

Mục tiêu Lab:

- Cài đặt và cấu hình hệ thống IDS/IPS trên pfSense bằng Snort hoặc Suricata.
- Phát hiện các hành vi tấn công mạng.
- Ngăn chặn các tấn công dựa trên luật cảnh báo.

Giới thiệu ngắn:

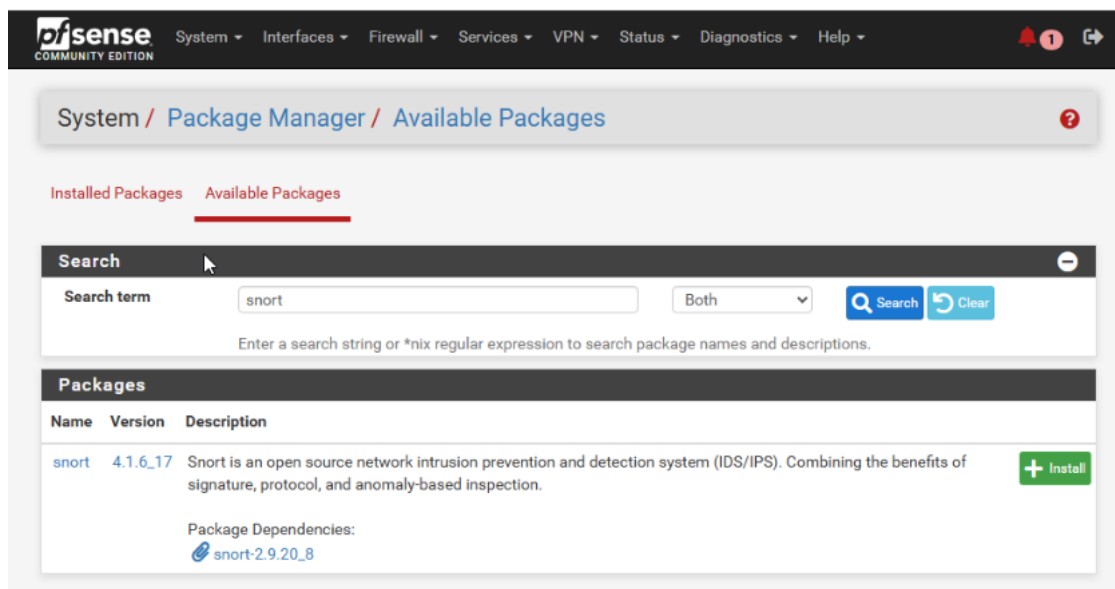
- **IDS (Intrusion Detection System):** Hệ thống phát hiện xâm nhập, cảnh báo khi phát hiện hành vi khả nghi.
- **IPS (Intrusion Prevention System):** Hệ thống ngăn chặn xâm nhập, ngoài việc phát hiện còn chủ động chặn tấn công.
- **pfSense:** Firewall/router mã nguồn mở, hỗ trợ cài đặt IDS/IPS rất tiện lợi với các package Snort hoặc Suricata.

Bước 1: Chuẩn bị môi trường

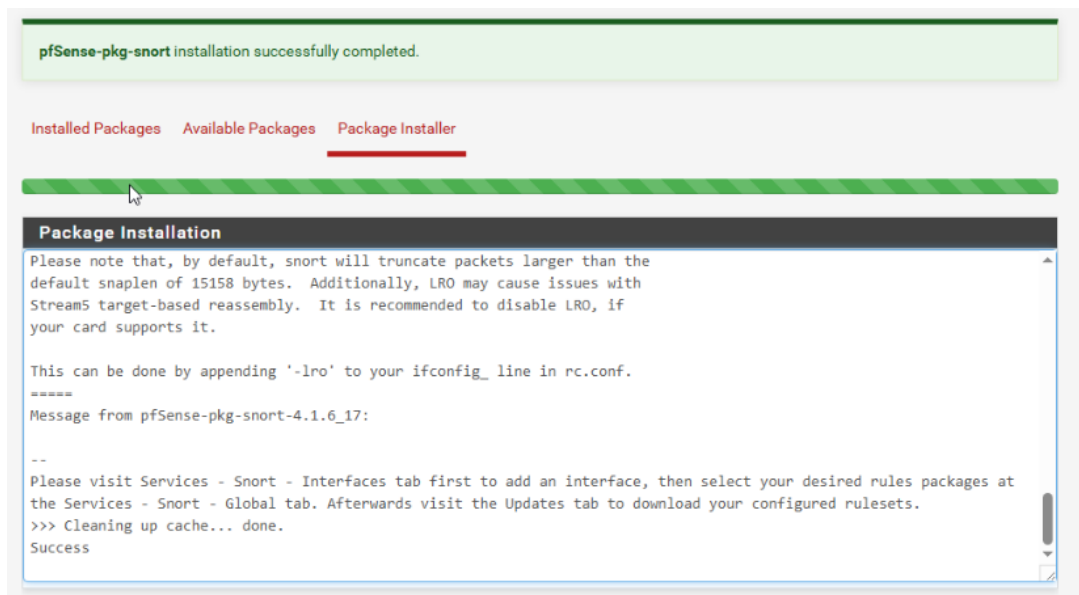
- Máy chủ cài pfSense, có kết nối mạng.
- Đảm bảo pfSense đã được cập nhật mới nhất.
- Truy cập giao diện quản trị pfSense.

Bước 2: Cài đặt Snort package trên pfSense

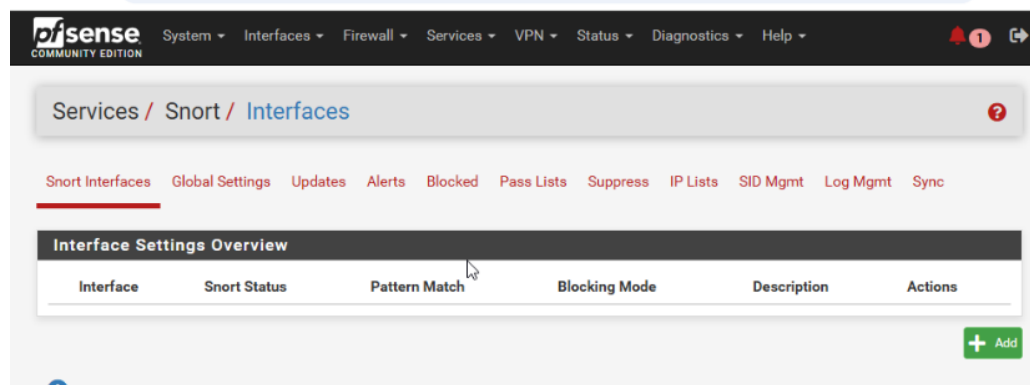
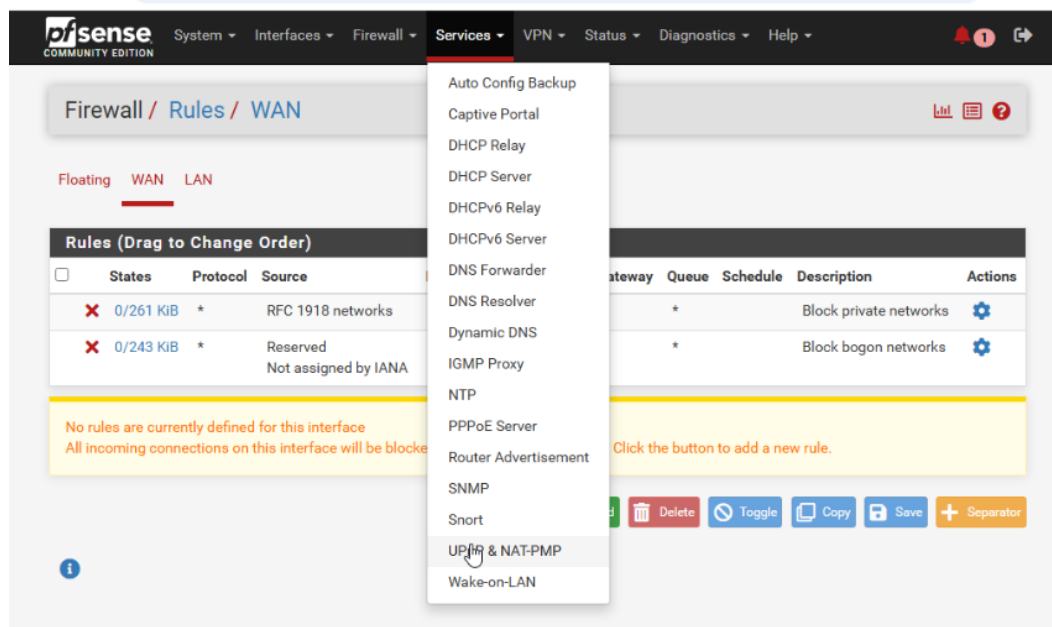
1. Đăng nhập vào pfSense qua trình duyệt (ví dụ: <https://ip-pfsense>).
2. Vào **System > Package Manager > Available Packages**.
3. Tìm **Snort** trong danh sách.



4. Nhấn **Install** rồi chờ pfSense tải về và cài Snort.



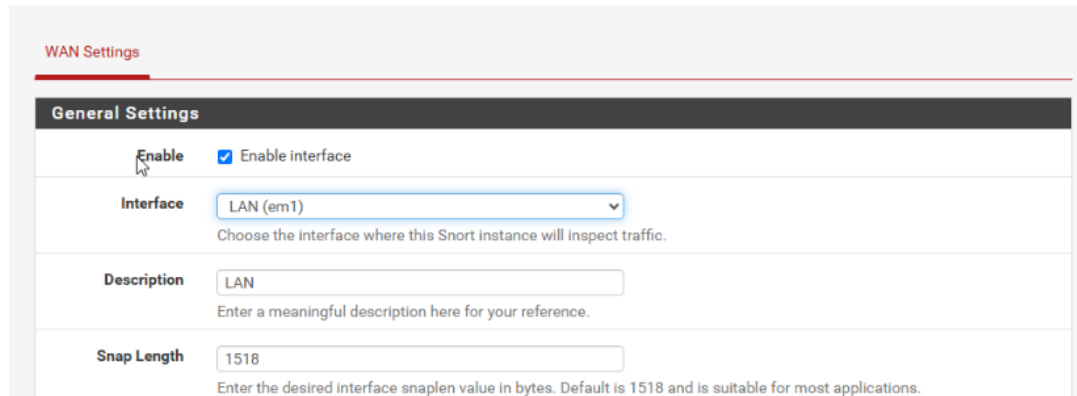
5. Sau khi cài xong, bạn sẽ thấy menu mới **Services > Snort** xuất hiện.



Cấu hình Snort giám sát LAN, cảnh báo ping tới IP cụ thể trên pfSense

Bước 1: Thêm interface LAN vào Snort

1. Đăng nhập pfSense, vào **Services > Snort > Interfaces**.
2. Nhấn + **Add** để thêm interface mới.



The screenshot shows the 'WAN Settings' tab in pfSense, specifically the 'General Settings' section for Snort. It includes fields for 'Interface' (set to LAN (em1)), 'Description' (set to LAN), and 'Snap Length' (set to 1518). There are also checkboxes for 'Enable' and 'Enable interface'.

WAN Settings

General Settings

Enable ☒ Enable interface

Interface LAN (em1)
Choose the interface where this Snort instance will inspect traffic.

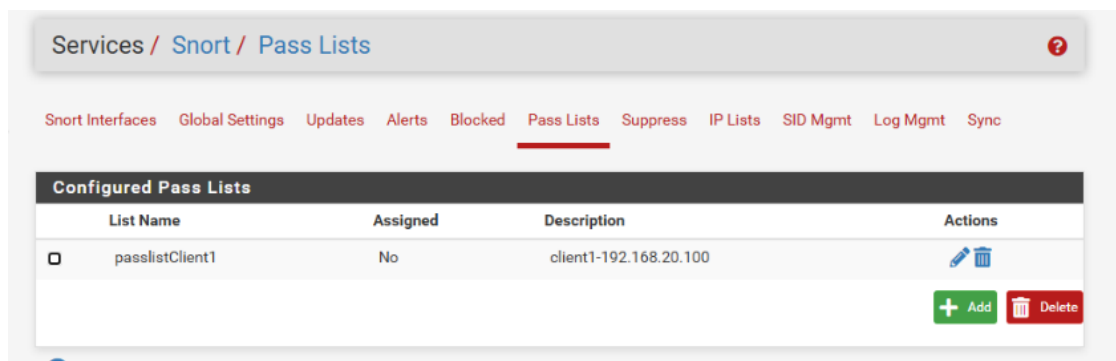
Description LAN
Enter a meaningful description here for your reference.

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

3. Chọn interface LAN.
4. Nhấn **Save**.

Bước 2: Cấu hình interface LAN cho Snort

1. Vào tab interface LAN mới tạo.
2. Tick **Enable Snort on this interface**.
3. **Home Net**: nhập dải mạng LAN của bạn, ví dụ 192.168.20.100/24.



The screenshot shows the 'Services / Snort / Pass Lists' page in pfSense. It displays a table of 'Configured Pass Lists' with columns for List Name, Assigned, Description, and Actions. A single entry 'passlistClient1' is shown with 'Assigned' set to 'No' and 'Description' set to 'client1-192.168.20.100'. There are 'Add' and 'Delete' buttons at the bottom right.

Services / Snort / Pass Lists

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

Configured Pass Lists

List Name	Assigned	Description	Actions
<input type="checkbox"/> passlistClient1	No	client1-192.168.20.100	

+ Add Delete

Trong PassList tạo một danh sách IP mà chúng ta cần theo dõi

General Information

Name

passlistClient1

The list name may only consist of the characters 'a-z, A-Z, 0-9 and _'.

Description

client1-192.168.20.100

You may enter a description here for your reference.

Auto-Generated IP Addresses

Local Networks

☒

Add firewall Locally-Attached Networks to the list (excluding WAN). Default is Checked.

WAN Gateways

☒

Add WAN Gateways to the list. Default is Checked.

WAN DNS Servers

☒

Add WAN DNS servers to the list. Default is Checked.

Virtual IP Addresses

☒

Add Virtual IP Addresses to the list. Default is Checked.

VPN Addresses

☒

Add VPN Addresses to the list. Default is Checked.

Custom IP Addresses and Configured Firewall Aliases

Hint

Enter as many IP addresses or alias names as desired. Enter ONLY an IP address, IP subnet or alias. FQDN (fully qualified domain name) directly! To use a FQDN, first create the necessary firewall alias, alias name here. FQDN aliases are periodically re-resolved and updated by the firewall. You can also with a proper netmask of the form network/mask such as 1.2.3.0/24.

IP or Alias

192.168.20.100

Delete

Save

Add IP

Choose the Networks Snort Should Inspect and Whitelist

Home Net

default

View List

Choose the Home Net you want this interface to use.

Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.

Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net

default

View List

Choose the External Net you want this interface to use.

External Net is networks that are not Home Net. Most users should leave this setting at default.

Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

"Choose the Networks Snort Should Inspect and Whitelist" – là nơi cấu hình mạng nào Snort sẽ **giám sát (inspect)** và **bỏ qua (whitelist)**.

Cụ thể:

1. Home Net

- **Ý nghĩa:** Đây là mạng nội bộ (local network) mà bạn muốn Snort giám sát, thường là mạng LAN.
- **Mặc định:** default – bao gồm các địa chỉ nội bộ như:
 - IP của LAN
 - IP của VPN, VIPs (Virtual IPs)
 - Gateway
 - WAN IP nếu cần
- **Mục đích:** Những địa chỉ này được coi là "đáng tin cậy". Snort sẽ kiểm tra các lưu lượng đến/từ các mạng này để phát hiện tấn công.

- **Tùy chọn nâng cao:** Bạn có thể tạo **Alias** để định nghĩa rõ dải IP nào là “Home Net” nếu không muốn dùng mặc định.

2. External Net

- **Ý nghĩa:** Đây là các mạng bên ngoài (Internet hoặc các mạng không thuộc Home Net).
- **Mặc định:** default – là **tất cả mạng không nằm trong Home Net**.
- **Mục đích:** Đây là nơi Snort xem là “không tin cậy”, thường là nguồn gốc của các tấn công hoặc lưu lượng nghi vấn.
- **Lưu ý:** Nếu bạn có danh sách IP ngoài mà bạn muốn tin tưởng (bỏ qua kiểm tra), bạn có thể:
 - Tạo một **Pass List**
 - Tạo một **Alias**
 - Gán Pass List đó cho External Net để tránh báo động sai (false positive).

Choose the Networks Snort Should Inspect and Whitelist

Home Net passlistClient1 View List
 Choose the Home Net you want this interface to use.
 Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.
 Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net default View List
 Choose the External Net you want this interface to use.
 External Net is networks that are not Home Net. Most users should leave this setting at default.
 Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

4. Nếu bạn chỉ muốn cảnh báo (không block), **không tick IPS mode**.

Block Settings

Block Offenders ☐ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

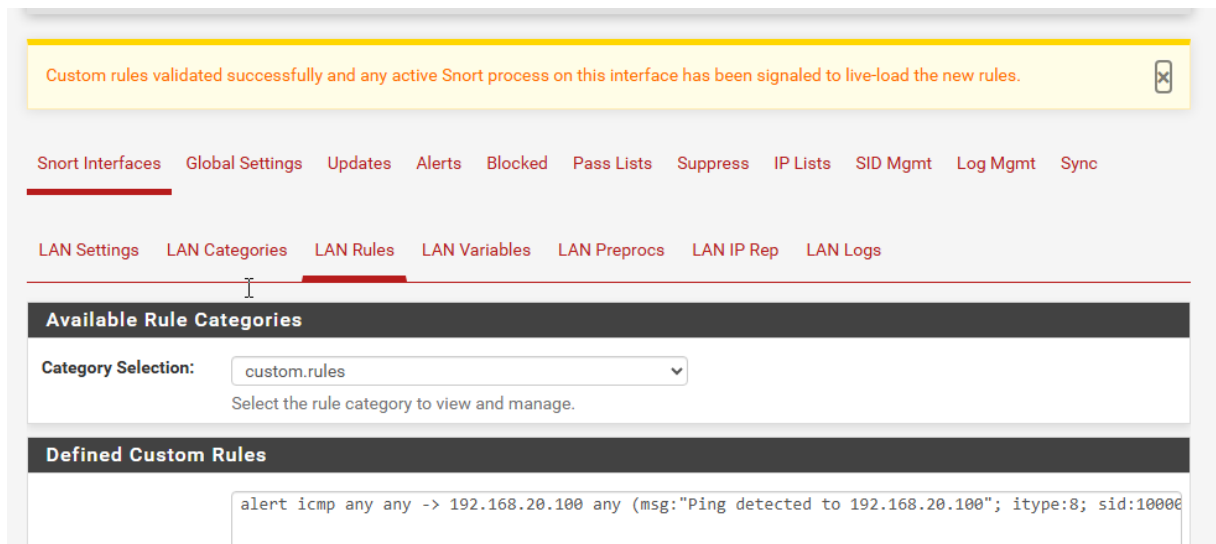
5. Nhấn **Save**.

Bước 3: Tạo rule Snort cảnh báo khi có ping tới IP 192.168.20.100

Snort dựa trên rule, bạn có thể tạo rule tùy chỉnh để cảnh báo gói tin ICMP Echo Request tới IP này.

1. Vào **Services > Snort > Interfaces**, chọn interface LAN.
2. Chuyển sang tab **Custom Rules**.
3. Thêm rule sau:

```
alert icmp any any -> 192.168.20.100 any (msg:"Ping detected to 192.168.20.100";
itype:8; sid:1000001; rev:1;)
```

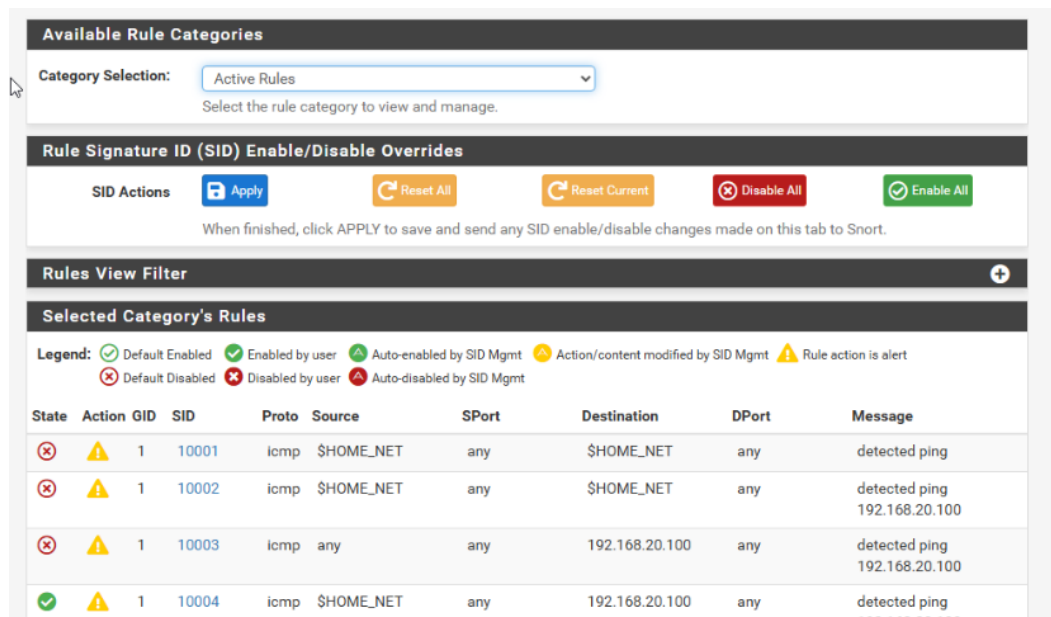


Giải thích:

- alert — tạo cảnh báo (alert).
- icmp — loại giao thức ICMP.
- any any — từ bất kỳ IP và port nguồn nào.
- -> 192.168.20.100 any — đến IP 192.168.20.100 với bất kỳ cổng nào (ICMP không có cổng).
- msg:"Ping detected to 192.168.20.100" — tin nhắn cảnh báo.
- itype:8 — chỉ loại ICMP Echo Request (ping).
- sid:1000001 — ID rule tự đặt, nên dùng số lớn để tránh trùng.
- rev:1 — revision của rule.

4. Nhấn **Save** để lưu rule.

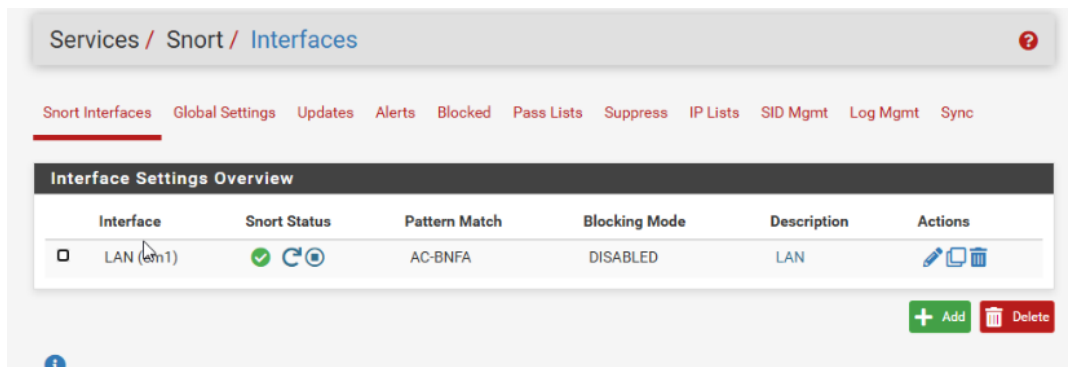
Bước 4: check active rule



Cấu hình Categories cân nhắc bật tắt rules phù hợp với nhu cầu

Bước 5: Khởi động lại Snort interface LAN

- Vào tab interface LAN, nhấn **Restart Snort** hoặc **Start Snort** nếu chưa chạy.



Bước 6: Kiểm tra hoạt động

- Từ một máy khác trong mạng LAN hoặc ngoài mạng LAN, thực hiện ping tới 192.168.20.100:

#ping 192.168.20.100

- Vào pfSense, menu **Services > Snort > Alerts**.
- Bạn sẽ thấy log cảnh báo có nội dung Ping detected to 192.168.20.100 xuất hiện khi máy khác gửi ping tới IP đó.

Lưu ý

- Rule này chỉ cảnh báo, không chặn (alert).
- Nếu muốn chặn ping, bạn có thể bật IPS mode và thay alert thành drop hoặc reject trong rule, nhưng nhớ kỹ test kỹ vì có thể gây gián đoạn.
- Đảm bảo rule tùy chỉnh không bị ghi đè khi cập nhật rule Snort.

Đặc biệt

🔗 Snort "nghe" ở đâu trên pfSense?

➤ Snort bắt gói tại cấp độ interface layer 3 (IP layer):

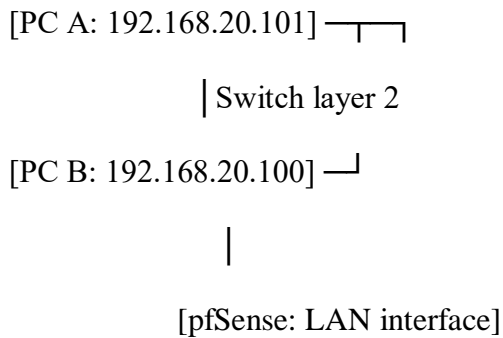
- Nó **không** hoạt động như một proxy hay chặn ở tầng ứng dụng (layer 7).
- Snort lắng nghe gói tin **trước khi** firewall rule xử lý hoặc **sau khi** gói tin vào hệ thống — tùy cấu hình và mô hình mạng.

☐ Gán Snort cho interface nào thì nó bắt gói ở đó:

Ví dụ:

Interface	Địa chỉ IP	Mô tả
WAN	DHCP	Nhận gói tin từ Internet vào
LAN	192.168.1.1	Giao tiếp nội bộ với người dùng
DMZ	172.16.0.1	Dành cho server công khai

🔗 Vấn đề: Switch chuyển tiếp nội bộ — bypass pfSense hoàn toàn



➡ Khi 2 máy trong cùng mạng LAN ping nhau, gói ICMP chỉ đi qua switch, không hề đi qua pfSense.

➡ Do đó, Snort chạy trên interface pfSense **KHÔNG** nhìn thấy gói tin, và rule không bao giờ khớp.

✅ Kết luận:

✓ Snort không thể phát hiện traffic nội bộ giữa 2 máy trong cùng subnet nếu traffic không đi qua router (pfSense).

🔗 Vấn đề cốt lõi nằm ở LAYER 2:

📁 Giao tiếp giữa 2 máy trong cùng subnet (same /24):

Giả sử:

PC A: 192.168.20.101

PC B: 192.168.20.100

Khi A ping B:

- A thấy B thuộc **cùng mạng** → Gửi gói ICMP trực tiếp qua switch
- Switch L2 chuyển tiếp gói từ A → B **mà không qua pfSense**

🔍 Snort trên pfSense không nhìn thấy gói này, vì nó nằm ngoài dòng truyền gói.



[Switch] —> [PC B]

|

[pfSense]