



## 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	<b>Sinh viên 1</b> MSSV: 21521182 Họ tên: Nguyễn Đại Nghĩa <b>Sinh viên 2</b> MSSV: 21521295 Họ tên: Phạm Hoàng Phúc <b>Sinh viên 3</b> MSSV: 21521848 Họ tên: Hoàng Gia Bảo <b>Sinh viên 4</b> MSSV: 21521386 Họ tên: Lê Xuân Sơn
Lớp	<b>NT534.O21.ATCL.1</b>
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.arp) (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)              | 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                          |                                  |

```
Enter an option: █
```



Không bảo mật | [https://10.10.10.200/status\\_logs\\_settings.php](https://10.10.10.200/status_logs_settings.php)

Log Retention Count   
The number of log files to keep before the oldest copy is removed on rotation.

**Remote Logging Options**

Enable Remote Logging ☒ Send log messages to remote syslog server

Source Address   
This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.  
NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol   
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

Remote Syslog Contents ☒ Everything  
☐ System Events  
☐ Firewall Events  
☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)  
☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)  
☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)  
☐ General Authentication Events  
☐ Captive Portal Events  
☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)  
☐ Gateway Monitor Events  
☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)  
☐ Network Time Protocol Events (NTP Daemon, NTP Client)  
☐ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfsense.

## SPLUNK

```
root@bao-virtual-machine: /home/bao/Desktop
bao@bao-virtual-machine:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.150 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::cc01:abc3:b07b:5b prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:9b:9c:34 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 60 bytes 7300 (7.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## 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 ?	<input type="text" value="514"/>	
	Example: 514	
Source name override ?	<input type="text" value="optional"/>	
	host:port	
Only accept connection from ?	<input type="text" value="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?



Add Data

Select Source Input Settings Review Done

Back Submit

Review

Input Type ..... UDP Port  
Port Number ..... 514  
Source name override ..... N/A  
Restrict to Host ..... 10.10.10.200  
Source Type ..... \*  
App Context ..... search  
Host ..... (IP address of the remote server)  
Index ..... default

## Kết quả :

splunk enterprise

Administrator Messages Settings Activity Help Find

Home

New Search

Save As Create Table View Close

source="udp:514" sourcetype="\*"

All time

11 events (before 5/26/24 7:39:56.000 PM) No Event Sampling

Job

Events (11) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

10 milliseconds per column

List Format 20 Per Page

	i	Time	Event
>	5/26/24 7:39:25.000 PM	May 26 19:39:25 10.10.10.200 May 26 12:39:24 nginx: 10.10.10.1 - - [26/May/2024:12:39:24 +0000] "GET /css/pfSense.css?v=1700067802 HTTP/2.0" 200 6931 "https://10.10.10.200/status_logs_settings.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"	
		host = 10.10.10.200 source = udp:514 sourcetype = *	
>	5/26/24 7:39:25.000 PM	May 26 19:39:25 10.10.10.200 May 26 12:39:24 nginx: 10.10.10.1 - - [26/May/2024:12:39:24 +0000] "GET /vendor/jquery-treegrid/css/jquery.treegrid.css?v=1700067802 HTTP/2.0" 200 177 "https://10.10.10.200/status_logs_settings.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"	
		host = 10.10.10.200 source = udp:514 sourcetype = *	
>	5/26/24 7:39:25.000 PM	May 26 19:39:25 10.10.10.200 May 26 12:39:24 nginx: 10.10.10.1 - - [26/May/2024:12:39:24 +0000] "GET /vendor/sortable/sortable-theme-bootstrap.css?v=1700067802 HTTP/2.0" 200 768 "https://10.10.10.200/status_logs_settings.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"	
		host = 10.10.10.200 source = udp:514 sourcetype = *	
>	5/26/24 7:39:25.000 PM	May 26 19:39:25 10.10.10.200 May 26 12:39:24 nginx: 10.10.10.1 - - [26/May/2024:12:39:24 +0000] "GET /vendor/font-awesome/css/v4-shims.css?v=1700067802 HTTP/2.0" 200 4773 "https://10.10.10.200/status_logs_settings.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"	
		host = 10.10.10.200 source = udp:514 sourcetype = *	

**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)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/4 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	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.
```





Status / System Logs / Firewall / Dynamic view

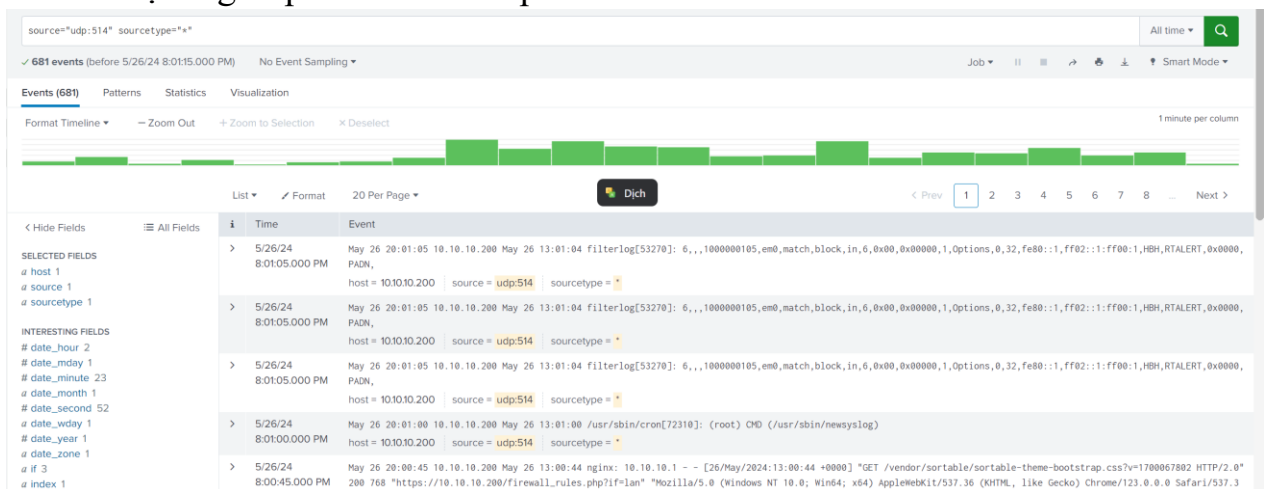
System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500) Pause

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



Search Analytics Datasets Reports Alerts Dashboards

New Search

block

318 events (5/25/24 8:00:00.000 PM to 5/26/24 8:41:48.000 PM) No Event Sampling

Events (318) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Save As Report Alert Existing Dashboard New Dashboard Event Type

Last 24 hours Smart Mode

1 hour per c

Search Analytics Datasets Reports Alerts Dashboards

BLOCK

Edit Export ...

i	Time	Event
>	5/26/24 8:41:04.000 PM	May 26 20:41:04 10.10.10.200 May 26 13:41:03 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,64,UDP,17,114,fe80::1,fe80::20c:29ff:feb4:ee8a,49508,546,114 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:40:48.000 PM	May 26 20:40:48 10.10.10.200 May 26 13:40:47 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PADN, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:40:48.000 PM	May 26 20:40:48 10.10.10.200 May 26 13:40:47 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PADN, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:40:48.000 PM	May 26 20:40:48 10.10.10.200 May 26 13:40:47 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PADN, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:40:48.000 PM	May 26 20:40:48 10.10.10.200 May 26 13:40:47 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PADN, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 filterlog[53270]: 6,,,1000000105,em0,match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1:HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:39:26.000 PM	May 26 20:39:26 10.10.10.200 May 26 13:39:26 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 host = 10.10.10.200 source = udp:514 sourcetype = *

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

Kết quả



## Log traffic

i	Time	Event
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 filterlog[53270]: 6,,,1000000105,em0_match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1,HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 filterlog[53270]: 6,,,1000000105,em0_match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1,HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 filterlog[53270]: 6,,,1000000105,em0_match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1,HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:42.000 PM	May 26 20:45:42 10.10.10.200 May 26 13:45:42 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 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:07.000 PM	May 26 20:45:07 10.10.10.200 May 26 13:45:06 filterlog[53270]: 6,,,1000000105,em0_match,block,in,6,0x00,0x00000,64,UDP,17,114,fe80::1,fe80::29ff:feb4:ee0a,49508,546,114 host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:45:00.000 PM	May 26 20:45:00 10.10.10.200 May 26 13:44:59 filterlog[53270]: 6,,,1000000105,em0_match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1,ff00:1,HBH,RTALERT,0x0000,PADN, host = 10.10.10.200 source = udp:514 sourcetype = *
>	5/26/24 8:43:37.000 PM	May 26 20:43:37 10.10.10.200 May 26 13:43:36 filterlog[53270]: 6,,,1000000105,em0_match,block,in,6,0x00,0x00000,1,Options,0,32,fe80::1,ff02::1,HBH,RTALERT,0x0000,PAD1,PAD1, host = 10.10.10.200 source = udp:514 sourcetype = *

192.168.1.26

24 events (5/26/24 7:39:24.000 PM to 5/26/24 8:26:19.000 PM) No Event Sampling

Jobs

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

Hide Fields All Fields

i	Time	Event
>	5/26/24 8:24:09.000 PM	May 26 20:24:09 10.10.10.200 May 26 13:24:09 nginx: 10.10.10.1 - - [26/May/2024:13:24:09 +0000] "GET /css/pfSense.css?v=1700067802 HTTP/2.0" 200 6931 "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 20:24:10 10.10.10.200 May 26 13:24:09 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,21249,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,17464
		May 26 20:24:11 10.10.10.200 May 26 13:24:10 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,21257,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,17564
		May 26 20:24:12 10.10.10.200 May 26 13:24:11 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,21457,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,17664
		May 26 20:24:13 10.10.10.200 May 26 13:24:12 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,21640,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,17764
		May 26 20:24:14 10.10.10.200 May 26 13:24:13 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,21895,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,17864
		May 26 20:24:15 10.10.10.200 May 26 13:24:14 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,21965,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,17964
		May 26 20:24:17 10.10.10.200 May 26 13:24:16 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22082,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18064
		May 26 20:24:17 10.10.10.200 May 26 13:24:16 filterlog[53270]: 70,,,12004,em0_match,block,in,4,0x00,,128,42747,0,DF,6,tcp,52,192.168.1.26,192.168.1.30,59809,80,0,5,568820
		744,,64240,,ms;nop;wscale;nop;nop;sackOK
		May 26 20:24:17 10.10.10.200 May 26 13:24:16 filterlog[53270]: 70,,,12004,em0_match,block,in,4,0x00,,128,42748,0,DF,6,tcp,52,192.168.1.26,192.168.1.30,59810,80,0,5,591049
		076,,64240,,ms;nop;wscale;nop;nop;sackOK
		May 26 20:24:18 10.10.10.200 May 26 13:24:17 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22178,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18164
		May 26 20:24:19 10.10.10.200 May 26 13:24:18 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22310,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18264
		May 26 20:24:20 10.10.10.200 May 26 13:24:19 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22541,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18364
		May 26 20:24:21 10.10.10.200 May 26 13:24:20 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22615,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18464
		May 26 20:24:22 10.10.10.200 May 26 13:24:21 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22729,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18564
		May 26 20:24:23 10.10.10.200 May 26 13:24:22 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,22869,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18664
		May 26 20:24:24 10.10.10.200 May 26 13:24:23 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,23103,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18764
		May 26 20:24:25 10.10.10.200 May 26 13:24:24 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,23316,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18864
		May 26 20:24:26 10.10.10.200 May 26 13:24:25 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,23525,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,18964
		May 26 20:24:27 10.10.10.200 May 26 13:24:26 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,23774,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,19064
		May 26 20:24:28 10.10.10.200 May 26 13:24:27 filterlog[53270]: 4,,,1000000103,em1_match,block,in,4,0x00,,64,24078,0,DF,1,icmp,84,0.0.0.0,10.10.10.200,request,52976,19164

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

