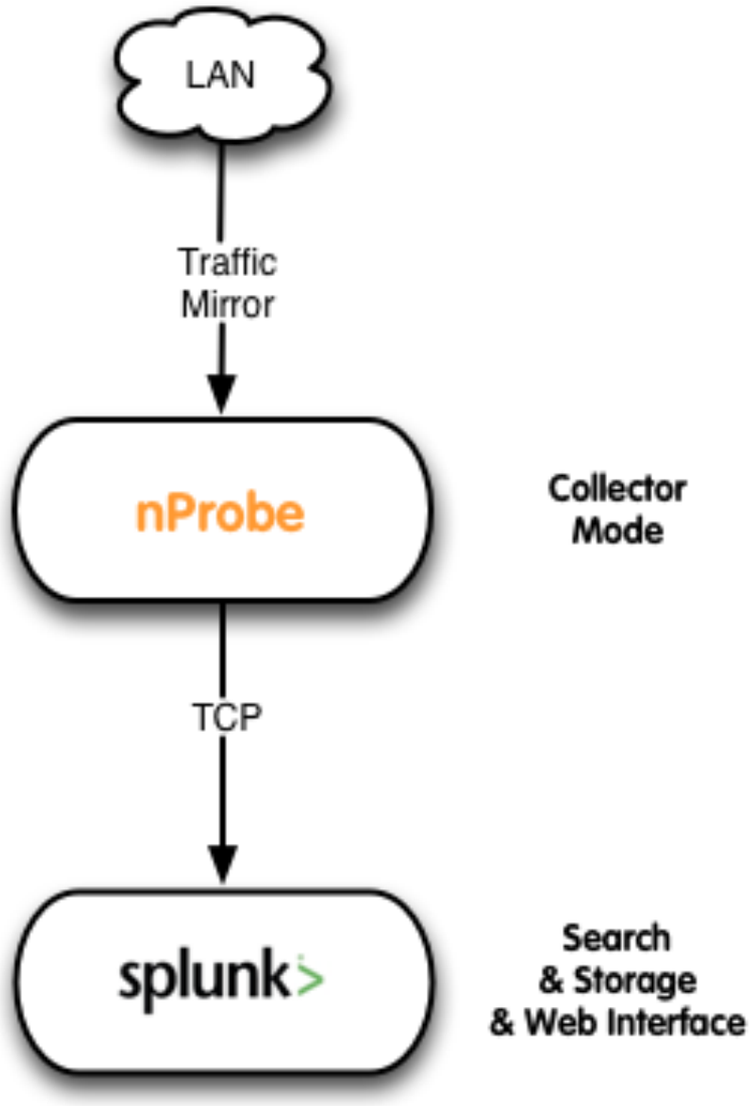
nProbe App for Splunk

Esportare flussi da nProbe a Splunk

Architettura

- Utilizzare nProbe in collector mode
  - Collezionando il traffico in ingresso e.g LAN
- Esportare i flussi verso Splunk
  - In formato JSON
  - Utilizzando TCP come protocollo di trasporto



nProbe side

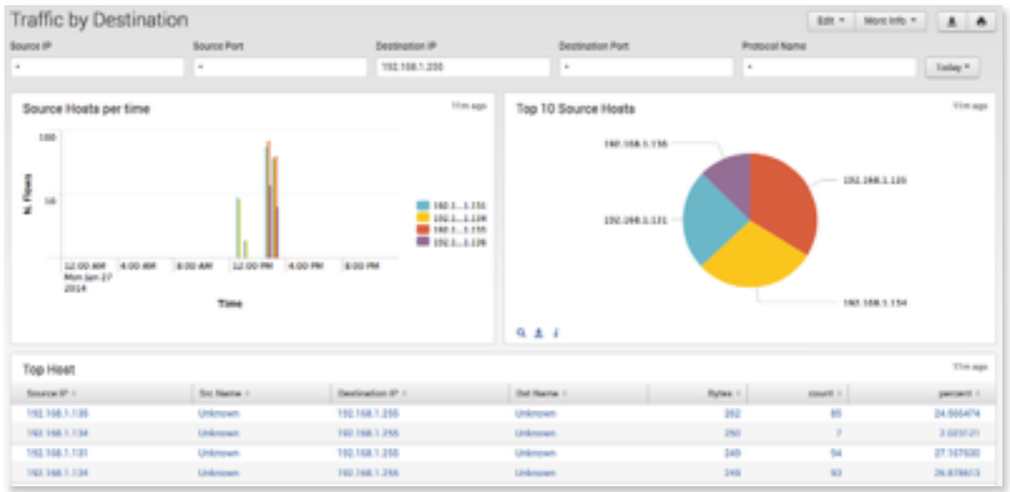
- Specificare il template
  - Le informazioni relative ai flussi che vogliamo esportare

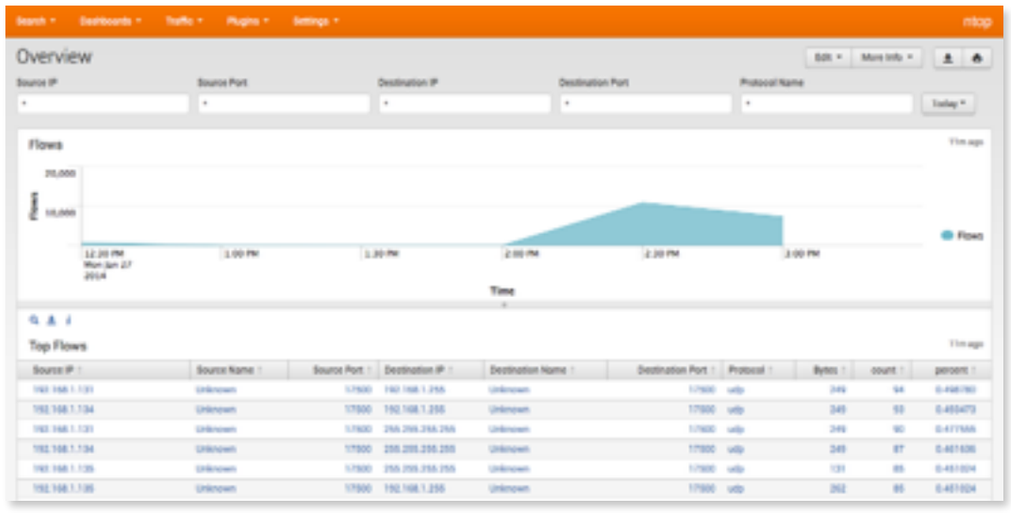
- Esportare i flussi verso Splunk
  - Specificando host e porta destinazione

```
nprobe -T  "%IPV4_SRC_ADDR %L4_SRC_PORT %IPV4_DST_ADDR %L4_DST_PORT %PROTOCOL
           %IN_BYTES %OUT_BYTES %IN_PKTS %OUT_PKTS
           %IP_PROTOCOL_VERSION %L7_PROTO_NAME
           %HTTP_SITE %HTTP_RET_CODE" - - tcp "127.0.0.1:3333" - - json_labels -i eth0
```

Splunk side

- Installare nProbe App for Splunk
  - Automaticamente inizierà a ricevere e decodificare i flussi in ingresso
- Utilizzare le dashboard presenti per visualizzare report standard (Top Host, Top Application, ecc..)
- Definire un sistema di allarmistica basato su apposite query di ricerca
- Esportare le informazioni aggregate
- Creare dashboard personalizzate





nprobe & elasticsearch

- Utilizzare nProbe in collector mode
  - Collezionando il traffico in ingresso e.g LAN

- Esportare i flussi verso Logstash
  - In formato JSON
  - Via TCP, ZMQ, DB

- Inoltrare i flussi elaborati da Logstash verso Elasticsearch

- Realizzare report & dashboard utilizzando Kibana 3