nProbe Splunk App
Quick Start Guide

Version 1.0
March 2014

ntop site	www.ntop.org
Splunk App Web	

Table of Contents

1. Installation

Step 1: Install and configure Splunk

First, download Splunk. Install it 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/).

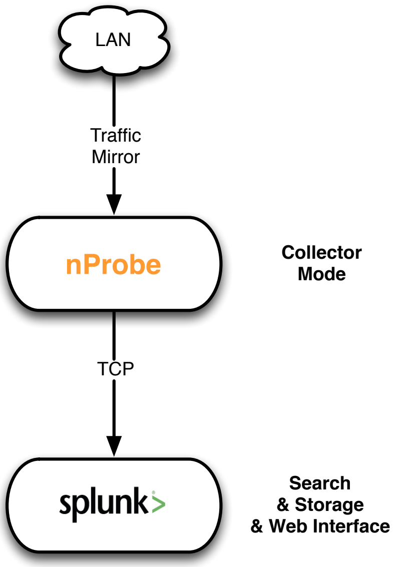
The application is now ready to be used and Splunk is listening for data from nProbe on port 3333. You will need to make sure that the machine on which your Splunk is running on has the appropriate firewall ports open (i.e. no traffic is blocked).

Step 3: Install nProbe

You need to install and use the nProbe as a flow 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. Note that you need a recent nProbe version (6.16 or later) that supports export to Splunk.

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

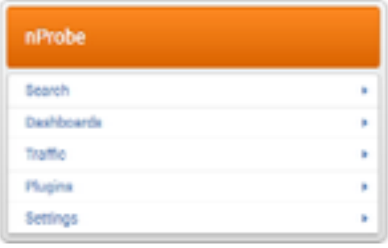
Flows exported by nProbe to splunk are formatted in JSON and not on standard sFlow/NetFlow format.

Done that, you can go to the Splunk GUI and visualise the flows information using the dashboards part of the nProbe spunk application. Please remember that Splunk takes about one or two minutes to indexing the first incoming flows, so do not be impatient to see results immediately.

3. nProbe splunk app

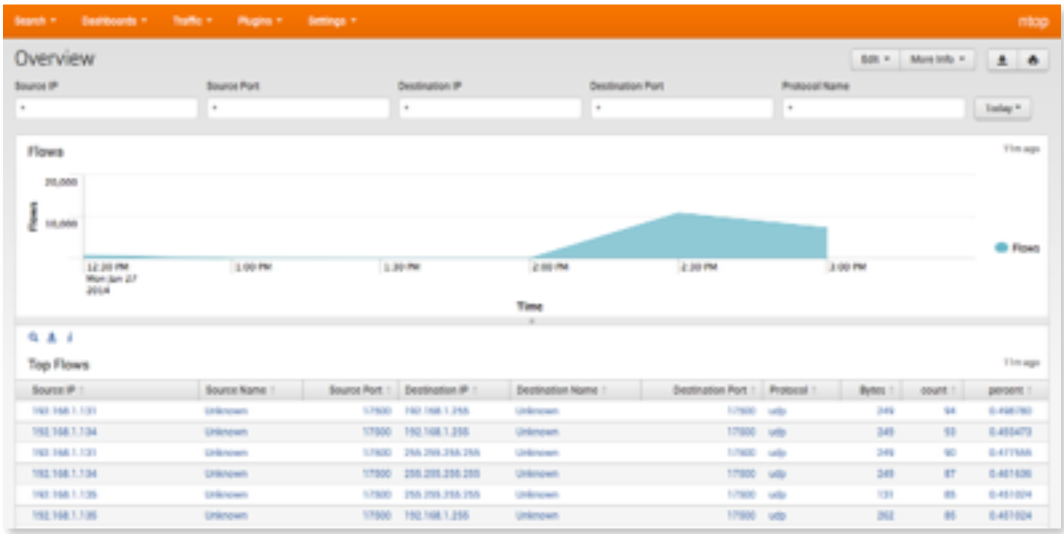
This application allows users to nProbe to export the flows information within Splunk. Once that is done, you can use the dashboards and reports already created to extract the standard information about the flow, host, protocols. You can also create new report or dashboard to visualise your monitoring data.

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



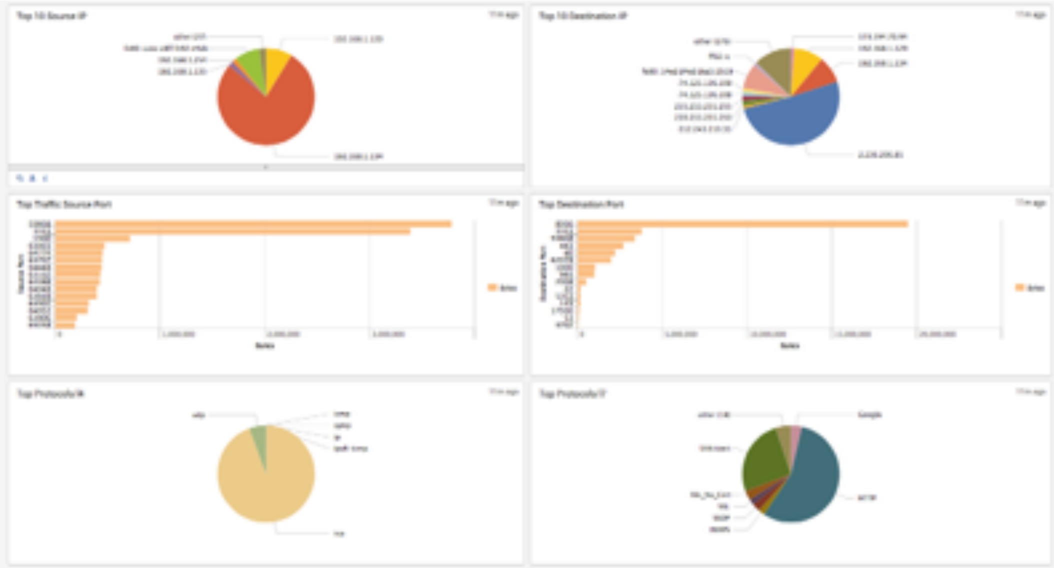
However, we have prepared a few simple dashboards to show what you can do using nProbe and splunk.

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

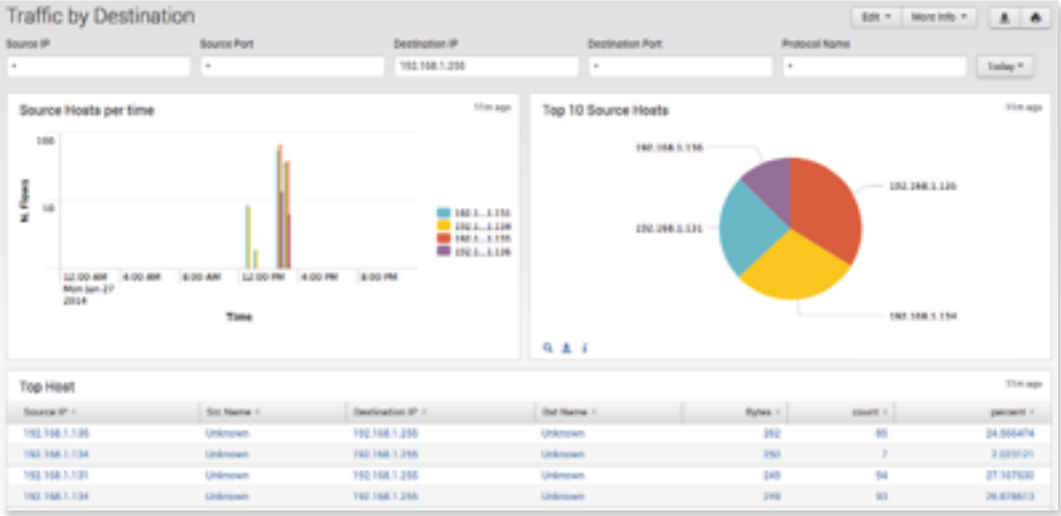


Source IP	Source Name	Source Port	Destination IP	Destination Name	Destination Port	Protocol	Bytes	count	percent
192.168.1.131	Unknown	17500	192.168.1.255	Unknown	17500	udp	249	94	0.498780
192.168.1.134	Unknown	17500	192.168.1.255	Unknown	17500	udp	249	93	0.493473
192.168.1.131	Unknown	17500	255.255.255.255	Unknown	17500	udp	249	90	0.477566
192.168.1.134	Unknown	17500	255.255.255.255	Unknown	17500	udp	249	87	0.461636
192.168.1.135	Unknown	17500	255.255.255.255	Unknown	17500	udp	131	85	0.451024
192.168.1.135	Unknown	17500	192.168.1.255	Unknown	17500	udp	262	85	0.451024

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 Destination

Source IP: *

Source Port: *

Destination IP: 192.168.1.255

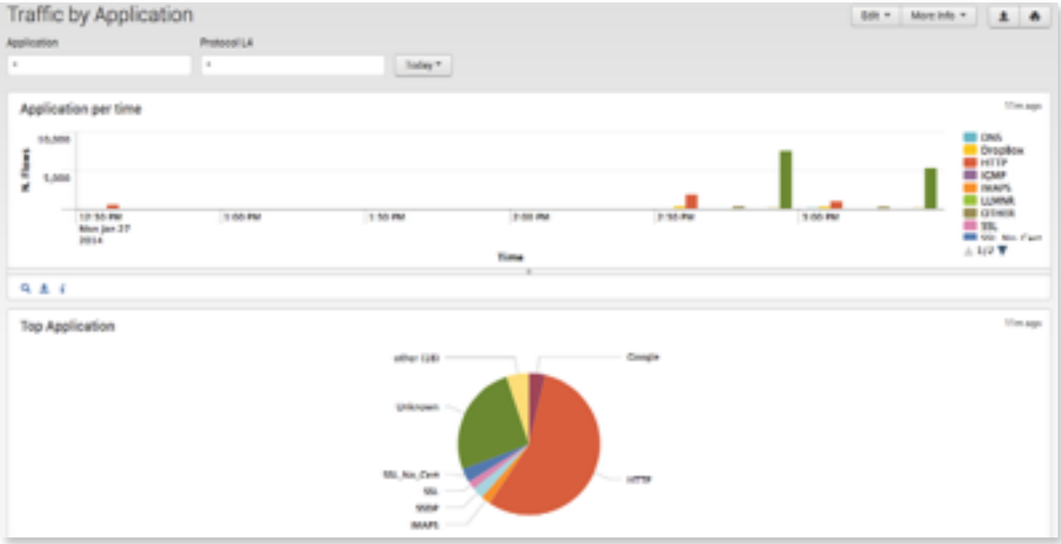
Destination Port: *

Protocol Name: *

Top Host

Source IP	Src Name	Destination IP	Dst Name	Bytes	count	percent
192.168.1.135	Unknown	192.168.1.255	Unknown	262	85	24.566474
192.168.1.134	Unknown	192.168.1.255	Unknown	250	7	2.023121
192.168.1.131	Unknown	192.168.1.255	Unknown	240	94	27.167630
192.168.1.134	Unknown	192.168.1.255	Unknown	248	93	26.878613

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

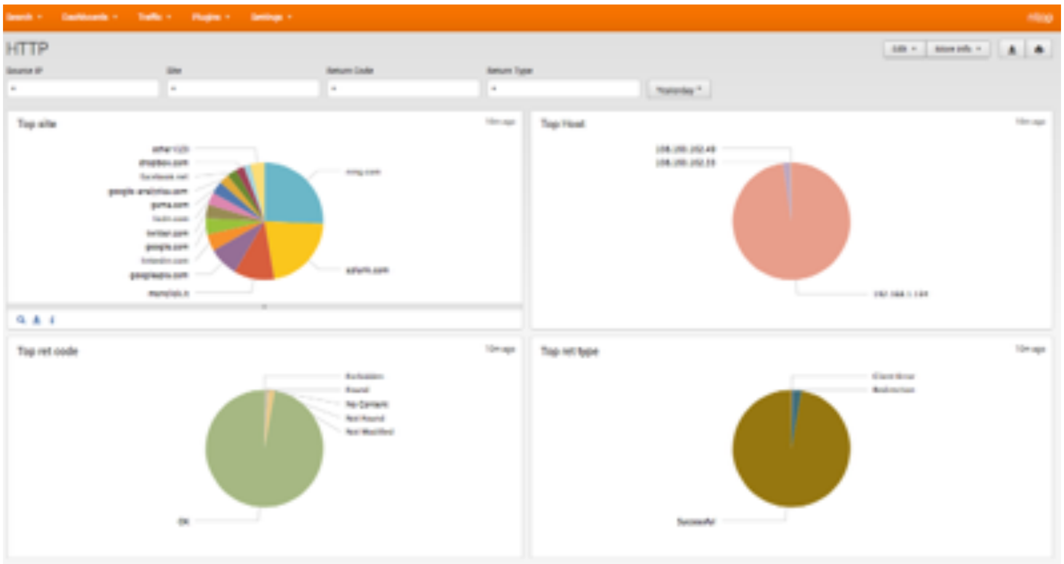


Traffic by Application

Application: *

Protocol L4: *

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


Search
Dashboards
Traffic
Plugins
Settings
HTTP
Source IP
Site
Return Code
Return Type
Yesterday
Top site
dropbox.com
google-analytics.com
twitter.com
google.com
splunk.com
Top Host
Top ret code
Forbidden
Found
No Content
Not Found
Not Modified
OK
Top ret type
Client Error
Redirection
Successful