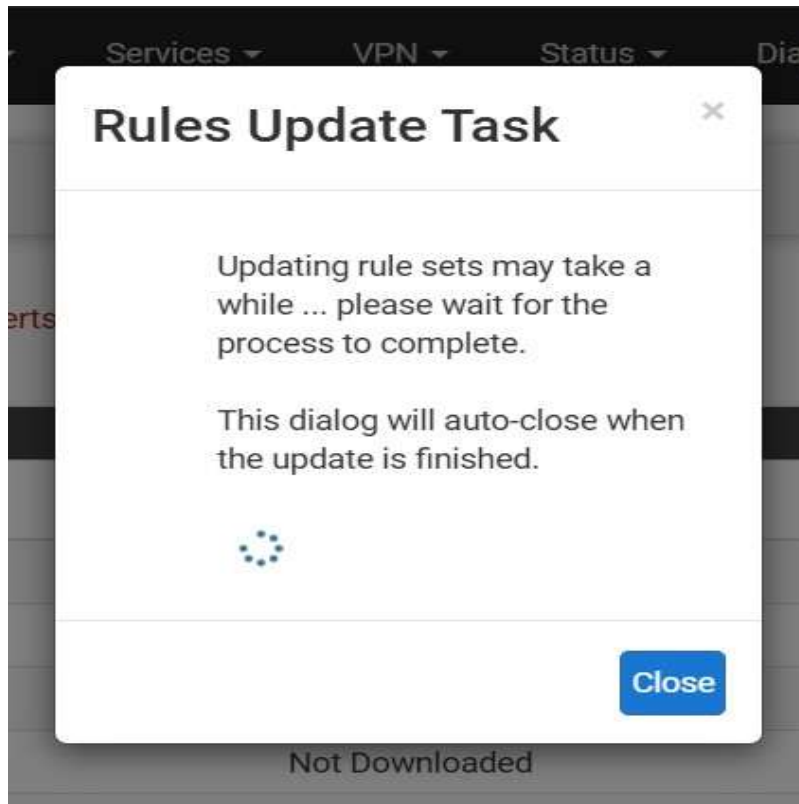
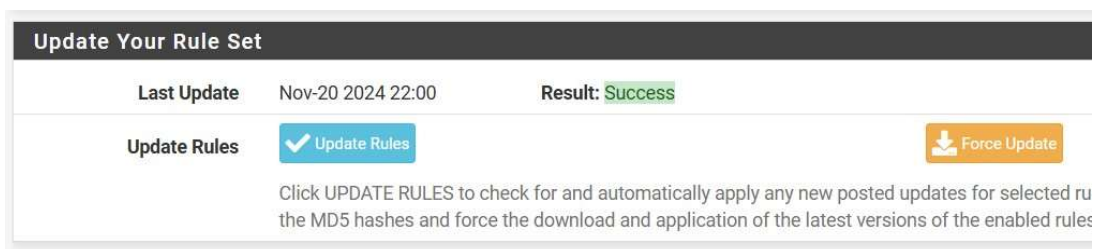


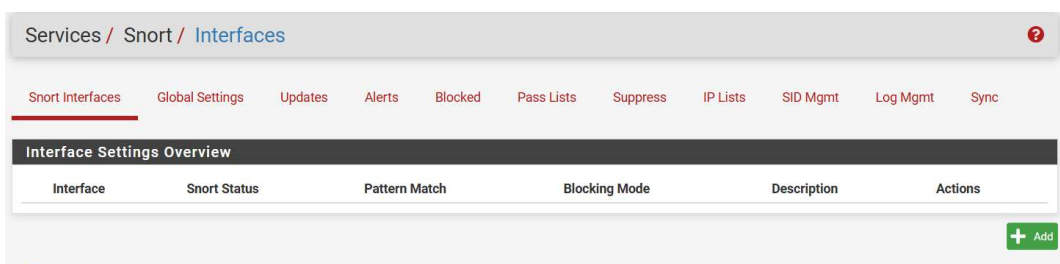
Trong pfSense, mục Services / Snort/ Global Settings Enable một số tính năng như: Snort VRT, Snort GPLv2, ET Open, OpenAppID, FEODO Tracker Botnet C2 IP Rules.



Hình 3. 21. Mạng mạnh thì đợi update rule tầm 5 phút



Hình 3. 22. Kết quả download thành công



Hình 3. 23. Để kích hoạt Snort thì trong Services / Snort / Interfaces chọn Add

- Cấu hình alert trên WAN

The screenshot shows the configuration interface for WAN settings and alerts. It is divided into two main sections: General Settings and Alert Settings.

General Settings

- Enable:** ☒ Enable interface
- Interface:** WAN (em0) [v]
Choose the interface where this Snort instance will inspect traffic.
- Description:** WAN
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.

Alert Settings

- Send Alerts to System Log:** ☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.
- System Log Facility:** LOG_AUTH [v]
Select system log Facility to use for reporting. Default is LOG_AUTH.
- System Log Priority:** LOG_ALERT [v]
Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
- Enable Packet Captures:** ☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
- Enable Unified2 Logging:** ☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.

Hình 3. 24. Chọn cổng WAN và bật tính năng alert

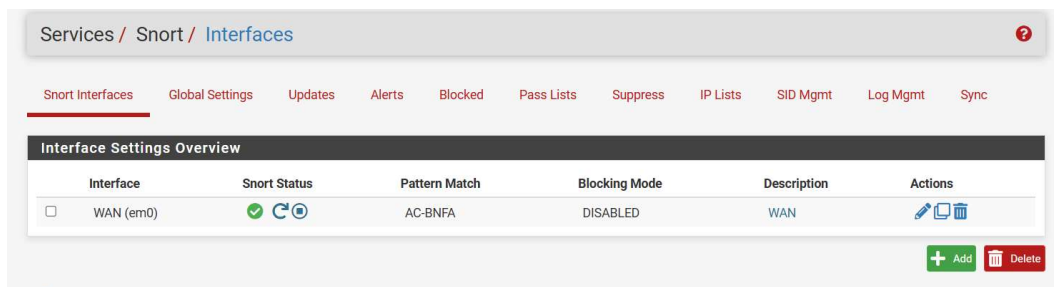
Trong Services / Snort / Interface Settings / WAN – Rules

The screenshot shows the 'WAN - Rules' configuration page in the Snort interface. The breadcrumb trail is 'Services / Snort / Interface Settings / WAN - Rules'. The page has a top navigation bar with tabs: Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. Below this, there is a sub-navigation bar with tabs: WAN Settings, WAN Categories, WAN Rules (selected), WAN Variables, WAN Preprocs, WAN IP Rep, and WAN Logs. The main content area is titled 'Available Rule Categories' and contains a 'Category Selection:' dropdown menu with 'custom.rules' selected. Below the dropdown, it says 'Select the rule category to view and manage.' The bottom section is titled 'Defined Custom Rules' and is currently empty.

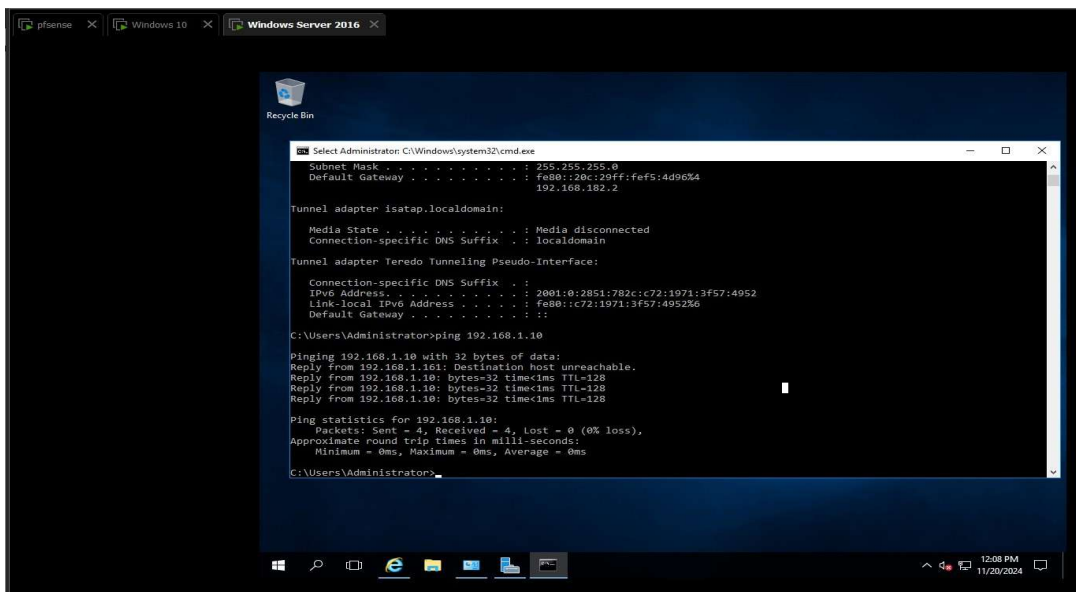
Hình 3. 25. Chọn Category Selection là custom.rules



Hình 3. 26. Tiến hành viết một số rule cơ bản và save



Hình 3. 27 Đảm bảo rằng rule đã được kích hoạt



Hình 3. 28. Ping từ máy attacker

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

4 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-21 03:06:56	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe
2024-11-21 03:06:55	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe
2024-11-21 03:06:54	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe
2024-11-21 03:06:51	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe

Hình 3. 29. Log phát hiện ping

- Cấu hình alert trên LAN

LAN Settings

LAN Categories

LAN Rules

LAN Variables

LAN Preprocs

LAN IP Rep

LAN Logs

General Settings

Enable

☒ Enable interface

Interface

LAN (em1)

Choose the interface where this Snort instance will inspect traffic.

Description

LAN

Enter a meaningful description here for your reference.

Snap Length

1518

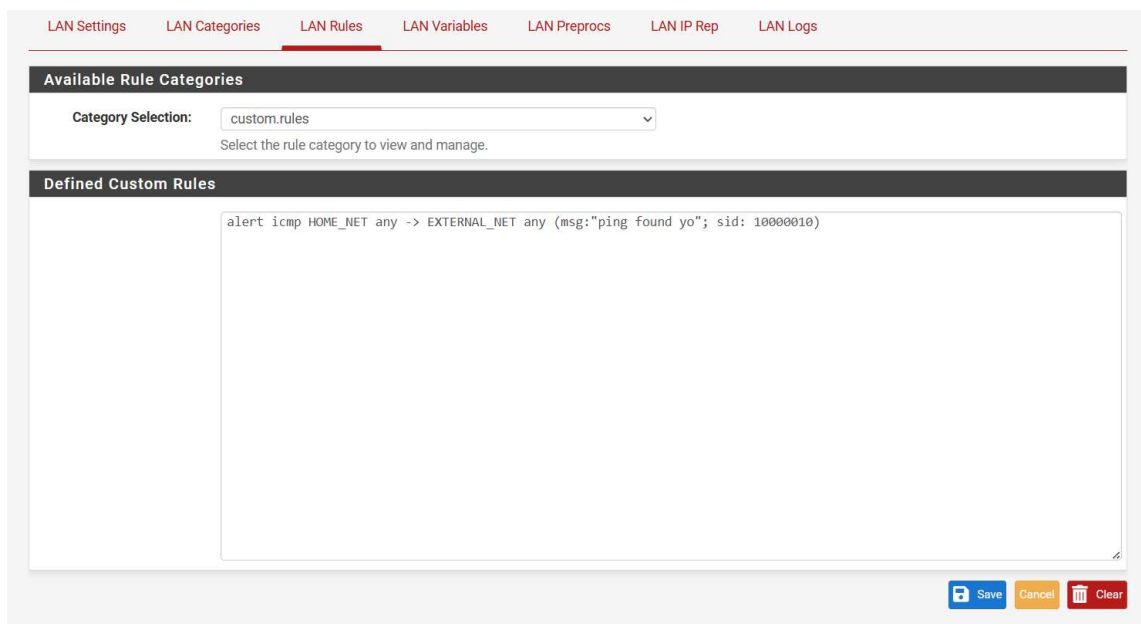
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings






Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Hình 3. 30. Chọn cổng LAN và bật tính năng alert



Hình 3. 31. Viết rule custom

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)	 	AC-BNFA	DISABLED	WAN	 
<input type="checkbox"/> LAN (em1)	 	AC-BNFA	DISABLED	LAN	 

Hình 3. 32. Kích hoạt rule

```

C:\Users\Ngoc Dai>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=57ms TTL=128
Reply from 8.8.8.8: bytes=32 time=56ms TTL=128
Reply from 8.8.8.8: bytes=32 time=56ms TTL=128
Reply from 8.8.8.8: bytes=32 time=57ms TTL=128

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 57ms, Average = 56ms

C:\Users\Ngoc Dai>

```

Hình 3. 33. Tiến hành ping

Alert Log View Settings

Interface to Inspect

LAN (em1)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

5 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-21 01:04:33		0			fe80::20c:29ff:fef5:4d96 Q		ff02::1 Q		1:10000010 	ping found yo
2024-11-21 01:03:12		0	ICMP		192.168.1.10 Q		8.8.8.8 Q		1:10000010 	ping found yo
2024-11-21 01:03:11		0	ICMP		192.168.1.10 Q		8.8.8.8 Q		1:10000010 	ping found yo
2024-11-21 01:03:10		0	ICMP		192.168.1.10 Q		8.8.8.8 Q		1:10000010 	ping found yo
2024-11-21 01:03:09		0	ICMP		192.168.1.10 Q		8.8.8.8 Q		1:10000010 	ping found yo

Hình 3. 34. Phát hiện trên log