Qe-Packets

Appliance de capture massive des flux IP échangés sur les réseaux

Qe-Packets est le système de capture massive d'allentis. Cette plateforme fonctionne de manière combinée avec la solution Qe-Streams, la solution d'analytique des flux d'allentis pour l'analyse et la performance des échanges sur les grands réseaux IP. C'est une appliance d'acquisition de flux et de tous les paquets échangés sur les liens sur lesquels elle est positionnée jusqu'à un débit de 20 Gbps (10 Gbps full duplex). Elle garantit une durée de rétention élevée par des modules de stockage de 96To en cluster.

Solution autonome

Qe-Packets copie et stocke l'intégralité du trafic échangé sur les liens en surveillance. L'utilisateur décide du volume global de rétention des données. L'espace de stockage est configuré de manière circulaire ou linéaire afin de garantir une durée de rétention conforme aux contraintes de la production. Pour faciliter la relecture et l'accès aux données, le paramétrage de la taille des fichiers pcap est paramétrable. Par exemple, pour un stockage global de 1 To de données en mode circulaire, il peut être demandé la constitution de 1.000 fichiers de 1 Go. Cette approche garantit une extraction rapide des données. Des fonctions de filtrage sont disponibles afin de ne retenir que les données qui apparaissent les plus pertinentes. Les données produites peuvent être lues directement sur l'appliance ou avec tous les produits du marché permettant la lecture de trames réseau.

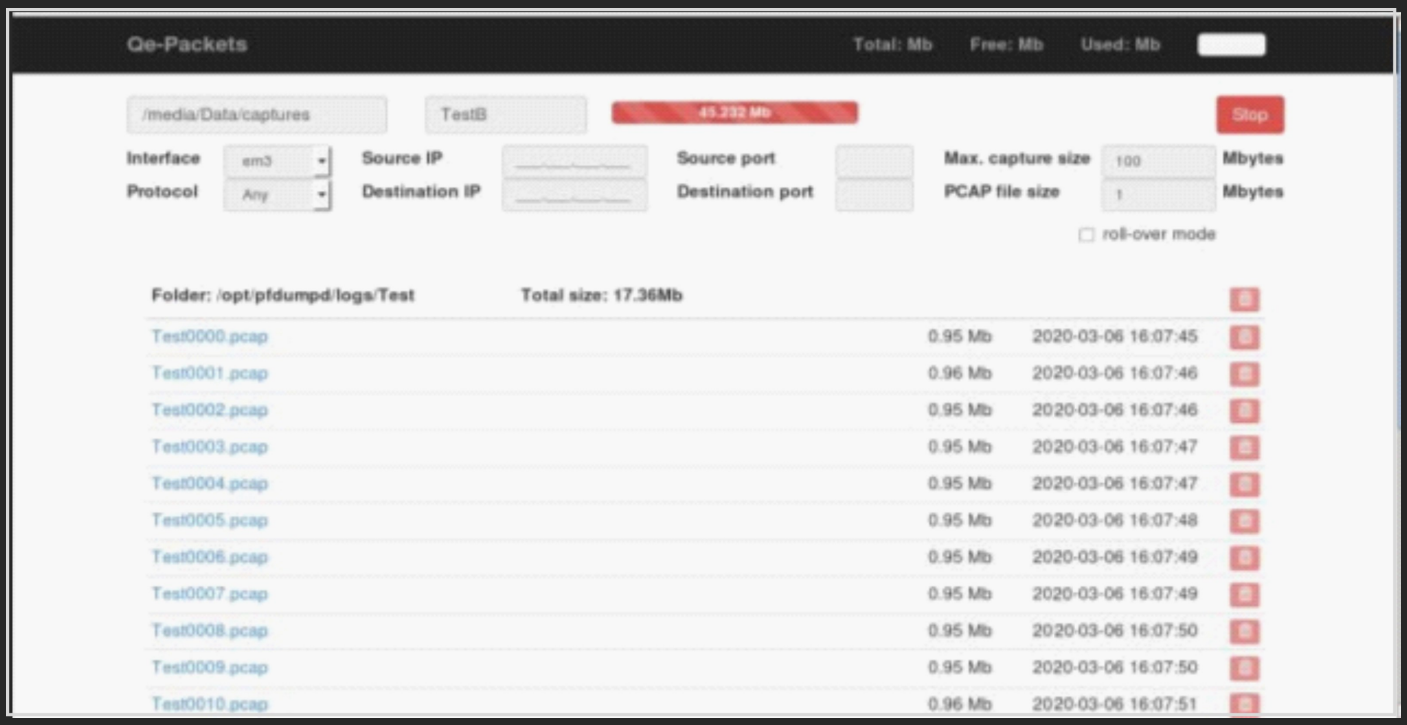

Illustration : Fichiers de stockage de l'intégralité du trafic par Qe-Packets

Accès aux données de capture depuis l'interface de Qe-Streams

Dans l'architecture des solutions Qe, Qe-Packets représente le module d'accès aux trames réseau dans les échanges nécessitant une investigation avancée par analyse de la trame des paquets impliqués dans les flux sur lesquels une analyse en profondeur apparaît nécessaire.

Qe

Cette approche combinée avec les indicateurs mis en évidence par Qe-Streams permet d'obtenir facilement le détail sur les transactions en cause d'une problématique donnée. Avec un *workflow* inédit, les échanges identifiés sur Qe-Streams peuvent donc facilement être accédés sur Qe-Packets pour en extraire les trames réseau échangées et ainsi d'obtenir le détail d'informations des échanges jusque là indisponibles par ailleurs sur les solutions standard analytiques.
Positionnée en des points de concentration stratégiques, l'appliance Qe-Packets autorise l'analyse de champs spécifiques disponibles dans les trames.

Intégration dans les baies mobiles InceptRack®

Qe-Packets répond à des problématiques de capture massive. Aussi, la solution participe à l'objectif global des baies InceptRack®. Intégrée aux baies, Qe-Packets fournit aux utilisateurs de ces systèmes toutes les fonctionnalités attendues par les experts dédiés à la recopie des flux sur les réseaux IP à des fins de traitement dédié des données. Avec InceptRack®, synthèse de l'ensemble des métiers d'allentis dans les architectures de recopie des flux et d'analyse des données à destination des grandes organisations, Qe-Packets complète le système pour délivrer des solutions intégrées prêtes au traitement de tous les sujets liés à la capture et l'analyse des échanges rencontrées sur les réseaux

Illustration : Baie InceptRack® intégrant Qe-Packets

Pour des besoins dans des environnements à fortes contraintes environnementales, Qe- Packets existe en version durcie permettant son intégration dans des baies destinées à des applications plus spécifiques comme notamment par exemple dans le cadre d'applications militaires.

Les baies InceptRack® sont mobiles pour déplacement sur des points de concentration nécessitant, dans le cas de celles embarquant Qe- Packets, une capture massive des données pour des applications spécifiques dans le domaine de la surveillance des flux réseau.

Gamme et références

QEPACK-10-96	Appliance Qe-Packets de capture massive, châssis long 2U, acquisition de données 1 x 10 GbE full duplex, capacité de stockage 96 To en cluster
QEPACK-10-40	Appliance Qe-Packets de capture massive, châssis long 2U, acquisition de données 1 x 10 GbE, capacité de stockage 40 To
QEPACK-10-20	Appliance Qe-Packets de capture massive, châssis long 2U, acquisition de données 1 x 10 GbE, capacité de stockage 20 To
QEPACK-4-20-M	Appliance Qe-Packets de capture massive, châssis court 1 U, acquisition de données 4 x 1 GbE, capacité de stockage 20 To. Equipement durci.

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