Progetto: "Uso di Elasticsearch-Logstash-Kibana (ELK) per l'analisi del traffico di rete (netflow) catturato in remoto"

DESCRIZIONE DELLA RETE

Per realizzare questo progetto abbiamo pensato di progettare una rete costituita da tre macchine virtuali.

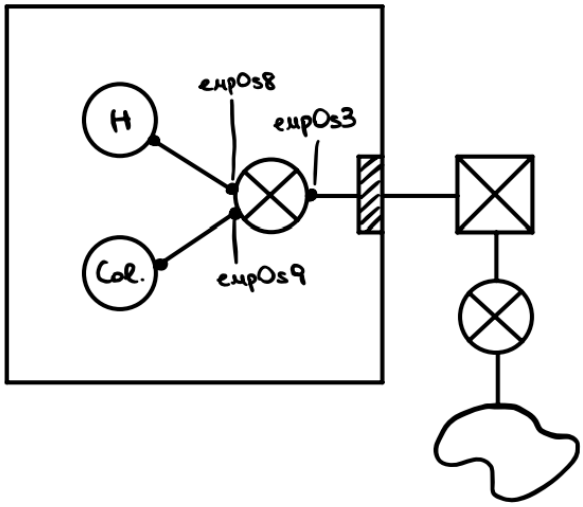
Una prima macchina virtuale, che agisce da *router*, con tre schede di rete:

1. Scheda con bridge
2. Rete interna (la stessa dell'host)
3. Rete interna (la stessa del server)

Una seconda macchina virtuale, che agisce da *host*, con una scheda di rete interna (la stessa della seconda scheda di rete del router).

Infine, una terza macchina virtuale, che agisce da *collettore*, anch'essa con una scheda di rete interna (la stessa della terza scheda di rete del router).

- SUBNET-1 [10.0.0.0/24]
  - [VM-1] Router – 10.0.0.1
  - [VM-3] Collettore – 10.0.0.15
- SUBNET-2 [192.168.0.0/24]
  - [VM-1] Router – 192.168.0.1
  - [VM-2] Host – 192.168.0.15
- SCHEDA CON BRIDGE
  - [VM-1] Router – IP assegnato tramite DHCP rete locale



DESCRIZIONE DEL SISTEMA

Una volta messa in piedi la rete, abbiamo innanzitutto connesso tra loro le varie macchine virtuali. Abbiamo quindi configurato la prima macchina per svolgere la funzione di router e dhcp server per le due subnet di host e collettore.

Per svolgere la funzione da router sono state aggiunte delle regole alle tabelle di routing tramite il seguente script bash:

---------- router.sh ----------

```
#!/bin/bash

sysctl -w net.ipv4.ip_forward=1
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
iptables -t nat -L -v -n --line-numbers
```

Mentre per svolgere la funzione di server dhcp sono stati utilizzati i seguenti comandi:

- Installazione Server DHCP
  - *sudo apt install isc-dhcp-server*

- Configurazione Server DHCP

---------- /etc/default/isc-dhcp-server ----------

```
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#      Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s8 enp0s9"
INTERFACESv6=""
```

----------/etc/dhcp/dhcpd.conf----------

```
# This is a very basic subnet declaration.

subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.15 192.168.0.45;
  option routers 192.168.0.1;
}

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.15 10.0.0.45;
  option routers 10.0.0.1;
}
```

A questo punto abbiamo lavorato sulla macchina router, installando come prima cosa netflow e nfdump. Una volta installati, abbiamo configurato netflow e iptables.

- Installazione Netflow
  - *sudo apt install iptables-netflow-dkms*
- Configurazione NetFlow
  - *sudo modprobe ipt_NETFLOW destination=10.0.0.1:2056 protocol=9 natevents=1*
- Configurazione Iptables
  Questa regola permette di intercettare tutti e solo i pacchetti che transitano per il router (non quelli che partono o arrivano al router) per la cattura Netflow
  - *sudo iptables -I FORWARD -j NETFLOW*
- Installazione nfdump
  - *sudo apt install nfdump*
  - *sudo systemctl enable nfdump.service*
  - *sudo systemctl status nfdump.service*
  - *sudo systemctl stop nfdump.service*
  - *sudo systemctl daemon-relaod*
  - *sudo systemctl start nfdump.service*
  - *sudo systemctl status nfdump.service*

Lo step successivo è stato quello dell'installazione e della configurazione degli applicativi dello Stack ELK.

Abbiamo installato prima Elasticsearch e Kibana sulla macchina collettore, e poi Filebeat sulla macchina router.

- Elasticsearch
  - *wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.11.3-linux-x86_64.tar.gz*
  - *wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.11.3-linux-x86_64.tar.gz.sha512*
  - *shasum -a 512 -c elasticsearch-8.11.3-linux-x86_64.tar.gz.sha512*
    Comando per la verifica dell'integrità del file scaricato
  - *tar -xzf elasticsearch-8.11.3-linux-x86_64.tar.gz*

- *sudo sysctl -w vm.max_map_count=262144*
  Modifica variabile del kernel che è associata alla mappatura massima del conteggio di pagine di memoria virtuale in un processo. Modifica necessaria per applicazioni che utilizzano una gran quantità di memoria virtuale come appunto Elasticsearch

- Kibana
  - *curl -O https://artifacts.elastic.co/downloads/kibana/kibana-8.11.3-linux-x86_64.tar.gz*
  - *curl https://artifacts.elastic.co/downloads/kibana/kibana-8.11.3-linux-x86_64.tar.gz.sha512 | shasum -a 512 -c -*
  - *tar -xzf kibana-8.11.3-linux-x86_64.tar.gz*

- Filebeat
  È uno dei sottosistemi della componente Beats dello Stack ELK e tra i vari moduli di cui dispone, ne ha uno apposito per Netflow.
  - *curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.11.3-linux-x86_64.tar.gz*
  - *tar xzvf filebeat-8.11.3-linux-x86_64.tar.gz*
  - *./filebeat modules enable netflow*
    Comando per l'attivazione del modulo Netflow di Filebeat

In seguito, si è resa necessaria la modifica di alcuni file di configurazione (per praticità verranno riportate soltanto le configurazioni modificate).

---------- elasticsearch-8.11.3/config/elasticsearch.yml ----------

```
…
cluster-name: NETFLOW
…
network.host: 10.0.0.15
…
http.port: 9200
…
xpack.security.enabled: false
xpack.security.enrollment.enabled: false
…
xpack.security.http.ssl:
        enabled: false
…
xpack.security.transport.ssl:
        enabled: false
…
```

---------- kibana-8.11.3/config/kibana.yml ----------

```
…
server.port: 5601
…
server.host: "10.0.0.15"
…
server.name: "netflow-kibana"
…
elasticsearch.hosts: ["http://10.0.0.15:9200"]
…
```

---------- filebeat-8.11.3/filebeat.yml ----------

…
setup.kibana
host: "10.0.0.15:5601"
…
output.elasticsearch:
hosts: ["10.0.0.15:9200"]
…

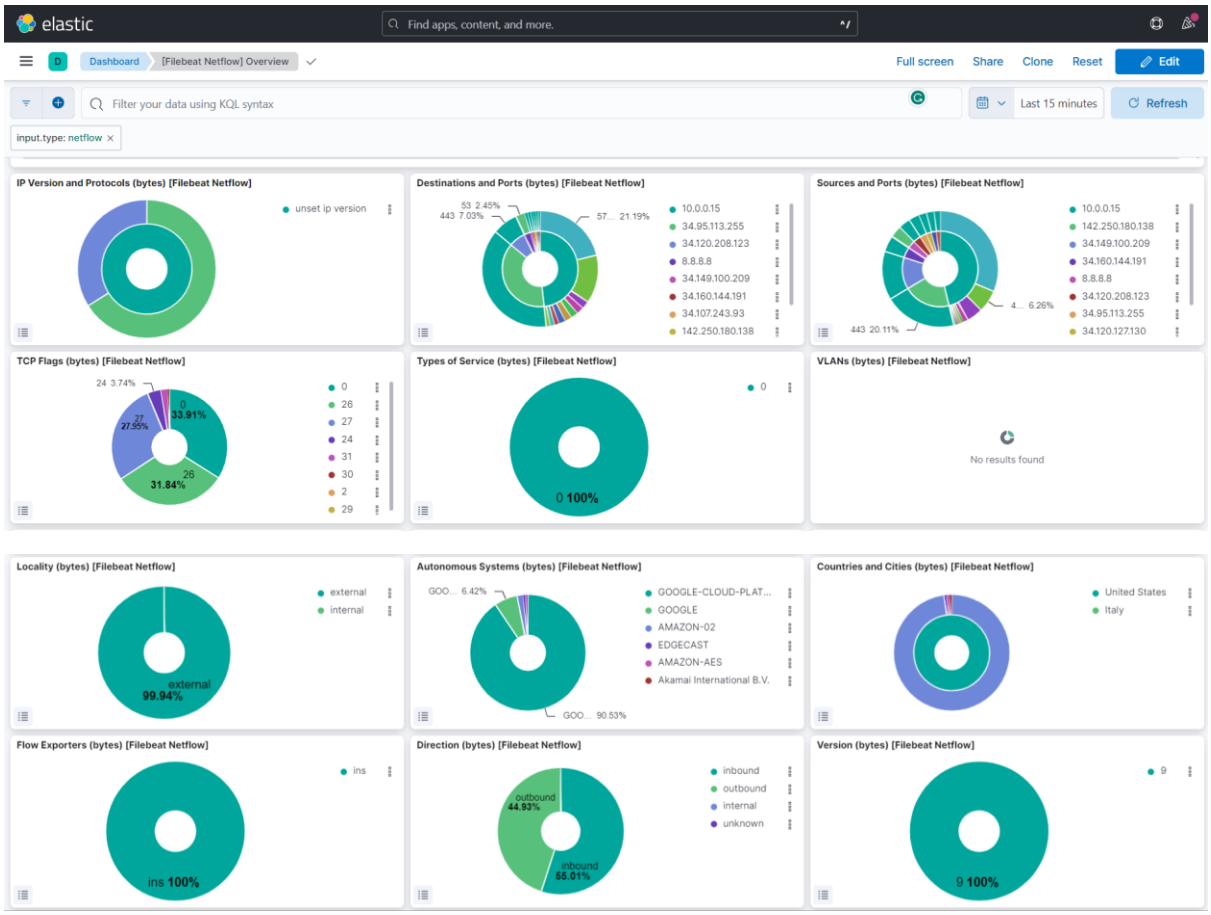
---------- filebeat-8.11.3/modules.d/netflow.yml ----------

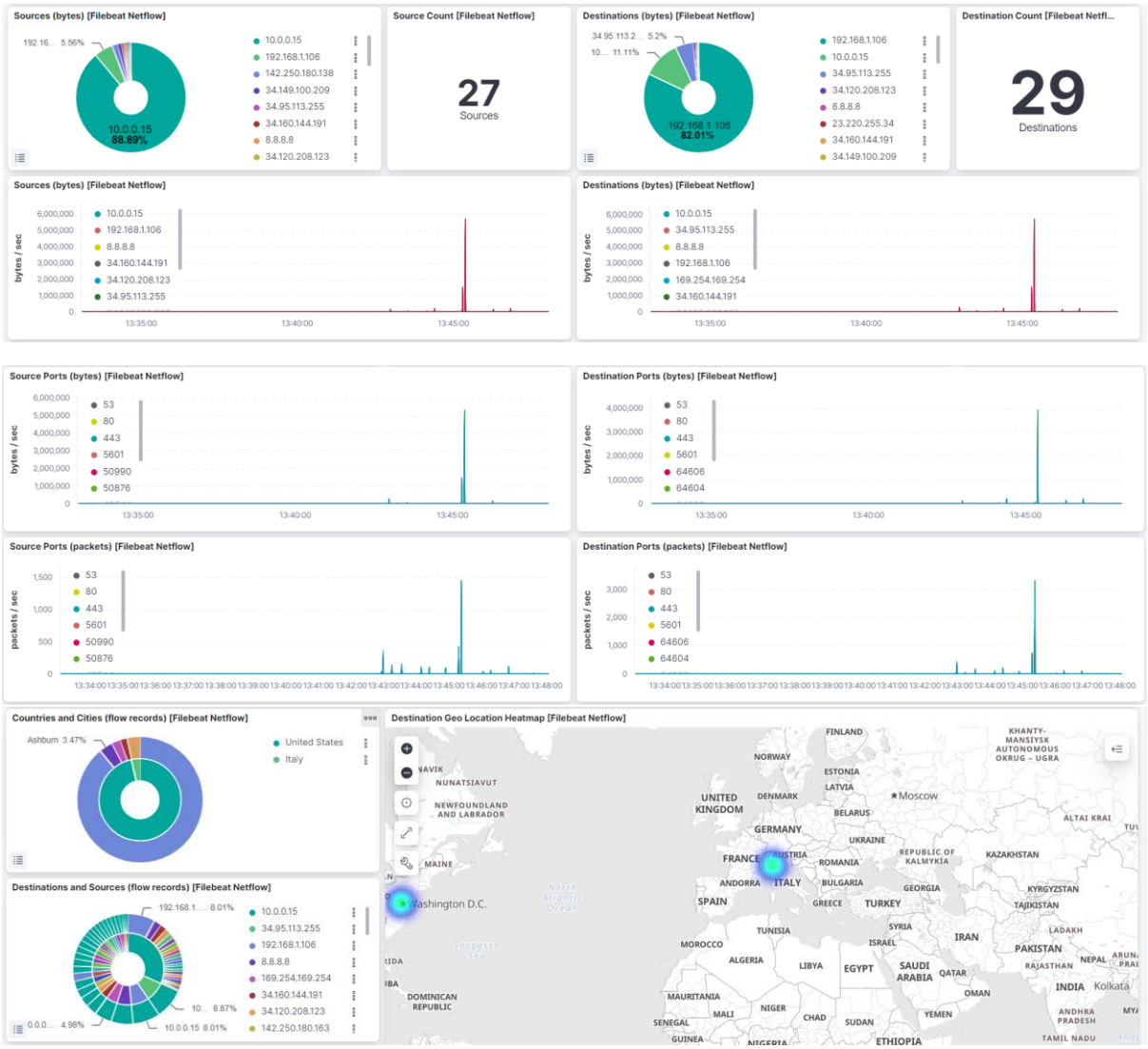
…
enabled: true
…
netflow_host: 10.0.0.1
netflow_port: 2056
…

A questo punto abbiamo iniziato ad utilizzare ELK per l'analisi del traffico di rete Netflow.

Grazie a questo stack, e in particolare alla componente Kibana, è stato possibile visualizzare ed esplorare i risultati dell'analisi del traffico di rete.

Sono riportate di seguito alcune immagini della visualizzazione dei dati tramite Kibana.





Kibana, infatti, permette la visualizzazione dei dati archiviati in Elasticsearch, e lo fa tramite l'uso di istogrammi, grafici a torta, mappe di calore, ecc.

Nota

Per una questione di praticità abbiamo aggiunto una regola iptables per visualizzare Kibana direttamente dal browser della macchina guest:

- *sudo iptables -t nat -A PREROUTING -p tcp --dport 5601 -j DNAT --to-destination 10.0.0.15:5601*