BÁO CÁO LAB 5

Xây dựng hệ thống giám sát mạng với PfSense và Splunk

Môn: An toàn mạng máy tính nâng cao

GVTH: Đỗ Thị Phương Uyên

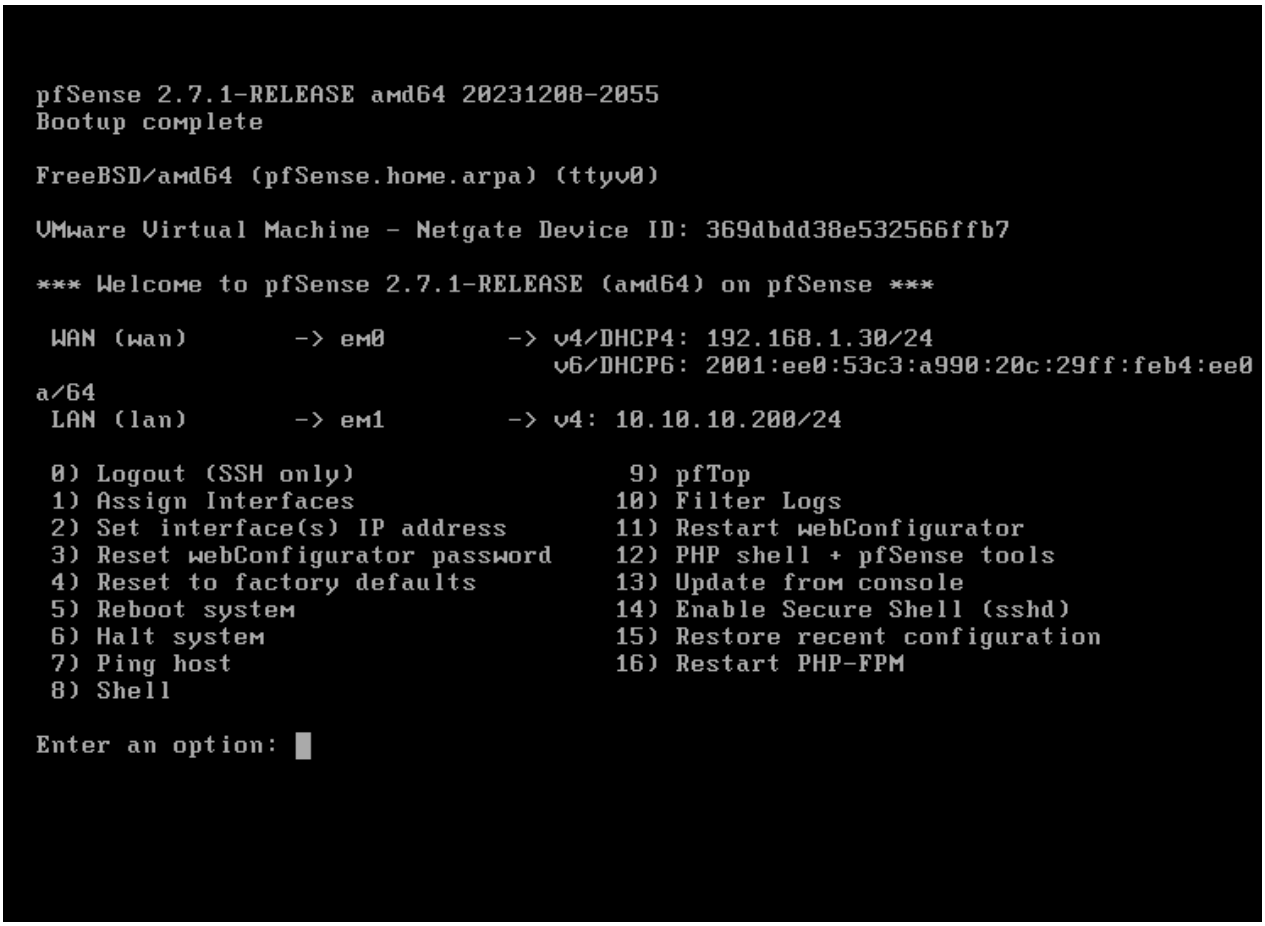
Sinh viên thực hiện	**Sinh viên 1** MSSV: 21521182 Họ tên: Nguyễn Đại Nghĩa **Sinh viên 2** MSSV: 21521295 Họ tên: Phạm Hoàng Phúc **Sinh viên 3** MSSV: 21521848 Họ tên: Hoàng Gia Bảo **Sinh viên 4** MSSV: 21521386 Họ tên: Lê Xuân Sơn
Lớp	**NT534.O21.ATCL.1**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	

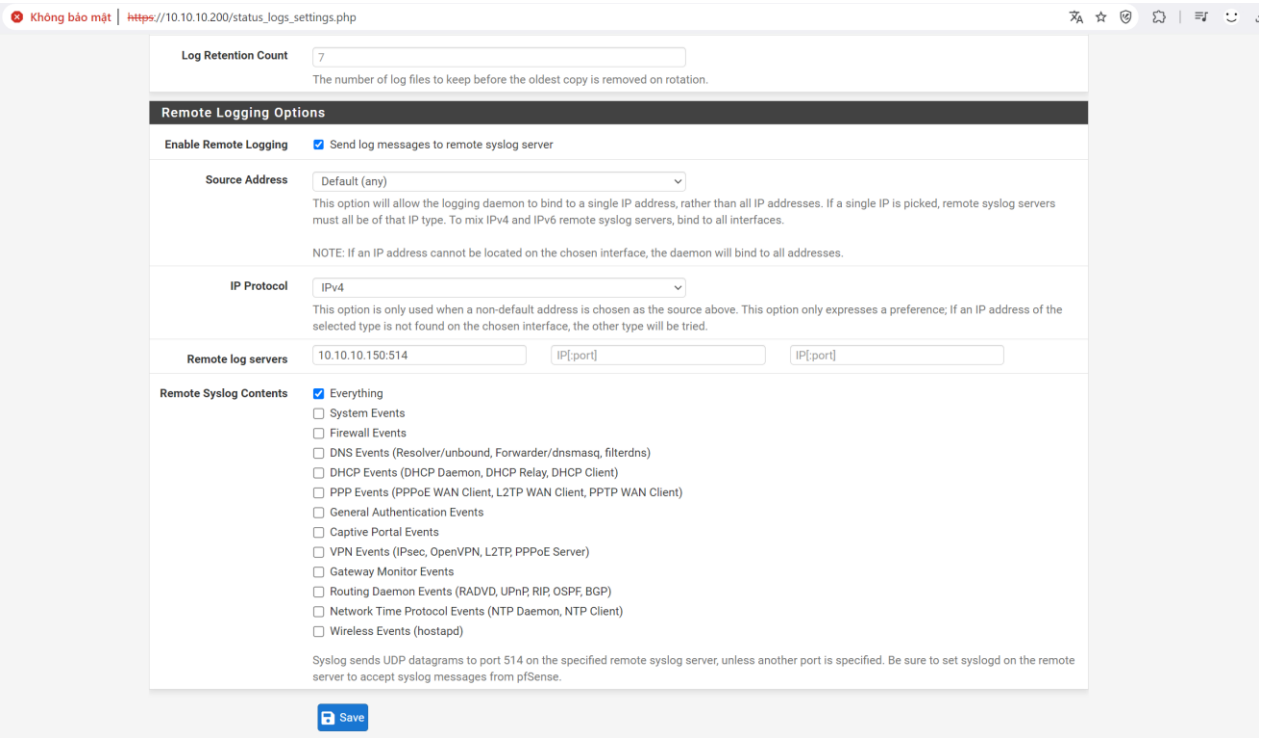
Link Video thực hiện *(nếu có yêu cầu)*	
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý...*	
Điểm tự đánh giá *(bắt buộc)*	9 /**10**

BÁO CÁO CHI TIẾT

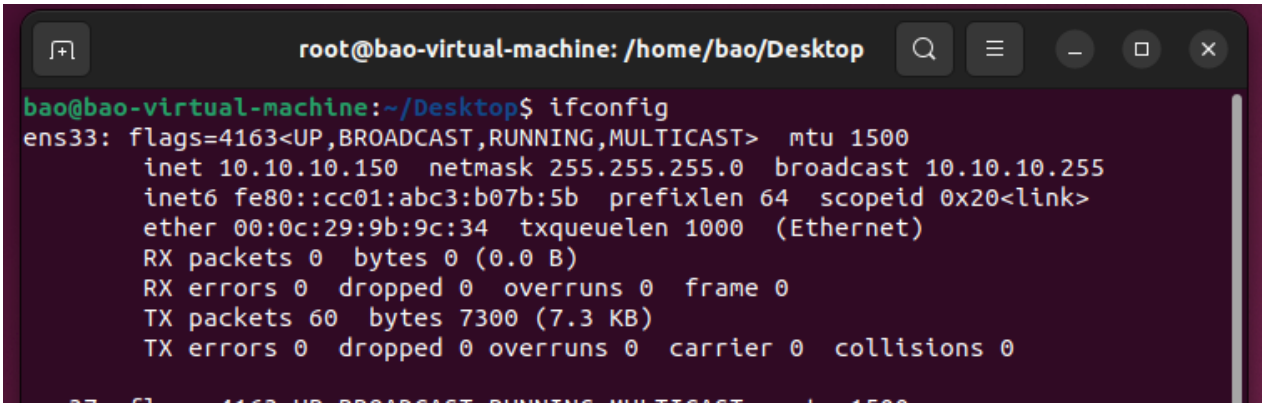
CẤU HÌNH CÁC MÁY

PFSENSE

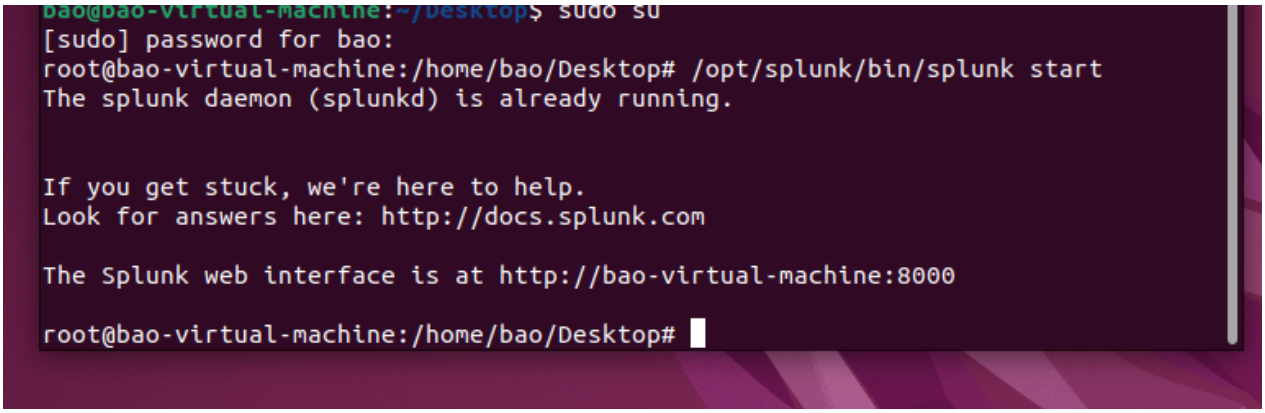

pfSense 2.7.1-RELEASE amd64 20231208-2055
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 369dbdd38e532566ffb7
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.30/24
v6/DHCP6: 2001:ee0:53c3:a990:20c:29ff:feb4:ee0
a/64
LAN (lan) -> em1 -> v4: 10.10.10.200/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:



SPLUNK



Khởi chạy splunk


bao@bao-virtual-machine:~/Desktop$ sudo su
[sudo] password for bao:
root@bao-virtual-machine:/home/bao/Desktop# /opt/splunk/bin/splunk start
The splunk daemon (splunkd) is already running.
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://bao-virtual-machine:8000
root@bao-virtual-machine:/home/bao/Desktop#

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

TCP | UDP

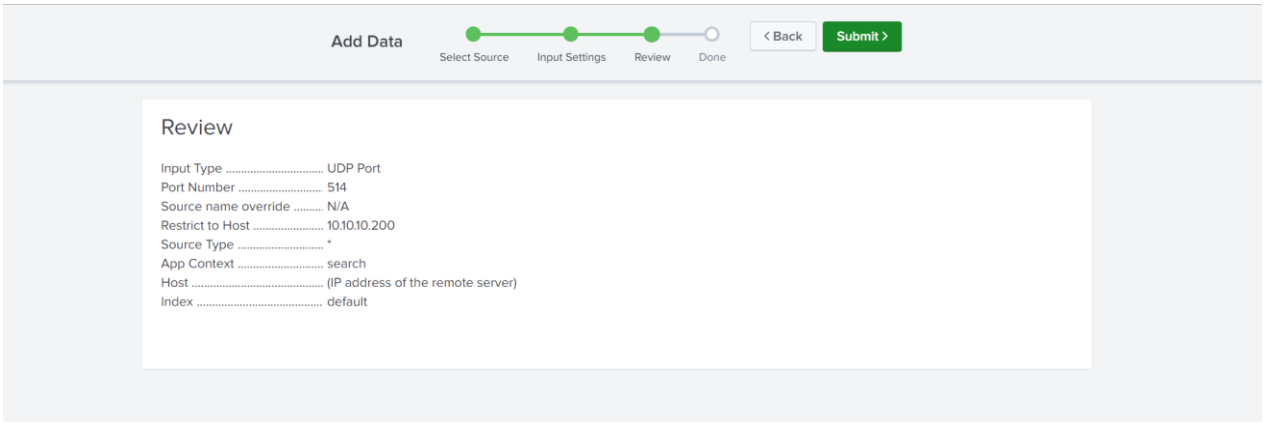
Port ?
514
Example: 514

Source name override ?
optional
host:port

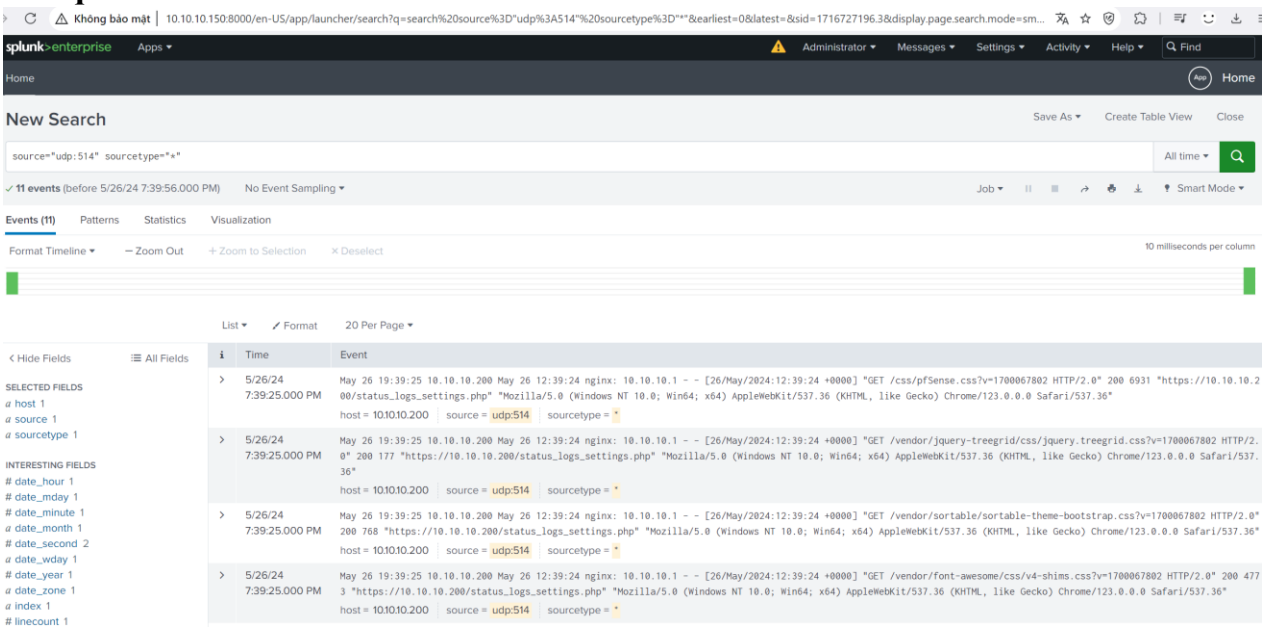
Only accept connection from ?
10.10.10.200
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ

- How should I configure the Splunk platform for syslog traffic?
- What's the difference between receiving data over TCP versus UDP?
- Can I collect syslog data from Windows systems?
- What is a source type?



Kết quả :



Task: Dùng công cụ Search của Splunk, lọc ra những log block traffic của PfSense, từ đó đề xuất và xây dựng một Dashboard đơn giản biểu diễn log traffic của PfSense

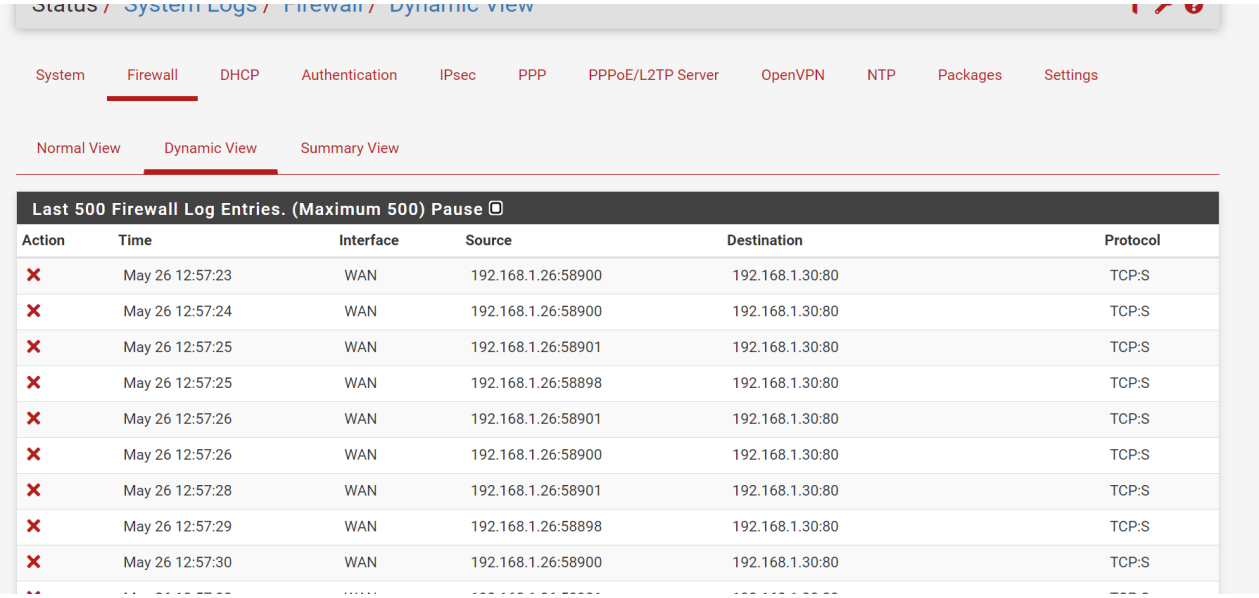
Rule tự động chặn ping đến địa chỉ WAN của pfsense

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✕	0/4 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✕	0/6 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

Sau khi máy tính cố gắng ping tới

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:ee0:53c3:a990:84b7:6f49:d9d6:98eb
   Temporary IPv6 Address. . . . . . : 2001:ee0:53c3:a990:d2:395f:8b9a:d8f7
   Link-local IPv6 Address . . . . . : fe80::3063:b454:76e9:d266%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.26
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%5
                                       192.168.1.1

Ethernet adapter vEthernet (WSLCore):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e60c:736a:4689:f949%73
   IPv4 Address. . . . . . . . . . . : 172.25.224.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Users\BaoBao>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

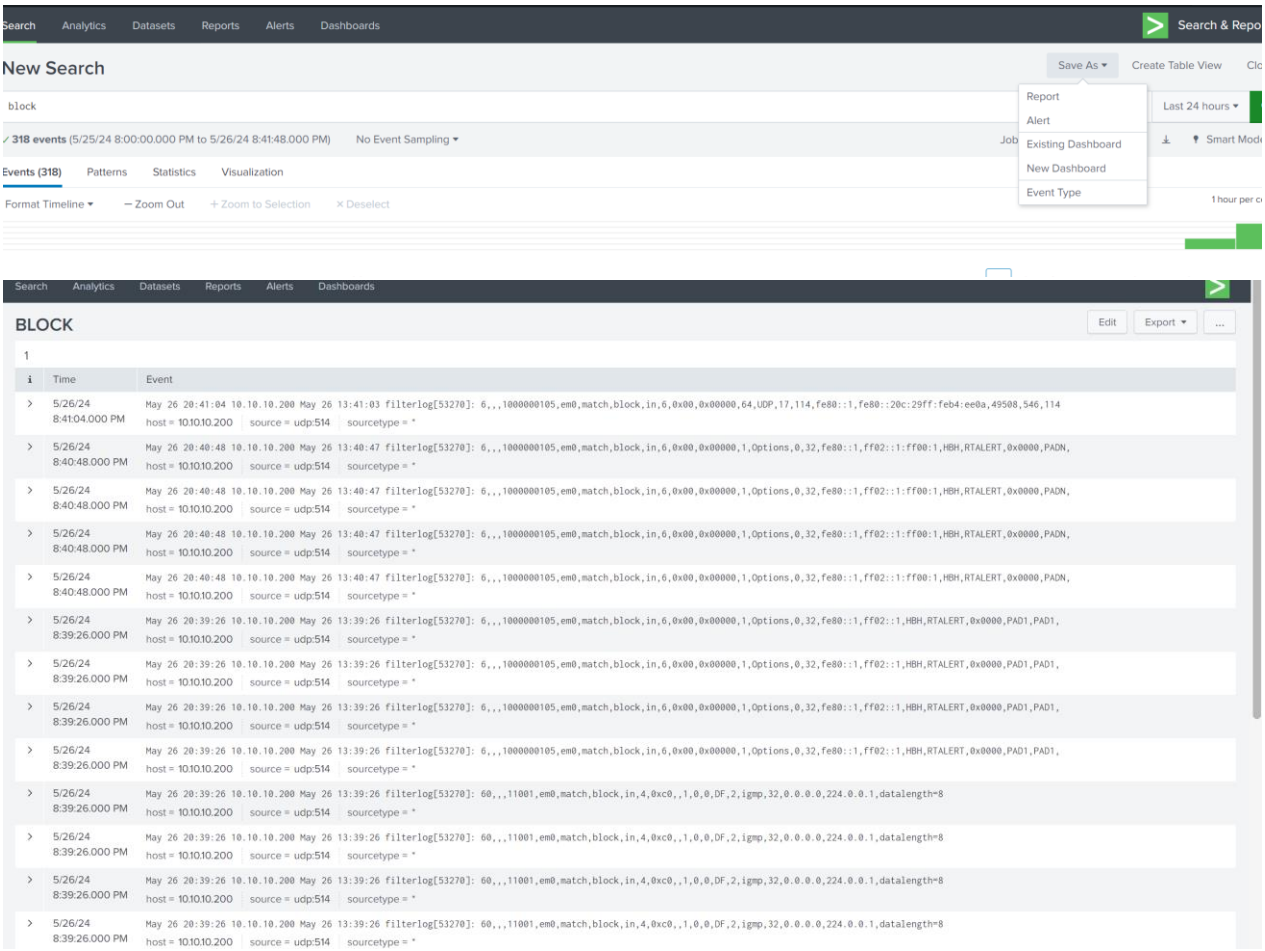


Action	Time	Interface	Source	Destination	Protocol
✖	May 26 12:57:23	WAN	192.168.1.26:58900	192.168.1.30:80	TCP:S
✖	May 26 12:57:24	WAN	192.168.1.26:58900	192.168.1.30:80	TCP:S
✖	May 26 12:57:25	WAN	192.168.1.26:58901	192.168.1.30:80	TCP:S
✖	May 26 12:57:25	WAN	192.168.1.26:58898	192.168.1.30:80	TCP:S
✖	May 26 12:57:26	WAN	192.168.1.26:58901	192.168.1.30:80	TCP:S
✖	May 26 12:57:26	WAN	192.168.1.26:58900	192.168.1.30:80	TCP:S
✖	May 26 12:57:28	WAN	192.168.1.26:58901	192.168.1.30:80	TCP:S
✖	May 26 12:57:29	WAN	192.168.1.26:58898	192.168.1.30:80	TCP:S
✖	May 26 12:57:30	WAN	192.168.1.26:58900	192.168.1.30:80	TCP:S

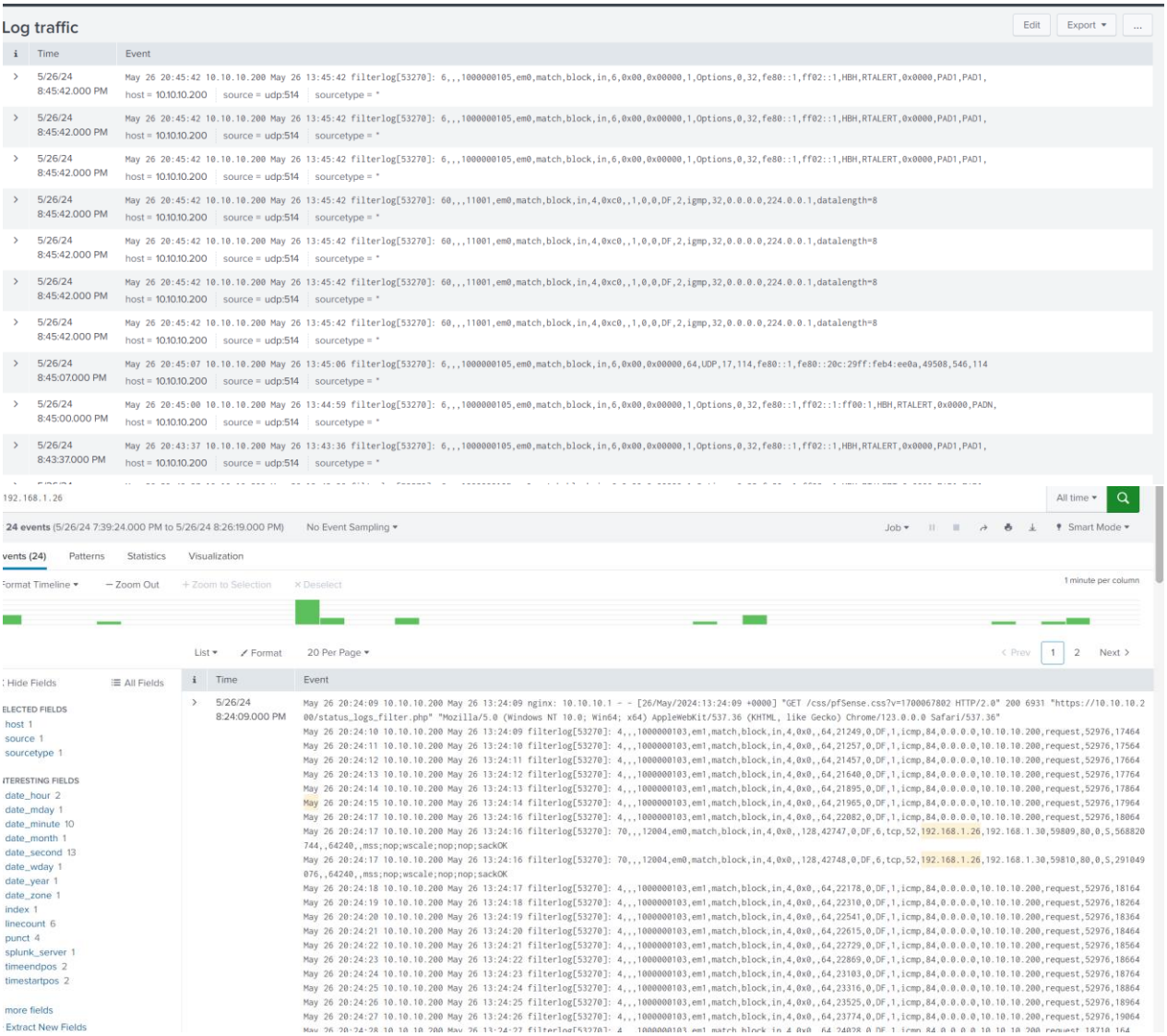
Thì ta được log từ pfsense trả về Splunk như sau :

Tạo Dashboard

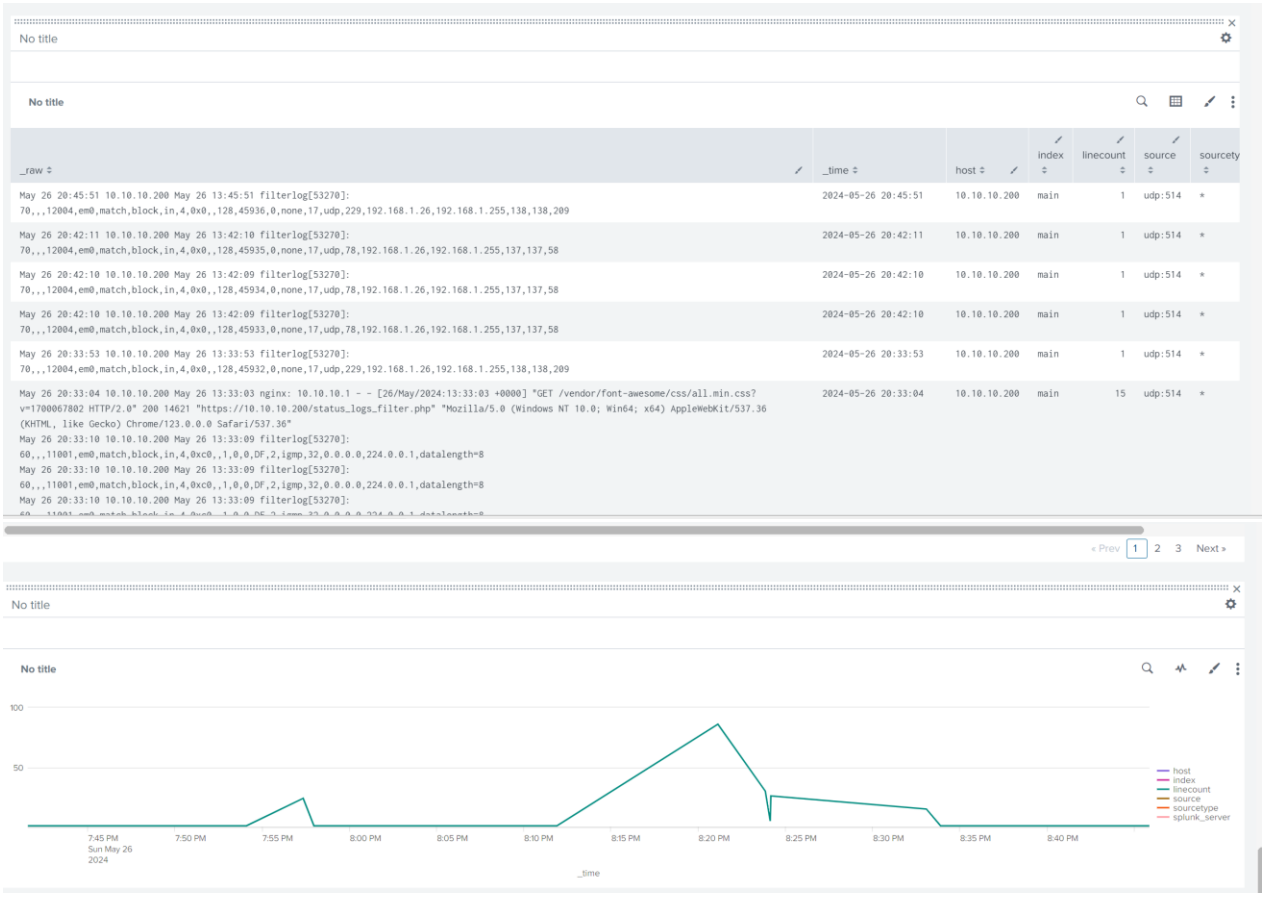
Ta tìm kiếm với từ khóa : Block, sau đó thì tạo dashboard



Tương tự với yêu cầu từ Task thì ta chỉ cần lọc với “filterlog”
Kết quả



Thêm panel lọc với ip : 192.168.1.26, tùy sở thích mà có thể chọn định dạng mà bản thân muốn xem


No title
No title
_raw
_time
host
index
linecount
source
sourcety
May 26 20:45:51 10.10.10.200 May 26 13:45:51 filterlog[53270]: 70,,,12004,em0,match,block,in,4,0x0,,128,45936,0,none,17,udp,229,192.168.1.26,192.168.1.255,138,138,209
2024-05-26 20:45:51
10.10.10.200
main
1
udp:514
May 26 20:42:11 10.10.10.200 May 26 13:42:10 filterlog[53270]: 70,,,12004,em0,match,block,in,4,0x0,,128,45935,0,none,17,udp,78,192.168.1.26,192.168.1.255,137,137,58
2024-05-26 20:42:11
10.10.10.200
main
1
udp:514
May 26 20:42:10 10.10.10.200 May 26 13:42:09 filterlog[53270]: 70,,,12004,em0,match,block,in,4,0x0,,128,45934,0,none,17,udp,78,192.168.1.26,192.168.1.255,137,137,58
2024-05-26 20:42:10
10.10.10.200
main
1
udp:514
May 26 20:42:10 10.10.10.200 May 26 13:42:09 filterlog[53270]: 70,,,12004,em0,match,block,in,4,0x0,,128,45933,0,none,17,udp,78,192.168.1.26,192.168.1.255,137,137,58
2024-05-26 20:42:10
10.10.10.200
main
1
udp:514
May 26 20:33:53 10.10.10.200 May 26 13:33:53 filterlog[53270]: 70,,,12004,em0,match,block,in,4,0x0,,128,45932,0,none,17,udp,229,192.168.1.26,192.168.1.255,138,138,209
2024-05-26 20:33:53
10.10.10.200
main
1
udp:514
May 26 20:33:04 10.10.10.200 May 26 13:33:03 nginx: 10.10.10.1 - - [26/May/2024:13:33:03 +0000] "GET /vendor/font-awesome/css/all.min.css?v=1700067802 HTTP/2.0" 200 14621 "https://10.10.10.200/status_logs_filter.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
May 26 20:33:10 10.10.10.200 May 26 13:33:09 filterlog[53270]: 60,,,11001,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,0.0.0.0,224.0.0.1,datalength=8
May 26 20:33:10 10.10.10.200 May 26 13:33:09 filterlog[53270]: 60,,,11001,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,0.0.0.0,224.0.0.1,datalength=8
May 26 20:33:10 10.10.10.200 May 26 13:33:09 filterlog[53270]:
2024-05-26 20:33:04
10.10.10.200
main
15
udp:514
« Prev
1
2
3
Next »

No title
No title
100
50
7:45 PM
Sun May 26
2024
7:50 PM
7:55 PM
8:00 PM
8:05 PM
8:10 PM
8:15 PM
8:20 PM
8:25 PM
8:30 PM
8:35 PM
8:40 PM
_time
host
index
linecount
source
sourcetype
splunk_server