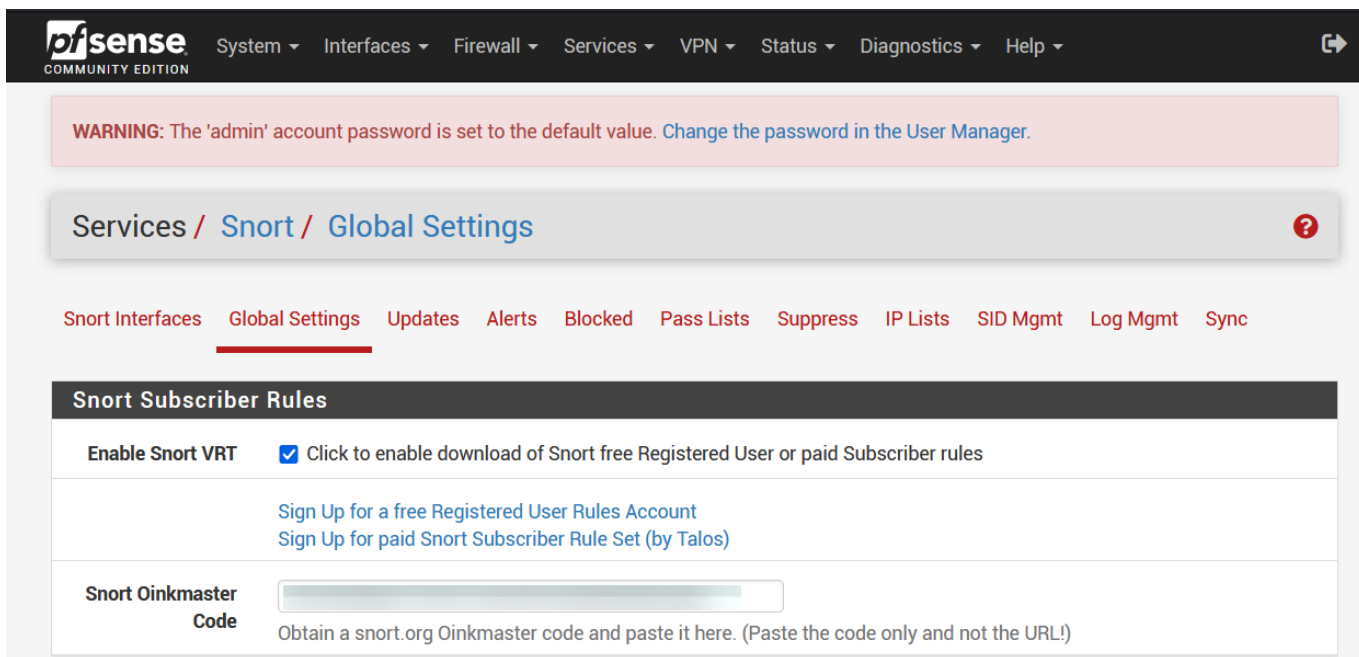


Security: pfSense IDS/IPS Snort

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

1. Konfiguracja kodu OinkCode



2. Wymuszenie aktualizacji zasad

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	<input checked="" type="checkbox"/> Enable interface
Interface	<input type="text" value="WAN2 (hn2)"/> Choose the interface where this Snort instance will inspect traffic.
Description	<input type="text" value="WAN2"/> Enter a meaningful description here for your reference.
Snap Length	<input type="text" value="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
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)

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: ▾
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

[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: Auto-refresh view Alert lines to display.

Alert Log Actions:

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

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