tcp any any -> any any (content:"|90 90 90|"; msg:"BLOCKED: NOP Sled
(Shellcode) Detected"; sid:1000005; rev:1;)

# BLOCK FTP Login Attempt
drop tcp any any -> any 21 (msg:"BLOCKED: FTP Connection Attempt"; flags:S;
sid:1000006; rev:1;)

# BLOCK Netcat Backdoor Attempt
drop tcp any any -> any 31337 (msg:"BLOCKED: Netcat Backdoor Connection
Attempt"; sid:1000007; rev:1;)

# BLOCK HTTP Directory Traversal
drop tcp any any -> any 80 (msg:"BLOCKED: HTTP Directory Traversal";
content:"../"; http_uri; sid:1000008; rev:1;)

# BLOCK Suspicious User-Agent (e.g., sqlmap)
drop tcp any any -> any 80 (msg:"BLOCKED: Suspicious User-Agent - sqlmap";
content:"User-Agent|3A| sqlmap"; http_header; sid:1000009; rev:1;)

# BLOCK IRC Bot Connection Attempt
drop tcp any any -> any 6667 (msg:"BLOCKED: IRC Bot Connection Attempt";
sid:1000010; rev:1;)
```

8. Przetestowanie za pomocą kali linux

Historia poleceń kali:

```
  104  ftp 172.16.32.1
  105  ping 172.16.32.1
  106  curl -A "Nikto" http://172.16.32.1/\n
  107  nmap -sS -p 80 172.16.32.1\n
  108  nmap -sN -p 80 172.16.32.1\n
  109  nmap -sX -p 80 172.16.32.1\n
  110  printf '\x90\x90\x90\x90\x90\x90' | nc 172.16.32.1 80\n
  111  telnet 172.16.32.1 21\n
  112  nc 172.16.32.1 31337\n
  113  curl http://172.16.32.1/../../../etc/passwd\n
  114  telnet 172.16.32.1 6667\n
  115  (echo "NICK bot123"; echo "USER bot123 0 * :bot") | nc 172.16.32.1
6667\n
  116  history | tail
```

Logi z snorta:

```
06/02/25-14:12:46.917675 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,59316,172.16.32.1,80,28762,,0,alert,Allow
06/02/25-14:12:56.162596 ,1,1000003,1,"BLOCKED: Null Scan
Detected",TCP,172.16.32.254,57001,172.16.32.1,80,20142,,0,alert,Allow
```

```
06/02/25-14:12:56.262709 ,1,1000003,1,"BLOCKED: Null Scan
Detected",TCP,172.16.32.254,57003,172.16.32.1,80,53859,,0,alert,Allow
06/02/25-14:13:02.802919 ,1,1000004,1,"BLOCKED: Xmas Scan
Detected",TCP,172.16.32.254,55633,172.16.32.1,80,941,,0,alert,Allow
06/02/25-14:13:02.902978 ,1,1000004,1,"BLOCKED: Xmas Scan
Detected",TCP,172.16.32.254,55635,172.16.32.1,80,14216,,0,alert,Allow
06/02/25-14:13:13.470221 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,50274,172.16.32.1,80,33290,,0,alert,Allow
06/02/25-14:13:13.470506 ,1,1000005,1,"BLOCKED: NOP Sled (Shellcode)
Detected",TCP,172.16.32.254,50274,172.16.32.1,80,33292,,0,alert,Allow
06/02/25-14:13:24.157371 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21358,,0,alert,Allow
06/02/25-14:13:24.157371 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21358,,0,alert,Allow
06/02/25-14:13:25.159722 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21359,,0,alert,Allow
06/02/25-14:13:25.159722 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21359,,0,alert,Allow
06/02/25-14:13:26.183775 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21360,,0,alert,Allow
06/02/25-14:13:26.183775 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21360,,0,alert,Allow
06/02/25-14:13:27.207614 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21361,,0,alert,Allow
06/02/25-14:13:27.207614 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21361,,0,alert,Allow
06/02/25-14:13:28.231515 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21362,,0,alert,Allow
06/02/25-14:13:28.231515 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21362,,0,alert,Allow
06/02/25-14:13:29.255534 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21363,,0,alert,Allow
06/02/25-14:13:29.255534 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21363,,0,alert,Allow
06/02/25-14:13:31.271781 ,1,1000006,1,"BLOCKED: FTP Connection
Attempt",TCP,172.16.32.254,36064,172.16.32.1,21,21364,,0,alert,Allow
06/02/25-14:13:31.271781 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,36064,172.16.32.1,21,21364,,0,alert,Allow
06/02/25-14:13:39.211300 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10892,,0,alert,Allow
06/02/25-14:13:39.211300 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10892,,0,alert,Allow
06/02/25-14:13:40.232112 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10893,,0,alert,Allow
06/02/25-14:13:40.232112 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10893,,0,alert,Allow
06/02/25-14:13:41.256123 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10894,,0,alert,Allow
06/02/25-14:13:41.256123 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10894,,0,alert,Allow
06/02/25-14:13:42.280290 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
```

```
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10895,,0,alert,Allow
06/02/25-14:13:42.280290 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10895,,0,alert,Allow
06/02/25-14:13:43.304868 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10896,,0,alert,Allow
06/02/25-14:13:43.304868 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10896,,0,alert,Allow
06/02/25-14:13:44.328926 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10897,,0,alert,Allow
06/02/25-14:13:44.328926 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10897,,0,alert,Allow
06/02/25-14:13:46.345070 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10898,,0,alert,Allow
06/02/25-14:13:46.345070 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10898,,0,alert,Allow
06/02/25-14:13:50.504788 ,1,1000007,1,"BLOCKED: Netcat Backdoor Connection
Attempt",TCP,172.16.32.254,60662,172.16.32.1,31337,10899,,0,alert,Allow
06/02/25-14:13:50.504788 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,60662,172.16.32.1,31337,10899,,0,alert,Allow
06/02/25-14:14:09.844453 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,49382,172.16.32.1,80,54462,,0,alert,Allow
06/02/25-14:14:22.932873 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,56748,172.16.32.1,80,50731,,0,alert,Allow
06/02/25-14:14:40.027235 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25393,,0,alert,Allow
06/02/25-14:14:40.027235 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25393,,0,alert,Allow
06/02/25-14:14:41.035377 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25394,,0,alert,Allow
06/02/25-14:14:41.035377 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25394,,0,alert,Allow
06/02/25-14:14:42.059513 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25395,,0,alert,Allow
06/02/25-14:14:42.059513 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25395,,0,alert,Allow
06/02/25-14:14:43.083451 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25396,,0,alert,Allow
06/02/25-14:14:43.083451 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25396,,0,alert,Allow
06/02/25-14:14:44.107513 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25397,,0,alert,Allow
06/02/25-14:14:44.107513 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25397,,0,alert,Allow
06/02/25-14:14:45.131737 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25398,,0,alert,Allow
06/02/25-14:14:45.131737 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25398,,0,alert,Allow
06/02/25-14:14:47.147642 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,43038,172.16.32.1,6667,25399,,0,alert,Allow
06/02/25-14:14:47.147642 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,43038,172.16.32.1,6667,25399,,0,alert,Allow
```

```
06/02/25-14:14:53.869755 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3048,,0,alert,Allow
06/02/25-14:14:53.869755 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3048,,0,alert,Allow
06/02/25-14:14:54.892010 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3049,,0,alert,Allow
06/02/25-14:14:54.892010 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3049,,0,alert,Allow
06/02/25-14:14:55.916047 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3050,,0,alert,Allow
06/02/25-14:14:55.916047 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3050,,0,alert,Allow
06/02/25-14:14:56.940076 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3051,,0,alert,Allow
06/02/25-14:14:56.940076 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3051,,0,alert,Allow
06/02/25-14:14:57.964416 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3052,,0,alert,Allow
06/02/25-14:14:57.964416 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3052,,0,alert,Allow
06/02/25-14:14:58.988306 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3053,,0,alert,Allow
06/02/25-14:14:58.988306 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3053,,0,alert,Allow
06/02/25-14:15:01.004515 ,1,1000010,1,"BLOCKED: IRC Bot Connection
Attempt",TCP,172.16.32.254,37488,172.16.32.1,6667,3054,,0,alert,Allow
06/02/25-14:15:01.004515 ,1,1000002,1,"BLOCKED: Nmap Stealth SYN
Scan",TCP,172.16.32.254,37488,172.16.32.1,6667,3054,,0,alert,Allow
```