ReactivOn
ANALYSE DES RÉSEAUX INFORMATIQUES

Sniffer portatif de collecte et de classification des flux
pour 250 postes utilisateurs

Points forts

- **Identification instantanée du «qui, comment, où»**
- **Suivi de l'usage de chaque application métier**
- **Cartographie flux par flux du global au détaillé**
- **Reporting en temps réel via un outil industriel**
- **Format ultra-portable pour collecte ponctuelle**
- **Seulement 560€ en location ou audit sur un mois**

L'analyseur RB35 est un outil de métrologie réseau très économique, à l'ergonomie accessible. Il permet d'automatiser le suivi (reporting) des communications sur tout ou partie de l'infrastructure. C'est une solution technique de pilotage de la sécurité du SI et de ses risques.

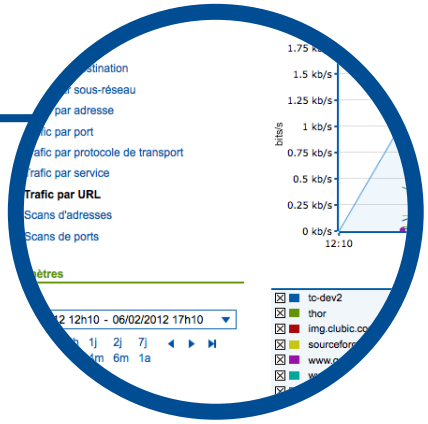
Au quotidien, cette sonde organise les flux ayant transité pour informer tel une base de données sur les usages incohérents, voire malveillants. La plateforme ReactivOn simplifie la réponse aux usagers sur la qualité ressentie en ciblant les comportements pour lesquels une réactivité est nécessaire pour éviter une **contre-performance**.

Objectif : **détecter immédiatement l'origine d'une panne !**

RB35

pour un agrégat réseau de taille modérée (35 Mbps) souvent à destination de :

- **Collectivité, C.H. & PME**
- **Filiale / agence (site distant)**



1 Limiter l'influence des pannes et des incertitudes sur le budget SI

- **Aider la prise de décision** pour retarder les investissements non prioritaires
- **Accompagner l'équipe réseau** lors du déploiement de nouveaux services
- **Anticiper les dysfonctionnements** en déterminant la périodicité des pannes

2 Garantir une réelle disponibilité de chaque accès réseau sensible

- **Etre averti au plus tôt des congestions** et anticiper l'usage de chaque segment
- **Améliorer l'efficacité de l'équipe** en charge de la résolution des «down-time»
- **Offrir une assistance réactive et ciblée** pour la satisfaction de chaque utilisateur

3 Mesurer l'audience de chaque applicatif et prévenir les lenteurs

- **Identifier les anomalies de sécurité** pour garder le contrôle total du réseau
- **Justifier les besoins réseau** en termes économiques avec un vrai suivi applicatif
- **Evaluer l'impact des applications** dans un environnement sensible et règlementé

Recommandé pour une liaison vers :

- **Internet pour surveiller les applications métiers ayant un accès au réseau « tout-public »**
- **WAN pour quantifier les trafics entre le site principal et les établissements distants**
- **LAN pour suivre pas à pas les communications transitées entre un serveur et ses usagers**

*« En tant que filiale d'un groupe international, les **indicateurs réseau** mis à notre disposition sont pertinents pour guider notre prise de décision dans les projets qui se révèlent les plus prioritaires »*

Bourbon Offshore Greenmare (100 utilisateurs, 90 IP, liens SDSL 2x4 Mbps)

Fonctionnalités et caractéristiques techniques

Cartographie du trafic réseau par tableau de bord automatisé

- Remontée d'indicateurs par usage (bande passante, top-talkers, volume, botnets, ...)
- Matrice des échanges inter-zones (ex : site A vers site B, serveur web vers base sql)
- Etude des services réseau (IP+port) et de l'évolution des usages par période
- Suivi en temps réel des dégradations de qualité (granularité : 120 secondes)
- Accès permanent à un historique consolidé des traces, de quelques minutes à 1 an

Analyse approfondie des paquets et de leur comportement

- Suivi des racines URL consultées (TOP10 et pour chaque flux HTTP)
- Envoi d'alerte sur franchissement de seuil pour 17 métriques : point haut / bas, délai avant alarme, criticité du seuil et graphe du trafic passé pour un positionnement

Archivage des communications flux par flux

- Parcours des flux à la demande (pré et post-filtrage par IP, VLAN, port, protocole, URL, zone connue ou avec un caractère générique tel que mail.google.*)
- Mise en mémoire de chaque rapport pour un partage rapide entre DSI et prestataires
- Capture PCAP instantanée ou programmable par calendrier avec pré-filtrage BPF, gestion de périodicité (tous les vendredis à partir de 17h) et archivage

Configuration et administration exhaustive

- Gestion du plan d'adressage et des zones dynamiques rattachées
- Paramétrage des ports spécifiques et droits utilisateur par annuaire LDAP ou AD
- Résolution DNS à la volée, synchronisation NTP et gestion SMTP intégrées
- Mise à jour logicielle par simple patch (et gestionnaire de licence)

Bénéfices du format industriel

Outil d'analyse «clé en main»

- Pré-installé pour un déploiement facilité sans opération coûteuse de mise en place
- Sonde dimensionnée pour une mise en production rapide et sans contre-temps

Base de connaissances centralisée

- Tous les indicateurs de l'activité du réseau à portée de main de toute l'équipe IP sur une interface unique de consultation
- Scrutation dès la couche 2 du modèle OSI jusqu'aux entêtes applicatives
- Temps de formation réduit (un seul outil)

Spécifications matérielles

- 1 port de capture Fast-E RJ45 full-duplex
- Rétention des données : 12 mois glissant
- Nombre de sous-réseaux : illimité
- Zone actives simultanément : Max. 10
- Stockage PCAP 300 Go, AC/DC externe
- Format portatif : 21x19,2x6 cm 2,5L 5 Kg

Solution idéale pour les liens WAN / VPN

- Analyse réseau recommandée jusqu'à 250 IP locales
- Fiabilité garantie jusqu'à 9 500 flux par minute
- Débit réel moyen et Burst max. : 35 et 100 Mbps
- Collecte des paquets possible en tout point du réseau
- Des dizaines de métriques automatiquement calculées et consolidées quelque soit la période de visualisation et le périmètre technique souhaité (Cf. zones virtuelles)

Simplicité de déploiement et d'exploitation

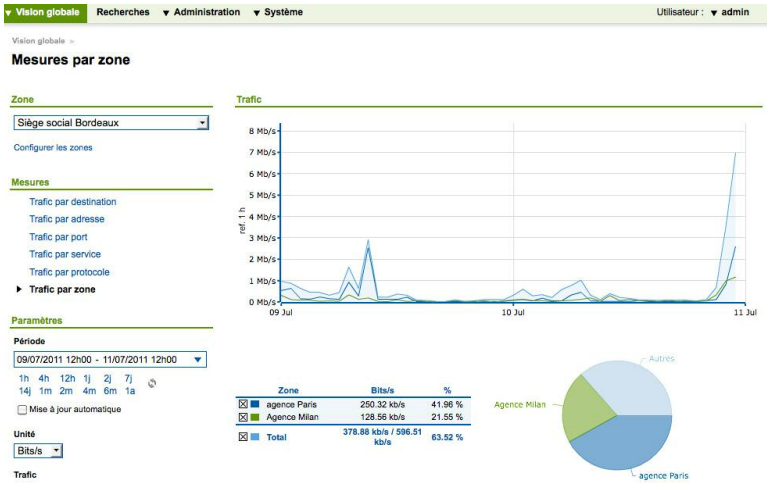
- Plateforme opérationnelle en seulement 15 minutes
- Interface GUI web-isée (via LAN ou accès distant)
- Dépannage à distance (client VPN intégré)

Intégration sans coupure non-intrusive

- Pas de génération de trafic supplémentaire (SPAN)
- Sans impact sur l'infrastructure existante
- Synchronisation sans délai additionnel (milliseconde)
- Haute disponibilité Failover (reprise après incident)

Adaptable à votre réseau et à vos besoins

- Vision par filiale / service / bureau / sous réseau
- Fonctionnalités modulables par achat de licence



Options disponibles

- Malette d'intervention + convertisseur fibre
- Générateur de rapports automatiques
- Suivi des temps de réponse (L7)
- Mise en fédération (slave probe)

Pour en savoir plus

- **Démonstration en ligne**
- **Documentations techniques**
- **Call / Visio conf. individualisée**

Meilleure est la visibilité, meilleure est l'anticipation et la résolution des menaces. Testez notre plateforme sur demo.reactivon.com

ReactivOn

Siège social Bordeaux, France
Standard tél. +33 (0)5 56 17 41 25

CONTACT@REACTIVON.COM

ReactivOn développe en France des solutions matérielles dédiées à la surveillance avancée des réseaux informatiques. Conçue initialement pour les grandes entreprises, cette technologie répond à une large palette de besoins tels que la lutte contre les attaques, l'optimisation des services IT, la refacturation, la rétention de données ou la reproduction de symptômes réseau.

Société par Actions Simplifiée au capital social de 95 000 Euros
RCS Bordeaux 512 398 744 ▪ TVA FR 93512398744

v2.1 - 20130313