**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**CÀI ĐẶT VÀ SỬ DỤNG**

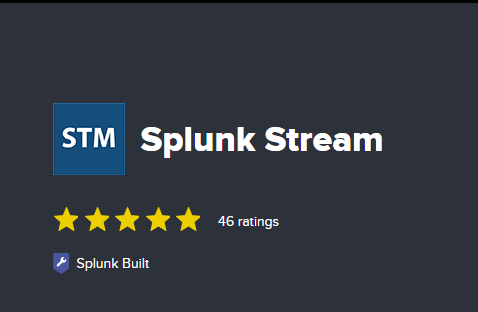
**SPLUNK APP FOR STREAM**

Người thực hiện: Mai Thành Thắng

Hà Nội 10/2019

# Cài đặt app Stream trên Splunk server

## 1, Thông tin cơ bản về app



* Một luồng( stream) là nhóm các sự kiện xác định từ giao thức mạng cụ thể và tập hợp trên nhiều trường
* App là một ứng dụng dùng để chụp, lọc, lập chỉ mục và phân tích luồng dữ liệu sự kiện.
* Chụp lại gói tin từ thiết bị NAS(Network Attached Storage) để phục vụ cho quá trình điều tra số gói tin thô.
* Chụp lại các thông tin lưu lượng bao gồm: NetFlow v5, v9, jFlow, and sFlow, and IPFIX,… gửi về indexer của bạn
* Lưu dạng gói PCAP theo thời gian thực hoặc có điều kiện. Tạo một hàm băm MD5 đính kèm tương ứng với mức nguy hiểm tương ứng sử dụng Splunk ES (Enterprise Security). Giải nén lưu trữ tập tin lại phục vụ cho điều tra số hoặc ngăn ngừa mất dữ liệu ( Data Loss Prevention (DLP))
* Phân tích câu lệnh SQL giúp ta hiểu hành động phía người dùng hơn, hiểu được kết nối IP client – server với mô hình hóa dữ liệu.
* Thành phần của Stream app:
  + Splunk\_app\_stream: cung cấp cấu hình quản trị Splunk\_TA\_Stream và cấu hình chụp lại sự kiện trên nhiều giao thức mạng
  + Splunk\_TA\_stream: Chứa luồng forwarder (streamfwd binary) , thu thập hay chụp sự kiện một cách thụ động từ các thiết bị mạng, gửi về indexer dạng dây dữ liệu theo từng module đầu vào.
  + Independent Stream forwarder( giao nhận độc lập): hộ trợ việc nhận dữ liệu độc lập từ os Linux ví dụ như chụp lại sự kiện về dữ liệu mạng của host linux mà bạn muốn theo dõi trong dịch vụ của Splunk IT Service Intelligence. Không có thành phần nào nền tảng Splunk yêu cầu bạn cài đặt Stream Forwarder

**Lưu ý**: set quyền root trên máy Linux thì Splunk\_TA\_stream mới có thể tiến hành chụp dữ liệu từ phía máy trạm:

$SPLUNK\_HOME/etc/apps/Splunk\_TA\_stream.

sudo ./set\_permissions.sh

Trên máy window server phải chạy quyền administrator hoặc cài đặt winpcap

## 2, Source and sourcetype :

"source=stream:stream-id" và "sourcetype=stream:protocol". Trường id thường là tên giao thức.  ví dụ: "sourcetype=stream:http."

## 3, Cài đặt app:

* Vào đường link: <https://splunkbase.splunk.com/app/1809/#/details> dowload app
* Click **Manage Apps > Install app from file**.
* Upload the splunk-stream\_<latest\_version>.tgz installer file.
* Restart Splunk Enterprise (if prompted). This installs splunk\_app\_stream and splunk\_TA\_stream

in $SPLUNK\_HOME/etc/apps.

* Run the set\_permissions.sh script to set permissions for Splunk\_TA\_stream.

# Cài đặt trên phía server splunk, máy trạm

## 1. Trên Server Splunk

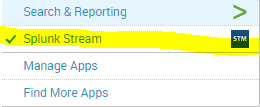
- Cài đặt cổng nhận event gửi từ máy trạm

- **Settings > Forwarding and Receiving**. Chọn **Configure Receiving -> add new**

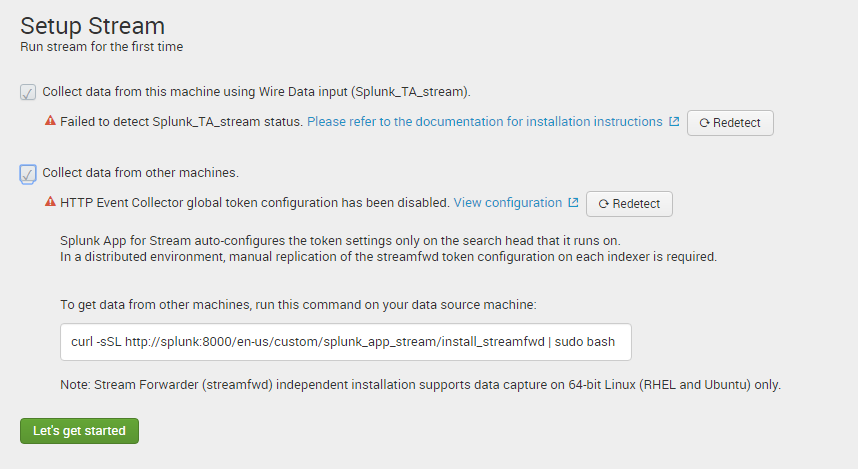
**-**  Nhập port 9997 và **save**



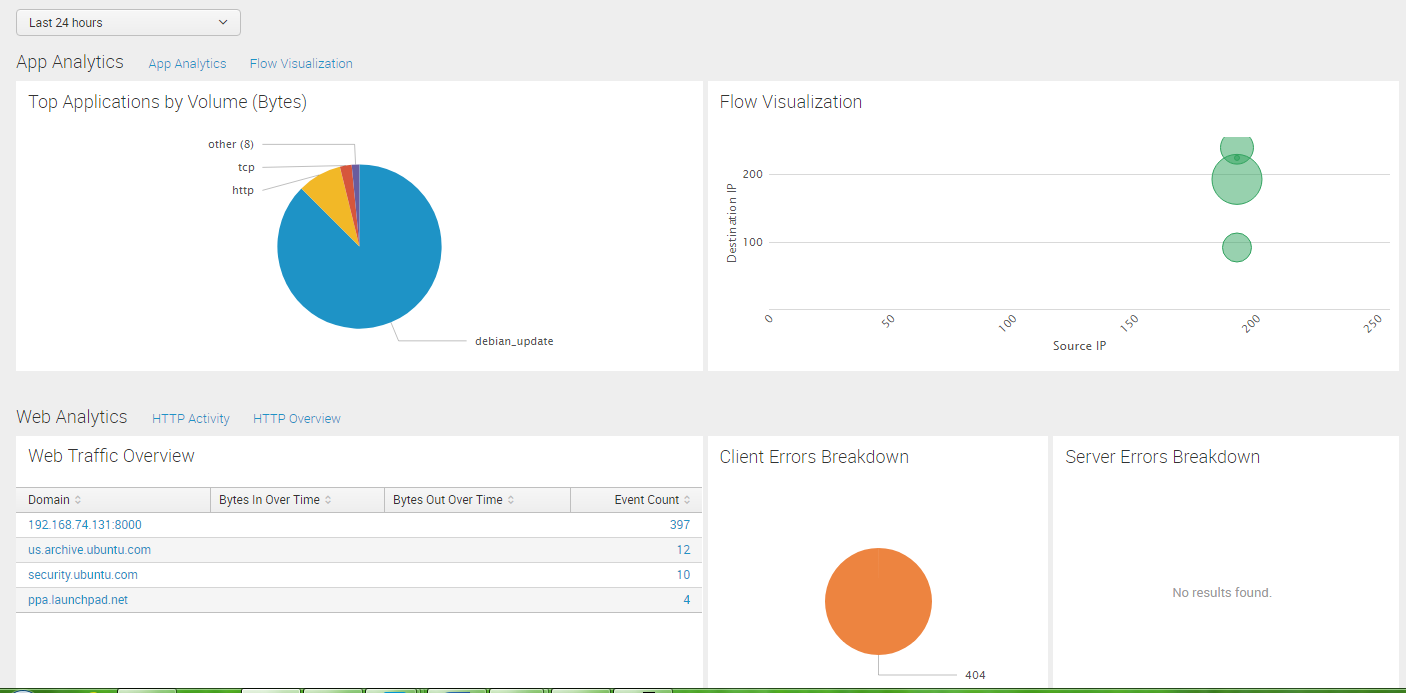
* Vào mục app chọn app Splunk stream



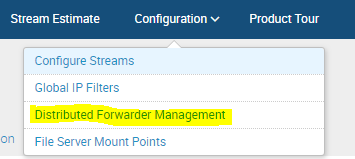
Sau đó sẽ có màn hình bạn lựa chọn nhận dữ liệu từ đâu bạn có thể tích ô “**collect data from other machine**” để lấy thông tin cấu hình trên máy trạm còn nếu không thì sau khi vào giao diện Splunk bạn phải thực hiện bước sau để lấy lệnh cấu hình.



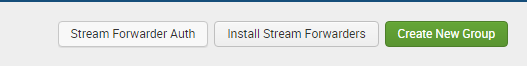
* Ban đầu khi vào chỉ có thông tin của máy splunk server do chưa cấu hình gửi thông tin từ máy trạm về.



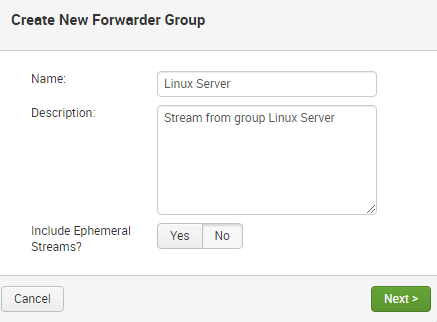
* Trên giao diện splunk chọn như hình để lấy thông tin cấu hình trên máy trạm



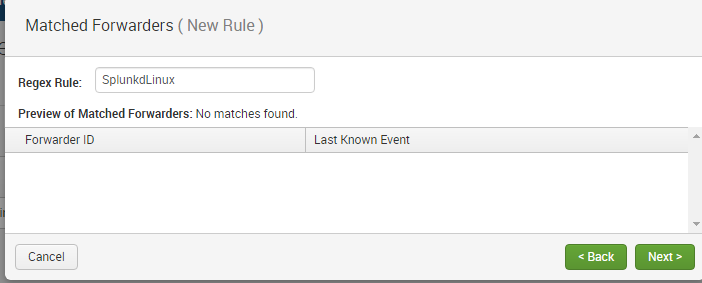
* Ở đây chúng ta có thể tạo group để theo dõi theo loại máy trạm nếu trong hệ thống có nhiều hoặc có thể intall trực tiếp một máy trạm cho nó vào group mặc định. Hoặc tạo “Stream Forwarder Auth” tức là cài đặt phương thức giao nhận an toàn trên web là https



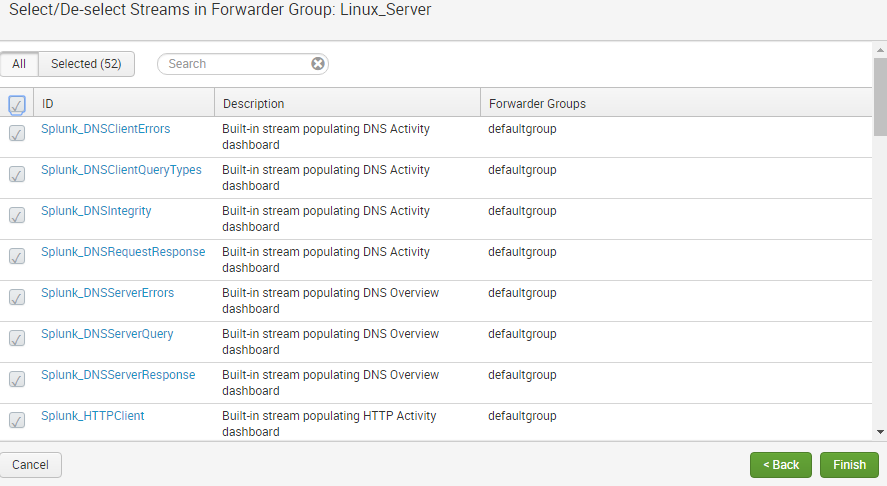
* Trong thông tin lấy bạn có lấy bao gồm thông tin phụ khác không mặc định là không.



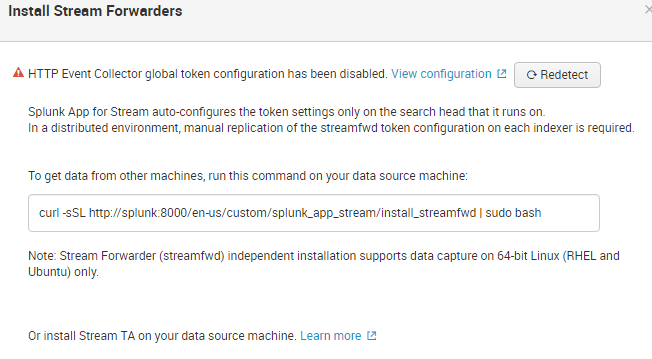
* Tạo môt quy tắc mới cho nhóm này ví du: SplunkdLinux



* Chọn luồng nhận cho nhóm. Ở đây lấy tất cả các loại event



* Install stream forward để lấy thông tin cho việc cài đặt.



## 2. Cài đặt trên máy trạm

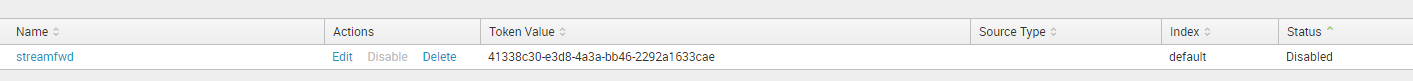
- Copy link: curl -sSL http:// ipsplunkSRV:8000/en-us/custom/splunk\_app\_stream/install\_streamfwd | sudo bash và thực hiện chạy trên máy trạm( tùy máy sẽ có thông tin cấu hình khác nhau)

- Có thể chạy lệnh này tự động đề không mất thời gian: curl -sSL http://ipsplunkSRV:8000/en-us/custom/splunk\_app\_stream/install\_streamfwd | sudo bash -s -- --accept-defaults

- Khởi động lại streamfwd: sudo service streamfwd start

## 3. Cấu hình bật HTTP Event Collector để nhận sự kiện từ forwarder

- Vào **setting->data input -> HTTP Event Collector**



* Chọn **Global setting**  và **Enable -> Save**
* Trường hợp trên máy trạm vẫn không thể khởi động streamfwd ta sử lý như sau:

Kill stream if its running “killall -9 streamfwd”

Remove the init script

“update-rc.d -f streamfwd remove”

rm /etc/init.d/streamfwd

Create a new service unit file for systemd /etc/systemd/system/streamfwd.service

[Unit]

Description= Splunk Stream Dedicated Service

After=syslog.target network.target

[Service]

Type=simple

ExecStart=/opt/streamfwd/bin/streamfwd –D

[Install]  
WantedBy=multi-user.target  
Alias=splunkstream.service

Enable the new service “systemctl enable streamfwd”

**Lưu ý:** Khi bị lỗi DNS không kết nối nguyên nhân là bạn chưa khai báo kết nối trỏ về DNS Nameserver của Splunk bạn phải vào sửa /etc/resolvconf/resolv.conf.d/base

**add thêm:**Nameserver ip\_splunk\_server

sudo resolvconf -u

**ảnh lỗi:**



## 4. Configure file extraction( cấu hình trích xuất tập tin)

Mục đích lưu trữ file trích xuất cơ bản được định nghĩa trong luồng siêu dữ liệu.

**Các bước thực hiện:**

**Bước 1:** Cài đặt thiết lập một file lưu trữ: đơn giản xây dựng một file server( NFS)

Mount dữ liệu từ splunkfwd về máy file server.

* Install and Config file server:

Update packet

sudo apt install nfs-kernel-server

sudo nano /etc/exports

/path/to/directory client-IP address(options)

(ví dụ: /home/streamload 192.168.74.139(rw,sync,no\_root\_squash,no\_subtree\_check))

* Configure the Client:

Update packet

sudo apt install nfs-common

sudo nano /nfs/home( file mount point)

ipserver:/dir mount dir mount point

vd:

mount –t nfs 192.168.74.131:/home/streamload(file mount) /nfs/home(mount point)

Bước 2: Add file server parameters to streamfwd.conf

Trong splunkserver sửa trong file local/streamfwd.conf

[streamfwd]

fileServerId =192.168.74.131:/StreamLoad

fileServerMountPoint = /home/streamload

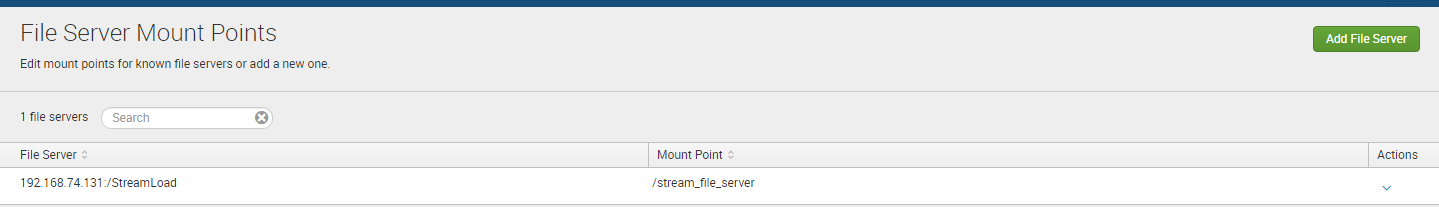
Khởi động lại splunk

Bước 3: Configure mount point for file server

In the splunk\_app\_stream UI, click **Configuration > File Server Mount Points**.

Click **Add File Server**.

Specify the File Server and Mount Point. Click **Create.**



## 5. Configure targeted packet capture

- Làm tương tự như cấu hình file trích xuất

[streamfwd]

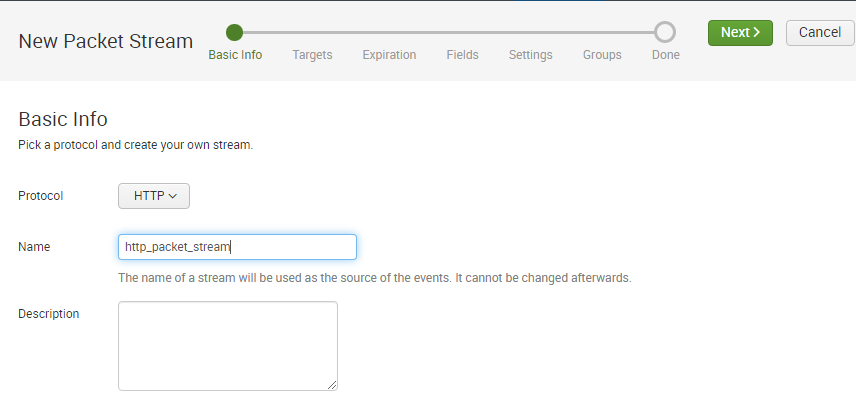
fileServerId = nfs:192.168.74.131:/StreamLoad

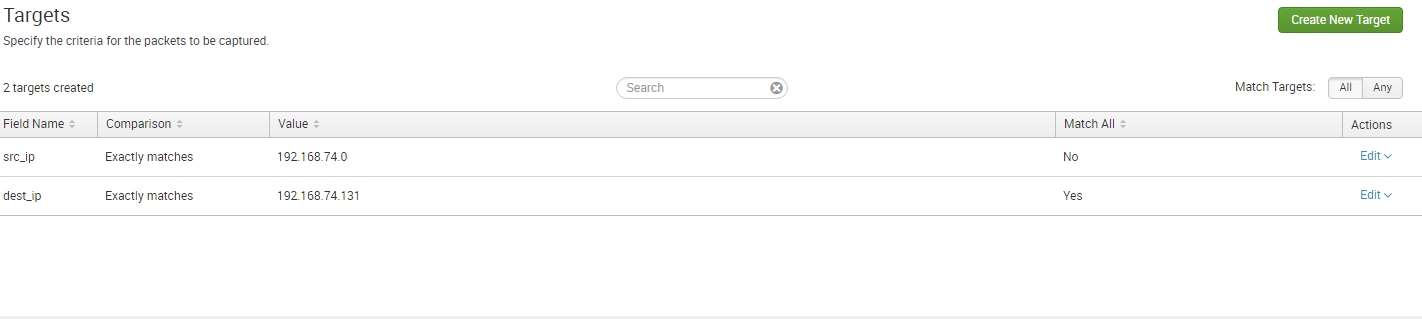
fileServerMountPoint = /usr/local/packetcaptures

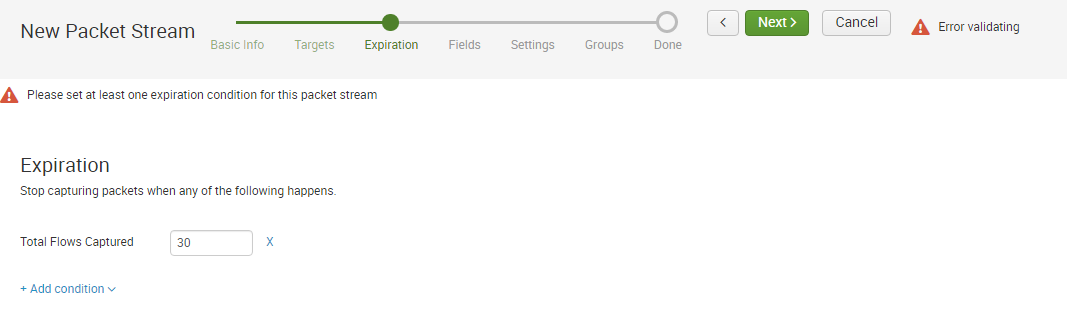
* Chúng ta tạo thêm 1 file packet stream

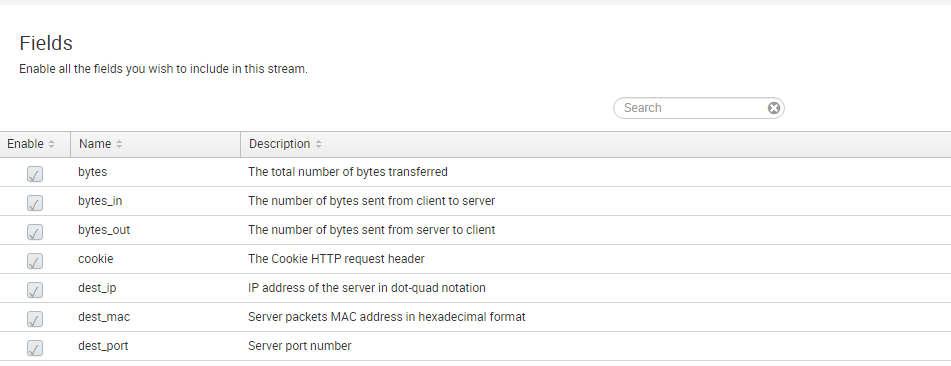
In splunk\_app\_stream, click **Configuration > Configure Streams.**

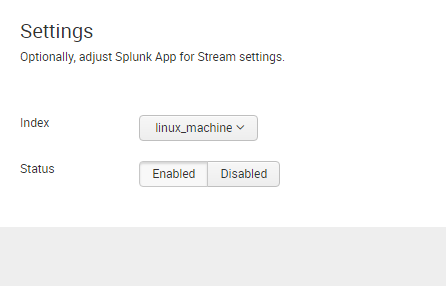
Click **New Stream > Packet Stream**

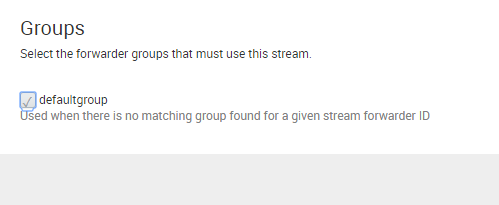


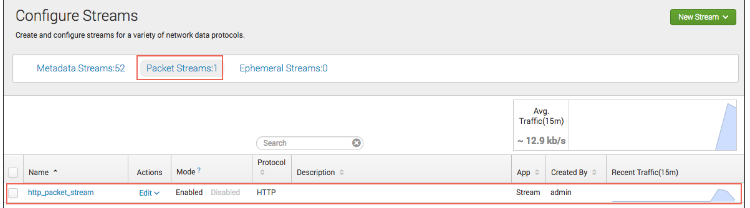












## 6. Configure Flow collector( cấu hình thu nhận dữ liệu mạng)

* Hỗ trợ nhận dữ liệu từ các thiết bị mạng. Một số flow protocol:

NetFlow version 5, 9 and IPFIX.

sFlow version 5

jFlow

* Cấu hình [Deploy Independent Stream forwarder](http://docs.splunk.com/Documentation/StreamApp/7.1.3/DeployStreamApp/InstallStreamForwarderonindependentmachine).
* Enable HTTP Event Collector
* Cấu hình nhận dữ liệu trong file local/streamfwd.conf cấu hình trên UF:

netflowReceiver.<N>.ip = <ip\_address>

netflowReceiver.<N>.port = <port\_number>

netflowReceiver.<N>.decoder = <flow\_protocol>

[streamfwd]

logConfig = streamfwdlog.conf

port = 8889

netflowReceiver.0.ip = 172.23.245.122

netflowReceiver.0.port = 9995

netflowReceiver.0.decoder = netflow

netflowReceiver.1.ip = 172.23.245.122

netflowReceiver.1.port = 6343

netflowReceiver.1.decoder = sflow

netflowReceiver.0.decodingThreads = 4( đối với lưu lượng lớn)

## 7. Configure 10Gbps network capture

- Đầu tiên phải tối ưu hóa môi trường linux( nếu bạn đang chạy nó)

Edit **/etc/grub.conf**.

Thêm các tham số này vào dòng khởi động kernel của bạn để định cấu hình mười sáu vòng đệm: **default\_hugepagesz=1G hugepagesz=1G hugepages=16**.

Tùy cấu hình phần cứng của bạn có thể add thêm :

kernel /vmlinuz-2.6.32-573.3.1.el6.x86\_64 ro root=/dev/mapper/vg\_cmload02-lv\_root rd\_LVM\_LV=vg\_cmload02/lv\_root rd\_NO\_LUKS LANG=en\_US.UTF-8 rd\_NO\_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto rd\_LVM\_LV=vg\_cmload02/lv\_swap KEYBOARDTYPE=pc KEYTABLE=us rd\_NO\_DM default\_hugepagesz=1G hugepagesz=1G hugepages=16 rhgb quiet

Sau khi chỉnh sửa phải reboot lại

**Configure 10Gb dedicated capture mode**

**+)** Enable dedicated capture:

* Sửa nội dung trong file local/streamfwd.conf

**[streamfwd]**

**port = 8889**

**ipAddr = 127.0.0.1**

**dedicatedCaptureMode = 1**

* Reboot

**+) Xác định các giao diện phù hợp:**

* Dùng lệnh: **./linux\_x86\_64/bin/streamfwd –iflist**

+) **Chỉ định địa chỉ lấy thông tin:**

**[streamfwd]**

**port = 8889**

**ipAddr = 127.0.0.1(** Ví dụ là lấy ip localhost của splunkserver**)**

**dedicatedCaptureMode = 1**

**streamfwdcapture.0.interface = 0000:04:00.0(** phù hợp với interface dùng cho ip machine của bạn)

Reboot

**Note**: Sử dụng lệnh này để xem trợ giúp **./streamfwd –h (** nó nằm trong $SPLUNK\_HOME/etc/apps/Splunk\_TA\_stream/<OS\_arch>/bin**)**

Xem hướng dẫn cấu hình streamfwd.conf trong **README/streamfwd.conf.spec**

## 8. Configure universal forwarder for Splunk\_TA\_stream

- Gửi dữ liệu về **\_internal index** splunk . Mọi log event, stats.streamfwd lưu trữ trong index này. Chúng ta có thể xem theo đường dẫn $SPLUNK\_HOME/var/log/splunk/

- Sửa đổi giới hạn nhận dữ liệu:

Sửa theo đường dẫn $SPLUNK\_HOME/etc/apps/SplunkUniversalForwarder/local/limits.conf.

Sửa khổ [thruput] . ví dụ:

[thruput]

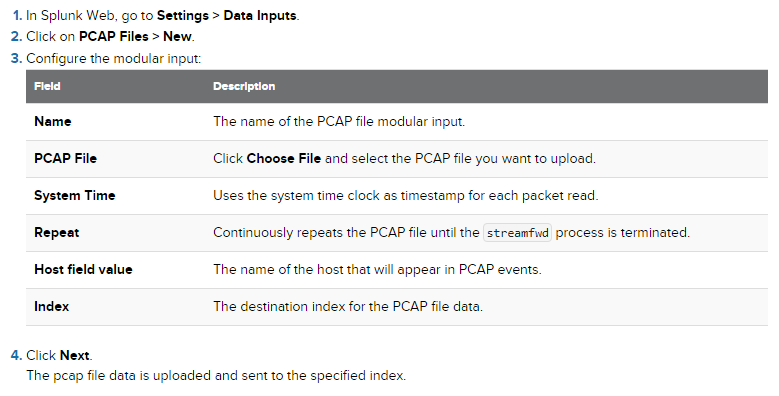
maxKBps = 0

## 9. Use Splunk Stream to parse pcap files:

- Lưu ý chỉ hỗ trợ định dạng .pcap hay .pcapng on linux và mac còn window chỉ có .pcap

- Nhập gói tin pcap: upload, dùng cli, chèn vào file streamfwd.conf

- **Upload file Pcap**



* **Sử dụng CLI:**

streamfwd [-r FILE1]... [--pcapdir DIR1]... [pcap\_options] [options] [output\_option]

* Chỉnh sửa file streamfwd.conf

Chúng ta sửa thành phần **streamfwdcapture**

Ví dụ:

* Tập tin duy nhất:

[streamfwd]

streamfwdcapture.0.offline = true

streamfwdcapture.0.interface = /tmp/server1.pcap

streamfwdcapture.0.repeat = true

* Giám sát thư mục:

[streamfwd]

streamfwdcapture.0.offline = true

streamfwdcapture.0.interface = /tmp/test\_pcap\_dir

* Giám sát trên nhiều thư mục:

[streamfwd]

streamfwdcapture.0.offline = true

streamfwdcapture.0.interface = C:\temp\pcap\_dir\_1

streamfwdcapture.0.sysTime = true

streamfwdcapture.1.offline = true

streamfwdcapture.1.interface = C:\temp\pcap\_dir\_2

streamfwdcapture.1.afterIngest = delete

(ý nghĩa từng khổ: khổ đầu là trong quá trình app stream chạy file .pcap lưu trữ trong thư mục C:\temp\pcap\_dir\_1 theo thời gian hệ thống.

Khổ thứ 2 : Nếu trong thư mục C:\temp\pcap\_dir\_2 đã tồn tại file cũ nó sẽ xóa bỏ và lưu file mới trong quá trình app stream chạy)

* Giám sát cả interface và thư mục:

streamfwdcapture.0.offline = false

streamfwdcapture.1.offline = true

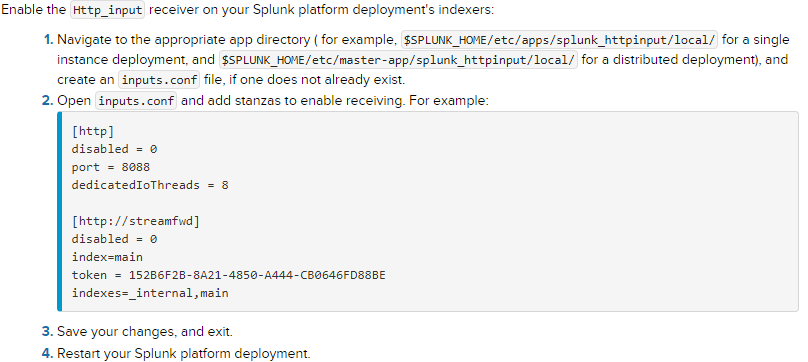
streamfwdcapture.1.interface = /tmp/test\_pcap\_dir

## 10. Use Splunk Stream chụp lấy dữ liệu Netflow and IPFIX:

- Netflow: (Cisco -1996) cung cấp khả năng thu thập lưu lượng truy cập mạng IP khi nó xâm nhập hoặc thoát khỏi giao diện

- IPFIX (IP Flow Information Export ): là một tiêu chuẩn IETF được tạo ra để giám sát và xuất luồng thông tin qua các router, switch và các thiết bị mạng khác.

**\* Cấu hình Indexer:**



**\*Cấu hình trình chuyển tiếp Stream độc lập**

Sửa trong file **streamfwd.conf:**

[streamfwd]

httpEventCollectorToken = 152B6F2B-8A21-4850-A444-CB0646FD88BE

#(Match this with the token in the indexers)

ipAddr = 0.0.0.0 ( ip máy chạm)

processingThreads = 4

#Set the minimum system Ulimits

Ulimit -n 64000

Ulimit -u 16000

* Điều hướng chuyển tiếp dữ liệu sang thư mục **etc/sysctl.conf**
* Chỉnh sửa cấu hình Kernel của máy đáp ứng luồng dữ liệu lớn

Sysctl -w net.core.rmem\_default = 33554432

Sysctl -w net.core.rmem\_max = 33554432

Sysctl -w net.core.netdev\_max\_backlog = 10000

* Load lại : **/sbin/sysctl –p**
* Khởi động lại streamfwd: **Service streamfwd restart**
* Triển khai cấu hình Netflow trong streamfwd.conf

[streamfwd]

httpEventCollectorToken = <GUID>

indexer.0.uri= <HEC VIP>

netflowReceiver.0.port = 9996

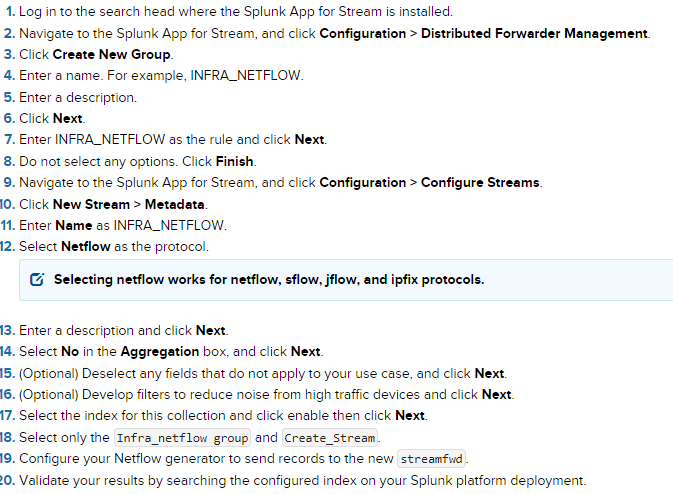
netflowReceiver.0.decoder = netflow

netflowReceiver.0.ip = 172.18.1.4

netflowReceiver.0.decodingThreads = 16

* Lưu lại và khởi động lại app

\***Cấu hình search head**



## 11. Sử dụng một cấu hình mẫu Stream

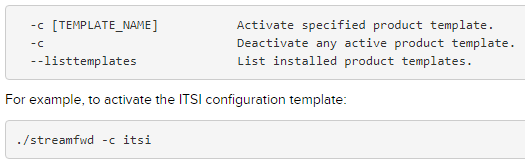
- Cung cấp cho chúng ta :

**Splunk IT Service Intelligence (ITSI):** mẫu cấu hình cung cấp các trường giao thức tùy chỉnh ánh xạ tới số liệu, dữ liệu.

**Enterprise Security (ES):** Mẫu cấu hình cung cấp trường giao thức tùy chỉnh tới cấu trúc CIM ( chuẩn của splunk thiết kết báo cáo)

- Cấu hình:add thêm dòng **configTemplateName=<product name>** trong **streamfwd.conf**

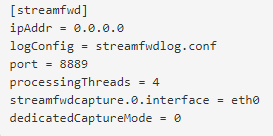
- CLI và ví dụ:



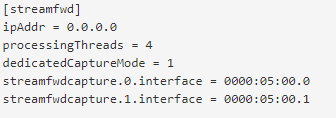
## 12. Splunk Stream performance tests and considerations( kiểm tra hiệu xuất và xem xét)

- Kiểm tra hệ phần cứng.

- Cấu hình trên UF phía máy trạm: /streamfwd/default/streamfwd.conf

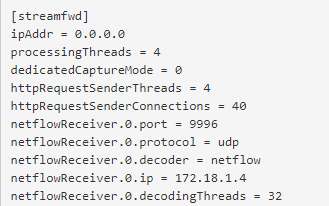


* Cấu hình mội trường nhận dữ liệu độc lâp trên Splunk server:



Gửi event theo từng giao diện khác nhau, Luồng sự kiện HTTP, TCP/UDP theo dòng hay là tổng hợp

* Cấu hình môi trường thu nhận lưu lượng splunk:



# Search and report

## Cấu hình tạo dashboard ssh

* Sau khi cấu hình deloyment uf xong ta sẽ luôn chạy file **set\_permissions.sh**  của trên + Splunkserver trong deployment-app/ Splunk\_TA\_stream và /apps/ Splunk\_TA\_stream/

+ Trên splunk máy trạm vào /opt/splunkforwarder/etc/apps/Splunk\_TA\_stream và sửa nội dung **input** thành:

[streamfwd://streamfwd]

splunk\_stream\_app\_location = http://192.168.74.131:8000/en-us/custom/splunk\_app\_stream/

stream\_forwarder\_id =

disabled = 0

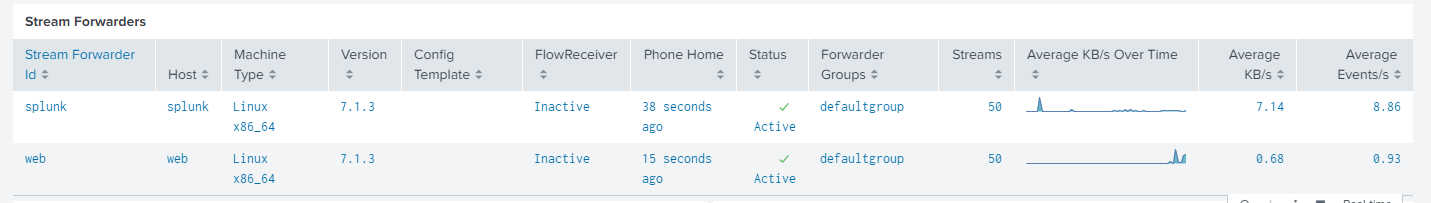
Và sửa cả file **input** trong /opt/streamfwd/local của UF

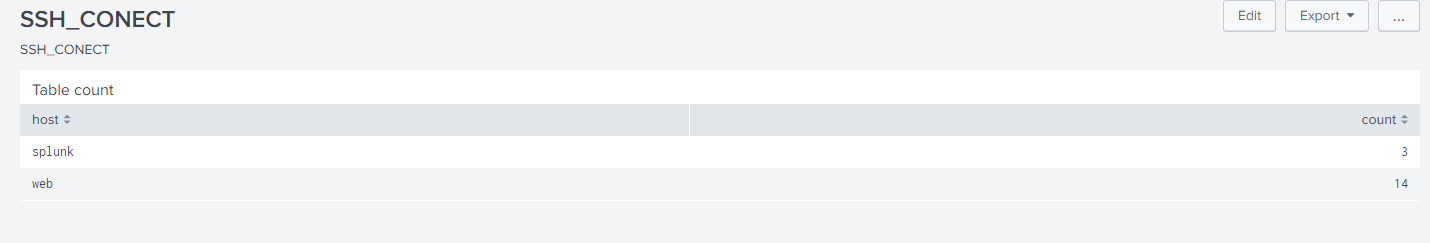
[streamfwd://streamfwd]

splunk\_stream\_app\_location = http://192.168.74.131:8000/en-us/custom/splunk\_app\_stream/

disable = 0

Kết quả:





## Giao diện dashbash tổng quát

