

BÁO CÁO BÀI TẬP

Tên chủ đề: Xây dựng hệ thống giám sát mạng
với Pfsense và Splunk

1. **THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

| STT | Họ và tên | MSSV | Email |
|-----|----------------|----------|------------------------|
| 1 | Phạm Thanh Tâm | 21522573 | 21522573@gm.uit.edu.vn |

2. **NỘI DUNG THỰC HIỆN:**¹

| STT | Công việc | Kết quả tự đánh giá |
|-----|--|---------------------|
| 1 | Tìm hiểu và triển khai Pfsense và Splunk | 100% |

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

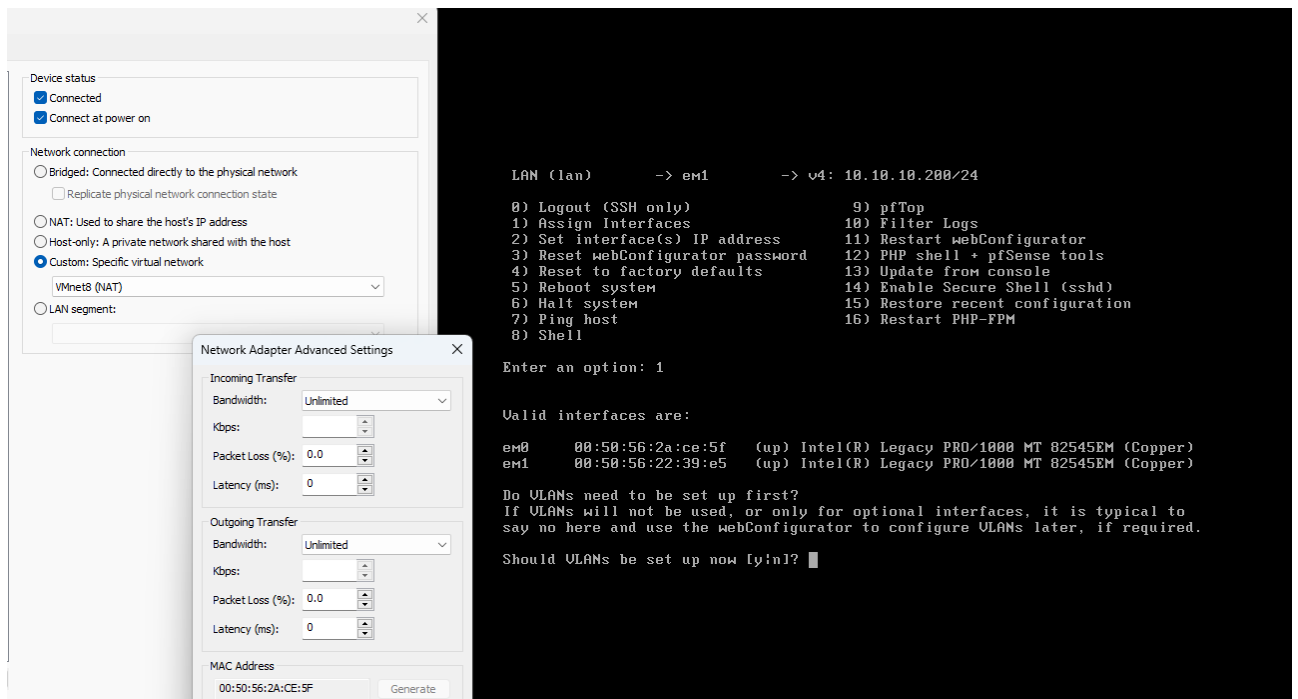
1. Thiết lập Pfsense Firewall:

- Cấu hình Pfsense:

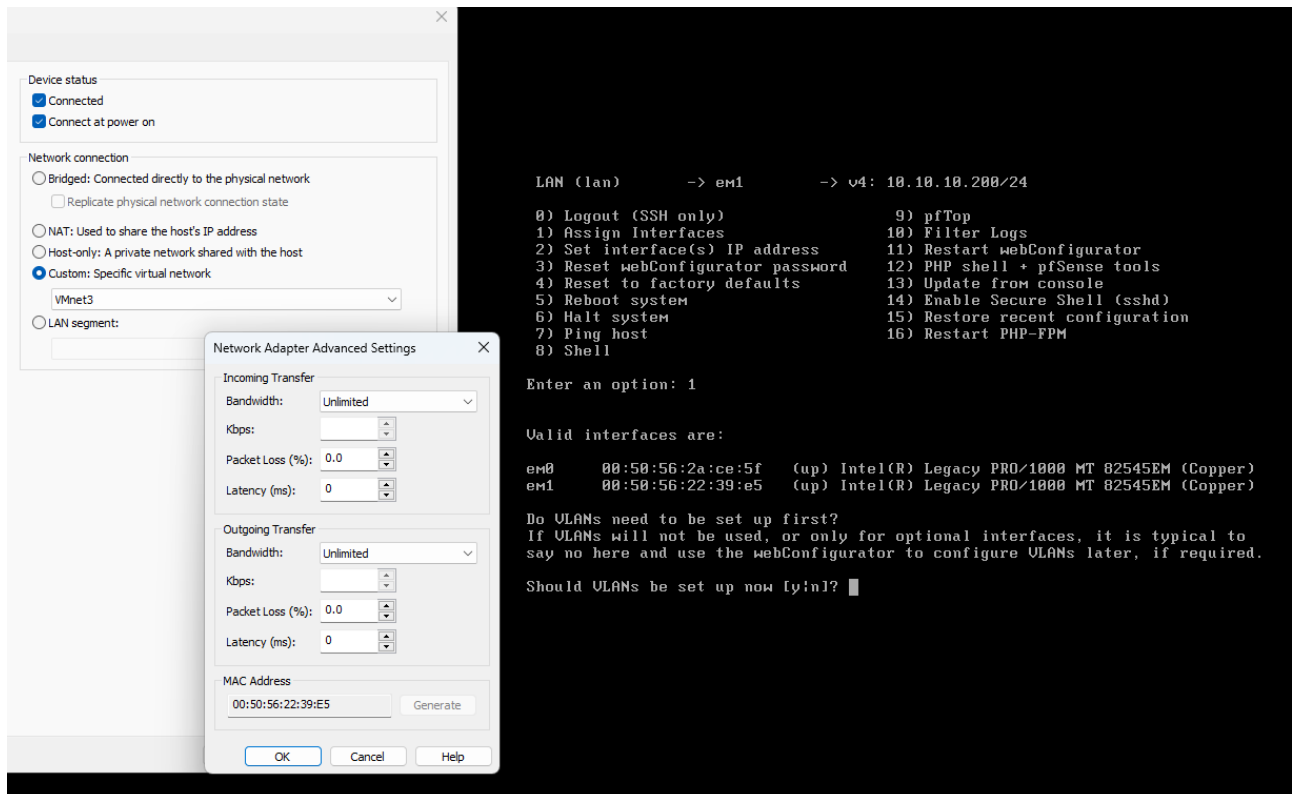
Bước 1: Thiết lập Network interface:

Tạo MAC Address sau đó kiểm tra interface trên Pfsense:

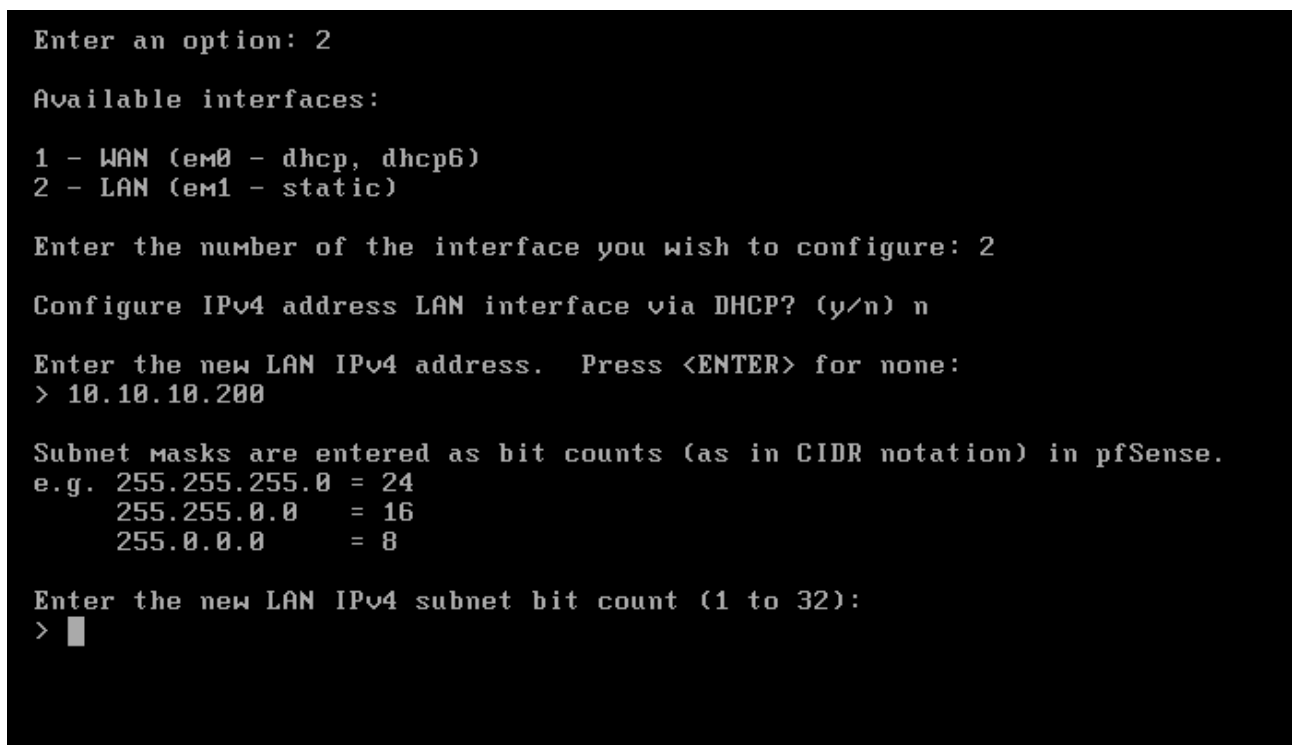
Interface em0:



Interface em1:



Bước 2: Cấu hình IP Address cho interface em1:



```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

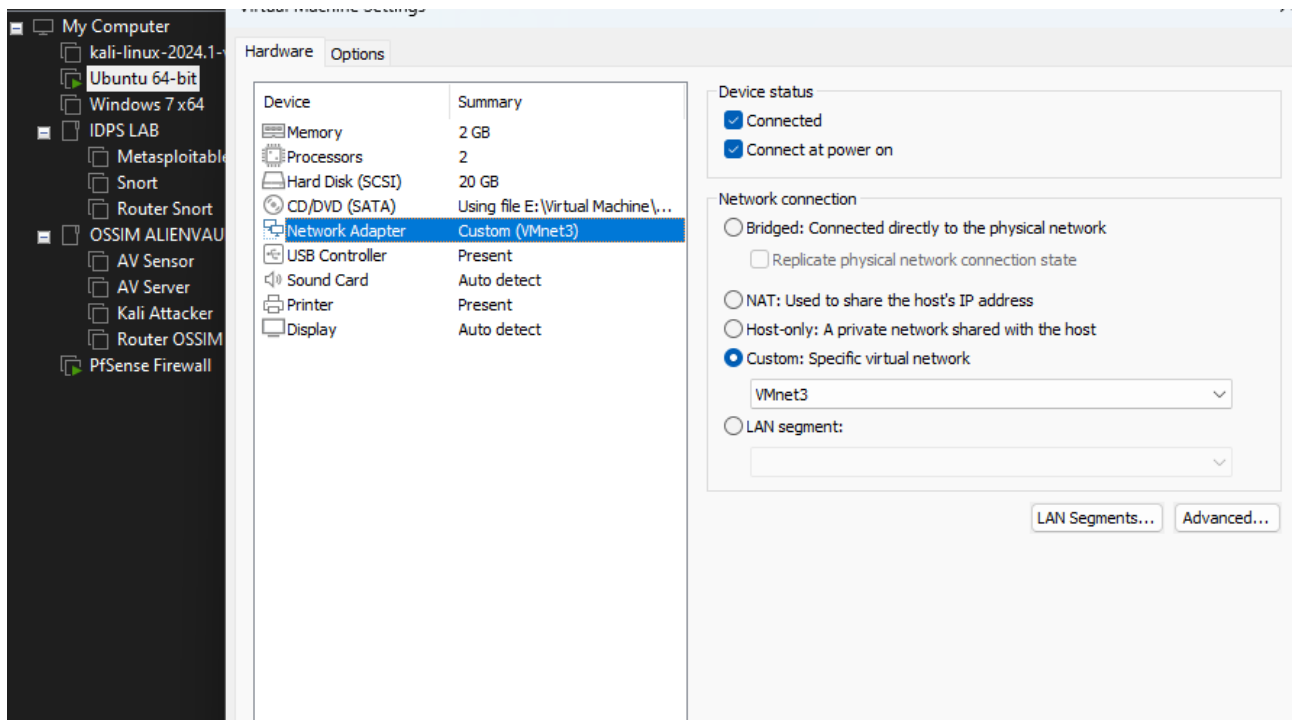
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.10.10.200/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://10.10.10.200/

Press <ENTER> to continue. █
```

Bước 3: Kiểm tra kết nối giữa Client, Pfsense và Internet :

- Setup card mạng cho máy Client trùng với card mạng LAN của máy pfsense:



- Chỉnh lại IP Address của máy Client:

Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

IPv4 Method

☐ Automatic (DHCP)

☐ Link-Local Only

☒ Manual

☐ Disable

☐ Shared to other computers

Addresses

| Address | Netmask | Gateway | |
|--------------|---------------|--------------|--|
| 10.10.10.100 | 255.255.255.0 | 10.10.10.200 | |
| | | | |

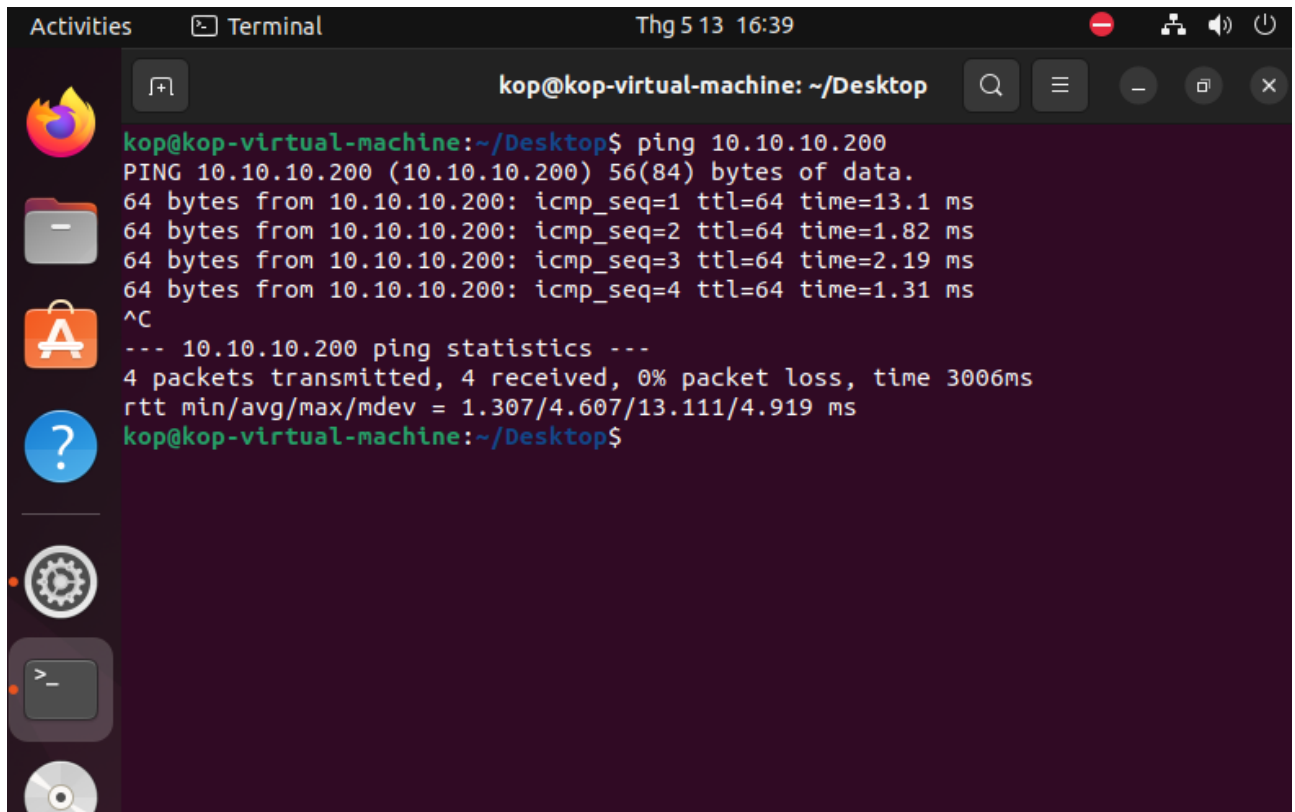
DNS

Automatic ☐

8.8.8.8

Separate IP addresses with commas

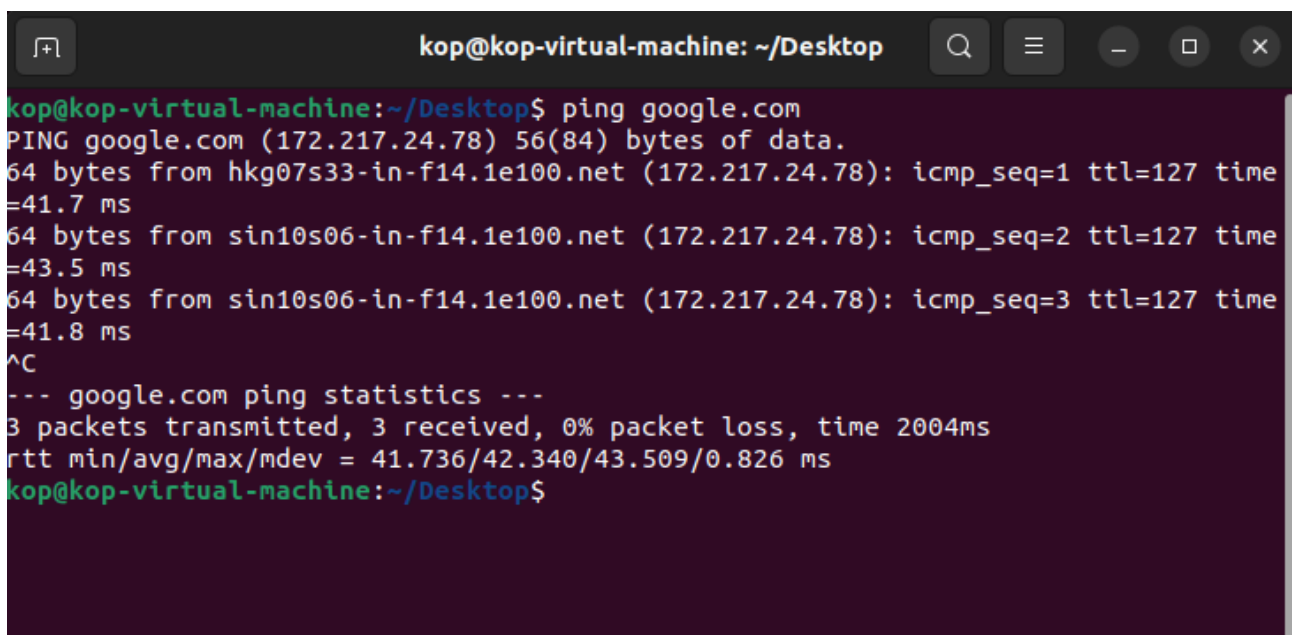
- Kiểm tra kết nối bằng cách ping đến IP Address của Pfsense:



The screenshot shows a terminal window titled "kop@kop-virtual-machine: ~/Desktop". The user has entered the command `ping 10.10.10.200`. The output shows four successful ping requests with varying response times. The statistics section indicates 4 packets transmitted, 4 received, 0% packet loss, and a total time of 3006ms.

```
kop@kop-virtual-machine: ~/Desktop$ ping 10.10.10.200
PING 10.10.10.200 (10.10.10.200) 56(84) bytes of data.
64 bytes from 10.10.10.200: icmp_seq=1 ttl=64 time=13.1 ms
64 bytes from 10.10.10.200: icmp_seq=2 ttl=64 time=1.82 ms
64 bytes from 10.10.10.200: icmp_seq=3 ttl=64 time=2.19 ms
64 bytes from 10.10.10.200: icmp_seq=4 ttl=64 time=1.31 ms
^C
--- 10.10.10.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.307/4.607/13.111/4.919 ms
kop@kop-virtual-machine: ~/Desktop$
```

- Ping ra internet:



The screenshot shows a terminal window titled "kop@kop-virtual-machine: ~/Desktop". The user has entered the command `ping google.com`. The output shows three successful ping requests to google.com (172.217.24.78) with response times around 41-43ms. The statistics section indicates 3 packets transmitted, 3 received, 0% packet loss, and a total time of 2004ms.

```
kop@kop-virtual-machine: ~/Desktop$ ping google.com
PING google.com (172.217.24.78) 56(84) bytes of data.
64 bytes from hkg07s33-in-f14.1e100.net (172.217.24.78): icmp_seq=1 ttl=127 time=41.7 ms
64 bytes from sin10s06-in-f14.1e100.net (172.217.24.78): icmp_seq=2 ttl=127 time=43.5 ms
64 bytes from sin10s06-in-f14.1e100.net (172.217.24.78): icmp_seq=3 ttl=127 time=41.8 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 41.736/42.340/43.509/0.826 ms
kop@kop-virtual-machine: ~/Desktop$
```

- Kiểm tra internet máy pfsense:

```
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: 7

Enter a host name or IP address: google.com

PING google.com (142.251.220.110): 56 data bytes
64 bytes from 142.251.220.110: icmp_seq=0 ttl=128 time=52.043 ms
64 bytes from 142.251.220.110: icmp_seq=1 ttl=128 time=45.548 ms
64 bytes from 142.251.220.110: icmp_seq=2 ttl=128 time=55.422 ms

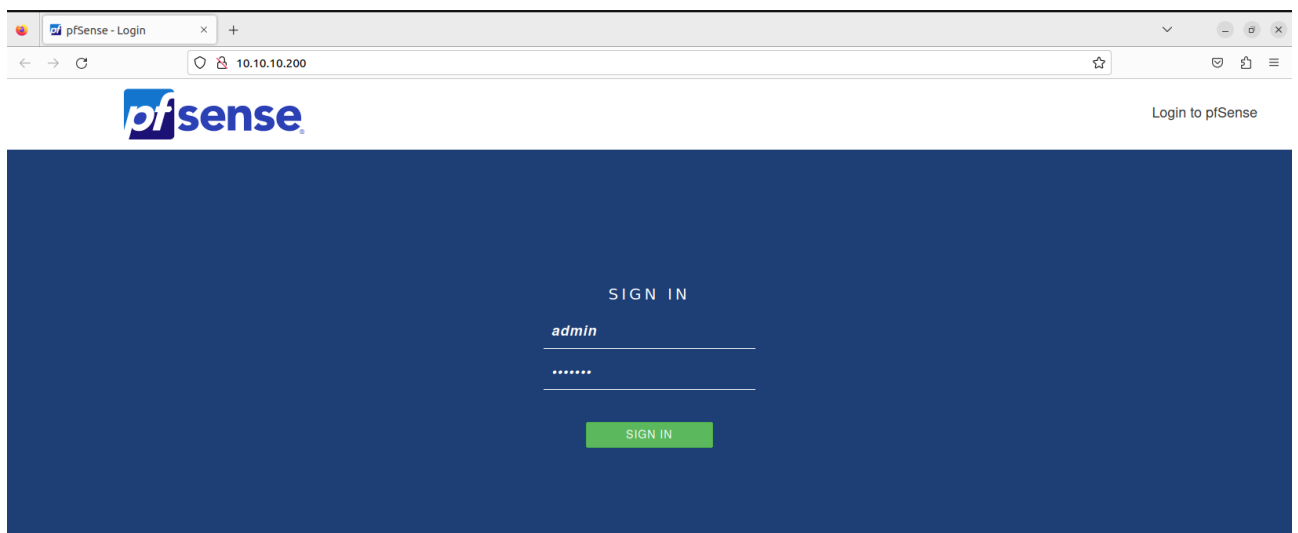
--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 45.548/51.004/55.422/4.097 ms

Press ENTER to continue.
█
```

Bước 4: Truy cập PfSense thông qua client theo địa chỉ IP :

Account : admin

Password : pfsense



Bước 5 : Setup PfSense :

- Chọn Domain tùy ý :

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

- Set timezone :

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

>> Next

- Set password mới cho admin account:

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

>> Next

- Reload và Finish:

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

Remember, we're here to help.

Click here to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

Anonymous User Survey

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our website
- To learn about Netgate appliances and other offers, visit our store
- Become part of the pfSense community. Visit our forum
- Subscribe to our newsletter for ongoing product information, software announcements and special offers.

Finish

2. Cài đặt Splunk:

Bước 1: Setup IP và kiểm tra Internet:

- Set up IP cho máy Splunk:

Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

IPv4 Method

☐ Automatic (DHCP)
 ☐ Link-Local Only
 ☒ Manual
 ☐ Disable
 ☐ Shared to other computers

Addresses

| Address | Netmask | Gateway | |
|--------------|---------------|--------------|--|
| 10.10.10.150 | 255.255.255.0 | 10.10.10.200 | |
| | | | |

DNS

Automatic ☐

8.8.8.8

Separate IP addresses with commas

- Kiểm tra internet:

```

kop@kop-virtual-machine: ~/Desktop
kop@kop-virtual-machine:~/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=127 time=233 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=93.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=176 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 93.587/167.373/232.518/57.046 ms
kop@kop-virtual-machine:~/Desktop$
    
```

- Tải gói ,unpackage và chạy Splunk:

```
kop@kop-virtual-machine: ~/Desktop
kop@kop-virtual-machine:~/Desktop$ wget wget -O splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb "https://download.splunk.com/products/splunk/releases/9.2.1/linux/splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb"
--2024-05-13 17:58:41-- http://wget/
Resolving wget (wget)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'wget'
--2024-05-13 17:58:41-- https://download.splunk.com/products/splunk/releases/9.2.1/linux/splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb
Resolving download.splunk.com (download.splunk.com)... 108.157.38.127, 108.157.38.90, 108.157.38.99, ...
Connecting to download.splunk.com (download.splunk.com)|108.157.38.127|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 545652596 (520M) [binary/octet-stream]
Saving to: 'splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb'

splunk-9.2.1-78803f 100%[=====] 520,37M  7,16MB/s   in 69s

2024-05-13 17:59:50 (7,52 MB/s) - 'splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb' saved [545652596/545652596]

FINISHED --2024-05-13 17:59:50--
Total wall clock time: 1m 9s
Downloaded: 1 files, 520M in 1m 9s (7,52 MB/s)
kop@kop-virtual-machine:~/Desktop$ ls /opt
kop@kop-virtual-machine:~/Desktop$ sudo dpkg -i ./splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb
[sudo] password for kop:
Selecting previously unselected package splunk.
(Reading database ... 141622 files and directories currently installed.)
Preparing to unpack .../splunk-9.2.1-78803f08aabb-linux-2.6-and64.deb ...
Unpacking splunk (9.2.1-78803f08aabb) ...
Setting up splunk (9.2.1-78803f08aabb) ...
/var/lib/dpkg/info/splunk.postinst: line 60: curl: command not found
complete
kop@kop-virtual-machine:~/Desktop$ ls /opt/
ls: cannot access '/opt/': No such file or directory
kop@kop-virtual-machine:~/Desktop$ ls /opt/
splunk
kop@kop-virtual-machine:~/Desktop$ sudo /opt/splunk/bin/splunk start
[sudo] password for kop:
SPLUNK GENERAL TERMS

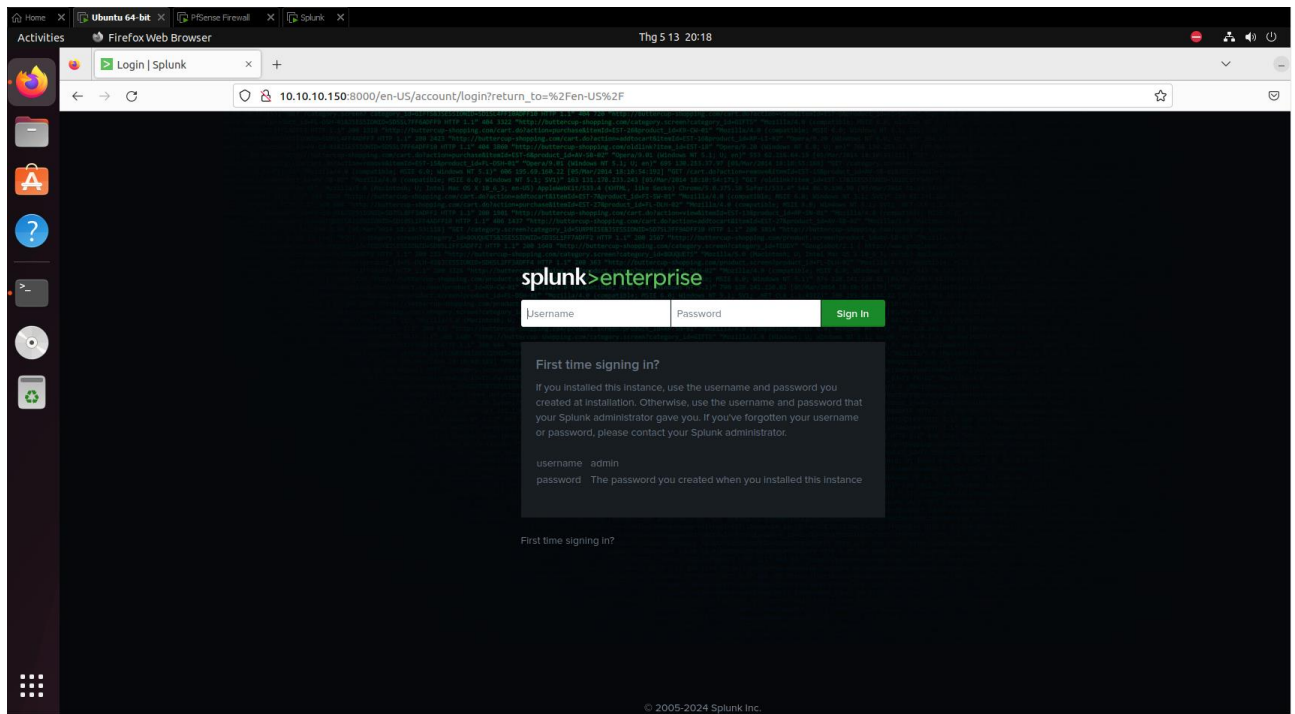
Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware corporation, with its principal place of business at 270 Brannan Street, San Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you ("customer" or "you" or "your") apply to the purchase of licenses and subscriptions for Splunk's Offerings. By clicking on the appropriate button, or by downloading, installing, accessing or using the Offerings, you agree to these General Terms. If you are entering into these General Terms on behalf of
```

- Splunk đã được mở trên cổng 8000:

```
kop@kop-virtual-machine: ~/Desktop
kop@kop-virtual-machine:~/Desktop$ sudo /opt/splunk/bin/splunk start
Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
Creating: /opt/splunk/var/run/splunk/upload
Creating: /opt/splunk/var/run/splunk/search_telemetry
Creating: /opt/splunk/var/run/splunk/search_log
Creating: /opt/splunk/var/spool/splunk
Creating: /opt/splunk/var/spool/dirmoncache
Creating: /opt/splunk/var/lib/splunk/auth0b
Creating: /opt/splunk/var/lib/splunk/hash0b
New certs have been generated in '/opt/splunk/etc/auth'.
Checking critical directories... Done
Checking indexes... Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems... Done
Checking default conf files for edits... Validating installed files against hashes from '/opt/splunk/splunk-9.2.1-78803f08aabb-linux-2.6-x86_64-nanifest'
All installed files intact. Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=kop-virtual-machine/0=SplunkUser
Getting CA Private Key
Writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
Waiting for web server at http://127.0.0.1:8000 to be available..... Done
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://kop-virtual-machine:8000
kop@kop-virtual-machine:~/Desktop$
```

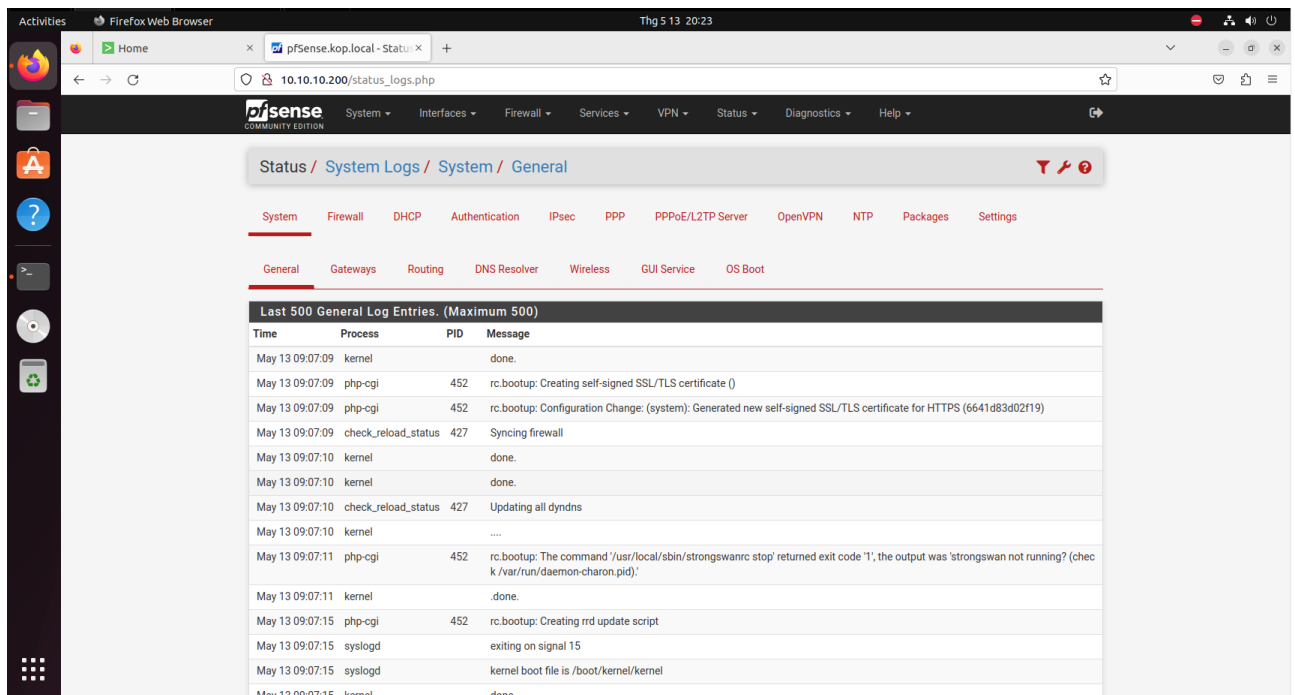
- Truy cập Splunk thành công:



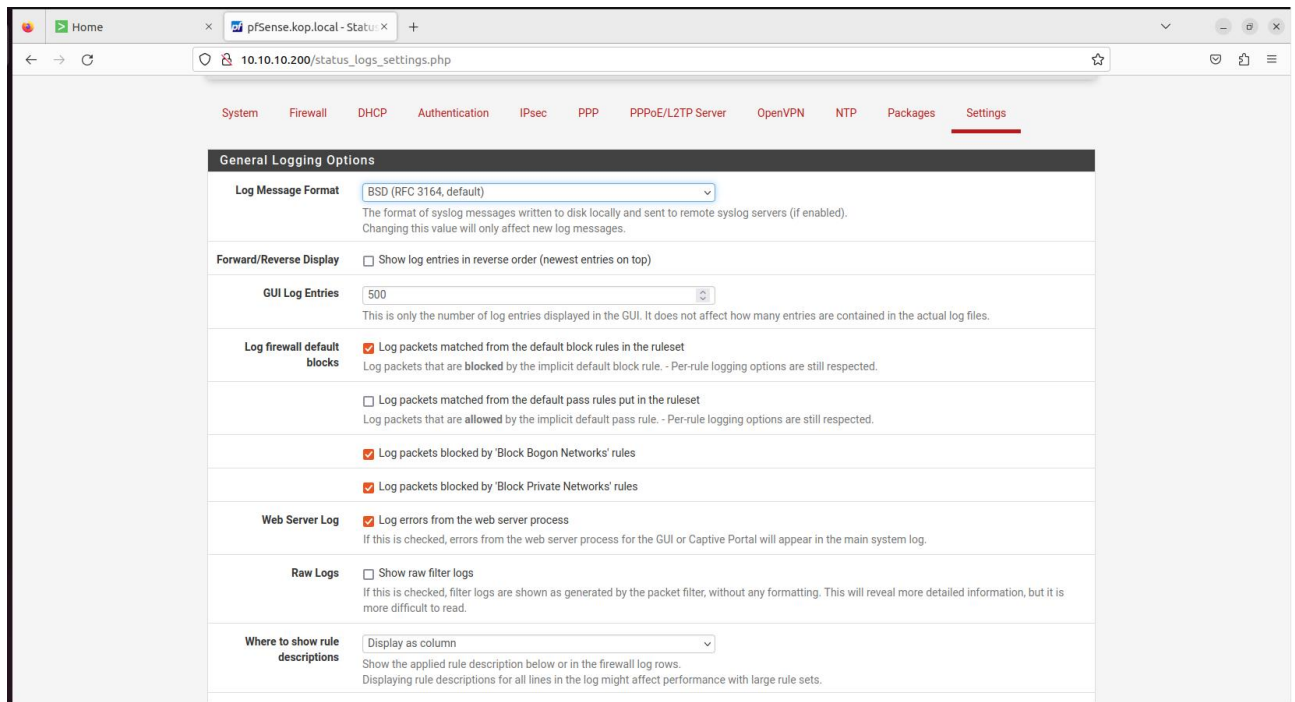
3. Cấu hình đẩy log từ Pfsense về Splunk:

Pfsense:

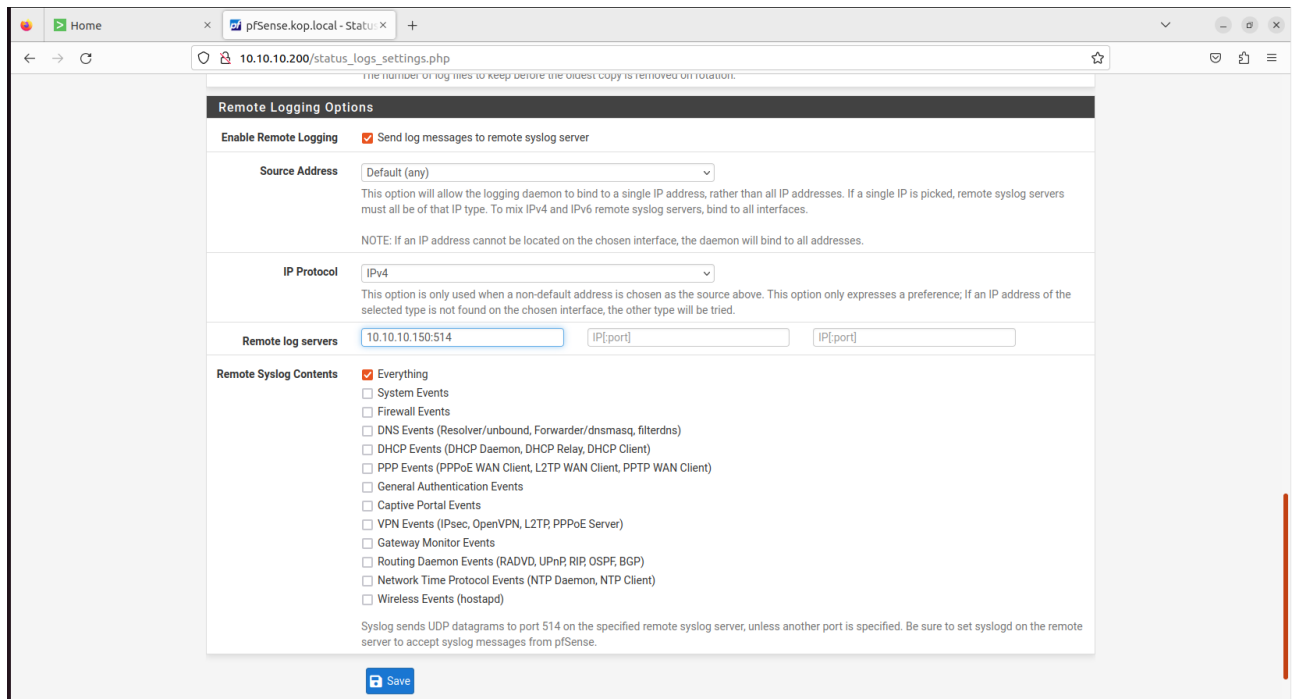
- Vào pfsense chọn Status -> System Logs:



- Chọn Settings:

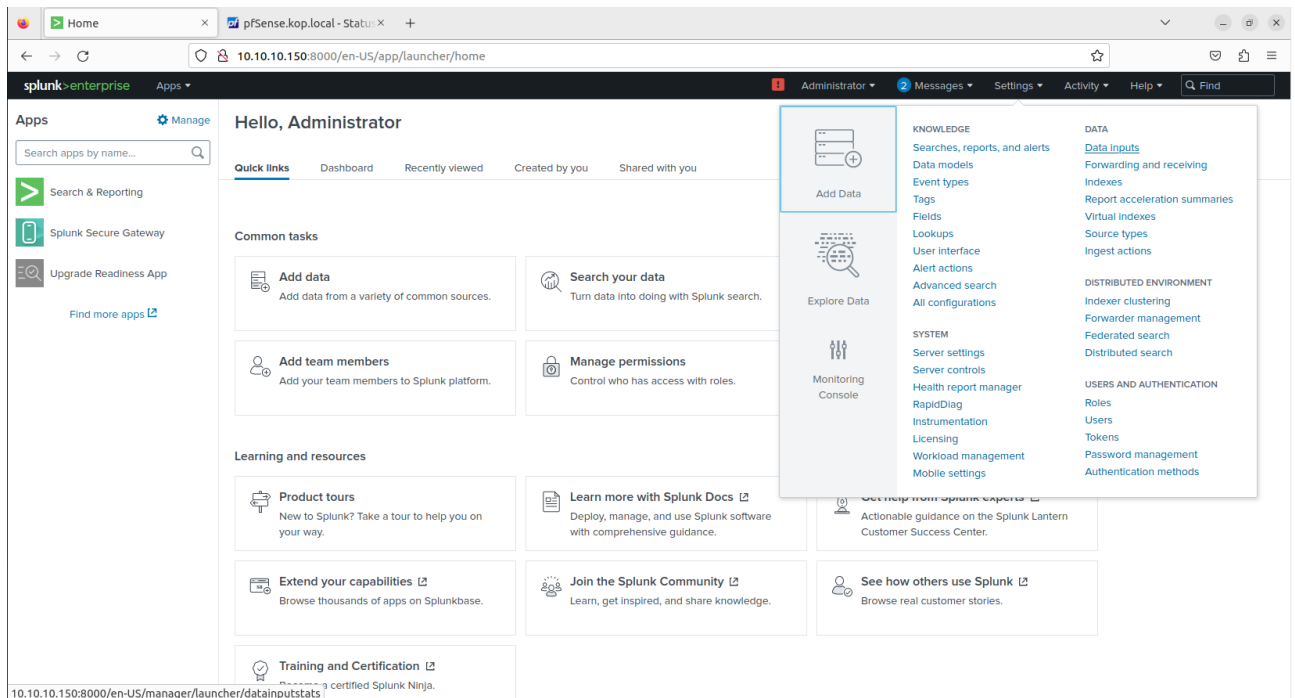


- Enable Remote Logging và set IP nhận log là máy Splunk (10.10.10.150:514):



Splunk:

- Truy cập Splunk trên máy Client, chọn Settings -> Data Inputs:



- Chọn Add new trong phần UDP:

| | | |
|---|----|-----------|
| TCP Listen on a TCP port for incoming data, e.g. syslog. | 0 | + Add new |
| UDP Listen on a UDP port for incoming data, e.g. syslog. | 0 | + Add new |
| Scripts Run custom scripts to collect or generate more data. | 25 | + Add new |
| Splunk Assist Instance Identifier Assigns a random identifier to every node | 1 | + Add new |

- Set up port là 514 và IP gửi log là địa chỉ IP của PfSense (10.10.10.200):

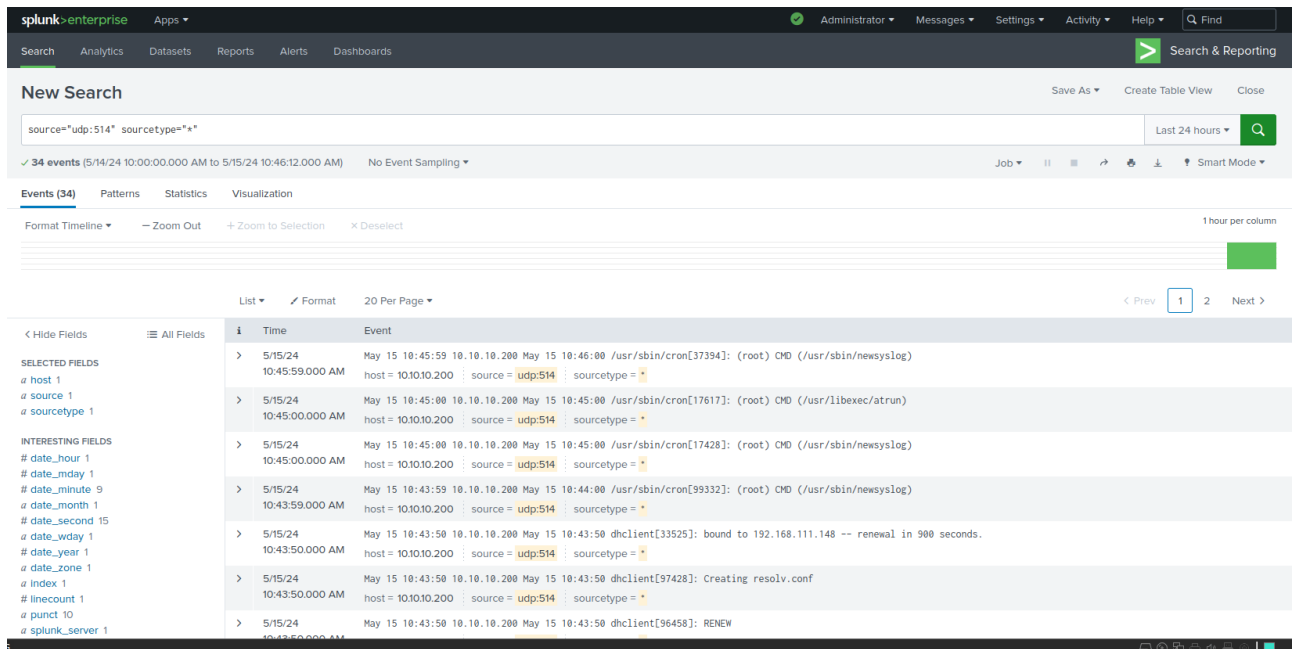
The screenshot shows the 'Add Data' configuration page in Splunk Enterprise. The 'Select Source' step is active. On the left, a list of source types includes 'Files & Directories', 'HTTP Event Collector', 'TCP / UDP' (selected), 'Scripts', 'Splunk Assist Instance Identifier', 'Systemd Journal Input for Splunk', 'Logd Input for the Splunk platform', 'Splunk Secure Gateway', 'Splunk Assist Self-Update', and 'Splunk Secure Gateway Mobile Alerts TTL'. The main area is titled 'Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog)'. It features a 'Port' field set to '514', a 'Source name override' field set to 'optional', and an 'Only accept connection from' field set to '10.10.10.200'. A 'FAQ' section is visible at the bottom right.

- Chỉ chỉnh sửa Source Type = * , App Context = “ Search & Reporting” ; Method = “IP”

- Review:

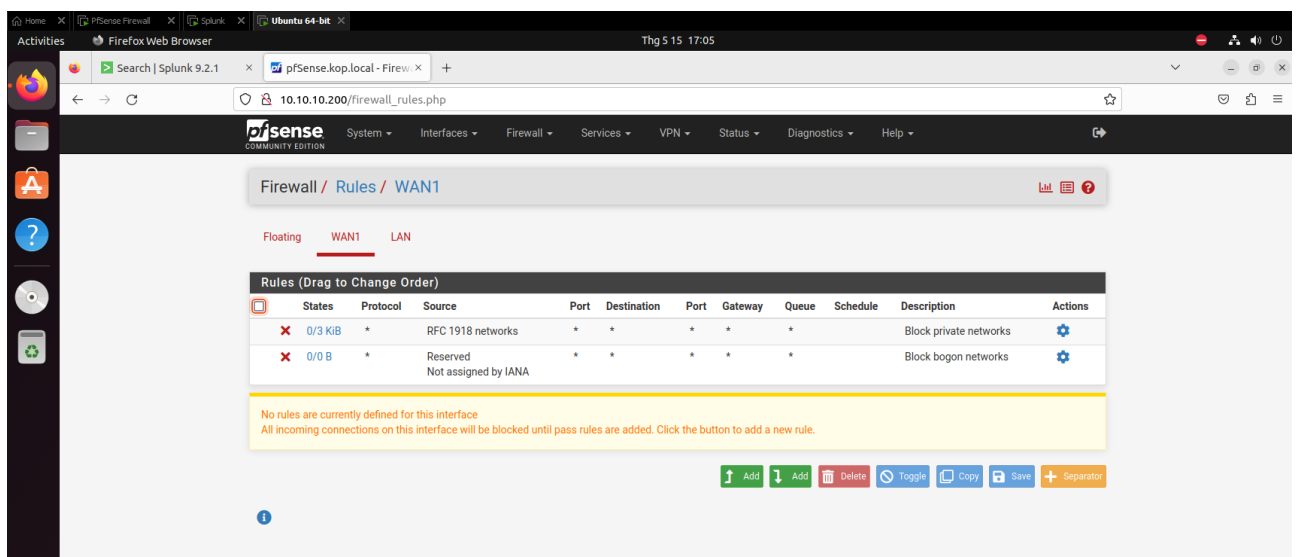
The screenshot shows the 'Review' step of the 'Add Data' configuration. The 'Review' box displays the following configuration details: Input Type: UDP Port, Port Number: 514, Source name override: N/A, Restrict to Host: 10.10.10.200, Source Type: *, App Context: search, Host: (IP address of the remote server), and Index: default. The 'Submit' button is visible at the bottom right of the configuration area.

- Kiểm tra log:



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

- Mở giao diện Pfsense lên chọn Firewall -> Rules -> Add



- Action = Pass; Interface = WAN1; Protocol = UDP

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface WAN1
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol UDP
 Choose which IP protocol this rule should match.

Source

- Nhập port 7001

Source

Source ☐ Invert match Any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Any Destination Address /

Destination Port Range (other) 7001 (other) 7001
 From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

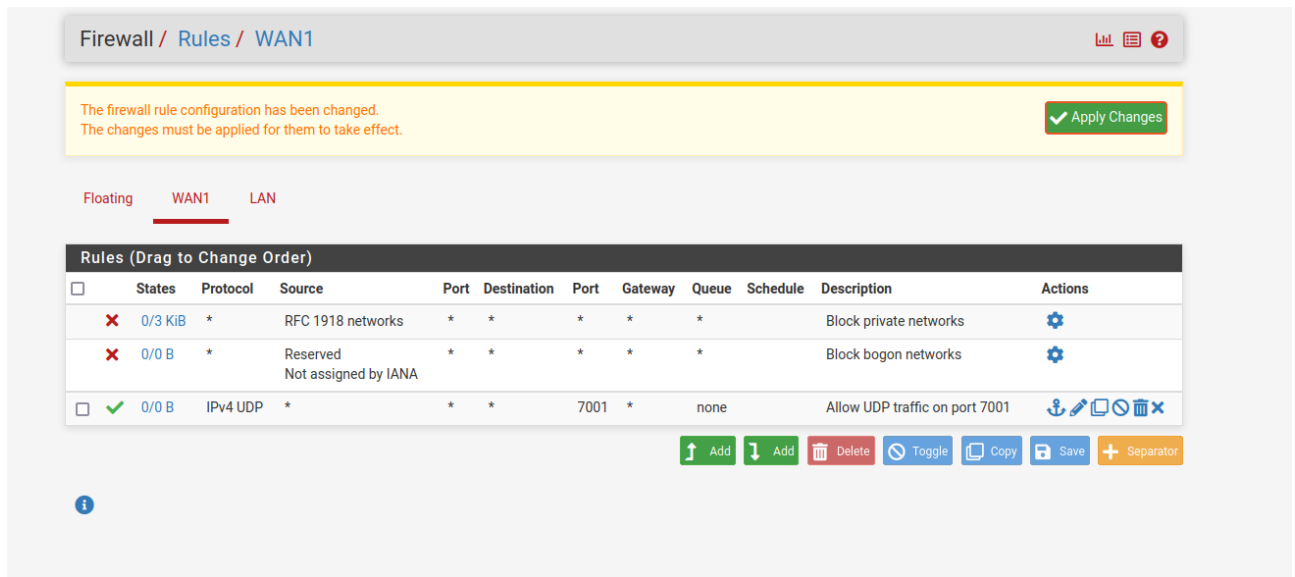
Log ☐ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description Allow UDP traffic on port 7001
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

- Rule đã được tạo trên Firewall:



=> Hoàn tất việc tạo Rule trên Firewall để cho phép IPv4 – UDP traffic có thể đi qua port 7001

- Trên máy ảo Splunk ta tạo file indexes.conf:

```
kop@kop-virtual-machine:/opt/splunk/etc/apps/inputs_fw/local$ sudo nano /opt/splunk/etc/system/local/indexes.conf
kop@kop-virtual-machine:/opt/splunk/etc/apps/inputs_fw/local$
```

- Nội dung như sau:

```

GNU nano 6.2 /opt/splunk/etc/system/local/indexes.conf
[Fw]
homePath = $SPLUNK_DB/fwdb/db
coldPath = $SPLUNK_DB/fwdb/colddb
thawedPath = $SPLUNK_DB/fwdb/thaweddb
    
```

- Tạo inputs configuration file:

```
kop@kop-virtual-machine:~/Desktop$ sudo mkdir /opt/splunk/etc/apps/inputs_fw
kop@kop-virtual-machine:~/Desktop$ sudo mkdir /opt/splunk/etc/apps/inputs_fw/local
kop@kop-virtual-machine:~/Desktop$ sudo cd /opt/splunk/etc/apps/inputs_fw/local
```

- Tạo file inputs.conf

```
kop@kop-virtual-machine:/opt/splunk/etc/apps/inputs_fw/local$ sudo nano inputs.conf
```

- Tạo file inputs.conf với nội dung như sau:

```
GNU nano 6.2
[udp://:7001]
index=fw
sourcetype=pfsense
```

- Restart lại Splunk

- Trên Pfsense chọn tab Status -> System Logs -> Settings. Setting như bên dưới:

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.

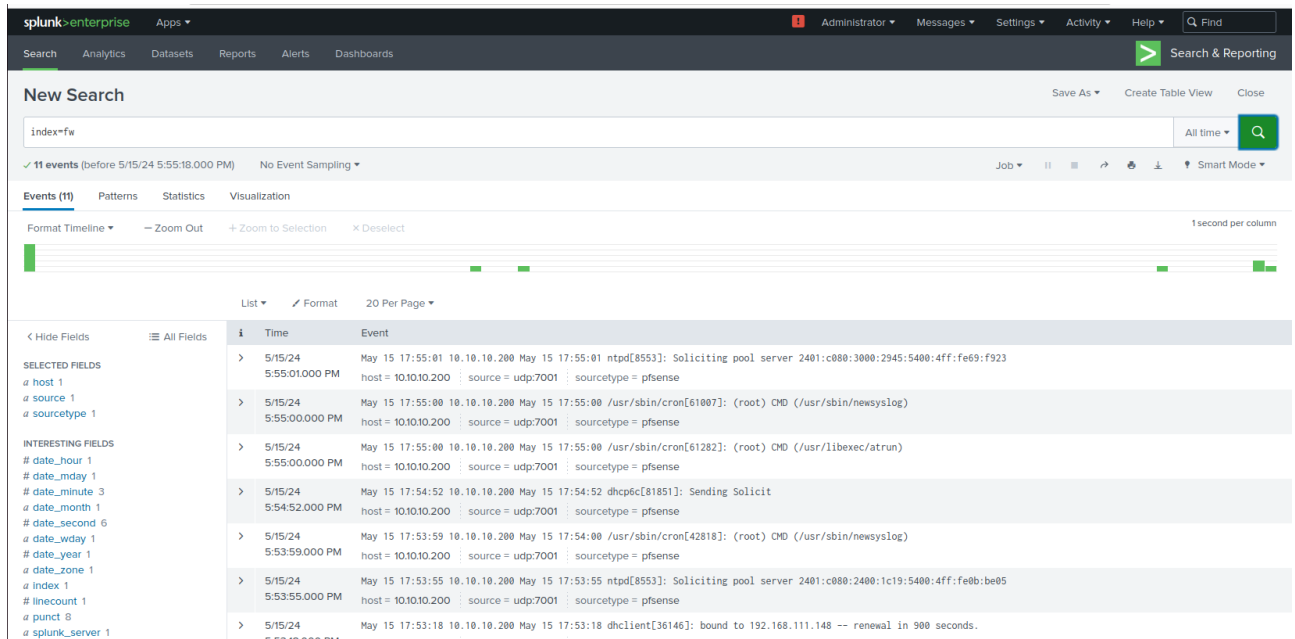
Remote log servers

Remote Syslog Contents

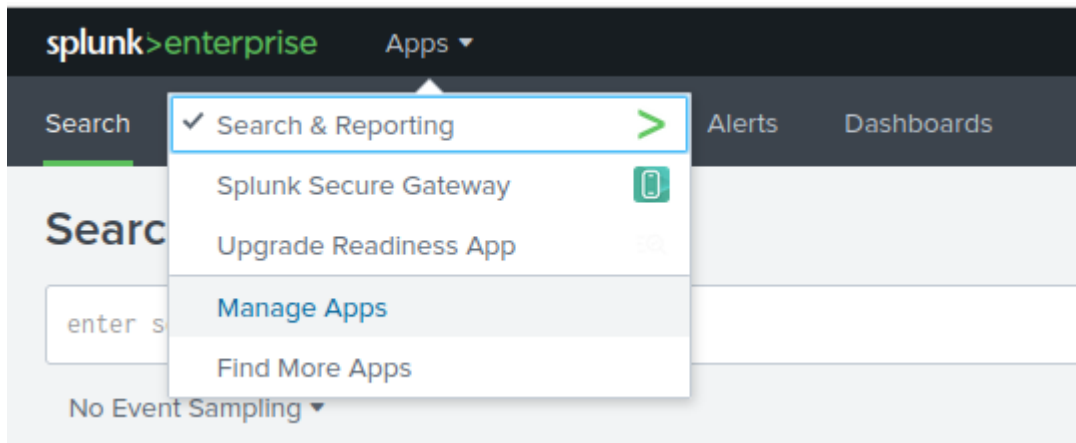
- ☒ Everything
- ☐ System Events
- ☐ Firewall Events
- ☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- ☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- ☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- ☐ General Authentication Events
- ☐ Captive Portal Events
- ☐ 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.

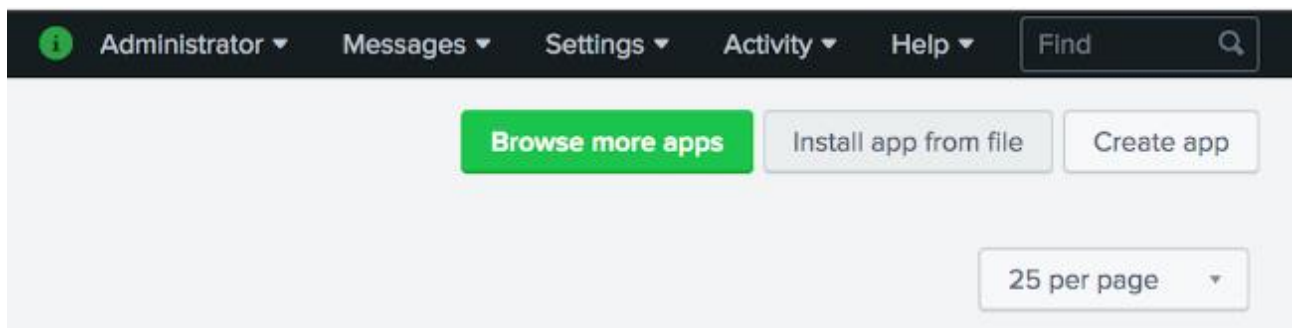
- Kiểm tra thử log với index=fw :



- Cài đặt Technical-Add-On theo đường dẫn <https://splunkbase.splunk.com/app/1527> , vào tập Apps chọn ManageApps:



- Chọn Install app from file:



- Chọn file TA đã tải và upload

Install App From File

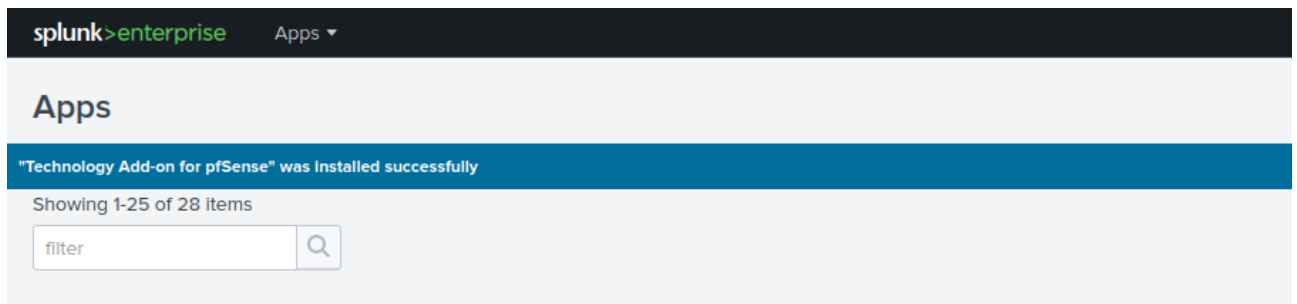
If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

☐ Upgrade app. Checking this will overwrite the app if it already exists.

- Cài đặt thành công :

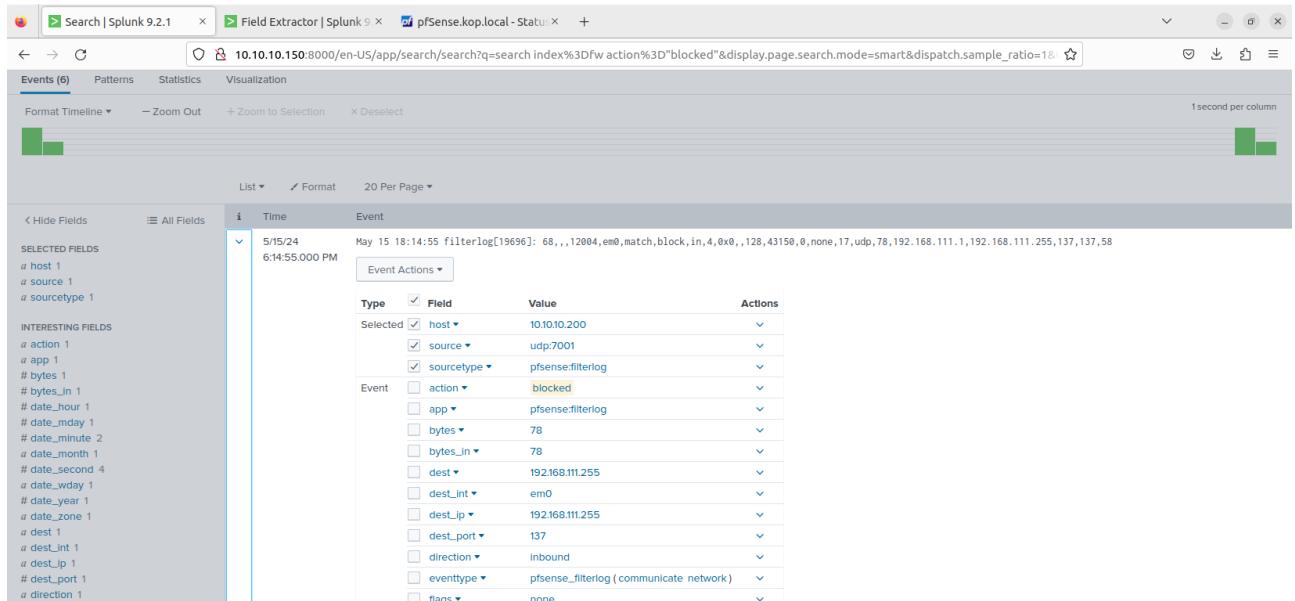


- Kiểm tra log block traffic của pfsense:

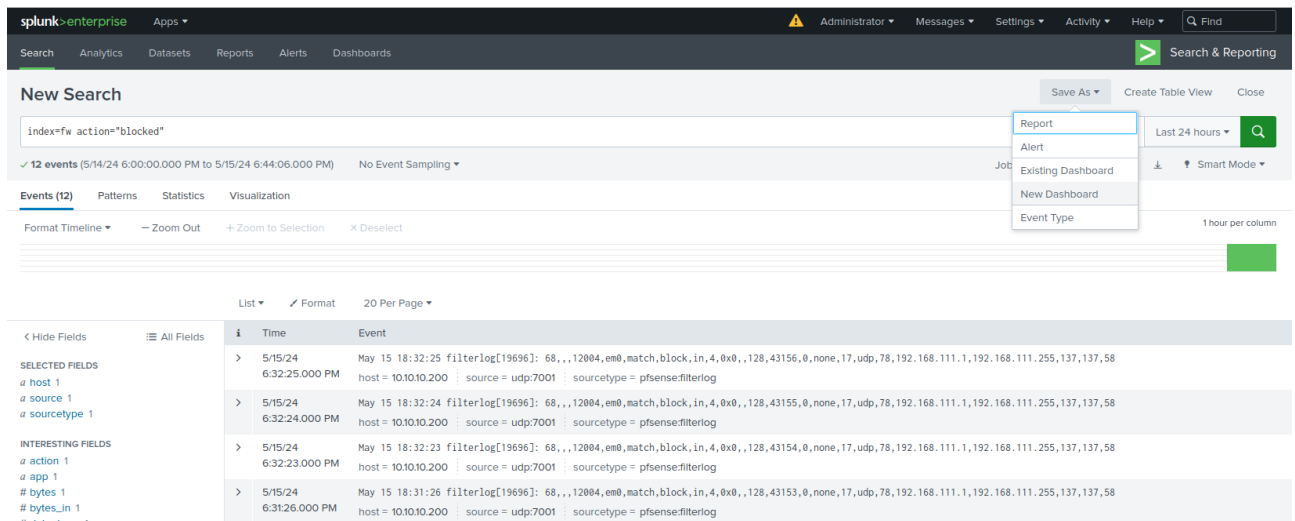
The screenshot shows the Splunk Search interface. The search bar contains the query "index=fw action=blocked". Below the search bar, it indicates "6 events (before 5/15/24 6:19:36.000 PM)". The results are displayed in a table with columns for Time, Event, and various fields.

| Time | Event |
|------------------------|--|
| 5/15/24 6:14:55.000 PM | May 15 18:14:55 filterlog[19696]: 68,,12004,em0,match,block,in,4,0x0,,128,43150,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 host = 10.10.10.200 : source = udp:7001 : sourcetype = pfsense:filterlog |
| 5/15/24 6:14:54.000 PM | May 15 18:14:54 filterlog[19696]: 68,,12004,em0,match,block,in,4,0x0,,128,43149,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 host = 10.10.10.200 : source = udp:7001 : sourcetype = pfsense:filterlog |
| 5/15/24 6:14:54.000 PM | May 15 18:14:54 filterlog[19696]: 68,,12004,em0,match,block,in,4,0x0,,128,43148,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 host = 10.10.10.200 : source = udp:7001 : sourcetype = pfsense:filterlog |
| 5/15/24 6:13:58.000 PM | May 15 18:13:58 filterlog[19696]: 68,,12004,em0,match,block,in,4,0x0,,128,43147,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 host = 10.10.10.200 : source = udp:7001 : sourcetype = pfsense:filterlog |
| 5/15/24 6:13:57.000 PM | May 15 18:13:57 filterlog[19696]: 68,,12004,em0,match,block,in,4,0x0,,128,43146,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 host = 10.10.10.200 : source = udp:7001 : sourcetype = pfsense:filterlog |
| 5/15/24 6:13:57.000 PM | May 15 18:13:57 filterlog[19696]: 68,,12004,em0,match,block,in,4,0x0,,128,43145,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 host = 10.10.10.200 : source = udp:7001 : sourcetype = pfsense:filterlog |

- Kiểm tra thử action của 1 event:



- Để xây dựng 1 dashboard ta search log, chọn Save As và chọn New Dashboard:



- Điền thông tin và Save to dashboard:

Save Panel to New Dashboard

Dashboard Title

BlockLogTraffic

blocklogtraffic

Edit ID

Description

Optional

Permissions

Private

How do you want to build your dashboard?

What's this?

Classic Dashboards

The traditional Splunk dashboard builder

Dashboard Studio

NEW

A new builder to create visually-rich, customizable dashboards

Panel Title

Optional

Visualization Type

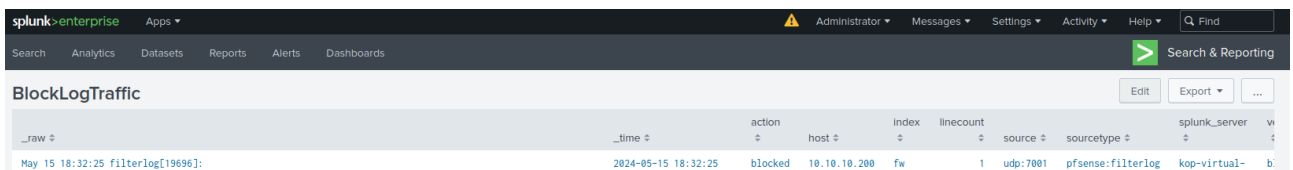
Events

Advanced Panel Settings

Cancel

Save to Dashboard

- Chọn Edit và tùy chỉnh visualization:



| raw | time | action | host | index | linecount | source | sourcetype | splunk_server | ... |
|-----------------------------------|---------------------|---------|--------------|-------|-----------|----------|-------------------|---------------|-----|
| May 15 18:32:25 filterlog[19696]: | 2024-05-15 18:32:25 | blocked | 10.10.10.200 | fw | 1 | udp:7001 | pfsense:filterlog | kop-virtual- | b: |

- Xây dựng thử 1 dashboard dựa trên các log blocktraffic:

The screenshot shows the Splunk Enterprise web interface. At the top, there are tabs for various dashboards and a search bar. The main content area displays the results of a search for 'BlockLogTraffic'. The results are presented in a table with columns for raw data, time, action, host, index, linecount, source, sourcetype, and splunk_server. The table shows several entries for blocked traffic from 10.10.10.200 to 10.10.10.255. A 'Select visualization' dropdown menu is visible next to the first result.

| _raw | _time | action | host | index | linecount | source | sourcetype | splunk_server |
|--|---------------------|---------|--------------|-------|-----------|----------|-------------------|---------------------|
| May 15 18:32:25 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43156,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:32:25 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:32:24 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43155,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:32:24 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:32:23 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43154,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:32:23 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:31:26 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43153,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:31:26 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:31:25 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43152,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:31:25 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:31:24 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43151,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:31:24 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:14:55 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43150,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:14:55 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:14:54 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43149,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:14:54 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:14:54 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43148,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:14:54 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |
| May 15 18:13:58 filterlog[19696]: 68,,12004,en0,match,block,in,4,0x0,,128,43147,0,none,17,udp,78,192.168.111.1,192.168.111.255,137,137,58 | 2024-05-15 18:13:58 | blocked | 10.10.10.200 | fw | 1 | udp:7801 | pfsense:filterlog | kop-virtual-machine |