Case Study: Cubro Probe Provides Lawful Interception Solution to Defense Organization

Industry >**Defense**

Challenge

A thorough understanding of the behaviour of the entire network to pinpoint any abnormal activity and detect unauthorized or suspicious application activity without losing lose sensitive data.

Solution

Cubro's Probe captures layer 2 through 7 packet header and payloads from each session for a complete record of network activity. The probe utilizes on board network processors, which are highly optimized CPUs, that allow the probe to easily handle high bandwidth network traffic with no lost or dropped packets.

Introduction

This is a case study of a European defense and security organization which uses Cubro products and solutions. The name of the organization is not mentioned due to the confidentiality agreement.

Organizational Challenges

This security agency requires real-time awareness and an understanding of all data traversing the network. The increased traffic and lack of network visibility is a big challenge and makes it difficult to perform well. A thorough understanding of the behaviour of the entire network is crucial to pinpoint any abnormal activity and detect unauthorized or suspicious application activity. And meanwhile, the organization cannot afford to lose sensitive data. Therefore, the organization was looking for the right tools which would provide both application-level awareness and rich network session details.

Business Benefit

The organisation improved the services as it was able to capture traffic and identify the problem. Cubro products have provided multiple secure data environments for the organization by identifying blind spots in the network.

- Improved Service Quality
- Increased Security
- Reduction of Blind Spots

Technical Solution

The organization deployed Cubro products to solves these challenges. Cubro's portfolio solutions in the Lawful Interception field include probes which can be conveniently customized to enable the organization to implement the Lawful Interception of content according to the specific requirements.

Cubro's probe captures full Layer 2 through 7 packet header and payloads from each session for a complete record of network activity. The probe utilizes on-board network processors, which are highly optimized CPU's that allow the probe to easily handle high-bandwidth network traffic with no lost or dropped packets. All information is organized by session, providing full context for application communications and content transferred across the network. By deriving a rich set of fully searchable metadata, network monitoring tools provide rapid access to highly valuable data, resulting in a rapid and in-depth understanding of network activity.

Cubro's network visibility tools provided these solutions to the organization:

- ✓ Load balancing in all layers
- ✓ Packet filtering in all 7 OSI layers
- ✓ Packet modification in all 7 OSI layers
- ✓ Keyword search
- ✓ Regular Expression search
- ✓ Probing application
- ✓ Network statistics

Customer Review

"With Cubro's Packetmasters and Probes, we have been able to improve our services as we are able to capture traffic and identify the problem. Cubro products have provided multiple secure data environments for our organization. They helped us gain end-to-end network visibility which is crucial for protecting the network."

Cubro Network Visibility
Ghegastrasse 3, 1030 Vienna Austria
Tel.:+43 1 29826660 Fax: +43 1 2982666399

Email: support@cubro.com