

Qe-Packets

Appliance de capture massive des flux IP échangés sur les réseaux

Capture massive des flux échangés Analyse Forensic et accès au détail des communications échangées sur les réseaux

Objectif

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.



Qe-Packets version Rack 1U châssis court 20 To

Capacités d'analyse

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.

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.

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.

Votre réseau, plus performant
et plus **sûr** au quotidien

Intégration dans les baies mobiles CyberPack®

Qe-Packets répond à des problématiques de capture massive. Aussi, la solution participe à l'objectif global des baies Cyberpack®. Intégré 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. Dans l'offre Cyberpack®, 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



Baie Cyberpack® intégrant Qe-Packets

représente la brique intégrée pour le traitement de tous les sujets liés à la capture et l'analyse des échanges rencontrés sur les réseaux.

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 Cyberpack® 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.

The screenshot shows the Qe-Packets web interface. At the top, there are status indicators for Total, Free, and Used memory. Below that, there are configuration fields for Interface (set to em3), Protocol (set to Any), Source IP, Destination IP, Source port, Destination port, Max. capture size (100 Mbytes), and PCAP file size (1 Mbytes). A 'TestIS' button shows 43,732 Mb of data. A 'Stop' button is also visible. Below the configuration, a table lists captured files in the folder /opt/pfdumpd/logs/Test, with a total size of 17.36Mb. The table includes columns for filename, size, and timestamp.

Folder: /opt/pfdumpd/logs/Test	Total size: 17.36Mb	
Test0000.pcap	0.95 Mb	2020-03-06 16:07:45
Test0001.pcap	0.96 Mb	2020-03-06 16:07:46
Test0002.pcap	0.95 Mb	2020-03-06 16:07:46
Test0003.pcap	0.95 Mb	2020-03-06 16:07:47
Test0004.pcap	0.95 Mb	2020-03-06 16:07:47
Test0005.pcap	0.95 Mb	2020-03-06 16:07:48
Test0006.pcap	0.95 Mb	2020-03-06 16:07:49
Test0007.pcap	0.95 Mb	2020-03-06 16:07:49
Test0008.pcap	0.95 Mb	2020-03-06 16:07:50
Test0009.pcap	0.95 Mb	2020-03-06 16:07:50
Test0010.pcap	0.96 Mb	2020-03-06 16:07:51

Accès aux fichiers de stockage de l'intégralité du trafic par Qe-Packets

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.
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

Contact : info@allentis.eu
www.allentis.eu

© 2025 allentis sas. allentis, le logo allentis, TAPICS, le logo TAPICS, vTAPICS, dTAPICS, Cyberpack, QE, Qe-Secure, Qe-Streams, Qe-Flows, Qe-Packets, Qe-MIND sont des marques déposées d'allentis. Les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.

allentis