Web-based Visualization of NetFlow and IPFIX Data

Degree programme: BSc in Informatik | Specialisation: IT-Security
Thesis advisor: Prof. Hansjürg Wenger
Expert: Dr. René Bach

As a network administrator it is essential to stay up to date with network metrics like flows and traffic. Open source software capable of collecting and visualizing such data has been around for decades, but some open source user interfaces are beginning to show their age. There are modern solutions, but it is not always feasible to migrate the existing data.
We developed a new NetFlow visualizer, positioned on top of the existing nfdump tools.

Problem to solve

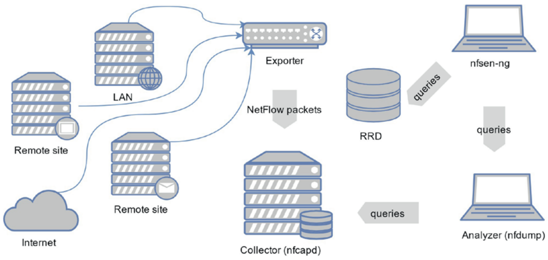
Metrics like traffic and load can help to detect attacks and to prevent possible bottlenecks in the network. NetFlow and IPFIX collectors are used to collect such metrics in the form of **flow data** from devices such as routers, firewalls, etc. There is an existing open source solution to collect such data which is called the nfdump tools.
Additionally, there is a web frontend called **NfSen**, developed by the same author, which visualizes the collected data and thus makes it much easier to analyze it.
As NfSen is more than 10 years old now and looks quite a bit outdated, it makes for a great opportunity to refresh it and at the same time address some of the issues it brings with it.

Objectives

The main goal was the implementation of an application with similar functionalities as NfSen, but in a more modern and easier-to-use way. The requirements of the new solution were defined after an analysis of the existing one; after some consideration, we named our solution **nfsen-ng**.

Design and Implementation

The front end of nfsen-ng is purely using the client-side technologies HTML, CSS and JavaScript. With the help of a few frameworks and libraries, putting together the new GUI was quite efficient and the outcome convincing.



Architecture overview

All non-static data the front end is displaying, is provided by a RESTful JSON API on the PHP-based back end. To ensure easy extendibility, it is using an object-oriented approach. For example, nfsen-ng is storing data in the same time-series database like NfSen (called RRD), but by specifying an interface class it is pretty straightforward to implement the logic to support a more modern database like Akumuli or InfluxDB. Another class acts as a proxy to nfdump for aggregating data and generating statistics.

Result

nfsen-ng has many of the functionalities of NfSen and adds a few more on top of it. The front end uses a mobile-first approach, so it is fully responsive. This means you can check your metrics from anywhere on the smartphone, but also by letting it run on a big TV in the datacentre or office.
The back end still uses nfdump and round-robin databases, though it is generally more extendible and the command-line interface provides more comfort in importing previously captured data.

Download/Contributing

nfsen-ng is available on GitHub and open for pull requests: https://github.com/mbolli/nfsen-ng

Looking good on multiple devices

Michael Bolli
michael@bolli.us

Donatello Gallucci