



Solution de Capture de Trafic pour la Supervision des Réseaux et la Sécurité

VSS Monitoring est le leader de l'innovation en technologies de capture de trafic réseau, ainsi que l'inventeur des Systèmes de Capture de Trafic Distribué, offrant la solution la plus sophistiquée, la plus riche en capacités, et proposant la seule véritable approche de tolérance aux pannes.

Le portfolio VSS Monitoring est constitué d'une gamme complète d'équipements de capture de trafic, permettant de répondre à tous les besoins sur n'importe quel réseau, simple ou complexe.

Tous les équipements de capture de trafic VSS sont des solutions hardware et passives sur le réseau, ce qui garantit une utilisation transparente, une capture en temps-réel, une disponibilité totale.

La flexibilité et l'exhaustivité du portfolio VSS garantissent une visibilité maximale, une plus grande efficacité et un ROI rapide de l'infrastructure de supervision.

Chaque équipement VSS dispose d'une double alimentation AC ou DC, en standard.

Solution Propriétaire d'Accès Passif pour le Cuivre Gigabit

vAssure™ est la technologie propriétaire de VSS pour la capture en ligne des liens cuivre Gigabit. En cas de défaillance ou de redémarrage du TAP, cette solution garantit le basculement en moins de 100ms de l'état de capture en coupure à l'état de connexion directe du lien Gigabit (typiquement 30-60ms). Cette solution unique est indispensable pour la capture sur des réseaux sensibles aux pannes. Sans le vAssure, le temps normal de rétablissement du lien (en mode d'auto-négociation standard) se situe entre 1 et 3 secondes, où toutes coupures dépassant les 150ms causeraient une perte du lien.

Taps Distribués

Les Taps distribués sont des équipements de captures intelligents, basés sur une architecture hardware, et conçus pour capturer les réseaux en ligne ou en SPAN, tout en redirigeant le trafic dupliqué vers les équipements de supervision. Ces équipements disposent de l'agrégation sélective, du filtrage, du load balancing "session-aware", d'une administration à distance, d'une solution de stackage intelligente avec le vStack+ et d'une flexibilité de configuration inégalable.

Les Taps distribués sont des outils de bases nécessaires pour créer une visibilité totale sur l'ensemble du réseau pour la supervision et la sécurité. En utilisant ces outils comme une composante du Système de Capture de Trafic Distribué, on apporte aux utilisateurs une vue centralisée de leur réseau, mais aussi un contrôle des paquets reçus par chaque équipements de supervision.

Interconnecter les Taps distribués dans une topologie en maille, permet de créer une couche réseau intelligente dédiée à la capture de trafic. Cette approche offre une solution de redondance sans équivalent, une latence faible, et une structure dynamique pour la supervision et l'infrastructure de sécurité, donnant aux utilisateurs un contrôle pro-actif et réduisant les délais d'intervention et les risques d'incidents de sécurité.

Les Taps distribués sont disponibles dans une large gamme de nombre de ports et débits supportés.

Agrégation sélective

Chaque port de supervision a un accès indépendant à l'ensemble des ports d'entrées réseaux. L'utilisateur peut donc sélectionner les ports d'entrée qui seront dirigés vers un port de supervision spécifique.

L'agrégation en bloc, où chaque port d'entrée réseau est dirigé vers chaque sortie de monitoring, peut potentiellement créer une surcharge du côté de la supervision. L'agrégation sélective permet d'éviter ce problème, permettant aux utilisateurs de sélectionner les ports d'entrée à aiguiller vers les ports de monitoring. Cette sélection peut être définie de manière dynamique par l'utilisateur, par le biais d'une interface utilisateur graphique intuitive.

Filtrage Hardware en Temps Réel

Le Filtrage permet à l'utilisateur de déterminer le type de trafic qui sera copié depuis les ports réseaux vers les ports de supervision, en se basant sur des paramètres propres aux couches 2 à 7 du modèle OSI. Le filtrage dans les Taps distribués est accompli intégralement par des composants Hardware (pas de microprocesseur), ce qui permet la réalisation d'un filtrage en temps-réel avant même que le trafic ne soit reçu par les outils de supervision. En aiguillant uniquement le trafic utile, le filtrage pré-analytique améliore l'efficacité et le ROI des outils de monitoring en les spécialisant.

Load Balancing Session-Aware

Le Load Balancing permet aux utilisateurs de répartir le trafic d'entrée vers de plusieurs ports de supervision, en additionnant efficacement la bande passante des ports Load Balanced.

Le Load Balancing Session-Aware répartit le trafic de manière à conserver l'intégrité des conversations. Il est possible de définir jusqu'à huit ports de supervisons pour un simple flux logique, avec une répartition automatique du trafic sur les ports suivant les critères de session définis par l'utilisateur. De plus, chaque perte de connexion est détectée par le Tap et le trafic est automatiquement transféré sur les ports restants.

Les utilisateurs peuvent configurer un port Load Balanced en se basant sur une combinaison de critères de sélections pour l'identification des sessions:

- adresse MAC de destination, Type d'Ethernet (EType) et numéro de port réseau
- adresse MAC de la source, Type d'Ethernet et numéro de port réseau
- adresses MAC de la source et destination, Type d'Ethernet et numéro de port réseau
- adresse IP de destination, et numéro de port TCP/UDP de destination
- adresse IP de la source, et numéro de port TCP/UDP de la source
- adresse IP de la source et destination, et numéro de port TCP/UDP de la source et destination

Le Load Balancing peut notamment permettre une supervision de liens à débits hybrides. Par exemple, des liens 10GigE peuvent être monitorés par des Outils 1G, avec une charge du trafic automatiquement distribuée sur un plusieurs ports de supervision 1G.

Administration

L'administration à distance des Taps distribués peut-être réalisée en utilisant le GUI ou les CLI. Les Taps distribués disposent des fonctions SNMP et RMON, incluant des triggers, des alertes et une identification pour des scenarii multiples.

- Autorisation, Authentification, Comptes
- Architecture d'Administration Distribuée

En utilisant le vStack+, l'ensemble des équipements interconnectés, peut être piloté à distance depuis n'importe quel unité, offrant ainsi une administration partagée.

Technologie vStack+

Le vStack+ est une technologie de connectivité intelligente qui apporte à la capture de trafic réseau, la virtualisation, la tolérance aux pannes et une latence minimale. La virtualisation permet une supervision d'une flexibilité exceptionnelle, capable de s'adapter rapidement aux évolutions des besoins internes. Le vStack+ crée une couche virtuelle de capture de trafic qui détecte et redirige le trafic aux autres équipements de capture et/ou aux outils de monitoring en utilisant le chemin le plus rapide. Le système vStack+ aiguille automatiquement le trafic vers le routage optimal. Les taps des autres fabricants sont uniquement configurables en daisy chain ou sont alors stackés en configuration point à point, ce qui représente des connexions en série introduisant des points de défaillance: si un tap est défaillant, toute une partie du système de capture est défaillante.

- Interconnexion en maille pour une tolérance aux pannes maximale
- Faible latence avec optimisation du routage automatique
- Équilibrage de charge par session
- Bande passante de 240 Gigabits par unité

Taps traditionnels

Les Taps traditionnels sont entièrement passifs pour la capture en ligne ou en port SPAN. De manière générale, ils sont limités en nombre de ports, avec des options de gestion de trafic limitées et une administration locale. Les Taps traditionnels sont idéaux pour de petits déploiements ou pour de la capture en ligne dans le cas de haute densité de ports, d'agrégation ou de filtrage.

Taps Distribués

VSS se démarque dans cette catégorie avec la technologie vAssure, garantissant un accès passif sur les réseaux, même pour des liens cuivre Gigabit.

Capture Full-Duplex

Capture en ligne entièrement passive en temps réel. Conçus pour être placé entre deux équipements réseaux, chaque côté du réseau (A et B)

est capturé et dirigé vers deux ports de supervision sans agrégation ou réplication.

Agrégation

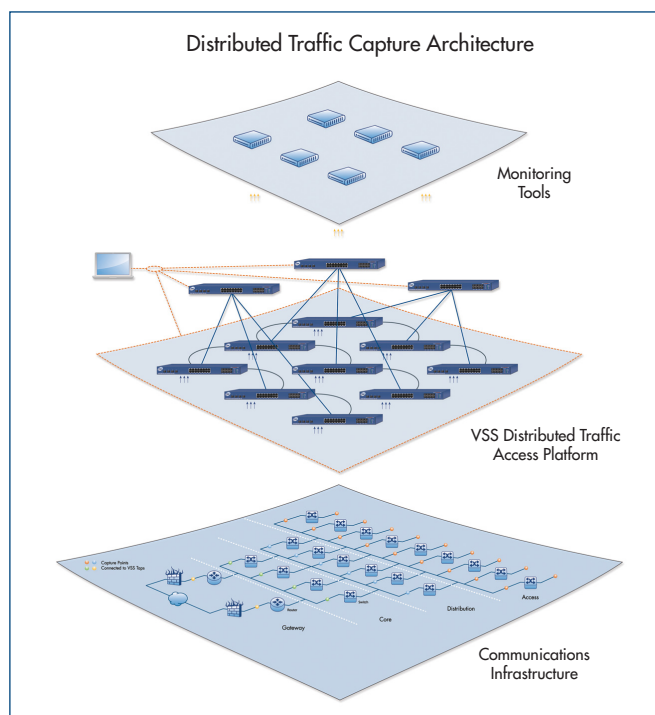
Agrégation des deux côtés du réseau ou de plusieurs réseaux vers un outil de monitoring. L'agrégation réduit le nombre de ports nécessaires sur les équipements de supervision.

Réplication

Réplication du trafic d'entrée vers plusieurs outils de monitoring. La réplication permet à plusieurs équipements de supervision de partager l'accès d'un même lien Inline ou SPAN.

Architecture des Systèmes

En déployant les TAPs traditionnels et distribués VSS Monitoring dans une architecture centralisée et tolérante aux pannes, les utilisateurs peuvent créer une visibilité totale, une supervision plus efficace avec un meilleur ROI, et anticiper les chutes de performances et les risques d'incidents de sécurité.



Network Visibility. Optimized.

USA
 (Corporate HQ)
 + 1 650 697 8770 phone
 + 1 650 697 8779 fax
 1850 Gateway Drive - Suite 500
 San Mateo, CA 94404
 USA
www.vssmonitoring.com

Japan
 + 81 422 26-8831 phone
 + 81 422 26-8832 fax
 T's Loft 3F, 1-1-9,
 Nishikubo, Musashino,
 Tokyo, 180-0013
 Japan
www.vssmonitoring.co.jp

China
 + 86 10 6563-7771 phone
 + 86 10 6563-7775 fax
 C519, 5 Floor,
 CBD International Tower
 16 Yong'An Dong Li,
 Beijing, China 100022
www.vssmonitoring.com.cn

VSS Monitoring, Inc. is the world's leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.

VSS, Distributed Traffic Capture System, vAssure, LinkSafe, and vStack+ are trademarks or registered trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.