**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**CÀI ĐẶT NHẬN LOG**

**TỪ THIẾT BỊ MẠNG**

Người thực hiện: Mai Thành Thắng

Hà Nội 2019

# CẤU HÌNH TRÊN THIẾT BỊ

**Cấu hình trên thiết bị CISCO**

router# config t  
router(config)# logging trap notifications  
router(config)# logging 1.1.1.1; log gửi về splunk server qua cổng 514udp mặc định hoặc có thể chỉnh sửa

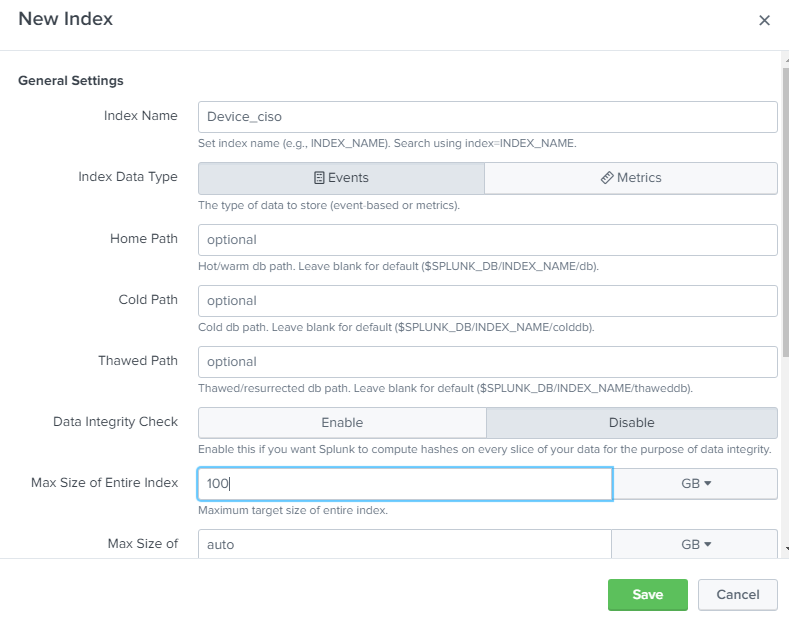
router(config)# archive  
router(config-archive)# log config  
router(config-archive-log-cfg)# logging enable  
router(config-archive-log-cfg)# logging size 1000  
router(config-archive-log-cfg)# hidekeys ;nó sẽ không gửi pass word lên syslog  
router(config-archive-log-cfg)# notify syslog  
router(config-archive-log-cfg)#exit

# Cấu hình trên Splunk server

## Cấu hình nhận Log trên Splunk server

### Cấu indexer Splunk

1. Click **Settings**
2. Click **Indexes**
3. Click **New index**
4. Creat as image



### b*. Splunk Settings:*

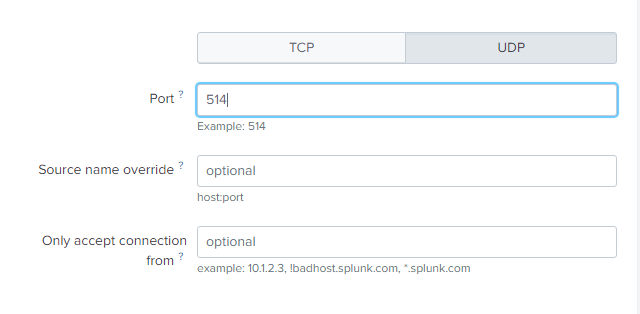
**1.** Click **Settings**.

**2.** Click **Data Inputs**.

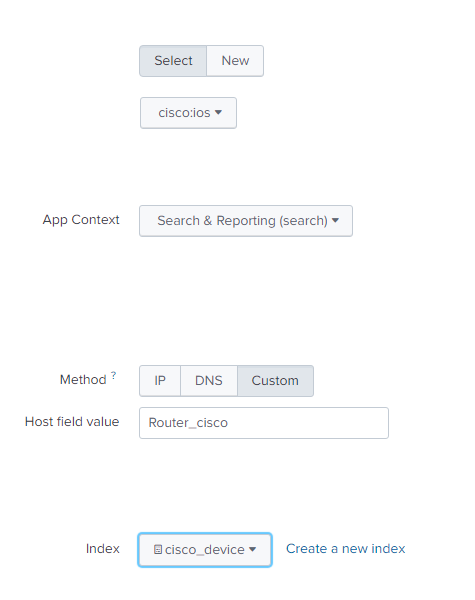
**3.** Choose **UDP**  in **Local Input**.

**4.** Click **Add New** to add an input.

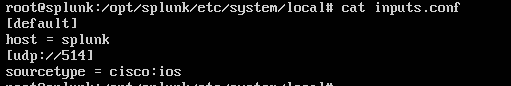
**5.** Config as image, click **Next**



**6**. Next config as image and review and test



### c. Cấu hình trong splunk server



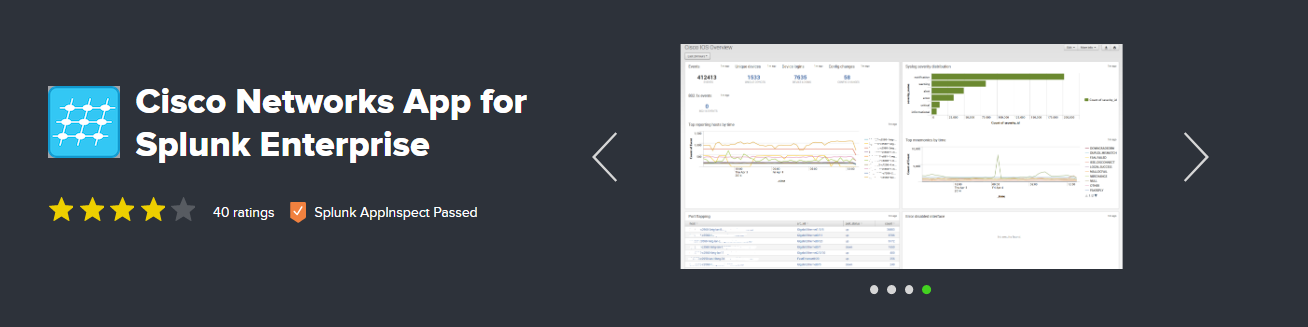
Ta có thể chính sửa nó nghe trên cổng TCP thay vì UDP trong mục này.

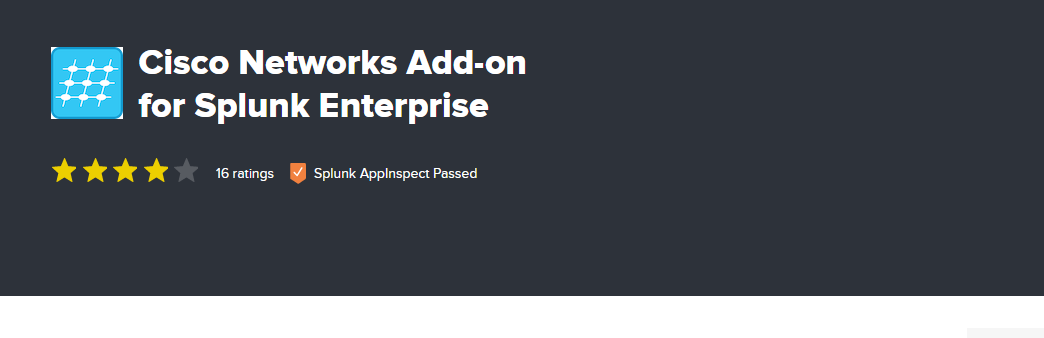
## 2. Cài đặt App và Add-on

- Lên web search app and add-on:

### **Cisco Networks App for Splunk Enterprise**

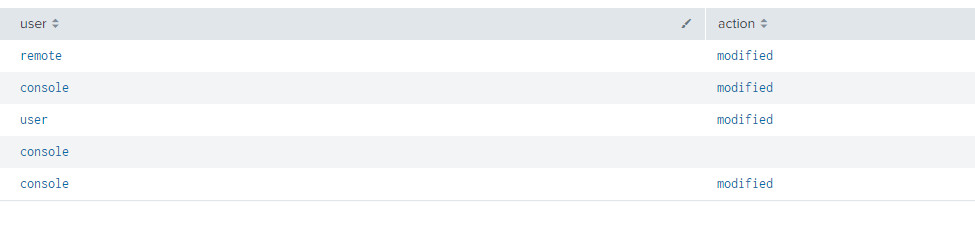
**Cisco Networks Add-on for Splunk Enterprise** (TA-cisco\_ios)





# Search and report

Khi tim kiếm tạo báo cáo thủ công về action của user:



Khi dùng app tạo mẫu báo cáo tồng hợp khá chi tiết trực quan cho người dùng



Thiết lập một cảnh báo thời gian thực khi thiết bị gặp lỗi

