nProbe Splunk App - Quick Start

Version 1.0
January 2014

ntop site	www.ntop.org
Splunk App Web	

Table of Contents

1. Installation 4
2. Export flows from nProbe to Splunk 5
3. nProbe splunk app 6

1. Installation

Step 1: Install and configure Splunk

First, download Splunk from our download site. Install using the documentation and default settings. Once Splunk is installed, you should open a browser and go to http://localhost:8000.

Step 2: Install the nProbe splunk app

Once installed Splunk, you can install the nProbe app for splunk by the Splunk App store (http://apps.splunk.com/app/1721/) or as follows:

The application is therefore ready to be used and Splunk is now listening for data from nProbe on port 3333. You will need to make sure that the machine on which your Splunk is running on has the appropriate firewall ports open.

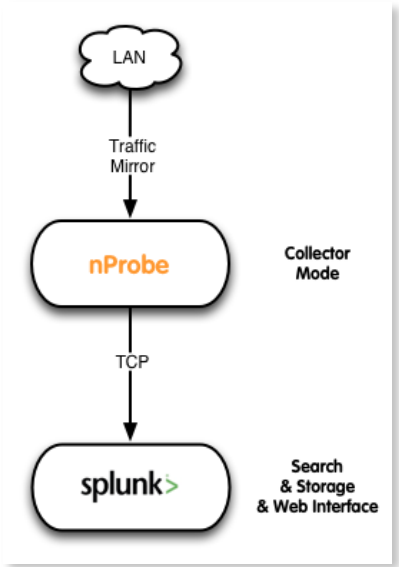
Step 3: Install nProbe

You need to install and use the nProbe as a probe for nProbe splunk app. If you want to test drive nProbe™ you can use our pre-build binary packages, for more information we refer you to the nprobe guide.

And that it's all.

2. Export flows from nProbe to Splunk

There are a few methods to export flows to Splunk, in the following section we describe the main and easiest way to export flows information from nProbe to nProbe splunk app.



The communication between nProbe and splunk happens through TCP that decouples nProbe from splunk.

You can collect/export flows as follows:

First, start nProbe that will act as a probe for nProbe splunk app

```
nprobe -T "%IPV4_SRC_ADDR %L4_SRC_PORT %IPV4_DST_ADDR %L4_DST_PORT %PROTOCOL
%IN_BYTES %OUT_BYTES %FIRST_SWITCHED %LAST_SWITCHED %HTTP_URL %HTTP_METHOD
%HTTP_RET_CODE %HTTP_REFERER %HTTP_UA %HTTP_MIME %HTTP_HOST %HTTP_SITE
%IN_PKTS %OUT_PKTS %IP_PROTOCOL_VERSION %APPLICATION_ID %L7_PROTO_NAME
%ICMP_TYPE" --tcp "127.0.0.1:3333" -b 2 -i eth0 --json-labels
```

Using the nprobe http plugin, you can add the %HTTP_SITE %HTTP_RET_CODE templates to export the http information.

However you can add all the templates that you need, but the nProbe splunk app will not be able to recognise the new templates, in order to show these new information you have to create a custom graphs.

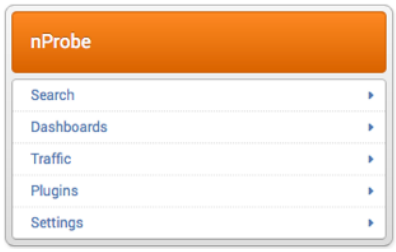
Flows exchanged between nProbe and splunk are formatted in JSON and not on standard sFlow/NetFlow format.

Now you can come back to Splunk GUI and view the flows information by a few simple Dashboards. Please remember that Splunk takes about one or two minutes to indexing the first incoming flows.

3. nProbe splunk app

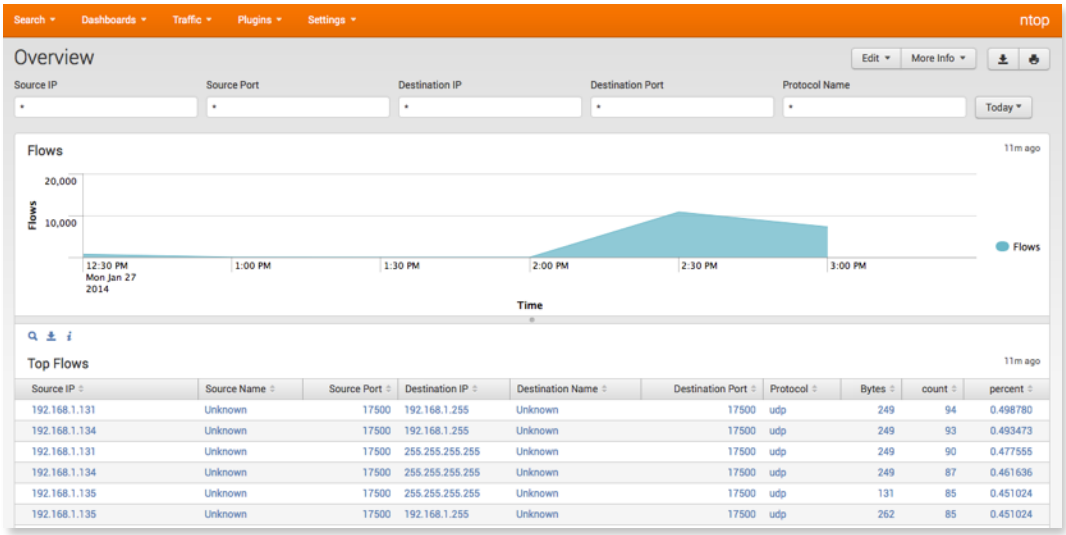
This application allows users to nProbe to export the flows information within Splunk. Once that is done, you can use the dashboards and reports already created to derive the standard information about the flow, host, protocols or create new report or dashboard to drive the information of your interest.

By the menu, you can create your customised dashboards or reports, set alarms for specific behaviour and use the pivot.

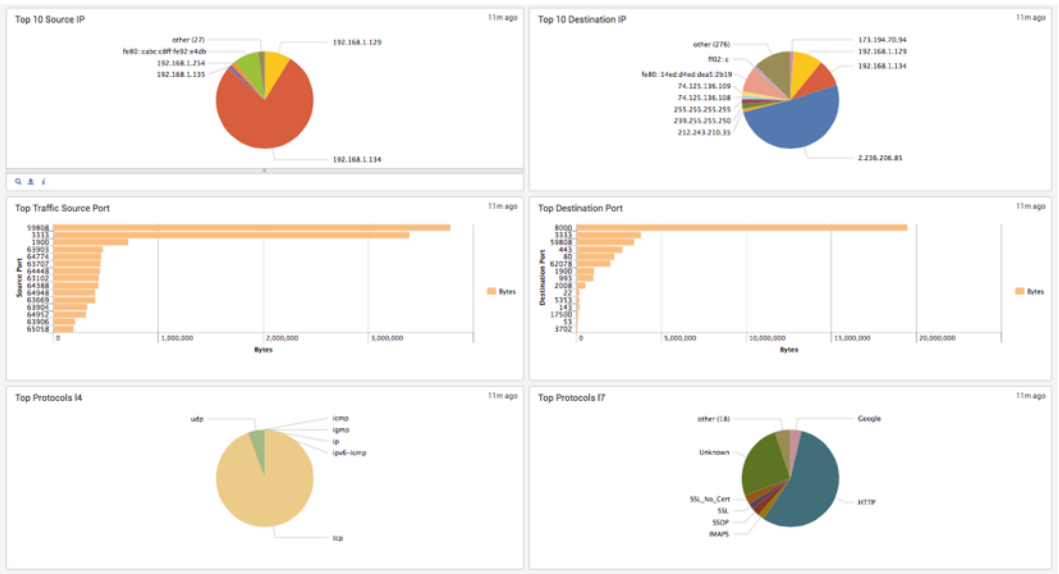


However, we have prepared a few simple dashboards to show what you can do using nProbe and splunk.

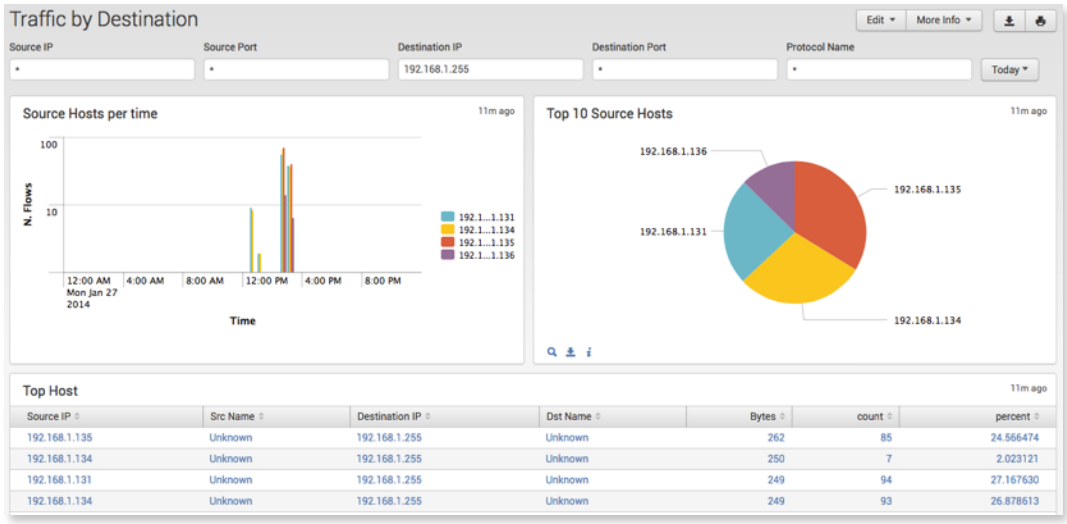
Overview, it is the main dashboard where you can view some general information about the collection of flows



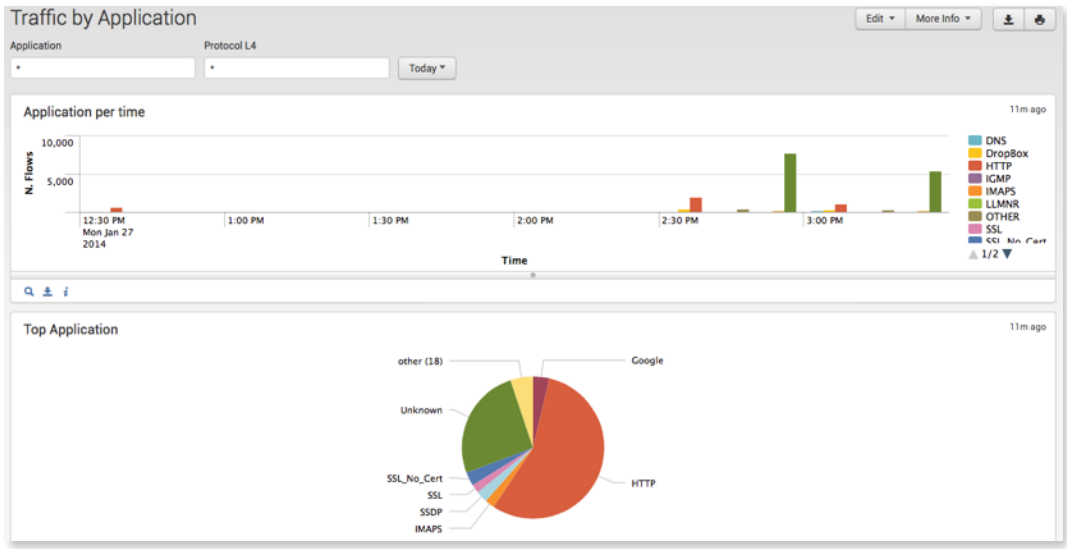
and the top 10 sources and destinations host, top protocols of level 4 and 7.



Traffic by Source and by Destination, where you can view and analyse the collected information focusing on the source or destination host.



Traffic by Application, where you can view the collected information focusing on the application.



HTTP, where you can analyse the collected information focusing on the http flows.