CASE STUDY

Lawful Intercept Focused Company Develops 100G IP Probe

SUMMARY

Lawful intercept focused service provider adopts ANIC-200Kflex, 2-port 100G adapter with advanced packet filtering for new 100G IP probe product

KEY CHALLENGES

- Initially available 100G adapters did not meet all requirements including packet filtering features

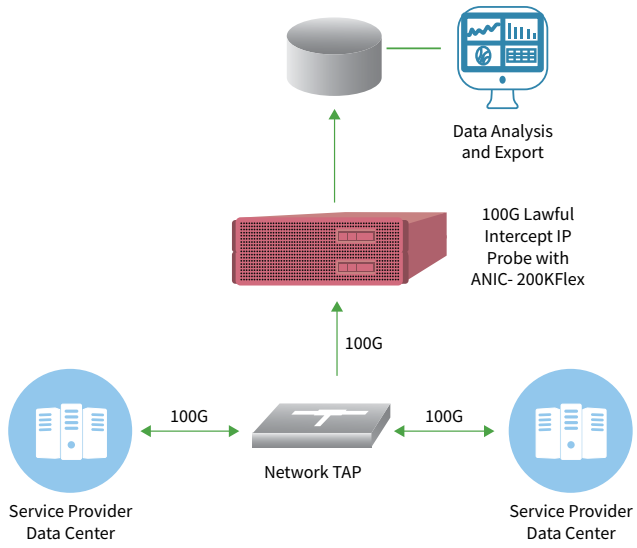
WHY ACCOLADE?

- Reliable technology partner with established track record in the marketplace for 100G CPU offload adapters
- Customized its advanced packet filtering feature to meet the company's requirements

ANIC FEATURES USED

- 100% packet capture at 100G
- Advanced Packet Filtering
- Nanosecond Precision Timestamping

The company is focused exclusively on the lawful intercept market and has gained a reputation as a technologically sophisticated solution provider. Due to its long history and success in the market, law enforcement agencies (LEAs) around the world have come to rely on the company for the latest cutting-edge solutions to solve their most difficult problems. The latest technical challenge facing the company was to develop a 100G IP probe that would be used by LEAs to monitor voice-over-IP (VoIP) calls, emails, instant message (e.g. Skype) communication and the like. Much of the base technology could be leveraged from previous generations of IP probes, but 100G speeds posed some new challenges which the company could not handle themselves and would require help from a technology partner such as Accolade Technology



THE PRODUCT

The diagram above illustrates the high-level architecture of a lawful intercept deployment. The service provider (i.e. wireline, wireless or cable) deploys an IP probe at a strategic location within their network where large volumes of traffic traverse the network. Traffic is copied and relayed (without disturbing the normal flow of traffic) to the IP probe that has specialized software to capture and analyze specific communication that has been authorized by a court for interception. The probe in turn outputs the relevant data for final scrubbing before exporting (usually in encrypted format) to the relevant law enforcement agency.

Lawful Intercept Focused Company Develops 100G IP Probe

LAWFUL INTERCEPT

Lawful intercept is a unique market because by its very nature it is heavily regulated and each country or jurisdiction has a different regulatory framework. A solution provider therefore must provide a product that is highly customizable to meet local requirements. In addition, the solution must be very reliable lest the wrong suspect be unfairly targeted and accused. As a result, very strict procedures have been developed by various regulatory bodies to govern how service providers must conduct lawful intercept related activities. The table below outlines high-level guidelines for lawful intercept as defined in the 1994 act by the United States Congress sometimes referred to as the "Digital Telephony Act", but formally called the "Communications Assistance for Law Enforcement (CALEA) Act. These guidelines serve as the basis for lawful intercept practice around the globe.

GUIDELINE	REQUIREMENT
Step 1	Ensure clear access to all data without any loss of information or impact on the network being monitored
Step 2	Create a filter to adhere to warrant parameters – time span, types of communications that can be monitored, evidence to be collected, etc.
Step 3	Set the lawful intercept device to capture and/or store data according to the warrant parameters
Step 4	Deliver data directly from the source to the mediation device without any human intervention or packet loss

Lawful intercept procedures as defined by US Communications Assistance for Law Enforcement Act (CALEA)

THE SOLUTION (ADVANCED FILTERING)

At the outset of development planning, the company's design team made a strategic decision to incorporate a third-party CPU offload adapter into the 100G IP probe. To date the company had not used "outside" technology, but 100G was uncharted territory and the team quickly realized that software alone could not achieve the desired goals. This decision was not taken lightly however, because if they chose the wrong technology partner and the new product failed in a service provider network, the consequences would be devastating as regulatory bodies would certainly punish the service provider and in turn their IP probe supplier.

So the company carefully surveyed the market for a suitable 100G CPU offload adapter with three main requirements in mind: 1) Technical reliability, judged largely by longevity in the marketplace and customer references 2) 100% packet capture and 3) Advanced filtering capability. The company was able to find vendors which met requirements 1 and 2, but number 3 proved to be more challenging. There was no commercially available adapter that met all the company's specific packet filtering requirements, largely because the requirements were unique to the lawful intercept market. For example, some adapters didn't have enough filtering rules onboard and others weren't able to filter on the precise fields required or didn't fully support IPv6. Accolade Technology agreed to make specific changes to the packet filtering rules on the ANIC-200KFlex adapter and after some joint collaboration the company qualified the adapter for use in their 100G IP probe which is now shipping to service providers and law enforcement agencies around the world.

Accolade Technology

Headquarters:
124 Grove Street, Suite 315
Franklin, MA 02038

phone: 877 653 1261
email: inquire@accoladetechnology.com
www.accoladetechnology.com