TCPDumping K8s using Kubeshark and Ksniff

Kubeshark

Speaker

Leon Nunes

Technical Support Engineer @ Solo.io

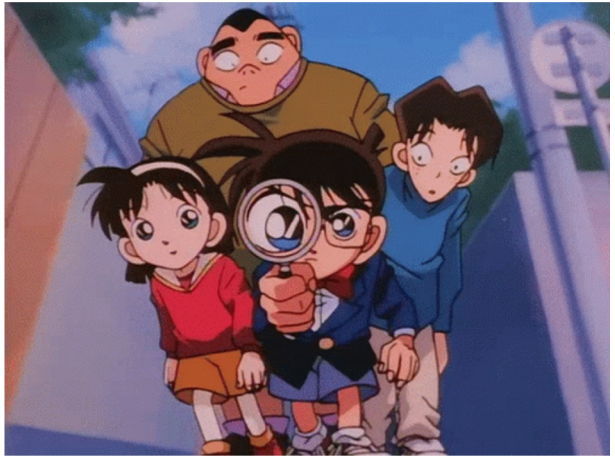
solo.io

Agenda

- What is Traffic Analysis
- Quick introduction to TcpDump and packets
- Understanding how these can help troubleshoot network problems.
- Introduction to Kubeshark and Kubectl ksniff via a Demo

What is traffic analysis?

- Inspecting network packets
- Looking for Network related information
- Seeing how data is sent and received



Use Cases for Traffic Analysis?

- Network Troubleshooting
- Curl command works, but your app doesn’t
- Inspecting how your data goes through the network.
- Performance Analysis
- Network Forensics

A Quick intro to TCPDump and Wireshark

TcpDump

- Network Analyzer
- Can filter traffic based on conditions(e.g Port 80)
- Can export to a Pcap

Wireshark

- A GUI/TUI based application
- Can read pcap files.
- Color codes the output for better visualization

Terms frequently seen in the Output

- **SYN**: a synchronization message typically used to request a connection between a client and a server
- **ACK**: an acknowledgment message employed to declare the receipt of a particular message
- **FIN**: a message that triggers a graceful connection termination between a client and a server
- **RST**: a message that aborts the connection (forceful termination) between a client and a server

What tools are commonly used?

- Tshark
- Tcpdump
- Wireshark
- Sysdig

Gloo Edge

Modern Cloud API Gateway built with Envoy Proxy

Demo

Applications used in this Demo

- K3d Clusters
- Gloo Edge (Open Source Api Gateway)
- Kubeshark
- Ksniff

Thank you!

solo.io