JOINT SOLUTION BRIEF

Improved network security posture with full visibility of all relevant network traffic

The Challenge

New networking technologies, such as 5G, SDN, NFV, SD-WAN, cloud, virtualisation and IoT, along with faster network speeds of 40/100/400Gbps, create new incremental network security blind-spots and expand an organization's security attack surface. This situation compromises an organization's security posture by increasing the risk of undetected security threats and vulnerabilities.

The Solution

A joint Cubro Omnia/McAfee Network Security Platform solution ensures that all network traffic is efficiently and cost-effectively secured 24/7. Omnia replicates, aggregates and filters network traffic collected from network TAPs and SPAN ports and passes the filtered traffic to McAfee Network Security Platform at high speeds up to 100 Gbps for intrusion prevention and detection analysis.
The filtered traffic can be load balanced across multiple McAfee Network Security Platform devices to maintain security posture in the event of a McAfee Network Security Platform outage.

Joint Solution Benefits

- Accelerated threat detection and mitigation
- Reduced costs and increased ROI
- Improved business continuity

Cubro Omnia and McAfee Network Security Platform (NSP) provide cost effective improved and accelerated network security threat detection

Overview

Cubro's Omnia is a range of physical and virtual Advanced Network Packet Brokers that improve network security posture by removing network blind-spots, increase the ROI of network security devices by reducing their network traffic loading, and reduce network security service downtime through load balancing and automated bypass.

The joint Cubro Omnia/McAfee Network Security Platform IDPS solution improves network security threat detection by reducing the time required for McAfee Network Security Platform to analyse network traffic and identify potential threats. It extends the lifespan of McAfee Network Security Platform solutions, and maintains McAfee Network Security Platform's security service in the event of an unscheduled or scheduled maintenance outage.

Unlike other Advanced Network Packet Brokers, Omnia includes integrated network test access points (TAPs) and packet capture capabilities to reduce the risk of connectivity issues, improve sustainability by reducing the amount of rack space and environmental resources required, and reduce total cost of ownership (TCO) of the combined solution compared to separate component solutions.

The Business Problem

As transformational network technologies, such as 5G, SDN, NFV, SD-WAN, cloud, virtualization, and IoT, and increased network speeds of 40/100/400Gbps are being deployed, networks are becoming more complex and higher performance. The complexity and faster network speeds create new, incremental blind-spots - blind-spots are network traffic that cannot be monitored and analysed by network security tools and which increase the risk of undetected security threats and vulnerabilities.

At the same time, the number of new security threats and attack surface is increasing significantly, exacerbating and amplifying the security risks created by network blind spots. To successfully manage the increased risks an organization's entire network traffic must be monitored and analyzed continuously.

Historically the approach has been to continue to expand the increasingly large number and disparate types of security solutions deployed, but this approach has become increasingly expensive and disruptive to deploy and maintain while not necessarily delivering the outcomes and security posture required. An alternative combined Cubro Omnia/McAfee Network Security Platform solution ensures that all network traffic is efficiently and cost effectively secured 24/7.

Cubro Omnia/McAfee Network Security Platform Combined Solution Description

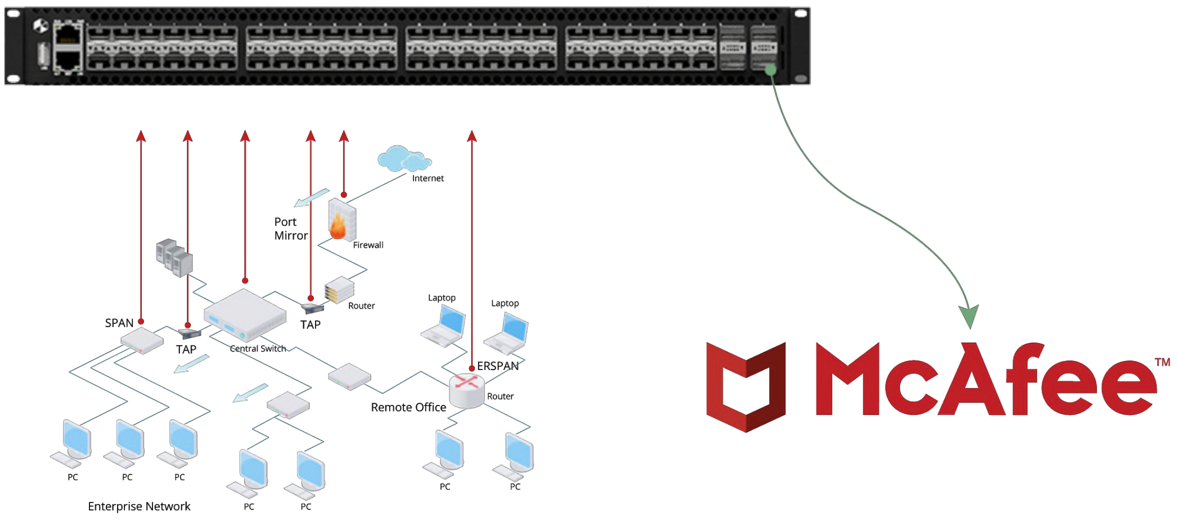

Figure 1: An example deployment of the combined Omnia/McAfee Network Security Platform solution.

Omnia observes all network traffic crossing an organization's network and can receive a copy of all traffic from multiple sources including external network TAPs, integral network TAPs, switched port analyzer (SPAN) ports or direct network sources. It supports both electrical and optical interfaces across a range of speeds from 10Mbps through to 100Gbps for connection to both the network traffic sources and McAfee Network Security Platform. It can also provide speed and media mitigation between the network and McAfee Network Security Platform if necessary.

Omnia optimizes the duplicated network traffic before sending it to McAfee Network Security Platform by aggregating the traffic from the multiple network sources across a reduced number of higher speed connections to McAfee Network Security Platform. It can further optimize the traffic by reducing the traffic load sent to McAfee Network Security Platform by filtering out traffic that does not require analysis and by deduplicating and removing duplicated data packets. Additionally it eliminates network blind-spots by removing network protocols that are not supported by McAfee Network Security Platform and presenting the raw network traffic to McAfee Network Security Platform for analysis. Omnia's out of band deployment means that the live network traffic is not affected in any way.

When McAfee Network Security Platform receives the optimized network traffic it can identify security threats more quickly because it has less traffic to analyse and because it receives the traffic at high speeds of up to 100Gbps. Multiple McAfee Network Security Platform devices can be load balanced across an Omnia appliance to maintain security service resilience in the event of a scheduled or unscheduled McAfee Network Security Platform outage, and to optimize their operational efficiency through shared workload.

Joint Solution Benefits

1. Removes security monitoring blind-spots from network traffic – to improve security posture
2. Reduces the time taken to identify potential security threats – to improve security posture
3. Maintains business continuity in the event of scheduled or unscheduled McAfee Network Security Platform service outage – to maintain security posture
4. Extends the lifespan and ROI, while reduces total cost of ownership (TCO), of McAfee Network Security Platform solutions – to reduce cost
5. Reduces the use of operational and environmental resources and extends McAfee Network Security Platform life span – to improve environmental sustainability

Use Cases

Example 1

Cubro TAPs passively copy traffic from multiple points in the network and feed the traffic to the Omnia120 Advanced Network Packet Broker. The Omnia120 performs aggregation, de-encapsulation, deduplication, and traffic filtering before load-balancing the traffic across multiple McAfee Network Security Platform sensors enabling complete visibility into network traffic as well as access to high-bandwidth (multiple 100Gbps) links.

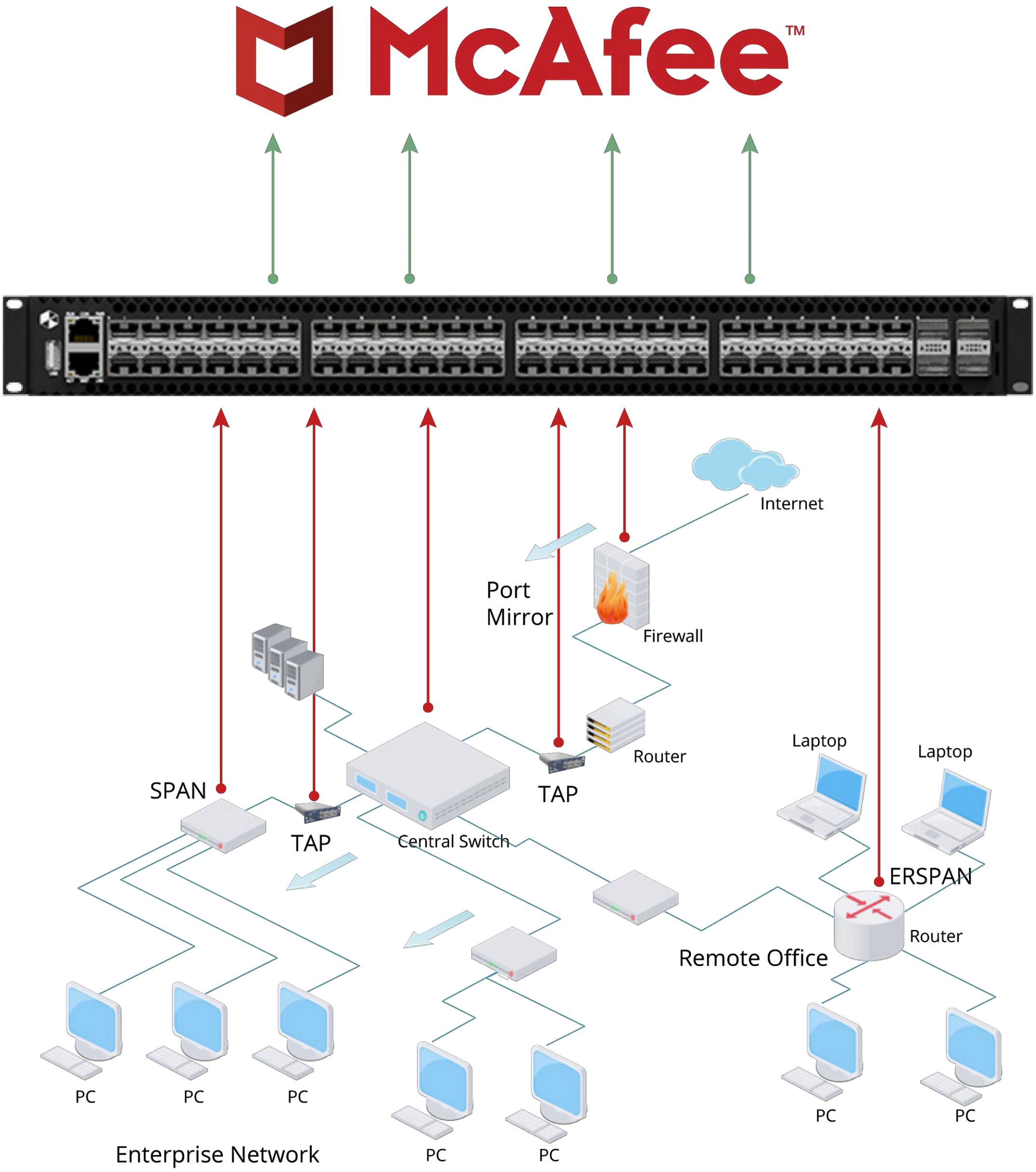

Figure 2. Load balanced network traffic.

Example 2

Omnia10 passively taps network traffic, aggregates, and forwards a copy to McAfee Network Security Platform sensors. Additionally, the Omnia10 can perform network analytics, such as NetFlow and IPFIX, to provide McAfee Network Security Platform with more data points for threat detection and analysis.

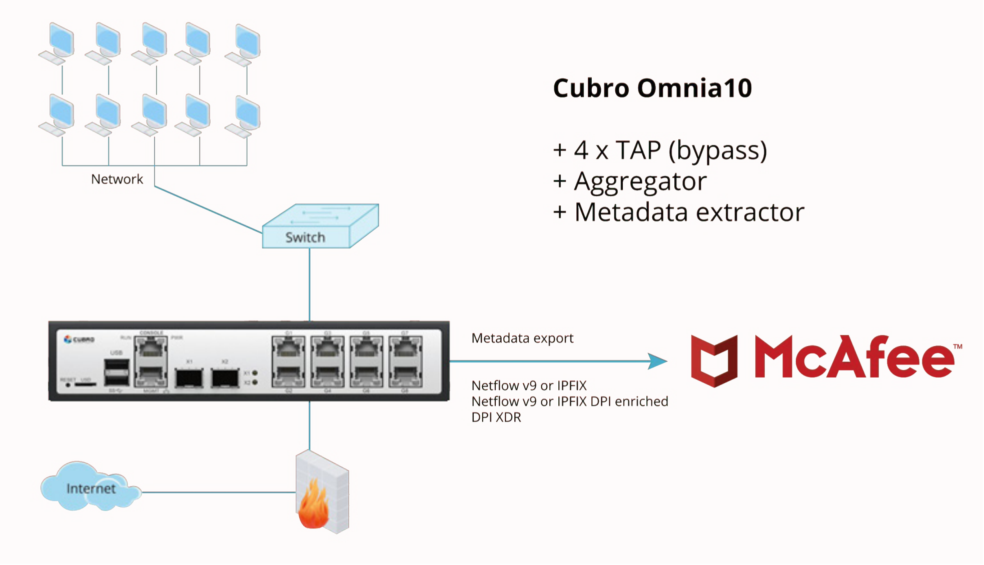

Figure 3. Metadata/DPI generation.

Example 3

Cubro TAPs and Advanced Network Packet Brokers are deployed at remote sites for comprehensive visibility and access to network traffic. The Cubro Advanced Network Packet Broker further encapsulates a copy of the aggregated traffic for backhaul to a centralized location where the tunnel is terminated on an Omnia120 and the remote traffic is forwarded to McAfee Network Security Platform.

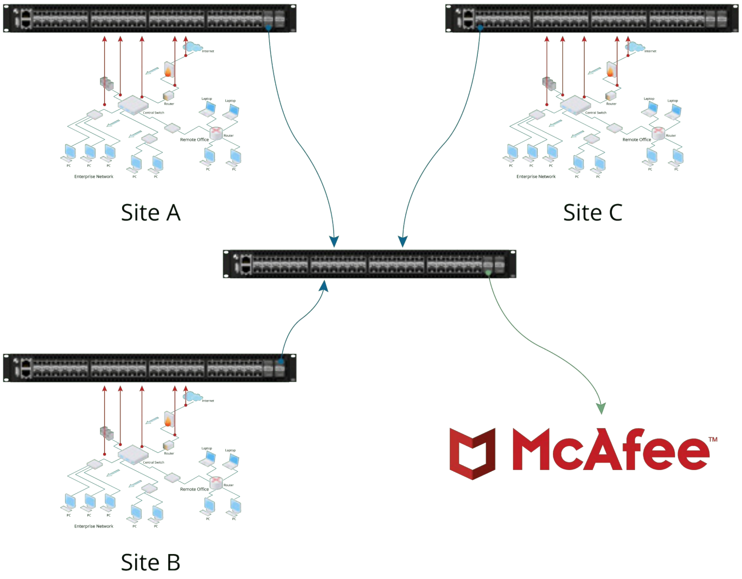

Figure 4. Network traffic backhaul to a centralized McAfee Network Security Platform.

About Cubro

Cubro is a leading vendor of network visibility solutions that include network TAPs, Advanced Network Packet Brokers, Bypass Switches and Network Probes, for Service Providers and private and public sector Enterprises worldwide.

Our solutions improve security posture while reducing costs by increasing the effectiveness and lifecycle of network security devices, improving business continuity, and reducing the total cost of ownership (TCO) while increasing the ROI of network security. Cubro's products remove network blind-spots to ensure all relevant network traffic is available for security analysis, filter out unnecessary network traffic for analysis, and provide high-availability capabilities for security solutions.

About McAfee Network Security Platform

McAfee Network Security Platform is a next-generation intrusion detection and prevention system. McAfee Network Security Platform combines both signature-based and signature-less intrusion detection methods to identify malicious traffic and stop threats before they take hold in the network.

Signature-less detection stops zero-days and unidentified attacks, unlike solutions that solely utilize signature-based detection where only known threats are detected. McAfee Network Security Platform supports VMware NSX and OpenStack, extending network security across both the physical and virtual infrastructure. Flexible deployments with hardware sensors that support up to 100Gbps network traffic and virtual sensors make McAfee Network Security Platform the ideal next-gen IPS for on-prem and cloud deployments.

Cubro/McAfee Compatible Solution

Cubro Omnia10/20/120

McAfee NS9500/7500/7350/7250/7150/5200/52100/3500/3200/3100

McAfee IPS-VM 600/VM 600-VSS

For more information please visit www.cubro.com and www.mcafee.com.