Solution Overview

Cubro and Netflow Logic address the issues of flow data volume in modern networks while leveraging Deep Packet Inspection and data enrichment to enhance the value of flow data collection to SIEMs and other tools, all while reducing associated costs

Components

- Omnia120 Advanced Network Packet Broker
- NetFlow Logic NetFlow Optimizer

Benefits

- 1:1 Netflow Generation on dedicated hardware
- DPI-enhanced IPFIX identifies protocols and applications
- Reduce volume of flow data sent to tools while retaining all meaningful data
- Enrich flow data with geolocation information and threat intelligence
- Reduce storage costs and SIEM subscription fees associated with flow data retention

Enriched flow data with intelligent compression

Introduction

When networked devices need to communicate with one another, they establish communication channels, commonly referred to as connections when TCP is used. A flow refers to any connection or connection-like communication channel. Specifically, a flow is defined by five specific data points: the source and destination IP addresses, the source and destination ports, if any (e.g. ICMP), and the OSI Layer 4 protocol type (e.g. 6 for TCP, 17 for UDP). By definition, all packets sharing these same 5 data points, referred to as a "5-tuple" belong to the same flow, or connection.

NetFlow is a feature built into network devices, such as routers, that collects measurements for each flow and exports them to another system for analysis. For example, NetFlow captures the timestamp of a flow's first and last packets (and hence its duration), the total number of bytes and packets exchanged, a summary of the flags used in TCP connections, and other details.

This feature has gone through multiple iterations of standards and has cemented itself as a common tool for monitoring network connections and is also leveraged for security applications. There is an increasingly apparent problem with modern connected devices and NetFlow collection though, namely data volume.

The Challenge

Put simply, there are millions of flows, with a single device often having hundreds of concurrent connections. Netflow was developed in 1996, in the early days of the Internet. In those days, only a few applications could run on a computer and they would typically not run simultaneously and talk to one or, at most, a few servers. This changed dramatically in 2000 with WEB 2.0 when web pages became dynamic and another huge leap forward was made with the appearance of smartphones.

Today a network attached device, be it a PC, Smartphone, or Tablet, can have hundreds of open sessions. The amount of traffic that is produced by a Netflow solution does not depend on the bandwidth but rather on the amount of sessions, each of which represent a flow record.

Netflow output is typically 1% to 3% of the input traffic, for example, 2% of the traffic on a 900 Gbit/s network would equal 18 Gbit/s of flow records to analyze and store.

A 30 day retention period for this amount of data would equal **5832 TB** of storage; which is not feasible in most cases. In addition to the sheer volume of sessions/flows per device there is the issue of perpetual sessions. These immediately lead to a major problem for flow-based monitoring systems. A flow-based probe reserves memory for each session/flow and holds it until the session is closed. If this never occurs, as is common with indefinitely open sessions and irregularly terminated sessions, the probe quickly runs out of memory. To remediate this a timeout period is used to close inactive sessions.

This timeout is an artificial value and it could easily be the case that a session is terminated due to timing out, however the session is still valid. This is especially true for IoT devices; the traffic is so low that they send, perhaps, one packet per day.

With today's massive amount of connected devices, combined with the huge increase in sessions that each device generates, NetFlow-based monitoring solutions are facing major challenges with scalability as the processing and storage requirements are exponentially more costly. Nevertheless, Netflow is a valuable data source for monitoring and troubleshooting. Cubro and NetFlow Logic have joined together to offer a combined solution to not only address the scalability problems with NetFlow, but enrich it with even more valuable data in the process.

Joint Solution

Passive Optoslim TAPs and the Omnia120 are used to obtain an out-of-band packet for packet copy of the network traffic and generate one-to-one IPFIX records. These records contain all information traditionally found in NetFlow as well as protocol and application detection from Cubro's Deep Packet Inspection engine. The result is enriched NetFlow records for every session transiting the network, rather than sampled flow records, which are often necessary to reduce data volume or due to limited resources on routers, but sacrifice comprehensive network visibility.These enriched IPFIX records are then forward to NetFlow Optimizer for further processing and data enrichment.

NetFlow Optimizer (NFO) uses patented streaming technology to aggregate records from multiple flow data and log sources, eliminating redundant data. Simultaneously, the data is enriched with valuable information, including geoIP data, domain reputation scores, and threat detection, adding another layer of intelligence and enhancing the organization's monitoring capabilities and security posture. The result is a drastic reduction in data output while not only retaining all of the original flow record information, but an enhancement of that data through Cubro and NetFlow Logic's combined enrichment. The output is also standardized according to user-selectable formats, such as Syslog or JSON, for compatibility across monitoring tools, such as SIEMs. Maintain all visibility, reduce processing and storage costs, and save on volume-based licensing fees.

Joint Solution Components

The Cubro Omnia120 Advanced Network Packet Broker

The Omnia120 is an advanced network packet broker designed from the ground up to address the needs of evolving networks and demanding throughput requirements. Omnia provides purpose-built hardware capable of handling network links from 1 Gbps to several 100 Gbps and a feature-set derived from years of experience and engineering. Omnia combines features included in Advanced Network Packet Brokers with high-performance multi-core CPUs to enable numerous network monitoring, security and analytics uses cases and applications, including those from partners and the open-source community.

NetFlow Logic NetFlow Optimizer

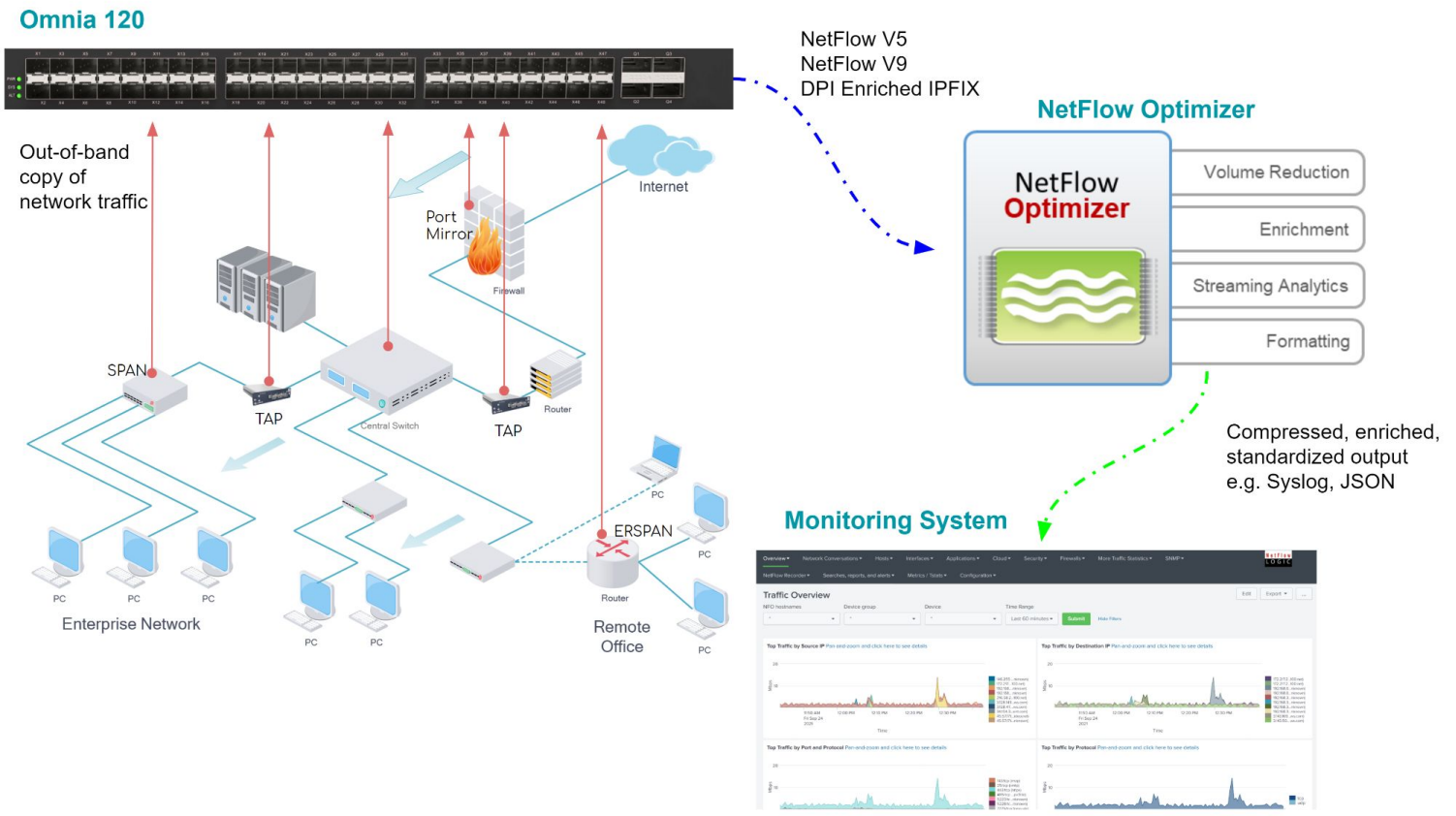
NetFlow Optimizer (NFO) uses patented streaming technology which allows the processing of flow data up to 10 times faster than competitive products. It is complementary to traditional network monitoring and security solutions.

NFO provides aggregation of records from multiple flow data and log sources, converts it into standard syslog or JSON format, filters to eliminate redundant data and enriches with useful additional information delivering a critical component for complete network visibility.

Example Deployment

A combination of Cubro TAPs and mirror ports (such as SPAN and ERSPAN feeds) provide a copy of all network traffic to an Omnia120. The Omnia120 generates NetFlow or DPI enriched IPFIX records from the traffic. These records are sent to an instance of NetFlow Optimizer for processing, compression, and further data enrichment. The output is standardized and forwarded to the downstream monitoring system(s). Additionally, the Omnia120 can aggregate, filter and distribute traffic to out-of-band security and monitoring tools, such as an IDS, and NetFlow Optimizer can ingest other structured data, such as public cloud flow logs (AWS/Google VPC Flow logs, Azure NSG Flow logs), for processing and forwarding to monitoring systems.

Cubro Network Visibility
EMEA USA APAC Japan
support@cubro.com



About NetFlow Logic

NetFlow Logic specializes in developing real-time, super-fast flow data (NetFlow, sFlow, IPFIX, J-Flow, Netstream, etc.) processing and analysis tools that are easy to deploy and integrate with other network management and security products. Our core product, NetFlow Optimizer (NFO), enhances the capabilities and value of log analyzers and SIEM systems from other vendors like Splunk, Exabeam, VMware, Sumo Logic, etc. and delivers a critical component for complete network visibility and User Behavior Analytics.

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.

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

Cubro Network Visibility
EMEA USA APAC Japan
support@cubro.com

Cubro Network Visibility
Ghegastraße 3
1030 Vienna, Austria

Tel.: +43 1 29826660
Fax: +43 1 2982666399
Email: support@cubro.com

Cubro Asia Pacific
8, Ubi Road 2 #04-12
Zervex
Singapore 408538

Tel.: +65-97255386
Email: jl@cubro.com

Cubro North America
Cubro Network Visibility Inc.
225 Peachtree Street NE,
Suite 1100, Atlanta, GA, 30303, USA

Email: americas@cubro.com

Cubro Japan
6-7-22, Shinjuku,
Shinjuku,
Tokyo, 160-0022 Japan

Tel: +81(0)50-3708-5839
Email: japan@cubro.com