NT534 – AN TOÀN MẠNG MÁY TÍNH NÂNG CAO

BÁO CÁO THỰC HÀNH LAB 4

Xây dựng hệ thống giám sát mạng với PfSense và Splunk

***

THÔNG TIN CHUNG

1. Tên nhóm

STT	Họ và tên	MSSV	Email
1	Dương Phạm Huy Thông	22521431	22521431@gm.uit.edu.vn

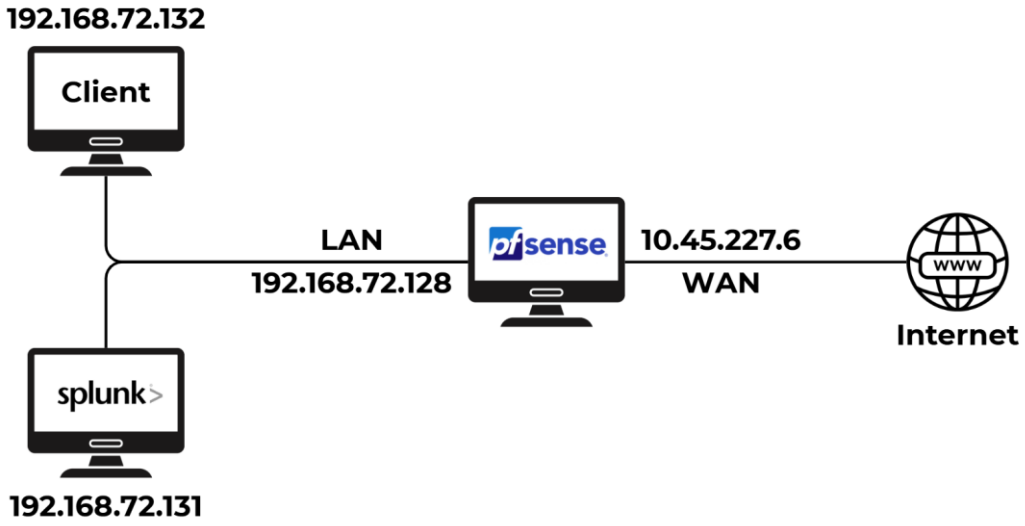
---

2. Nội dung thực hiện

STT	Nội dung	Tự đánh giá	Phụ trách
1	Phần 1	Done	
2	Phần 2	Done	

Bên dưới đây là toàn bộ bài báo cáo chi tiết đã được nhóm thực hiện.

Mô hình sau được sử dụng trong cả bài thực hành:



BÀI LÀM

I. YÊU CẦU 1. CẤU HÌNH CHUNG

- Thực hiện cấu hình pfSense theo hướng dẫn của bài lab

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.45.227.6/16
 LAN (lan)       -> em1        -> v4/DHCP4: 192.168.72.128/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell
```

+ Trong đó nếu chưa có địa chỉ IP cho cả WAN và LAN thì phải thực hiện setting thông qua lựa chọn **2) Set interface(s) IP address.**

+ Nếu chưa cấu hình chọn interface cho WAN và LAN thực hiện chọn **1) Assign Interfaces.**

- Đảm bảo các máy **Client** và **Splunk** có cùng lớp mạng với địa chỉ **LAN.**

- Đối với các máy còn lại (**Client** và **Splunk**) thực hiện cấu hình thêm về địa chỉ IP của default gateway để có thể kết nối thông qua cổng LAN của pfSense.

- Thực hiện cấu hình thông qua file cấu hình **netplan** (/etc/netplan/01-network-manager-all.yaml)

+ Với máy Client:

```
 GNU nano 7.2                    /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  ethernets:
    ens33:
      addresses:
        - 192.168.72.132/24
      routes:
        - to: default
          via: 192.168.72.128
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
```

+ Với máy Splunk

```
 GNU nano 7.2                          /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  ethernets:
    ens33:
      addresses:
        - 192.168.72.131/24
      routes:
        - to: default
          via: 192.168.72.128
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
```

- Sau khi chỉnh sửa xong file cấu hình, thực hiện cấu quyền (***chmod 600***) file cấu hình. Thực hiện chạy lệnh **sudo netplan apply.**

- Kiểm tra lại thông qua lệnh **ping** đến 8.8.8.8 và google.com

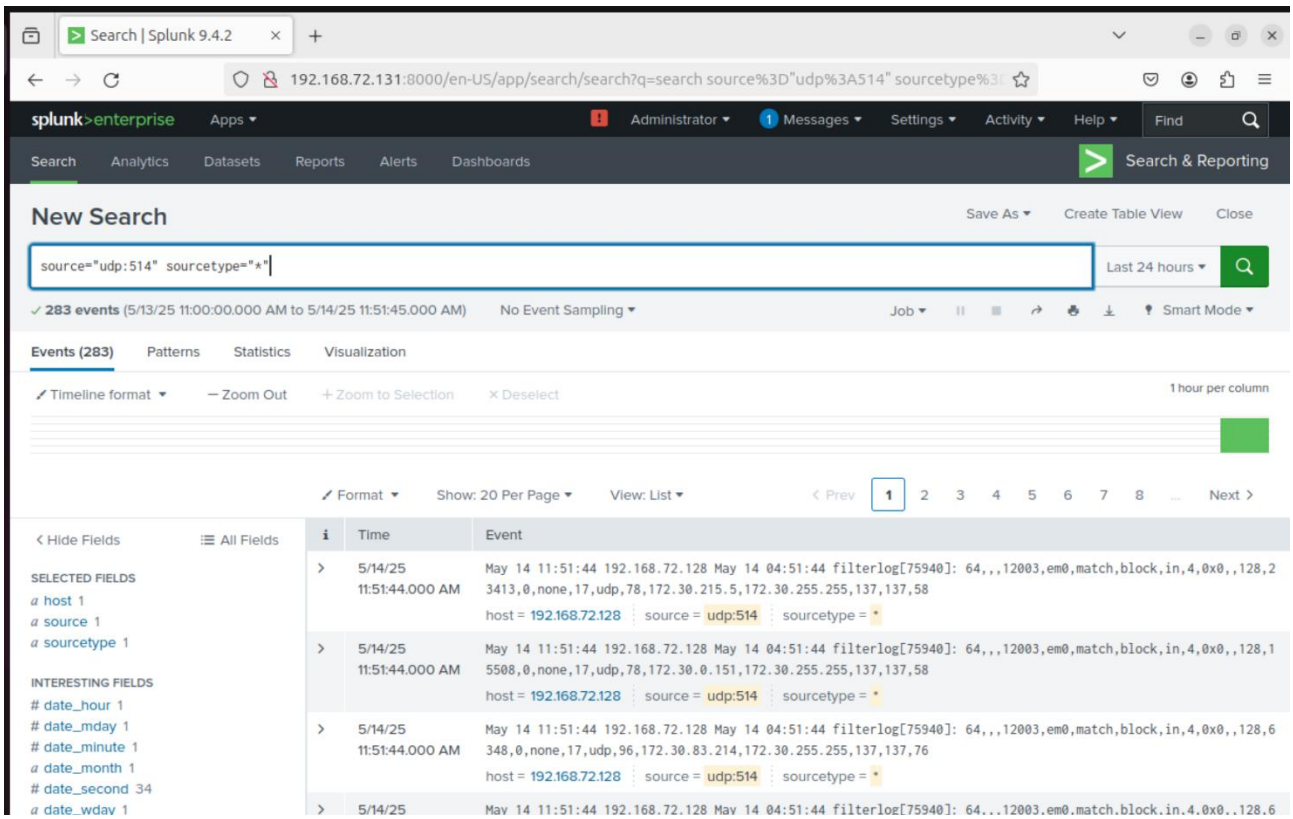
+ Trên máy Client:

```
^Chytong@hytong:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=141 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=59.1 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 59.129/105.187/140.711/34.128 ms
hytong@hytong:~$ ping google.com
PING google.com (74.125.68.113) 56(84) bytes of data.
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=1 ttl=106 time=58.6 ms
64 bytes from sc-in-f113.1e100.net (74.125.68.113): icmp_seq=2 ttl=109 time=89.5 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 58.556/74.043/89.531/15.487 ms
```

+ Trên máy Splunk:

```
hytong@hytong:~/Desktop$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=55.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=51.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=40.4 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 40.388/49.148/55.668/6.436 ms
hytong@hytong:~/Desktop$ ping google.com
PING google.com (142.250.199.78) 56(84) bytes of data.
64 bytes from nchkgb-ai-in-f14.1e100.net (142.250.199.78): icmp_seq=1 ttl=113 time=70.3 ms
64 bytes from nchkgb-ai-in-f14.1e100.net (142.250.199.78): icmp_seq=2 ttl=114 time=137 ms
64 bytes from nchkgb-ai-in-f14.1e100.net (142.250.199.78): icmp_seq=3 ttl=114 time=62.2 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 62.170/89.683/136.612/33.348 ms
```

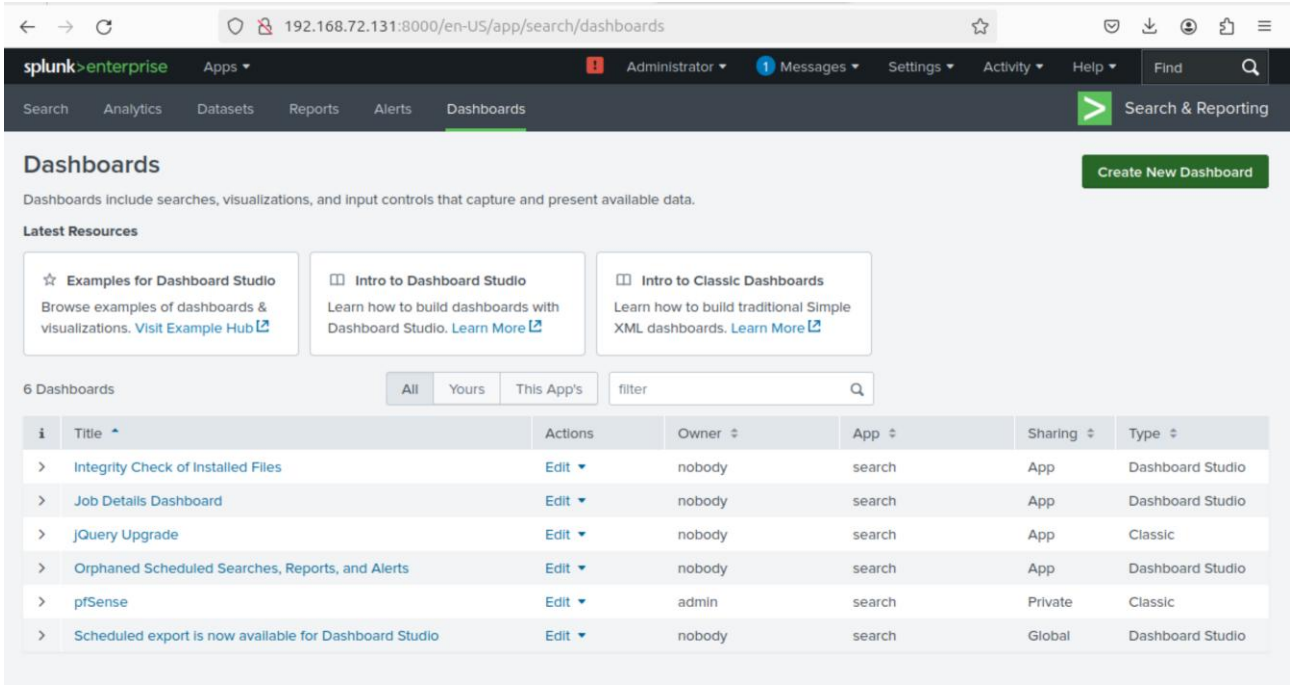
- Sau khi thực hiện cấu hình như hướng dẫn để có thể đổ log từ pfSense về Splunk, ta thực hiện kiểm tra lại cấu hình:



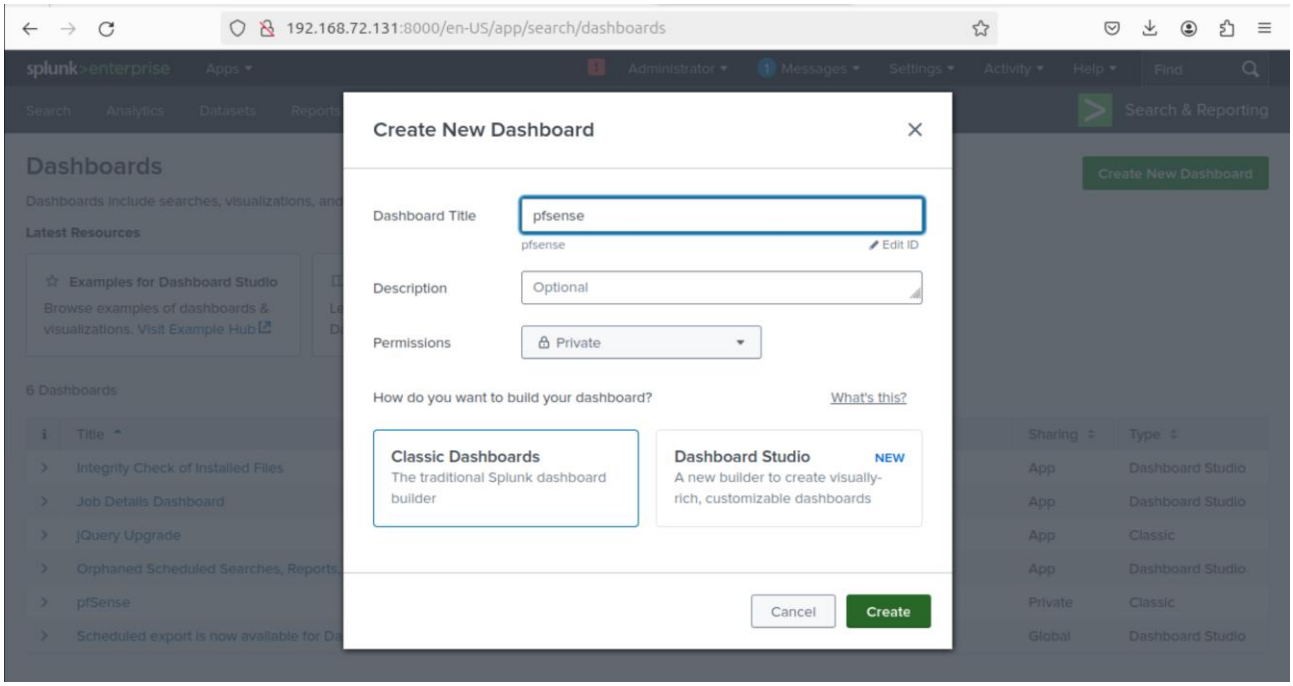
II. YÊU CẦU 2.

a. Tạo Dashboard đơn giản

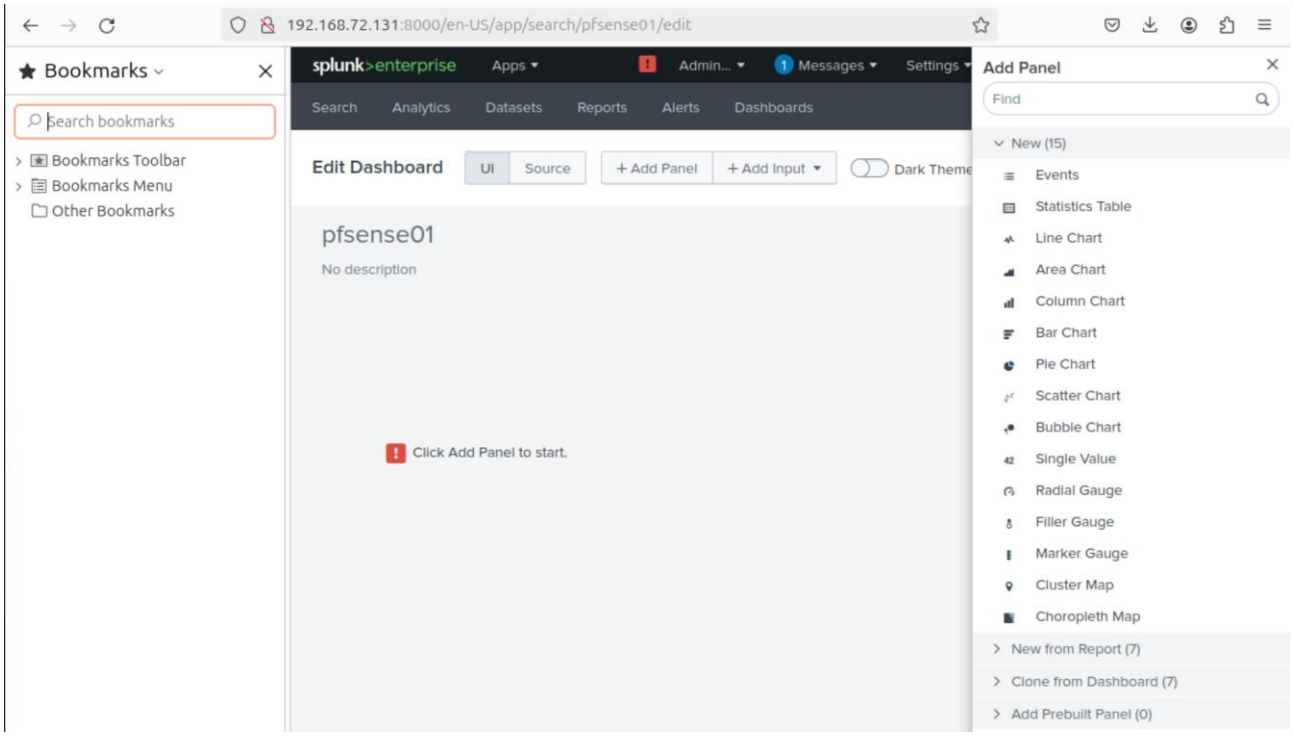
- Trong Splunk Dashboard, thực hiện chọn vào phần **Search and Report**, sau đó chọn vào tùy chọn **Dashboards**. Tại đây chọn **Create New Dashboard**



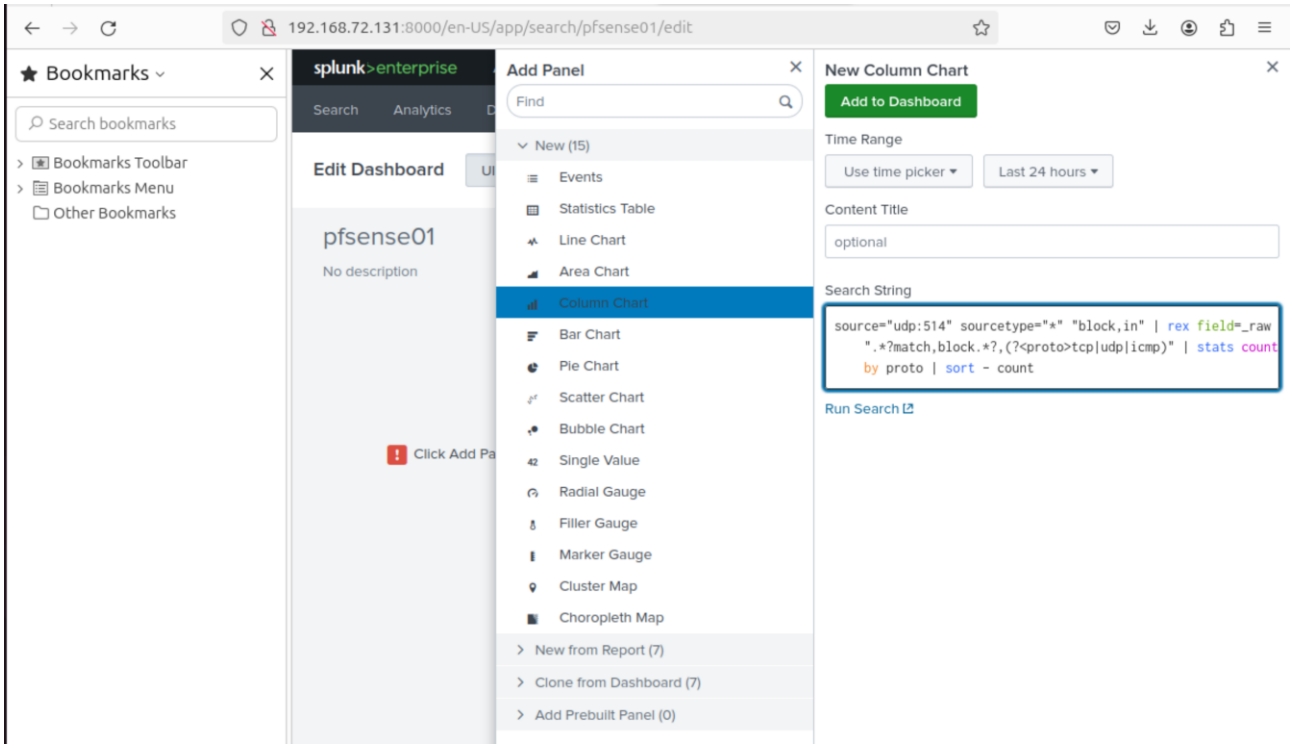
- Tiếp đó thực hiện điền tên mong muốn dành cho Dashboard, chọn **Classic Dashboard** (hoặc các lựa chọn khác tùy vào nhu cầu). Sau đó chọn **Create**.



- Tiếp theo, với mỗi một câu lệnh search, ta thực hiện chọn **Add Panel**, sẽ có một bảng lựa chọn để chọn hình thức hiển thị



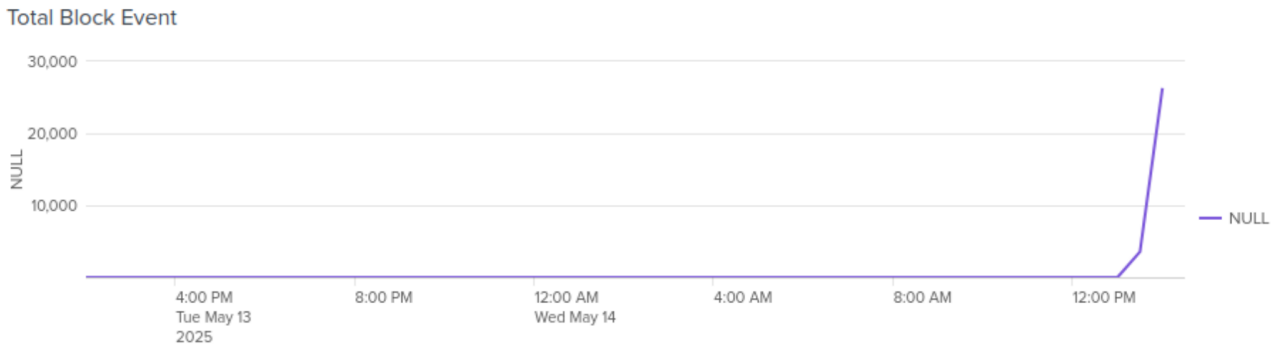
- Sau khi chọn hình thức biểu thị kết quả tìm kiếm, ta thực hiện điền câu truy vấn để tìm kiếm thông tin trên log. Để đảm bảo câu truy vấn thực hiện đúng theo yêu cầu, có thể lựa chọn **Run Search** để kiểm tra kết quả trả về trước khi tạo Panel.



b. Đề xuất các yêu cầu để xây dựng Dashboard đơn giản

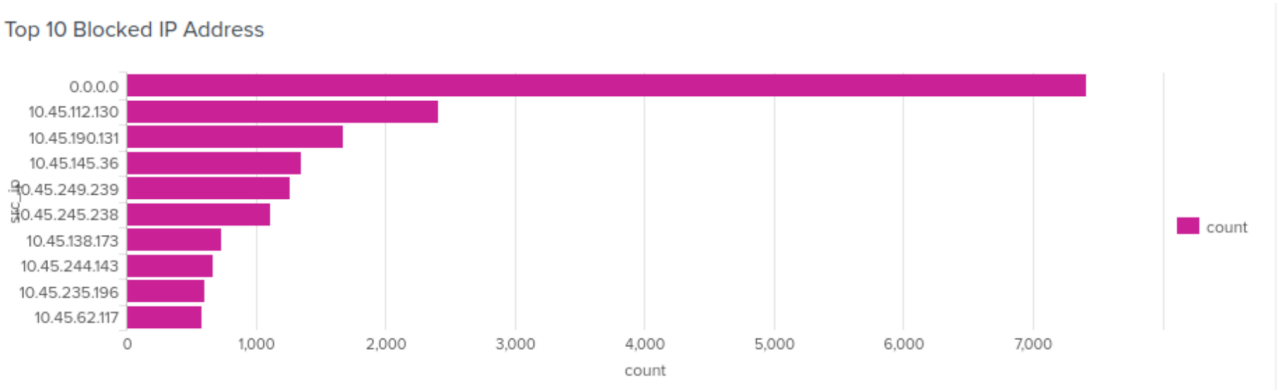
- **Panel 1:** Tổng số sự kiện block theo thời gian (sử dụng **line chart**)

```
source="udp:514" sourcetype="*" "match, block"
| timechart count by src_ip
```



- **Panel 2:** Top địa chỉ IP nguồn bị block nhiều nhất (sử dụng **bar chart**)

```
source="udp:514" sourcetype="*" "match, block"
| stats count by src_ip
| sort -count
| head 10
```



- **Panel 3:** Bảng chi tiết các log block (sử dụng **Statistics Table**)

```
source="udp:514" sourcetype="*" "match, block"
| rex field=_raw "match,
lock.*?(\d+,\d+,\w+),.*?(?<src_ip>\d+\.\d+\.\d+\.\d+),(?<dst_ip>\d
+\.\d+\.\d+\.\d+),(?<proto>\d+),(?<src_port>\d+),(?<dst_port>\d+)"
| table _time src_ip dst_ip proto src_port dst_port
```

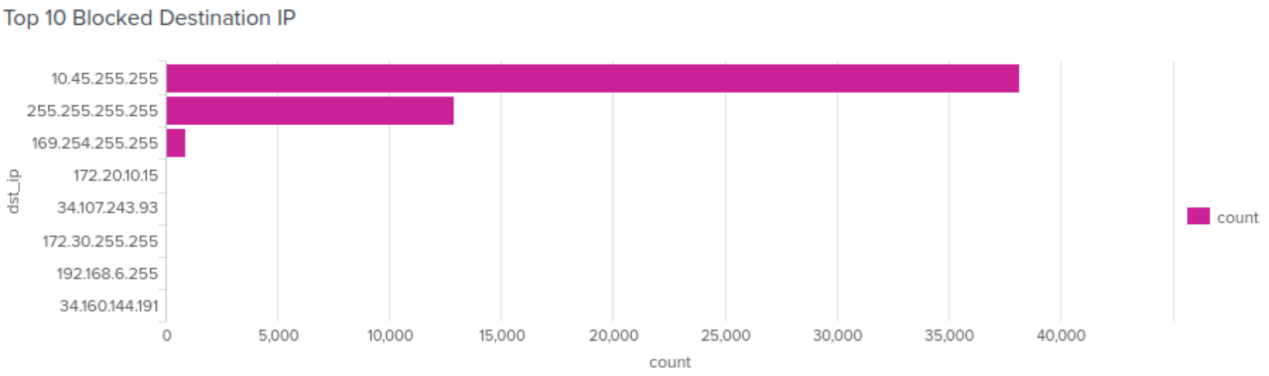
Table All Block Information

_time	src_ip	dst_ip	proto	src_port	dst_port
2025-05-14 14:26:29	0.0.0.0	255.255.255.255	68	67	310
2025-05-14 14:26:29	10.45.138.173	10.45.255.255	137	137	58
2025-05-14 14:26:29	0.0.0.0	255.255.255.255	68	67	308
2025-05-14 14:26:29	10.45.112.130	10.45.255.255	137	137	58
2025-05-14 14:26:29	10.45.75.58	10.45.255.255	27036	27036	49
2025-05-14 14:26:29	10.45.75.58	10.45.255.255	27036	27036	171
2025-05-14 14:26:29	10.45.141.119	10.45.255.255	53765	137	58
2025-05-14 14:26:29	10.45.77.142	10.45.255.255	137	137	76
2025-05-14 14:26:29	10.45.77.142	10.45.255.255	137	137	76
2025-05-14 14:26:29	0.0.0.0	255.255.255.255	68	67	310

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

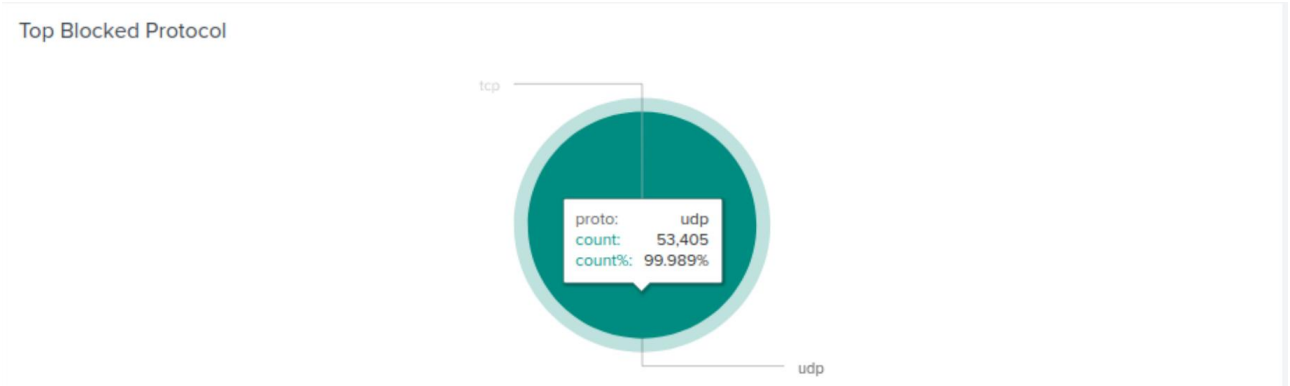
- **Panel 4:** Top 10 Destination IP bị chặn nhiều nhất (sử dụng **Bar char**)

```
source="udp:514" sourcetype="*" "match, block"
| rex field=_raw ".*?match,
block.*?,udp,(?<src_ip>\d+\.\d+\.\d+\.\d+),(?<dst_ip>\d+\.\d+\.\
d+\.\d+)"
| stats count by dst_ip
| sort -count
| head 10
```



- **Panel 5:** Thống kê loại giao thức bị chặn (sử dụng **Pie char**)

```
source="udp:514" sourcetype="*" "match, block"
| rex field=_raw ".*?match, block.*?,(?<proto>tcp|udp|icmp)"
| stats count by proto
| sort -count
```



- Tổng hợp báo cáo được in ra file PDF đính kèm.

--Hết--