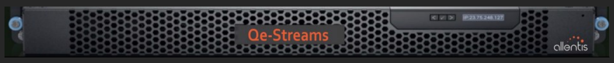
Qe-Streams

100 Gbps network and application traffic analysis appliance, IP flow matrices

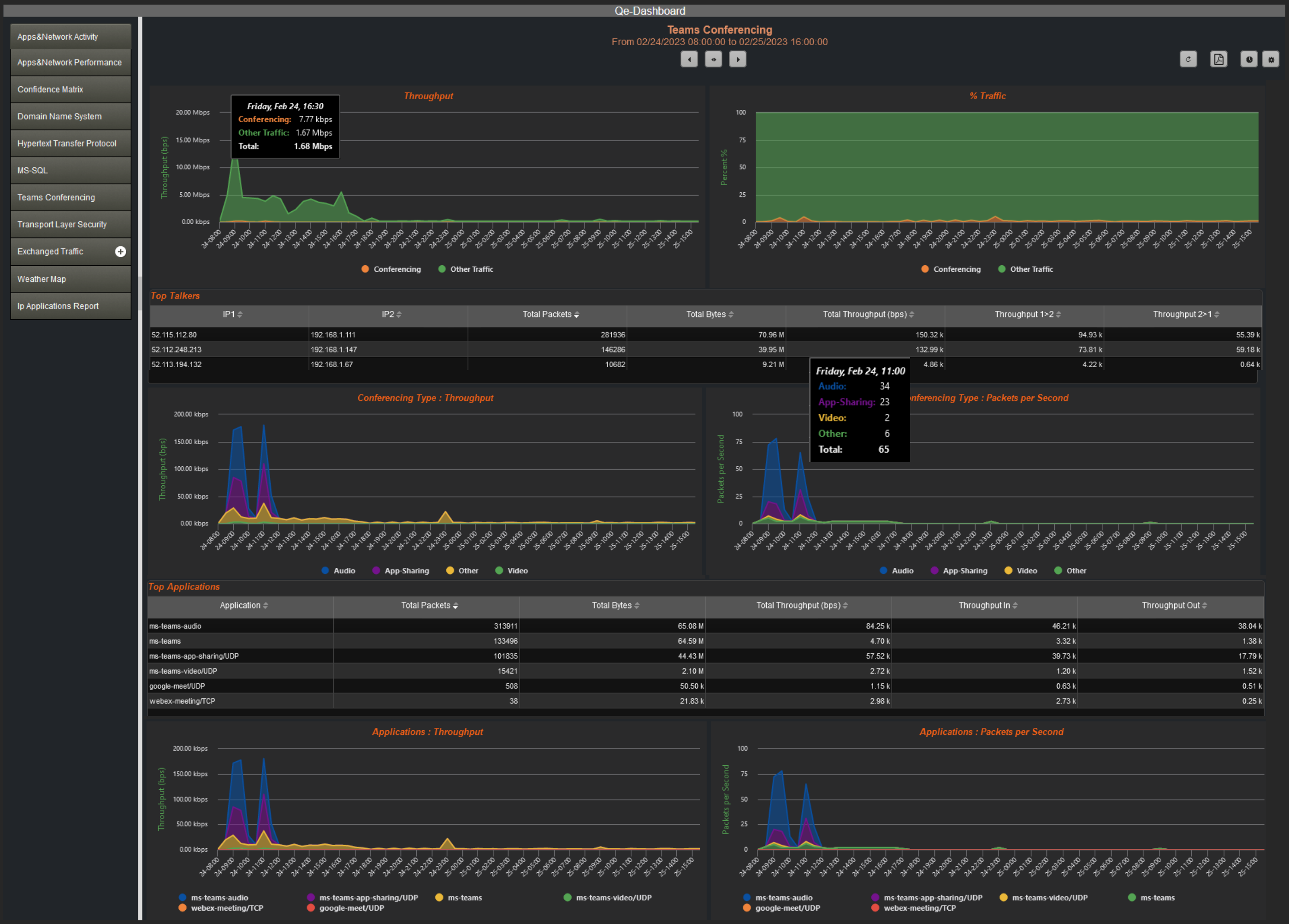


The analysis and understanding of the North-South flows exchanged on the networks remain essential on the large information systems to ensure their control, both from the point of view of exchange performance and from that of security. Qe-Streams meets these needs perfectly. Up to 100 Gbps, this appliance analyzes all packets to provide a detailed traffic flow matrix. The results of this analysis are stored in statistical databases accessible via dedicated REST APIs.

Analysis of activity on large networks from a single point

Qe-Streams discovers client and server addresses. Their activity and behavior on the networks are analysed. The associated available measurements relate in particular to the volumes exchanged and the corresponding speeds, the response time of the exchanges broken down into network time and server time and the levels of retransmissions. Absence of responses from servers following client requests are analysed. The certificates used in https are detailed and their validity dates are all reviewed.

Integration with Qe-Manager



Top Talkers

IP1	IP2	Total Packets	Total Bytes	Total Throughput (bps)	Throughput 1>2	Throughput 2>1
52.115.112.80	192.168.1.111	281936	70.96 M	150.32 k	94.93 k	55.39 k
52.112.248.213	192.168.1.147	146286	39.95 M	132.99 k	73.81 k	59.18 k
52.113.194.132	192.168.1.67	10682	9.21 M	4.86 k	4.22 k	0.64 k

Top Applications

Application	Total Packets	Total Bytes	Total Throughput (bps)	Throughput In	Throughput Out
ms-teams-audio	313911	65.08 M	84.25 k	46.21 k	38.04 k
ms-teams	133496	64.59 M	4.70 k	3.32 k	1.38 k
ms-teams-app-sharing/UDP	101835	44.43 M	57.52 k	39.73 k	17.79 k
ms-teams-video/UDP	15421	2.10 M	2.72 k	1.20 k	1.52 k
google-meet/UDP	508	50.50 k	1.15 k	0.63 k	0.51 k
webex-meeting/TCP	38	21.83 k	2.98 k	2.73 k	0.25 k

Illustration : reporting on videoconference flows

Qe-Streams appliances can be connected to Qe-Manager, the virtual appliance of the Qe range. Qe-Manager allows centralized management of multi-probe deployments to manage large configurations. The configuration of the probes and the reporting are thus available through a single connection to the system thus constituted.

Opening the solution

The technological choices made for the storage part and the presentation part are deliberately oriented towards open approaches. The REST API available on Qe-Streams guarantees its openness to all presentation solutions. Thus, it is easy for operators to rely on Qe-Streams to feed the solutions already integrated within the technical teams by the KPIs available in the databases of the appliances. With Qe-Streams, allentis provides its customers with the essential tools for analyzing flows entering data centers. The statistical data presented in the GUI brings together the main information expected in this area.

Cross-functionality of the solution

Qe-Streams now represents, for large organisations, the source of reference data for analyzing flows with a view to producing valued reporting according to business lines. The proposed approach overturns the standards hitherto encountered in the field of proprietary probes for analyzing flows on large networks. On all IS, it is becoming essential to promote solutions whose ease of access to APIs guarantees real cross-functionality. This is what Qe-Streams represents with the mix of advanced analyzes on high-speed access and a data query architecture compatible with expectations of openness to third-party solutions.

Easy access to analytics data

To guarantee very easy access to the analyzed information, Qe-Streams embeds advanced "Dashboarding" features. On business issues encountered on a daily basis, dedicated analysis reports provide on the same page all the technical data allowing a quick understanding of the indicators measured. Identifying the origin of the slowdowns or malfunctions encountered is thus greatly simplified. The continuous operation of the solution allows a pro-active approach in order to anticipate the sources of dissatisfaction likely to impact users.

Critical Security Indicators

It is necessary to know quickly how the essential safety elements work. This is why, positioned on the main points of your infrastructure, the Qe-Streams probe constantly monitors the state of the TLS (Transport Layer Secutity) part of the exchanges. The Server Names are analyzed, the ciphers implemented are monitored and the TLS alerts are monitored in order to provide a rapid and centralized overview of this essential level of exchange security.

Detailed IP flow matrices and trust matrices

Performance and security issues are also linked to those of authorized or unauthorized exchanges between different groups of machines. The flow matrices available on Qe-Streams automatically provide details of the exchanges between the different groups of IP addresses. The traffic between these IP groups and the protocols and applications on which these exchanges take place are identified and listed. Alerts are displayed when these exchanges fall outside user-defined flow matrix templates. With trust matrices, it is easy to quickly identify IP addresses connecting to "unauthorized" machines or through protocols or applications for which authorizations are not granted.

Qe-Packets - Full packet capture in parallel with analysis

The massive storage features of monitored frames are available on Qe-Streams in parallel with the analysis features. On Qe-Packets, all the analyzed frames are stored for a retention period determined by the disk space available on the selected model depending on the analyzed throughput. After identification on Qe-Streams of sensitive events requiring further investigation, in this hybrid mode of operation, it is thus easy, through an intuitive "workflow", to switch from Qe-Streams statistical data to the detail of frames related to these events.

About allentis

allentis is a French company specializing in systems for monitoring the performance and security of data flow network exchanges. It has designed and manufactures QE flow analysis systems (Qe-Secure for threat detection, Qe-Streams and Qe-Flows for performance analysis and mapping of WAN, SD-WAN and LAN flows, Qe -Packets for massive data capture, Qualevent for business hypervision), and the TAPICS range of network components for traffic replication and isolation.

allentis
info@allentis.eu
www.allentis.eu