CUBRO
NETWORK VISIBILITY

# LEADING FINANCIAL INSTITUTION OPTIMIZES PERFORMANCE OF SECURITY SOFTWARE WITH SOLUTION FROM CUBRO

CASE STUDY

**Industry » Enterprise**

**Network Visibility and Cybersecurity Challenges**

*With the increase in cybersecurity threats and data breaches, network security has become more and more vital in all financial institutions.*

# Introduction

This case study deals with a medium sized enterprise in the financial sector in Japan that was required to integrate a McAfee security solution into the network infrastructure. Key technical criteria was to collect relevant traffic from branch offices and to feed it to a McAfee security solution that was centrally located and managed.

## About the Financial Institution

A leading financial institution headquartered in Japan with offices in 20 locations, wanted to implement cybersecurity measures to protect their customers' assets. The financial institution has around 2000 employees and its capital is approximately 500 Billion Yen.

## Network Visibility and Cybersecurity Challenges

Financial institutions are more dependent on networks for running business successfully and as a result they deploy more and more tools to get visibility and security. With the increase in cybersecurity threats and data breaches, network security has become more and more vital in all financial institutions.

The major impact of the challenges faced by the financial institution included:

1. Limited market availability of 1000Base-T aggregation devices that were required.
2. Increase in tool cost due to growing monitoring points.
3. Lack of centralized visibility.
4. Getting 100% network traffic visibility to run the network smoothly

Deploying a security tool/security software without full view of the network traffic from network domains was not enough to achieve the desired result. The financial institution wanted a cost-efficient solution that could provide agility and security while reducing the complexity.

**Integrated Solution from Cubro**

*Cubro offered EX5-3 to help eliminate blind spots by offering high port count. These network packet brokers support aggregation of many 1 Gbps inputs to a single 10 Gbps output towards IDS and other analyzing tools.*

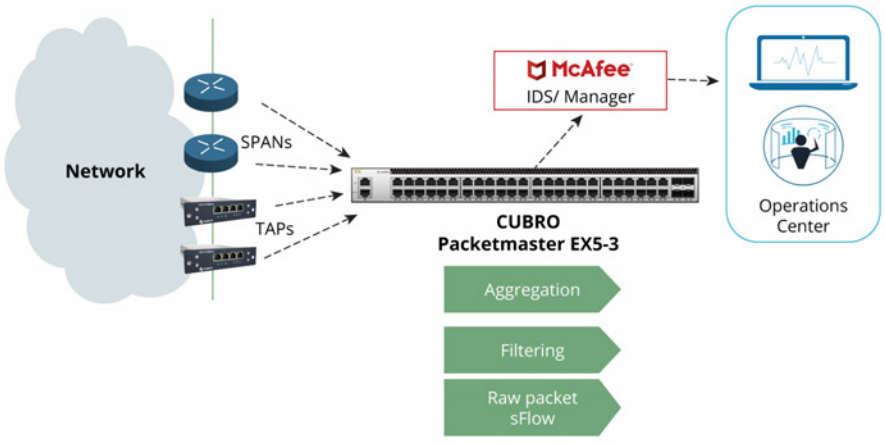
The financial sector in Japan wanted to integrate a McAfee security solution into the network infrastructure. Key technical criteria was to collect relevant traffic from branch offices and to feed it to a McAfee security solution that is centrally located and managed.

## Integrated Solution from Cubro to Manage Security

Cubro offered EX5-3 to help eliminate blind spots by offering high port count. These network packet brokers support aggregation of many 1 Gbps inputs to a single 10 Gbps output towards IDS and other analyzing tools.

### Deployment Scenario

The Cubro Network Packet Broker EX5-3 is installed in the remote Data Centers in the customer network and collects traffic from span ports as well as tapping devices, aggregates and filters this traffic and forwards it further to the McAfee analyzing tools.



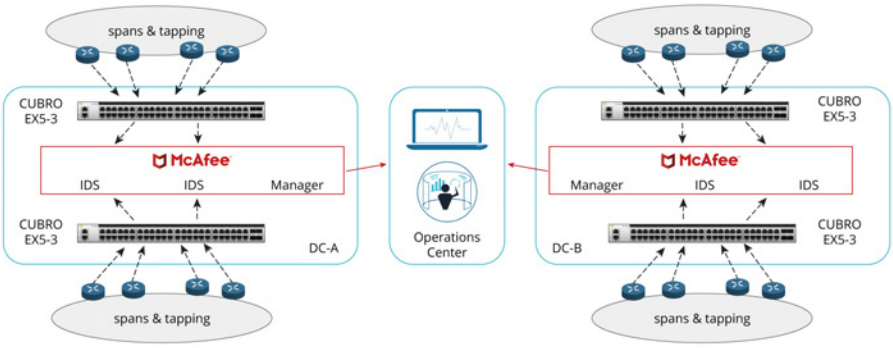

Besides raw packet forwarding, the EX5-3 produces also sflow information and sends it the IDS for further checks.

*Relevant network traffic from all span ports and tapping points is aggregated and provided to McAfee Security solution. A central operation center is thus able to analyze this traffic and to keep the network safe.*

## Key highlights of the solution:

- Does not affect service and is kept totally separate from live traffic
- By aggregating the traffic from various inputs (taps and spans) less interfaces on IDS monitoring equipment is needed > cost reduction.
- By using filtering out non required traffic the traffic load that is sent to monitoring tools is reduced. Thus less capacity on monitoring equipment is required saving costs of the overall deployment.
- Cubro EX5-3 helps to eliminate blind spots by offering high port count and supports aggregation of many 1 Gbps inputs to a single 10 Gbps output towards IDS and other analyzing tools.
- sFlow generation directly on the Cubro EX5-3 reduces the performance requirements of the monitoring solution by offloading this task to the EX5-3.

## Full Deployment across multiple Data Centers




Relevant network traffic from all span ports and tapping points is aggregated and provided to McAfee Security solution. A central operation center is thus able to analyze this traffic and to keep the network safe.

*The customer was able to reduce the number of tools by aggregating the monitor points. Besides the other benefits, the customer reduced cost and gained higher ROI.*

## Business Benefits

The solution offered by Cubro reduced the traffic flowing into the tool by filtering only the packets needed for monitoring. As a result, the customer was able to reduce the number of tools by aggregating the monitor points. The main benefits of the solution include:

- Optimised performance of network analysis and security tool
- Maximized utility despite constrained budgets by increasing network traffic visibility
- Removed blind spots from all network environments, and get access for integrated, cost-effective network monitoring, security and analytics.
- Failsafe deployment and efficient operation of security software
- Cost reduction and higher ROI
- Improved customer satisfaction