

# Transformer ses opérations réseau avec des données de flux enrichies



# Résumé analytique

La transformation numérique des entreprises à travers le monde a entraîné une connectivité omniprésente, des échanges de données à grande vitesse, ainsi qu'une croissance massive de la productivité. L'infrastructure réseau joue un rôle tellement fondamental qu'il est absolument vital pour chaque entreprise d'aujourd'hui de garantir sa fiabilité et sa sécurité.

Pourtant, les réseaux sont devenus de plus en plus abstraits, et même appréhendés au travers de métaphores du type « Cloud public ». Dès lors, nous ne pensons même plus en termes de commutateurs ou de routeurs, et encore moins à la manière de les configurer manuellement. Les fournisseurs d'équipements réseau rendent la mise en réseau plus transparente et, par conséquent, l'expertise des ingénieurs réseau évolue lentement. Ces derniers sont désormais capables de gérer la sécurisation d'un réseau avec des dizaines de milliers d'appareils IoT. Le SDN, le NFV et la virtualisation vont de pair avec cette tendance - permettant aux entreprises de concentrer leurs ressources sur le cœur de métier plutôt que sur la gestion du réseau. Cela conduit à une explosion de la bande passante au sein des réseaux d'entreprise, ce qui rend les approches traditionnelles de surveillance réseau primitives. Chez Progress, nous repensons les anciens concepts et nous nous efforçons d'abattre les murs qui freinent le progrès.

Ce livre blanc est le fruit de notre conviction selon laquelle la fusion de la visibilité au niveau du flux et du paquet sous forme d'une solution polyvalente constitue la technologie qui vous aidera à vous adapter aux besoins émergents en matière de performance et de capacité. Notre solution conserve également des informations détaillées sur le trafic réseau et présente les résultats de manière simple et compréhensible. Vous êtes sur le point de découvrir comment les données de flux, souvent perçues comme un outil de facturation et de statistiques de pointe, peuvent, lorsqu'elles sont maîtrisées, remplacer totalement la capture et l'analyse de paquets et fournir une évolutivité inédite et tournée vers l'avenir.

## L'histoire de la surveillance réseau : L'analyse de paquets

L'analyse de paquets se penche sur les communications pour en analyser le contenu. Il n'y a pas d'agrégation, de compression ou de découpe, les données sont stockées dans leur taille d'origine. Par conséquent, cette méthode est extrêmement exigeante en termes de performances et de capacité de disque.

Imaginez la capture d'un réseau avec un trafic moyen de 250 Mbit/s. Cela équivaut à une charge de données de plus de 31 Mo par seconde, 1,8 Go par minute, 108 Go par heure et 2,6 To par jour. Dans le cas de réseaux à 10 Gbps, nous atteignons des chiffres à peine croyables - plus de 100 To de données stockées par jour.

Cependant, les grands volumes de données ne sont pas le seul inconvénient. La principale limite de l'analyse de paquets est le trafic crypté. Sans la clé de chiffrement, nous ne pouvons pas comprendre le contenu des données transférées, et souvent nous ne pouvons même pas découvrir le protocole de transfert ou l'application. Néanmoins, les volumes de trafic crypté ne cessent de croître.

L'enregistrement continu et à grande échelle du trafic (full packet capture) nécessite l'équipement technique adéquat, en particulier des baies de stockage à grande vitesse dotées d'une capacité suffisante. Une telle approche de la surveillance réseau est très coûteuse et ne convient qu'aux infrastructures essentielles et aux réseaux ayant une finalité spécifique. Il faut souligner que le stockage de ces données n'est pas le seul problème. Une fois les données stockées, tout dépannage implique une extraction intensive d'informations qui nécessite une expérience et des compétences considérables. Pour la majorité des incidents réseau qui sortent du cadre de la capture continue et coûteuse de l'ensemble des paquets, les entreprises s'appuient sur une autre approche. Il s'agit de la capture de paquets à la demande. Cette approche consiste à capturer des paquets uniquement lorsque cela est nécessaire, généralement lorsque nous traitons des problèmes de compatibilité du système, par exemple lorsque nous découvrons des paquets manquants ou endommagés. La capture de paquets à la demande est une méthode simple, à la portée de tout administrateur réseau, mais elle a ses avantages et ses inconvénients. La limite de cette approche réside dans le fait que l'administrateur doit décider à l'avance quel trafic doit être stocké. Par conséquent, il n'est pas possible d'accéder aux archives du trafic pour obtenir les informations nécessaires à l'analyse en cas d'incident. L'administrateur réseau doit se rendre sur place (par exemple, dans une salle de serveurs) avec son ordinateur portable, le connecter à un port miroir ou à un TAP et procéder à l'enregistrement du trafic réseau. Des problèmes peuvent se poser lorsque l'emplacement est éloigné, ainsi que pour les interfaces de réseau optique et les infrastructures 10Gbps - des limitations qui peuvent difficilement être surmontées à l'aide d'un ordinateur portable.

Bien que la nécessité de capturer des paquets ne soit pas révolue, la demande, elle, est certainement en train de décroître. Il existe un problème évident d'évolutivité, notamment en raison du nombre croissant d'appareils connectés à un réseau ou du nombre d'applications et de services fournis à partir de l'informatique dématérialisée qui nécessitent des largeurs de bande plus importantes. Les solutions d'enregistrement et d'analyse du trafic à grande échelle sont très gourmandes en ressources et, par conséquent, coûteuses. En outre, il existe des limites technologiques dans un environnement de réseau à grande vitesse et des possibilités d'utilisation restreintes lorsque le trafic est crypté.



# L'avenir de la surveillance réseau : Des données de flux enrichies

Lorsqu'il s'agit de surveiller le trafic réseau, de dépanner ou de détecter des menaces, les ingénieurs réseau pensent rarement qu'ils ont deux options à leur disposition. La première est la capture et l'analyse complètes des paquets, lesquels permettent une visibilité totale du réseau. L'autre option est celle des données de flux.

**Les données de flux** constituent une abstraction du trafic réseau lui-même. Les statistiques de flux sont créées en tant qu'agrégation du trafic réseau, en utilisant l'adresse IP source, l'adresse IP de destination, le port source, le port de destination et le numéro de protocole comme attributs permettant d'identifier les enregistrements de flux individuels. Le contenu de la communication n'est pas stocké et le taux d'agrégation réalisable est d'environ 500 : 1. Avec les informations énumérées ci-dessus, nous sommes en mesure d'analyser la structure du trafic, d'identifier les stations finales qui transfèrent de grandes quantités de données ou de résoudre les problèmes de réseau et les mauvaises configurations. En d'autres termes, nous pouvons traiter 80 % des incidents de réseau, comme l'indique Gartner depuis 2013.

Il est évident que les données de flux ne contiennent pas suffisamment d'informations pour certaines tâches. En revanche, à la suite de l'analyse des paquets, le service informatique est généralement surchargé par des volumes de données détaillées à peine gérables. Lorsque nous combinons les deux perspectives et que nous ajoutons aux données de flux traditionnelles des informations provenant de la couche d'application, nous pouvons obtenir les détails appropriés, ce qui permet de mieux comprendre la communication des données, d'établir des rapports flexibles et de résoudre efficacement les problèmes opérationnels, ainsi que de détecter automatiquement les incidents de sécurité. Cette approche est appelée « données de flux enrichies » et tire parti de la flexibilité du **protocole IPFIX**. D'après notre expérience, nous sommes désormais en mesure de traiter 95 % des incidents de réseau grâce à la solution la plus évolutive, la plus rentable et la plus facile à utiliser, basée sur les données de flux.

La mise en œuvre la plus connue de cette technologie est la technologie NBAR2 (*Next Generation Network-Based Application Recognition*) de Cisco. La surveillance des données de flux est combinée à une analyse continue des paquets qui complète les statistiques de trafic par le nom d'une application ou d'un protocole d'application. Sur la base de ces informations, les **collecteurs de flux** contemporains permettent d'établir des rapports sur le trafic et de l'analyser.

L'un des protocoles de communication les plus répandus est le protocole HTTP, ou sa version cryptée HTTPS. Aujourd'hui, ce protocole est utilisé pour fournir un accès aux sites web, mais ce n'est pas sa seule fonction. Le protocole HTTP est également à la base de la communication entre les composants des systèmes d'entreprise, ou des applications travaillant avec des données sensibles (par exemple, la banque électronique). En identifiant ce protocole de transfert, nous pouvons étendre les statistiques de flux de données par des attributs fondamentaux des requêtes HTTP - un nom d'hôte ou des informations sur l'URL. Grâce à SNI (Server Name Indication), nous pouvons obtenir des informations sur le nom d'hôte même lorsque le protocole HTTPS est utilisé. De même, nous pouvons obtenir d'autres informations

à partir de la communication HTTP, par exemple le système d'exploitation et sa version, l'identification d'un navigateur et sa version ou un type d'appareil dans le cas des téléphones mobiles. Et ce n'est là qu'un exemple des nombreux protocoles pour lesquels nous pouvons utiliser les informations L7 sans devoir procéder à une exploration manuelle des données.

Néanmoins, les données de flux peuvent être enrichies par ce qui est peut-être encore plus puissant dans notre monde contemporain : la surveillance des performances réseau (*Network Performance Monitoring - NPM*). Les mesures NPM peuvent aider considérablement à résoudre les problèmes de performance du réseau. En utilisant les mesures Server-Response-Time et Round-Trip-Time, il est possible de distinguer les retards dans l'infrastructure réseau (par exemple, un point d'accès défectueux) des retards dans le serveur (par exemple, des ressources matérielles insuffisantes). Ce type d'information est crucial pour un dépannage rapide du réseau. Les mesures de délai et de gigue nous intéressent particulièrement lorsque nous utilisons des appels VoIP ou des vidéoconférences, car elles peuvent indiquer une mauvaise qualité audio et vidéo. Lorsqu'il s'agit de transférer de gros volumes de données, nous nous intéressons principalement au nombre de retransmissions TCP, qui peuvent indiquer des problèmes au niveau de la couche physique (par exemple, des interférences, un port défectueux) et un débit binaire plus faible, ou des paquets désordonnés, qui peuvent signaler des défaillances dans les liaisons de communication.

Et lorsque ce niveau d'information est encore insuffisant, **Flowmon** permet de déclencher une capture complète de paquets à la demande. Cette opération peut être effectuée manuellement ou automatiquement lors de la détection d'un événement. Dans ce cas, le filtre de capture est déterminé de manière autonome par le système, réduisant le volume de données capturées à un minimum absolu, en ne conservant que la partie pertinente du trafic. Cette opération peut évidemment être effectuée à distance dans n'importe quelle partie du réseau et à des vitesses de 100 Gbps, ce qui est impossible à réaliser avec Wireshark ou WinPCAP.

Les avantages de la **surveillance des données de flux** et de l'analyse de la couche d'application sont évidents. Les informations sur la communication des données sont plus détaillées et les capacités d'analyse du trafic sont meilleures. En même temps, nous conservons l'excellent taux de compression des statistiques du trafic réseau par rapport au volume de trafic d'origine afin de nous adapter à des réseaux de plusieurs centaines de gigabits. En outre, le système regroupe les informations les plus importantes, de sorte qu'elles peuvent être fournies en un coup d'œil, évitant ainsi la nécessité d'une exploration manuelle des données par l'analyse des paquets. Cela permet de réduire considérablement le temps moyen de résolution tout en diminuant les compétences nécessaires à l'utilisation de la solution. Avec Flowmon, il est toujours possible d'effectuer un enregistrement du trafic à grande échelle si nécessaire, en utilisant la même plateforme.

**Flowmon permet également de déclencher une capture complète de paquets à la demande en cas de besoin. Le filtre de capture est déterminé de manière autonome par le système, réduisant le volume de données capturées à un minimum absolu, ne conservant que la partie pertinente du trafic.**

# Pourquoi préférer le flux au paquet ?

## Avantages commerciaux et techniques.

Dans la première partie de ce livre blanc, nous avons identifié les différences entre la capture de paquets en continu et les données de flux dans le contexte de l'utilisation de ces technologies pour surveiller avec succès le trafic réseau. Résumons les avantages des données de flux enrichies par rapport à la capture de paquets :

- ▶ Les exigences budgétaires des technologies d'analyse de paquets permettent rarement de surveiller l'ensemble du trafic réseau. Elles ne sont donc déployées que pour surveiller les systèmes les plus importants, contrairement aux flux, pour lesquels la couverture de l'ensemble du trafic réseau de l'entreprise, y compris les centres de données et l'informatique dématérialisée, constitue un schéma standard.
- ▶ En général, **le dépannage** n'est pas effectué en temps réel. Dans les entreprises, il faut souvent des jours pour qu'un incident signalé soit examiné par un administrateur réseau. Avec une période de conservation des données limitée, l'analyse rétrospective est impossible. La surveillance des flux peut facilement permettre de conserver des données pendant des semaines ou des mois, ce qui permet de hiérarchiser les priorités et de se concentrer sur l'analyse rétrospective lorsque des tâches plus importantes ont été accomplies.
- ▶ Le déploiement transparent, l'intégration avec les équipements de réseau existants, la compatibilité avec une large gamme de sources de flux, la formation rapide des administrateurs sont autant de raisons pour lesquelles il est si facile d'introduire une technologie de flux dans votre réseau et d'en tirer un bénéfice immédiat.
- ▶ Le niveau de détail fourni par l'analyse de paquets permet d'effectuer une analyse forensique approfondie des problèmes persistants. Les entreprises se tournent vers Flowmon pour minimiser le temps nécessaire à l'analyse des causes profondes et gagner du temps pour y remédier grâce à des tableaux de bord lisibles par l'homme, des présentations contextuelles et des capacités d'analyse approfondie.
- ▶ Une granularité trop détaillée de l'analyse de paquets se traduit par des coûts plus élevés, une évolutivité moindre et un ensemble de compétences requises beaucoup plus important. Cependant, seul un petit pourcentage des données capturées est pertinent. Les données de flux enrichies, en revanche, ne conservent que les informations les plus intéressantes et les plus importantes, de sorte qu'elles permettent de résoudre 95 % des incidents de réseau. En outre, Flowmon permet la capture complète de paquets à la demande pour les autres cas.
- ▶ L'analyse de paquets a été conçue dans l'optique d'une visibilité illimitée. Elle est bien adaptée à l'analyse des problèmes persistants, lesquels exigent beaucoup de temps. Pour rétablir rapidement le cours normal des affaires, les entreprises se tournent vers Flowmon qui leur fournit des workflows analytiques et une automatisation permettant de rationaliser la résolution des problèmes.
- ▶ Le trafic étant de plus en plus crypté, l'analyse des paquets devient inutile. Tout en exportant des données de flux à partir du trafic crypté, Flowmon se concentre sur les en-têtes IP non cryptés qui aideront à résoudre 80 % des incidents. En outre, Flowmon recourt à différentes techniques pour extraire des informations de la couche d'application qui seraient autrement invisibles à un œil inexpérimenté.
- ▶ Les fournisseurs de clouds publics n'autorisent pas l'accès à leur réseau pour permettre une analyse complète des paquets. Cependant, les fournisseurs de cloud et les hyperviseurs virtuels exportent souvent des données de flux compatibles avec Flowmon, ce qui permet de déployer de manière transparente une surveillance de qualité du réseau.



# Cas d'usage

## Dépannage à l'aide de la capture de paquets

J'ai mis en place mon analyseur de paquets avec capture continue. Espérons donc que mon tampon roulant conserve les données dont j'ai besoin. Heureusement, nous pouvons télécharger le PCAP contenant le trafic de l'adresse IP 193.29.206.1 et ouvrir le trafic sous Wireshark.

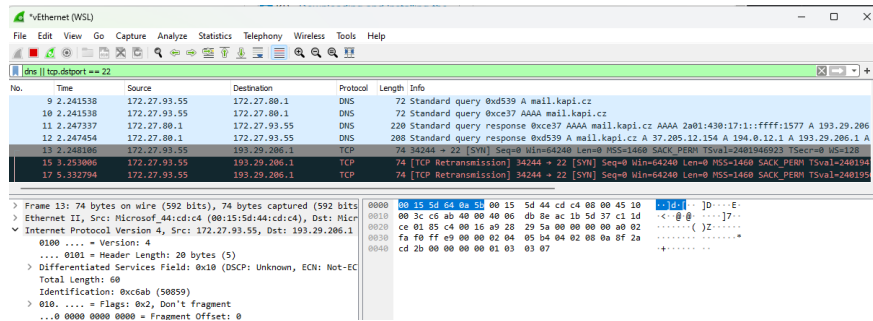


Figure 1: Analyse du trafic réseau capturé par Wireshark.

La figure ci-dessus montre la communication entre l'utilisateur et mail.kapi.cz. Le domaine mail.kapi.cz est correctement résolu à l'adresse IP 193.29.206.1, mais après réception de la réponse DNS, un utilisateur a tenté d'établir une session TCP sans obtenir de réponse de l'adresse IP externe. Nous devons vérifier les paramètres de notre pare-feu pour savoir si cette communication est autorisée.

Le second problème est lié à un domaine inexistant interrogé par la machine de l'utilisateur. Nous pouvons voir que update.invea.com n'existe pas, ce qui implique probablement une mauvaise configuration de l'utilisateur et non un problème lié au réseau.

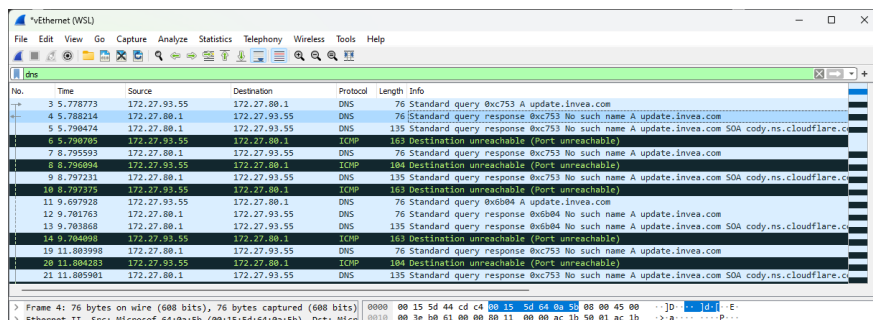


Figure 2: Requêtes de l'hôte pour résoudre un domaine inexistant.

# Dépannage à l'aide de données de flux enrichies

J'ai des sondes Flowmon en place qui surveillent le réseau et un collecteur Flowmon avec des semaines d'historique de statistiques de trafic non échantillonnées et non agrégées. Je peux donc poser directement la question du DNS au domaine winatp-gw-weu-microsoft.com.

▼ FILTER

dns-qtname = "winatp-gw-weu-microsoft.com" and ip:10.99.48.51 and dns-type "A"

My filters <None> SAVE FILTER

PROCESS

All Sources  
2023-08-03 12:25:00 - 2023-08-03 12:30:00  
20 Flows sort by Start time of Flows  
dns-qtname = "winatp-gw-weu-microsoft.com" and ip:10.99.48.51 and dns-type "A"

START TIME	FIRST SEEN	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	DNS QUERY/RESPONSE	DNS QUESTION TYPE	DNS QUESTION NAME	DNS RESPONSE NAME	DNS RESPONSE DATA	DNS RESPONSE CODE	PACKETS	BYTES
2023-08-03 12:25:28.228	0%	10.99.48.51	10.100.16.21	Query	A	winatp-gw-weu-microsoft.com			NoError	1	72 B
2023-08-03 12:25:28.343	0%	10.100.16.21	10.99.48.51	Response	A	winatp-gw-weu-microsoft.com	mga-mde-prd-weu-15.westeurope.cloudapp.azure.com	20.103.246.163	NoError	1	208 B

Figure 3: Filtrage du trafic DNS - statistiques de flux enrichies d'informations DNS.

Je peux voir l'adresse IP fournie par le serveur DNS comme réponse et vérifier facilement le trafic allant vers cette adresse IP. Cela est possible parce que les flux de la sonde correspondant au DNS sont enrichis des informations L7 les plus importantes du protocole DNS.

▼ FILTER

ip:10.99.48.51 and ip:20.103.246.163

My filters <None> SAVE FILTER

PROCESS

All Sources  
2023-08-03 07:25:00 - 2023-08-03 11:30:00  
20 Flows  
ip:10.99.48.51 and ip:20.103.246.163

START TIME	FIRST SEEN	DURATION	PROTOCOL	SOURCE IP ADDRESS	SOURCE PORT	DESTINATION IP ADDRESS	DESTINATION PORT	TCP FLAGS	PACKETS	BYTES	FLOWS	TCP WINDOW SIZE	TCP SYN SIZE
2023-08-03 07:29:52.003	0%	31.434 s	TCP	10.99.48.51	52430	20.103.246.163	https	...S.	6	360 B	1	64240	60
2023-08-03 07:30:52.388	0%	31.849 s	TCP	10.99.48.51	43498	20.103.246.163	https	...S.	6	360 B	1	64240	60

Figure 4: Filtrage de la communication de l'utilisateur avec le service externe. L'hôte ne reçoit aucune réponse.

Je constate que seuls des paquets SYN sont transmis au réseau sans réponse d'une adresse IP externe, ce qui implique la nécessité de vérifier les règles du pare-feu. Outre les informations L3/L4 courantes, j'ai une visibilité sur des éléments spécifiques à TCP tels que la taille du segment (fenêtre) TCP par défaut, ce qui peut m'aider à dépanner la session TCP.

Le domaine inexistant figure également dans ma preuve de flux. Le domaine flowmonos n'existe pas, le serveur DNS répond donc « NXDomain ».

▼ FILTER

dns-qtname = "flowmonos" and ip:10.100.56.146

My filters <None> SAVE FILTER

PROCESS

All Sources  
2023-08-03 11:50:00 - 2023-08-03 12:20:00  
20 Flows sort by Start time of Flows  
dns-qtname = "flowmonos" and ip:10.100.56.146

START TIME	FIRST SEEN	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	DNS QUERY/RESPONSE	DNS QUESTION TYPE	DNS QUESTION NAME	DNS RESPONSE NAME	DNS RESPONSE DATA	DNS RESPONSE CODE	PACKETS	BYTES
2023-08-03 11:54:30.285	0%	10.100.56.146	10.100.2.9	Query	A	flowmonos			NoError	1	55 B
2023-08-03 11:54:30.285	0%	10.100.2.9	10.100.56.146	Response	A	flowmonos			NXDomain	1	130 B

Figure 5: Filtrage du trafic DNS - recherche du code de réponse DNS NXDomain



# Témoignage : Workflow de l'enquête sur les causes profondes

Imaginons un département d'ingénieurs de niveau 3+ dans une banque de 50 000 personnes. Ces ingénieurs se concentrent sur l'analyse des causes profondes des incidents réseau qu'aucune autre équipe n'a pu résoudre auparavant. Par exemple, pour comprendre pourquoi une connexion VPN entre le client et la banque, tous deux situés sur des continents différents, a connu des pannes. Il est très fréquent que ces ingénieurs passent de nombreuses heures à fouiller dans Wireshark des pétaoctets de données générées par des centaines de systèmes différents dans un environnement compliqué et hétérogène. C'est exactement la situation d'un client de Flowmon qui nous a demandé de lui fournir une solution alternative et plus efficace pour traiter les incidents opérationnels.

Il est important de préciser que notre client a construit une plateforme complète pour l'aider dans ses tâches opérationnelles de réseau. Cette plateforme était basée sur un outil commercial pour la capture continue de paquets, un logiciel open source personnalisé pour la surveillance des flux, et un outil SNMP montrant des cartes thermiques de transfert de données en temps réel.

Il est rapidement apparu que la maintenance, le support et la mise à niveau de la solution personnalisée pour l'adapter aux opérations quotidiennes étaient trop coûteux et prenaient trop de temps. La banque s'est donc tournée vers la technologie NetFlow/IPFIX pour remplacer la solution d'origine. Le département informatique de la banque a cherché une solution pour remplacer complètement la solution d'origine. Bien que le budget ne soit pas un problème, le choix n'a pas été aussi facile qu'il n'y paraissait au premier abord. En testant différents fournisseurs, le problème résidait parfois dans l'agrégation des données, parfois dans l'absence de virtualisation, mais toujours dans la lenteur à fournir des résultats mesurés.

La solution dont ils rêvent doit :

- ▶ Fournir non seulement des tableaux de bord de haut niveau tenant compte du contexte, mais aussi un tableau de bord permettant d'effectuer des recherches manuelles dans n'importe quel flux.
- ▶ Ne pas agréger les données stockées et conserver les flux bruts aussi longtemps que dure le stockage.
- ▶ Ne pas nécessairement dépendre de ses propres capteurs, car leur environnement hétérogène ne leur permet pas de se cantonner à une seule technologie.

- ▶ Être virtualisée, afin que la gestion et la migration soient aussi souples que possible.
- ▶ Combiner la surveillance des flux avec la capture complète de paquets à la demande.
- ▶ Fournir, surtout, des résultats des statistiques mesurées des données de flux plus rapidement que la plateforme qu'ils ont construite eux-mêmes il y a dix ans à partir d'un outil open source.

C'est alors que l'équipe a découvert Flowmon, qui répondait parfaitement à ses besoins. Depuis le projet de validation du concept, Flowmon est devenu un élément fondamental de leur suite d'outils. C'est devenu le workflow même de toute enquête sur les causes profondes du moindre incident. Les ingénieurs commencent maintenant par le tableau de bord, passent aux statistiques de haut niveau, approfondissent les niveaux de NetFlow et ne se concentrent plus que sur une petite partie du trafic où ils peuvent effectuer une capture complète des paquets.



**« Flowmon donne à KBC une excellente vue d'ensemble des métriques de flux de données dans le réseau, de sorte que la santé du réseau peut être facilement évaluée. En cas de problème, l'outil permet un dépannage très rapide et efficace en visualisant le trafic à l'origine du problème. »**

**Marc Deamen**  
Ingénieur système principal, KBC



# Conclusion

La dynamique et la diversité des réseaux d'aujourd'hui remettent en question l'approche dominante de la supervision réseau. Face à l'augmentation de la vitesse des réseaux, aux lacunes de visibilité causées par la migration vers le cloud, l'IoT et les réseaux définis par logiciel, les solutions de capture de paquets peinent à apporter les résultats escomptés rapidement et à un prix raisonnable.

Les solutions de capture de paquets ont été conçues à une époque où la dynamique des environnements réseau actuels était difficile à imaginer. Aujourd'hui, elles fonctionnent bien dans des cas d'utilisation spécifiques, mais elles ne peuvent pas faire face à la flexibilité, à l'évolutivité et à la facilité d'utilisation des données de flux dans la plupart des cas d'utilisation quotidiens auxquels les ingénieurs réseau sont confrontés.

Nous avons démontré un cas d'utilisation où les données de flux avec une visibilité étendue sont aussi puissantes que la capture et l'analyse complètes des paquets. D'un autre côté, il est juste de dire que même avec une visibilité étendue au niveau du flux, vous pouvez toujours être confronté à des problèmes où l'analyse des PCAP est inévitable.






Chez Progress Flowmon, nous pensons que la fusion de la visibilité des flux et des paquets en une seule et unique solution polyvalente constitue la technologie qui vous aidera à vous adapter à vos besoins futurs en termes de performance et de capacité. Ainsi, surveillons le flux en continu et capturons les paquets lorsque cela est nécessaire. En fin de compte, vous aurez probablement besoin d'analyser les PCAP moins souvent que vous ne le pensez. Passez à Flowmon et découvrez comment cette solution peut contribuer au succès de votre entreprise !



**Demandez votre essai gratuit de Flowmon  
pour 30 jours**

## À propos de Progress

Dans un monde où la technologie est omniprésente, [Progress](#) (Nasdaq : PRGS) accompagne les entreprises dans l'accélération de leurs cycles d'innovation et de leur réussite. En tant que fournisseur de confiance des meilleures solutions pour développer, déployer et superviser des applications métiers critiques, Progress permet à ses clients de développer les solutions et les expériences dont ils ont besoin, de les déployer où et comme ils le souhaitent et de les superviser en toute sécurité. Des centaines de milliers d'entreprises, dont 1 700 éditeurs de logiciels et 3,5 millions de développeurs, font confiance à Progress pour atteindre leurs objectifs, en toute sérénité. Pour en savoir plus, rendez-vous sur [www.progress.com](http://www.progress.com), et retrouvez-nous sur [LinkedIn](#), [YouTube](#), [Twitter](#), [Facebook](#) et [Instagram](#).

 /progresssw  
 /progresssw  
 /progresssw  
 /progress-software  
 /progress\_sw\_

© 2023 Progress Software Corporation et/ou ses filiales ou sociétés affiliées. Tous droits réservés. Rev 2023/09 RITM0212205FR