NS1 Labs

Deep Network Traffic Observability with Pktvisor and Prometheus

Posted by
Shannon Weyrick on
February 2, 2022

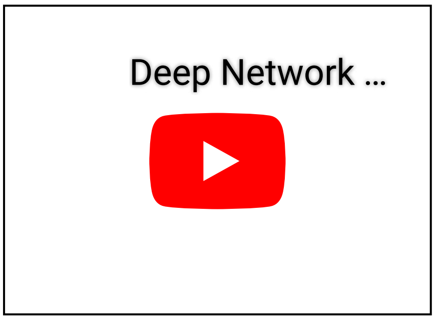
One of the most challenging problems in operating global edge infrastructure is understanding what is happening in edge networks in real time, to diagnose and solve problems before they become catastrophes.

Up until recently, this was primarily a challenge only for certain companies - like NS1 - who manage large parts of the **infrastructure powering the internet**. Increasingly, however, we are hearing from customers who are building out global edge footprints of their own that real-time, actionable edge visibility has become a major challenge.

Orb and **pktvisor** are two open source tools we developed at **NS1 Labs** specifically to solve our own challenges with deep network observability. Keep reading to learn more about how Orb and pktvisor work and how they help companies with large, distributed edge environments improve reliability through dynamic, real-time visibility at the edge.

Watch Shannon's Full Session at Promcon 2021

Check out the replay to learn more about pktvisor and Orb and see them in action



What is Deep Network Observability?

Deep network observability involves unwrapping and inspecting your network traffic and activity to gain insights useful for ops, debugging, security, and more. Gathering and analyzing traffic across a distributed and ephemeral set of end-points, however, is challenging to achieve with existing observability tools. It can be difficult to extract the right data points at the right time given the volume of traffic and corresponding data points.

Deep Network Observability and NS1

Deep network observability has been a challenge for NS1 from the beginning. To provide **reliable and performant DNS** to our customers (who represent **a large portion of the internet**) we need to do the following in real-time:

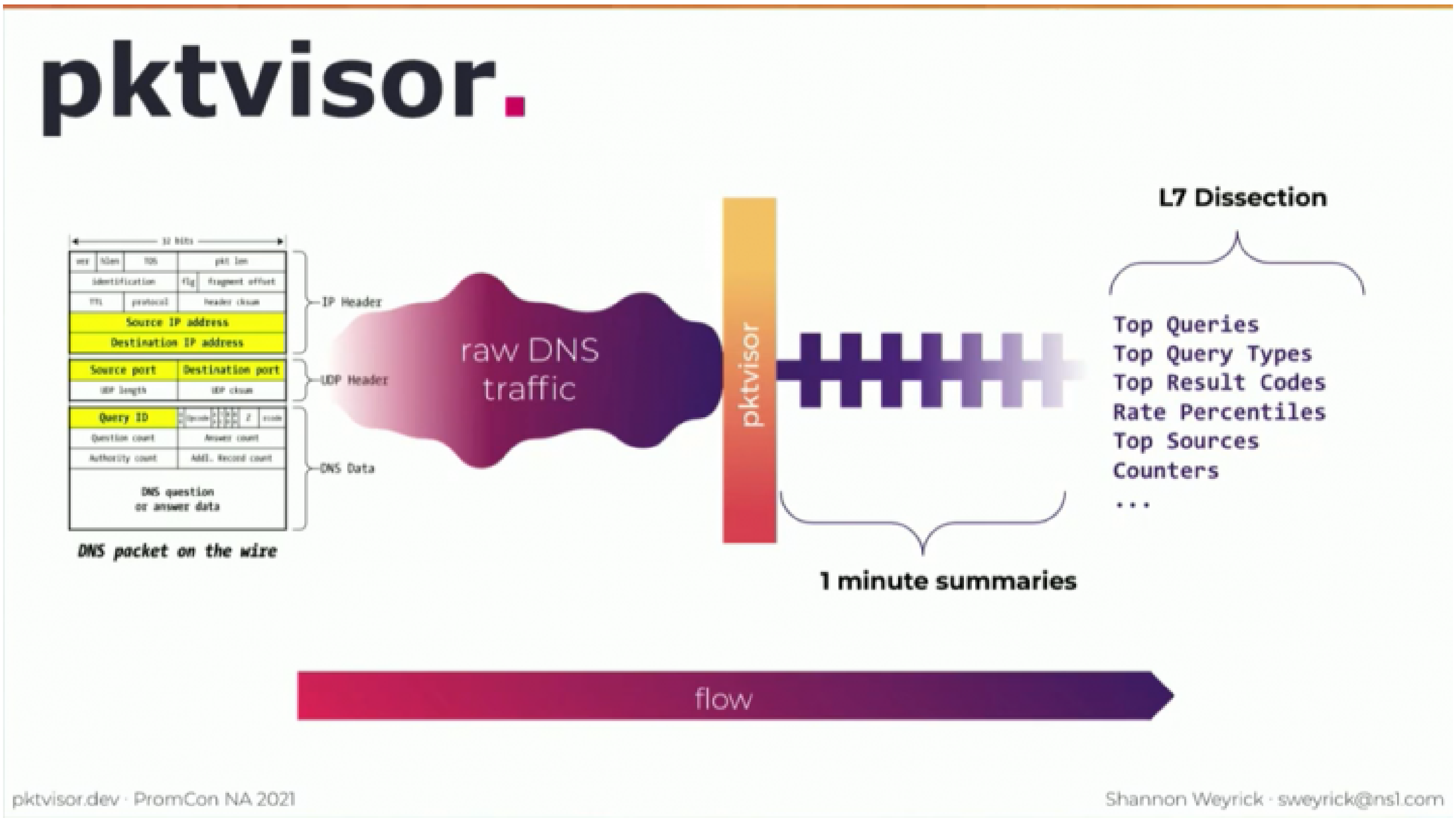
- Tune our anycast networks for best delivery time
- Protect against malicious traffic
- Debug individual delivery nodes at high resolution
- And provide a global view of all nodes to drill into different dimensions of network traffic data

We developed pktvisor, an open source tool, in response to these needs. With pktvisor, we can answer some of the following questions about our own network traffic:

- What are the counters, rates, histograms, cardinality, and frequent items across common network traffic dimensions?
- How many unique IP addresses and query names are there?
- What are the important quantiles of transaction timings? What's the histogram of response payload sizes?
- What is the amplification factor from query to response size?
- What is still querying deleted DNS records?
- From what ASN and geo regions is traffic coming from?
- Is this traffic spike malicious or legitimate? Is it widely distributed?

How Does pktvisor Solve for Network Observability?

We use pktvisor to monitor our critical infrastructure. It observes and summarizes our edge traffic in real-time. Our goal when building pktvisor was to create a tool that sat close to the data source, supported modern observability, and would allow us to drive observability via dynamic policies over REST API. Additionally, we wanted to make it accessible, so it is structured as an easy Docker install, and integrates with Prometheus.



pktvisor.

L7 Dissection

Top Queries
Top Query Types
Top Result Codes
Rate Percentiles
Top Sources
Counters
...

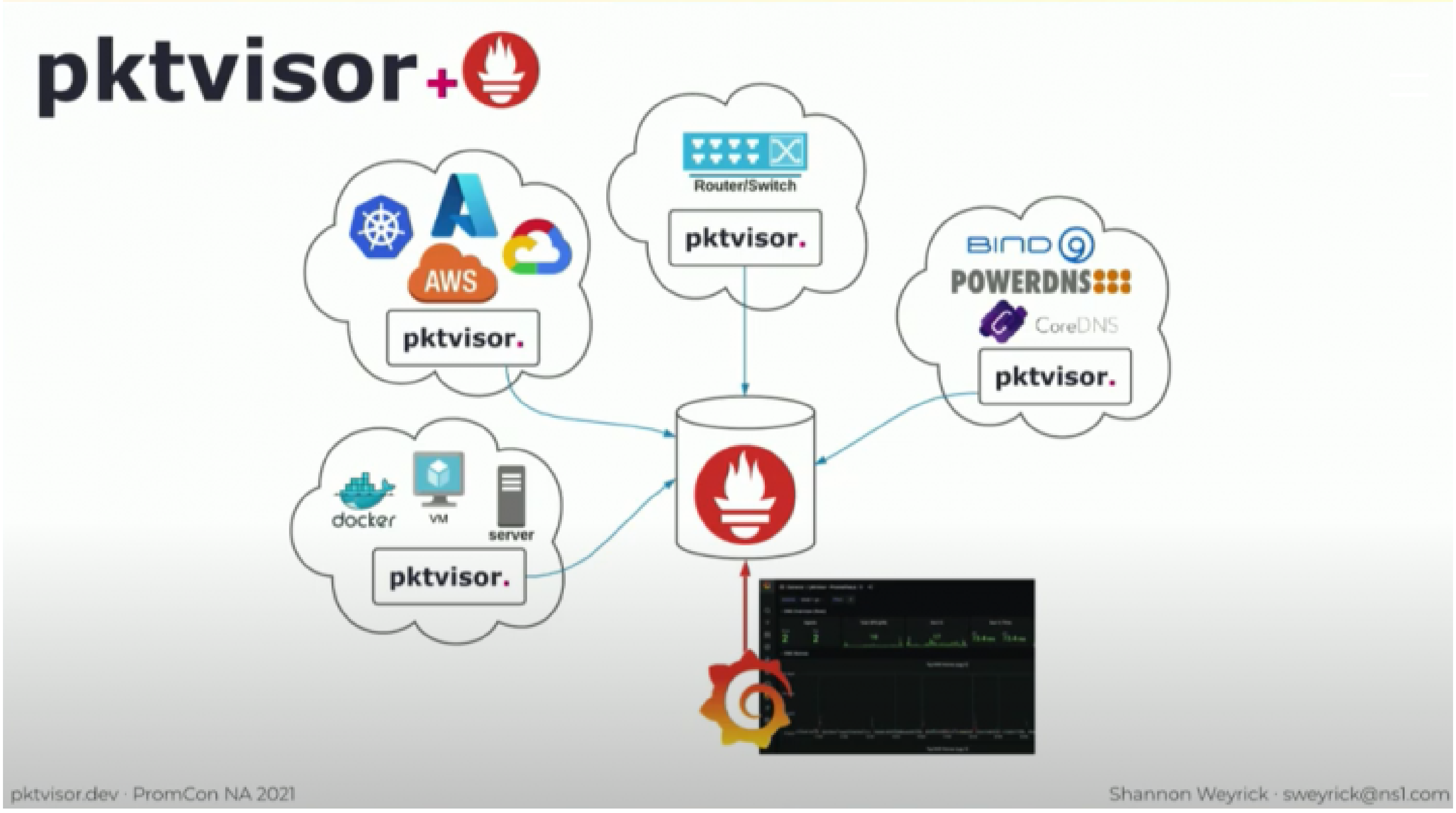
1 minute summaries

pktvisor.dev · PromCon NA 2021

Shannon Weyrick · sweyrick@ns1.com

How pktvisor Works with Prometheus

When connected to Prometheus, pktvisor exposes Prometheus metrics per policy. It provides a global view of distributed pktvisor agents, and allows you to scrape or push with remote write. It also allows you to use Grafana and other tools for exploring, visualizing, and alerting. If you're interested, we have **sample Grafana dashboards available for use**.

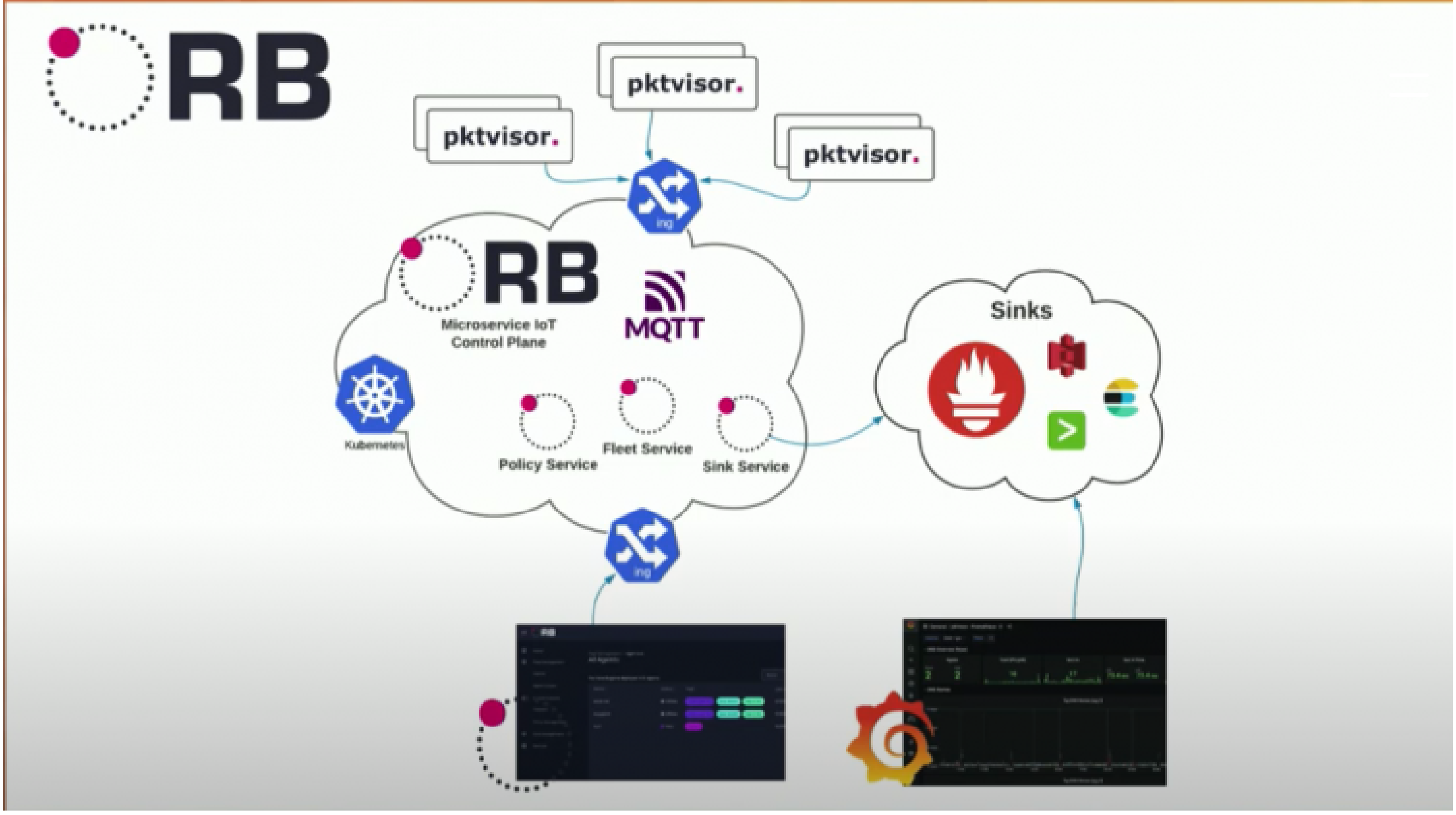


And to further extend the functionality of pktvisor, we've recently launched Orb, **an open source tool** that allows you to manage and reprogram fleets of pktvisors in real-time.

How pktvisor and Orb Work Together

Orb is based on IoT principles, and provides UI, API, and agent communications. It allows you to orchestrate agents and their policies by collecting and sinking agent output.

With Orb, we add critical functionality beyond just collecting the extracted information centrally: we connect the edge agents (pktvisor) into a centralized control plane, which is able to communicate with the agents and to give them instructions in real time.



You can learn more and test our first iteration of Orb out for yourself by visiting: **https://getorb.io/**. If you're interested in contributing to Orb and testing out the platform, please star us on Github and join our **NS1 Labs OSS Slack**.

For more information, check out the following resources:

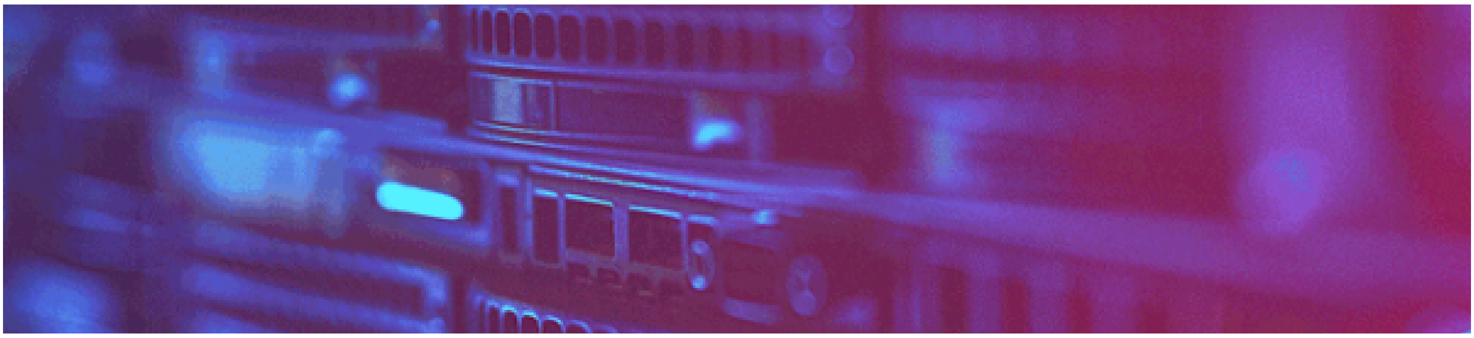
Further Reading

FEATURED

A Wave of Open Source Innovation at NS1 Labs

Solving challenges in modern application delivery through innovation in foundational technologies supporting the global internet

Read the Ebook



Top 14 Edge Computing Influencers & Experts to Follow in 2022

Read the Article

* View all Resources

NS1.
an IBM Company