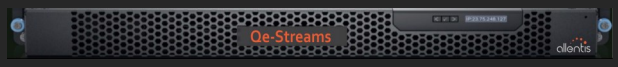
Qe-Streams

Appliance 100 Gbps d'analyse du trafic réseau et applicatif , matrices des flux IP



L'analyse et la compréhension des flux Nord-Sud échangés sur les réseaux demeurent primordiales sur les grands systèmes d'information pour s'assurer de leur maîtrise, tant sous l'angle des performances des échanges que sous celui de la sécurité. Qe-Streams répond parfaitement à ces besoins. Jusqu'à 100 Gbps, cette appliance analyse l'intégralité des paquets pour fournir une matrice des flux détaillée des échanges. Les résultats de cette analyse sont stockés dans des bases de données statistiques accessibles via des API REST dédiées.

Analyse de l'activité sur les grands réseaux depuis un seul point de concentration

Qe-Streams découvre les adresses clientes et celles des serveurs. Leur activité et leur comportement sur les réseaux sont analysés. Les mesures disponibles associées portent notamment sur les volumétries échangées et les débitmétries correspondantes, le temps de réponse des échanges décomposé en temps réseau et temps serveur et les niveaux de retransmissions. Les absences de réponses des serveurs suite aux requêtes des clients sont analysées. Les certificats utilisés en https sont détaillés et leurs dates de validité sont toutes passées en revue.

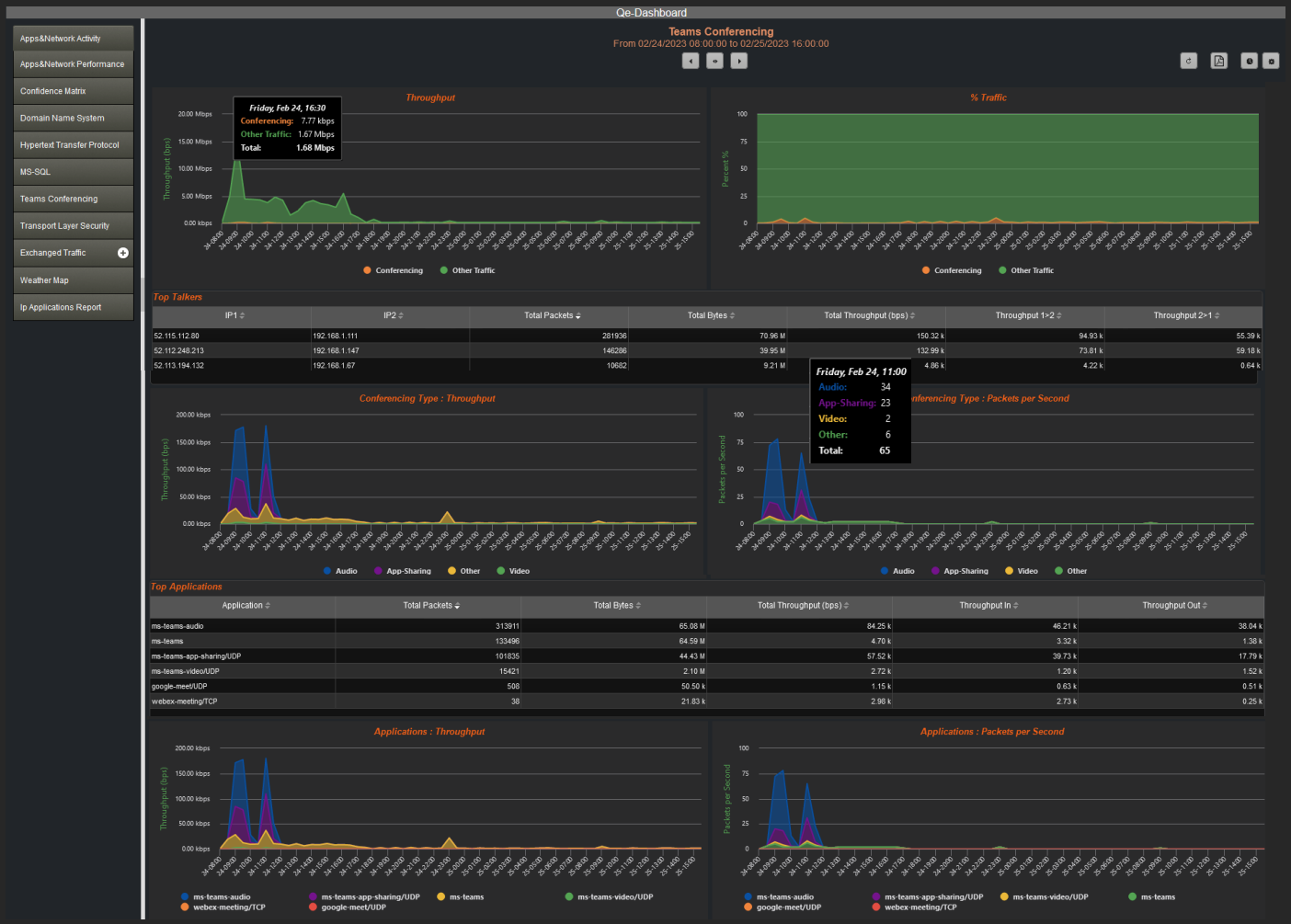


Illustration : reporting des flux de visioconférence

Qe

Intégration à Qe-Manager

Les appliances Qe-Streams peuvent être connectées à Qe-Manager, l'appliance virtuelle de la gamme Qe. Qe-Manager permet la gestion centralisée des déploiements multi-sondes afin de gérer les configurations étendues. Le paramétrage des sondes et le reporting sont ainsi disponibles au travers d'une connexion unique au système ainsi constitué.

Ouverture de la solution

Les choix technologiques retenus pour la partie stockage et celle de présentation sont volontairement orientés vers des approches ouvertes. L'API REST disponible sur Qe-Streams garantit son ouverture vers toutes les solutions de présentation. Ainsi, il est aisé pour les exploitants de s'appuyer sur Qe-Streams pour alimenter les solutions déjà intégrées au sein des équipes techniques par les KPI disponibles dans les bases de données des appliances. Avec Qe-Streams, allentis délivre à ses clients l'essentiel des outils d'analyse des flux en entrée des datacenters. Les données statistiques présentées en interface d'accueil regroupent les informations principales attendues dans ce domaine.

Transversalité de la solution

Qe-Streams représente désormais, pour les grandes organisations, la source de données de référence d'analyse des flux en vue de produire le *reporting* valorisé en fonction des métiers. L'approche proposée bouleverse les standards jusque là rencontrés dans le domaine de la sonde propriétaire d'analyse des flux sur les grands réseaux. Sur tous les SI, il devient incontournable de favoriser des solutions dont la facilité d'accès aux API garantit une réelle transversalité. C'est ce que représente Qe-Streams avec le mix d'analyses avancées sur des accès hauts débits et une architecture d'interrogation des données compatible avec les attentes d'ouverture sur des solutions tierces.

Facilité d'accès aux données d'analyse

Pour garantir une très grande facilité d'accès aux informations analysées, Qe-Streams embarque des fonctionnalités de "*Dashboarding*" avancées. Sur des problématiques métier rencontrées au quotidien, des rapports d'analyse dédiés fournissent sur une même page toutes les données techniques permettant une compréhension rapide des indicateurs mesurées. L'identification de l'origine des ralentissements ou des dysfonctionnements rencontrés est ainsi largement simplifiée. Le fonctionnement continu de la solution permet une approche pro-active afin d'anticiper les sources d'insatisfaction susceptibles d'impacter les utilisateurs.

Indicateurs essentiels de sécurité

Il est nécessaire de connaître rapidement le fonctionnement des éléments essentiels de sécurité. C'est pourquoi, positionnée sur les points principaux de votre infrastructure, la sonde Qe-Streams surveille en permanence l'état de la partie *TLS* (Transport Layer Secutity) des échanges. Les *Server Name* sont analysés, les *ciphers* mis en œuvre sont surveillés et les alertes *TLS* sont monitorées afin de fournir une vision de synthèse rapide et centralisée de ce niveau essentiel de sécurité des échanges.

Matrices détaillées des échanges et matrices de confiance

Les problématiques de performance et de sécurité sont aussi liées à celles des échanges autorisés ou non entre différents groupes de machines. Les matrices de flux disponibles sur Qe-Streams fournissent automatiquement le détail des échanges entre les différents groupes d'adresses IP. Les trafics entre ces groupes IP et les protocoles et applications sur lesquels ces échanges ont lieu sont identifiés et répertoriés. Des alertes sont affichées lorsque ces échanges sortent des gabarits de matrices de flux définies par les utilisateurs. Avec les matrices de confiance , il est aisé d'identifier rapidement des adresses IP se connectant sur des machines "non autorisées" ou au travers de protocoles ou d'applications pour lesquelles les autorisations ne sont pas accordées.

Qe-Packets - Stockage massif des trames en parallèle de l'analyse

Les fonctionnalités de stockage massif des trames monitorées sont disponibles sur Qe-Streams en parallèle des fonctionnalités d'analyse. Sur Qe-Packets, l'intégralité des trames analysées sont stockées pour une durée de rétention déterminée par l'espace disque disponible sur le modèle retenu fonction du débit analysé. Après identification sur Qe-Streams d'événements sensibles nécessitant une investigation plus poussée, dans ce mode de fonctionnement hybride, il est ainsi aisé, par un "workflow" intuitif, de basculer des données statistiques de Qe-Streams vers le détail des trames liées à ces événements.

A propos d'allentis

allentis est une PME française spécialisée dans les systèmes de contrôle de la performance et de la sécurité des échanges en réseau de flux de données. Elle a conçu et fabrique les systèmes QE d'analyse de flux (Qe-Secure pour la détection de menaces, Qe-Streams et Qe-Flows pour l'analyse de performances et la cartographie des flux WAN, SD-WAN et LAN, Qe-Packets pour la capture massive de données, Qualevent pour l'hypervision métier), et la gamme TAPICS de composants réseau pour la réplication et l'isolation de trafic

allentis
info@allentis.eu
www.allentis.eu