Visibilité : Cas d'utilisation

GUIDE POUR LES INTÉGRATEURS SYSTÈMES ET LES PARTENAIRES TECHNOLOGIQUES D'IXIA

ixia
A Keysight Business

915-8135-01-0171 Rev A |

UNE OPPORTUNITÉ À SAISIR

Qu'est-ce qu'une solution de visibilité et quelle valeur ajoutée apporte-t-elle à une société IT ? En quelques mots, il s'agit d'une solution dans laquelle c'est l'infrastructure réseau elle-même qui accède aux trafics de tous types et les distribue aux appliances opérationnelles qui gèrent la surveillance de la sécurité, des analyses, de la conformité et des performances. Une bonne solution de visibilité peut accéder aux données depuis tout emplacement, à n'importe quelle vitesse et avec une précision parfaite. Elle permet en outre de collecter, d'agréger, de dédupliquer, de décrypter et de distribuer les flux de données sans ajouter de latence ou perdre des paquets.

Les solutions de visibilité peuvent être implémentées de deux manières : soit en mode « inline » (en ligne), avec prise en charge des services de sécurité en temps réel, soit en mode « out-of-band » (déconnecté) pour les services de surveillance, d'analyse et de mise en conformité des données en temps différé. Dans les deux cas, il importe de sélectionner l'infrastructure la mieux adaptée aux besoins réseau de votre client. Vous devrez en outre choisir l'approche d'architecture de visibilité qui procure à vos partenaires et à vous-même le plus de souplesse, le moins de pannes système et les options de mise à niveau les plus simples.

En tant que prestataire de solutions, l'inclusion d'une architecture de visibilité renforcera votre cycle de vente en dynamisant vos ventes additionnelles et complémentaires. Grâce à la flexibilité accrue de l'architecture, vous pourrez aider vos clients à actualiser et développer leurs conceptions au fil des ajouts et changements de leur infrastructure informatique et gagner ainsi un avantage concurrentiel.

Les solutions de visibilité d'Ixia vous aident à raccourcir vos cycles de vente, à libérer votre activité des fenêtres de maintenance et à créer de nouvelles opportunités en rendant possible des combinaisons de services réseau et de sécurité plus souples, tout en concevant une architecture extensible qui soit propice à de nouvelles ventes additionnelles et complémentaires. Les cas d'utilisation récapitulés dans ce guide constitueront pour vous un modèle de départ pour planifier et implémenter des solutions de visibilité qui procureront des avantages économiques immédiats. Chaque cas présenté aborde les problèmes réseau courants rencontrés par les clients, les solutions d'Ixia en matière d'architecture de visibilité, ainsi que les avantages que celles-ci présentent aussi bien pour vous et vos partenaires que pour vos clients finals.

En collaborant avec Ixia dans le cadre d'un partenariat et en adoptant une architecture de visibilité comme meilleure pratique, vous serez rapidement apte à fournir des solutions puissantes et innovantes dont le succès sera garanti, et tout cela pour un coût réduit.

SOMMAIRE

SUPERVISION « OUT-OF-BAND » CAS D'UTILISATION

Surmonter les limitations liées aux ports SPAN :

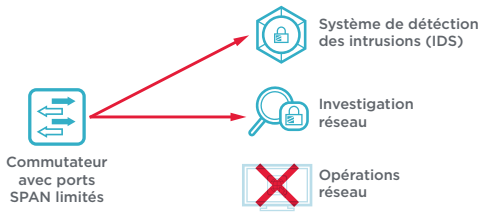
Lorsqu'il y a trop peu de ports SPAN pour prendre en charge les outils

SITUATION

Lorsque le nombre ou la capacité des port SPAN limite le nombre d'outils de sécurité et de surveillance connectables, des angles morts en termes de visibilité apparaissent dans l'infrastructure. L'ajout ou la reconfiguration de ports SPAN occasionne des coûts supplémentaires et retarde l'obtention d'une visibilité complète par vos systèmes de sécurité.

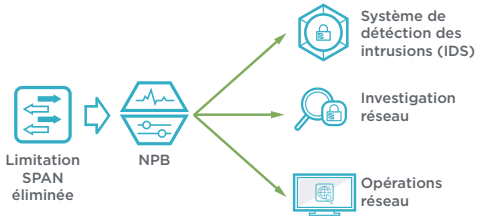
SOLUTION

SANS LA VISIBILITÉ IXIA



Envoi du trafic à tous les outils impossible

AVEC LA VISIBILITÉ IXIA



Visibilité complète. Trafic envoyé à tous les outils

L'ajout d'une matrice Network Packet Broker (NPB) permet la distribution et l'inspection simultanées du trafic par de nombreux outils de surveillance. Les NPB d'Ixia peuvent être facilement déployés et gérés pour résoudre un problème de limite de nombre de ports SPAN. Le portefeuille de NPB Vision d'Ixia inclut une interface graphique par glisser déposer conviviale qui, en un simple clic, permet la connexion aisée des outils de surveillance aux sources de trafic appropriées.

RÉSULTAT

Une visibilité complète du trafic pour tous les outils de surveillance.

Prestataire de solutions	Clients
• Vendez plus de solutions de sécurité et de surveillance en éliminant les contraintes de limitation des ports SPAN • Faites du problème de limitation des ports SPAN le point de départ de votre argumentation sur le passage à des vitesses réseau supérieures • Déployez une architecture qui favorise les ventes additionnelles et complémentaires d'un plus grand nombre de solutions de surveillance	• Réduisez vos coûts de surveillance en partageant les données de trafic avec tous les outils d'analyse et de surveillance souhaités • Effectuez des captures TAP partout et en toute confiance, sans risque de perdre des données. • Réduisez vos coûts de dépannage sans changer le réseau grâce à un accès plus rapide aux données et à un meilleur filtrage de ces dernières • Essayez et déployez facilement de nouveaux systèmes de surveillance

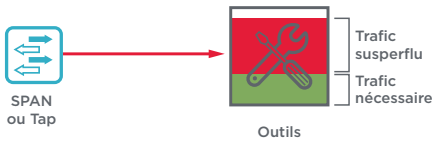
Alléger le trafic pour les outils de surveillance :

Lorsque le trafic en double monopolise les ressources

SITUATION

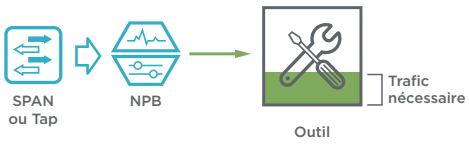
Il existe deux moyens courants d'accéder aux données de surveillance du réseau : soit par le biais de Taps réseau, soit au moyen des ports SPAN de commutateur réseau. Dans l'un et l'autre scénarios, des paquets en double sont généralement créés. Selon l'architecture de votre ensemble de données particulier et la méthode d'accès à celles-ci, le volume de ces paquets en double peut croître de façon excessive – voire représenter jusqu'à 50 % des données traversant votre réseau. L'envoi des paquets en double aux outils d'analyse et de mise en conformité monopolise en pure perte la capacité de ces outils, ce qui peut engendrer un allongement des temps de réponse ou des pertes de paquets.

SANS LA VISIBILITÉ IXIA



Gaspillage de ressources.
Totalité du trafic envoyé à l'outil

AVEC LA VISIBILITÉ IXIA



Grâce à la fonction de filtrage d'Ixia, l'outil ne reçoit que la quantité de trafic nécessaire

SOLUTION

L'une des meilleures solutions est de faire appel à la matrice NPB d'Ixia pour supprimer ces paquets en double. Le NPB peut effectuer cette suppression à la vitesse de ligne maximale avant de transmettre le trafic aux outils de surveillance. Les copies redondantes sont simplement ôtées du flux de données, empêchant ainsi toute surcharge de ces outils.

RÉSULTAT

Une plus grande efficacité et une durée de vie accrue des outils de surveillance et de sécurité.

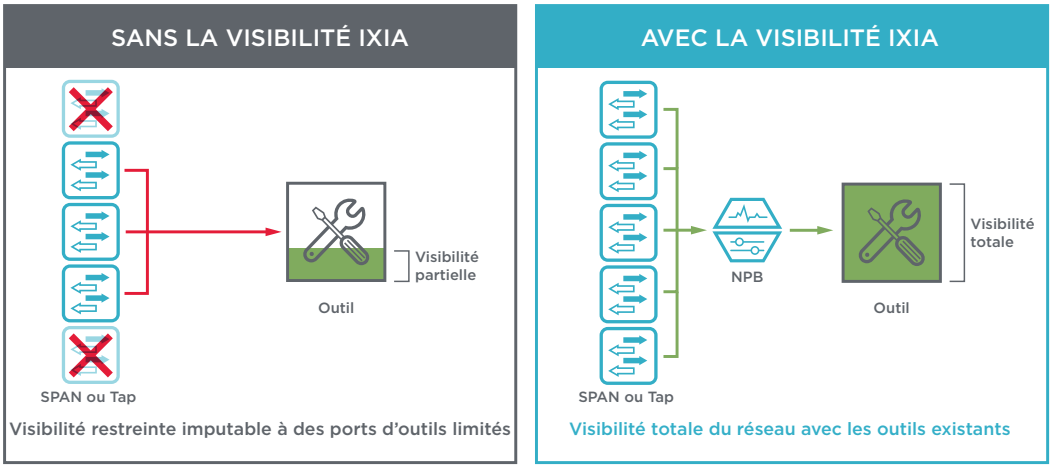
Prestataire de solutions	Clients
• Augmentez la vitesse et le temps de fonctionnement des solutions de surveillance de vos clients, et engrangez ainsi des ventes additionnelles • Vendez une solution de visibilité en complément de l'infrastructure réseau de base	• Réduisez vos coûts liés aux outils de surveillance en supprimant les données en double à traiter et augmentez de 30 à 50% de l'efficacité de vos outils • Rendez les outils plus efficaces en éliminant la consommation de mémoire superflue des sessions en double • Réduisez les risques liés à la sécurité réseau résultant des pertes de paquets grâce à la déduplication sans perte de paquets assurée par les NPB d'Ixia.

Étendre la surveillance à l'ensemble du centre de données :

Lorsqu'il y a trop peu d'outils pour tous les segments réseau

SITUATION

Lorsque le nombre de segments réseau dépasse celui des outils de surveillance ou de sécurité disponibles, certains segments restent parfois sans surveillance. Ceci augmente les risques d'incidents lié à la sécurité et allonge potentiellement le temps de résolution des problèmes de performances. L'ajout ou la reconfiguration des ports de surveillance occasionne des coûts supplémentaires et retarde l'obtention d'une visibilité complète par tous vos systèmes de surveillance.



SOLUTION

L'ajout d'une matrice NPB (NPB) permet d'agréger le trafic issu de plusieurs segments réseau dans l'ensemble du centre de données et de distribuer ces données aux outils de surveillance disponibles. Les matrices NPB d'Ixia peuvent être facilement déployées et gérées depuis un point central pour assurer la transmission des données correctes à l'outil adéquat. Le portefeuille de NPB Vision d'Ixia inclut une interface graphique par glisser déposer conviviale qui, en un simple clic, permet la connexion aisée des outils de surveillance aux sources de trafic appropriées.

RÉSULTAT

Visibilité de l'ensemble du centre de données à l'aide d'un minimum d'outils de surveillance.

Prestataire de solutions	Clients
• Vendez plus de services réseau en éliminant les contraintes d'infrastructure réseau • Vendez une solution de visibilité en complément de l'infrastructure réseau existante	• Réduisez vos coûts d'outils en agrégeant les données de trafic afin d'accroître l'efficacité des systèmes de sécurité et de surveillance • Essayez et déployez facilement de nouveaux services réseau • Les NPB d'Ixia disposent d'une visibilité auto-maintenue - leur reconfiguration étant gérée automatiquement

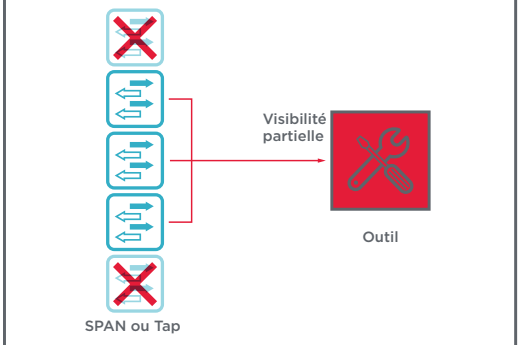
Dimensionner la surveillance du trafic :

Lorsque la croissance du trafic dépasse la capacité des outils

SITUATION

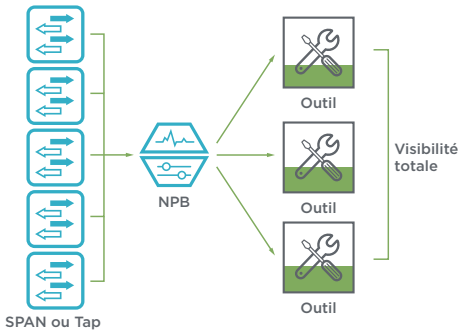
Lorsque le nombre de ports ou la capacité de traitement des outils de surveillance et de sécurité sont insuffisants pour couvrir la quantité de trafic, seule une partie du trafic global peut être inspectée, ce qui crée des angles morts dans l'infrastructure. L'ajout et la configuration d'une capacité d'outil supplémentaire peut en outre retarder l'obtention d'une visibilité complète par vos systèmes de surveillance.

SANS LA VISIBILITÉ IXIA



La capacité limitée de l'outil se traduit par une visibilié partielle

AVEC LA VISIBILITÉ IXIA



L'équilibrage de la charge redimensionne la surveillance à mesure que le trafic augmente

SOLUTION

L'ajout d'une matrice NPB permet d'agréger le trafic côté réseau et d'équilibrer automatiquement la charge entre les outils de surveillance multiples côté inspection. Les NPB d'Ixia peuvent être facilement déployés et gérés depuis un point central pour assurer la transmission des données correctes à l'outil adéquat. Le portefeuille de NPB Vision d'Ixia inclut une interface graphique par glisser déposer conviviale qui, en un simple clic, permet la connexion aisée des outils de surveillance aux sources de trafic appropriées.

RÉSULTAT

L'équilibrage de la charge redimensionne la surveillance à mesure que le trafic augmente.

Prestataire de solutions	Clients
• Améliorez les performances et la disponibilité des outils de sécurité et de surveillance côté client • L'ajout d'une « intelligence applicative » et d'informations sur les menaces accroît la flexibilité de choix quant aux options de sécurité • L'architecture contribue à dynamiser les ventes additionnelles et complémentaires de solutions de surveillance	• Optimisez l'utilisation de vos outils de sécurité et de surveillance multiples en équilibrant la charge de données entre ces derniers, afin de prévenir toute surcharge des systèmes individuels • Déployez une stratégie de « survie N + 1 » peu coûteuse et réductrice de risque pour les solutions de surveillance • Une fonctionnalité d'agrégation/ désagrégation permet à la fois le regroupement vers des outils de plus grande capacité et la dispersion vers des outils de capacité moindre

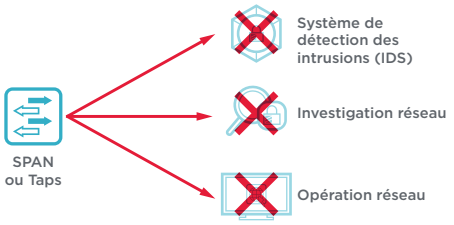
Connecter divers types d'outils :

Lorsque la vitesse du réseau et les supports ne correspondent pas

SITUATION

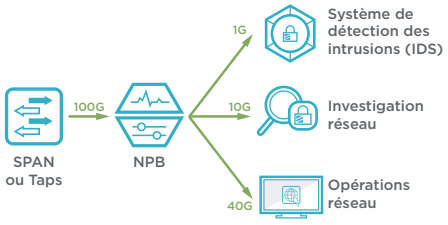
Lorsque l'incompatibilité d'interfaces réseau, sur des sources de trafic telles que les ports Span ou les Taps, empêche la connexion directe aux outils de sécurité et de surveillance, les équipes informatiques perdent toute visibilité des événements survenant sur leurs réseaux. Les changements de vitesse de connexion et de types de support alors nécessaires occasionnent des coûts supplémentaires et retardent l'obtention d'une visibilité complète par vos systèmes de sécurité.

SANS LA VISIBILITÉ IXIA



Visibilité nulle due à l'incompatibilité des supports et des vitesses

AVEC LA VISIBILITÉ IXIA



Souplesse de l'architecture pour les outils nouveaux et existants

SOLUTION

L'ajout d'une matrice NPB prenant en charge un grand nombre de vitesses et de types d'interfaces réseau permet la distribution et l'inspection immédiates du trafic par de nombreux outils de sécurité. Les NPB d'Ixia peuvent être facilement déployés et gérés pour résoudre des problèmes d'incompatibilité de connectivité réseau. Le portefeuille de NPB Vision d'Ixia inclut une interface graphique par glisser déposer conviviale qui, en un simple clic, permet la connexion aisée des outils de surveillance aux sources de trafic appropriées..

RÉSULTAT

Une architecture souple qui optimise l'utilisation des outils nouveaux et existants.

Prestataire de solutions	Clients
• Surmontez les contraintes budgétaires en séparant le cycle de vente des outils de sécurité et de surveillance du cycle de mise à niveau du réseau • L'architecture est propice à l'accélération des ventes additionnelles et complémentaires de solutions de surveillance	• Étendez la durée de vie utile des dispositifs de surveillance et de sécurité à basse vitesse existants • Permet à un ensemble de systèmes de surveillance divers d'opérer conjointement quels que soient la vitesse du réseau ou le support • Contrôlez le budget CAPEX. Mettez les services réseau à niveau sans que cela entraîne une mise à niveau globale de l'infrastructure

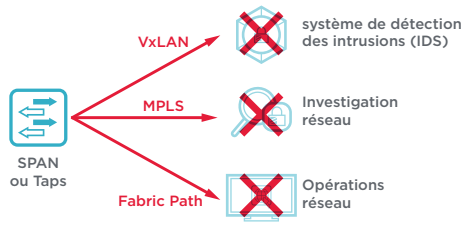
Surveiller les protocoles tunnelisés :

Lorsque les paquets sont incompréhensibles par les outils de surveillance

SITUATION

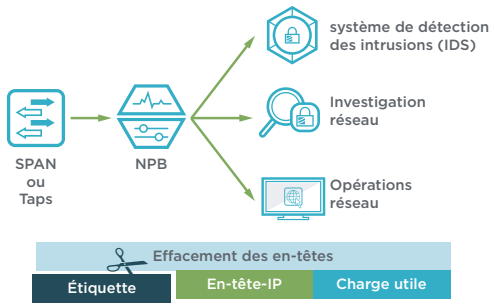
Les nouvelles générations de solutions réseau, telles que SDN, aident les ingénieurs informatiques à moderniser leur infrastructure réseau. Ces technologies récentes peuvent cependant perturber les stratégies de surveillance existantes lorsqu'elles emploient des techniques comme l'encapsulation, la tunnelisation ou des nouvelles en-têtes que les plates-formes de surveillance et de sécurité existantes ne sont pas aptes à interpréter ou 'inspecter.

SANS LA VISIBILITÉ IXIA



Les outils ne peuvent pas comprendre les protocoles débouchants sur une visibilité nulle

AVEC LA VISIBILITÉ IXIA



L'effacement des en-têtes aide à regagner de la visibilité même sur le trafic étiqueté non pris en charge

SOLUTION

Une architecture à base de matrices NPB procure visibilité et réduction des coûts en convertissant les nouveaux types de trafic réseau en des formats que les plates-formes de surveillance et de sécurité existantes comprennent. Les NPB d'Ixia préparent les paquets pour le traitement des outils en supprimant leurs en-têtes et données superflues à la vitesse de ligne. De puissantes fonctions de filtrage de données, d'effacement des en-têtes et de capture partielle de paquet permettent de combiner facilement les nouvelles générations de solutions réseau et les systèmes de surveillance actuels.

RÉSULTAT

Assure la visibilité aussi bien avec les anciennes technologies qu'avec les nouvelles.

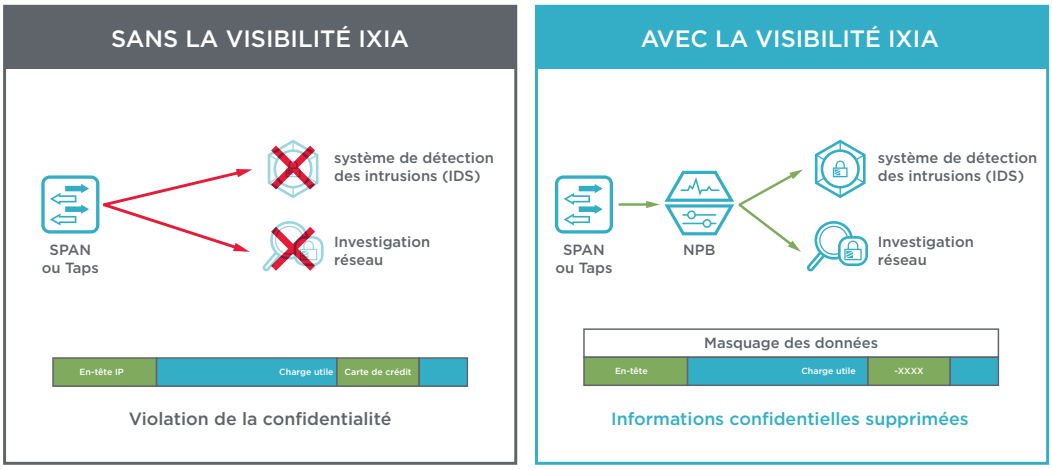
Prestataire de solutions	Clients
• Déployez les nouvelles solutions, telles qu'ACI, en séparant le cycle de vente des outils de sécurité et de surveillance du cycle de mise à niveau du réseau • Créez de nouvelles opportunités de vente en rendant possible des combinaisons flexibles mêlant solutions réseau et systèmes de surveillance et de sécurité existants	• Maximisez la valeur à long terme de vos investissements dans des systèmes de surveillance et de sécurité en supprimant les en-têtes ou données de paquets superflus • Permet à un ensemble de plates-formes diverses d'opérer conjointement quelle que soit la génération à laquelle elles appartiennent • Déployez de nouvelles technologies sans que cela entraîne une mise à niveau des systèmes de surveillance et de sécurité

Protéger les données personnelles identifiables :

Lorsque des données sensibles sont envoyées à des outils de surveillance multiples

SITUATION

La plupart des entreprises ont un certain nombre de règles à respecter en matière de conformité. Les réglementations telles que HIPAA, PCI, GDPR, ainsi que les politiques de meilleure pratique interne, préconisent que les données personnelles identifiables (DPI) soient gérées avec le plus grand soin. L'envoi de contenus DPI à des systèmes de surveillance ou de sécurité peut, par conséquent engendrer, des violations de l'obligation de confidentialité.



SOLUTION

Le masquage total ou partiel des données aide les entreprises à restreindre l'accès aux informations DPI sensibles comme les numéros de compte ou de sécurité sociale avant la transmission des données aux outils d'analyse. Les matrice NPB d'Ixia ôtent les données spécifiées des paquets en temps réel et les remplacent par une valeur fixe avant de les acheminer vers les outils de sécurité et de surveillance. Des masques de données peuvent facilement être configurés à l'aide de l'interface graphique par glisser déposer du NPB.

RÉSULTAT

La mise en conformité est facilitée par l'enlèvement aisé des données confidentielles.

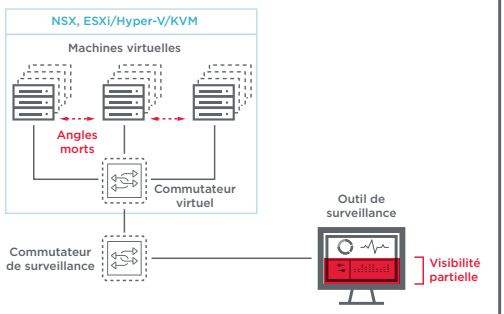
Prestataire de solutions	Clients
• Vendez des solutions de surveillance et de sécurité dans les secteurs d'activité hautement régulés • Vendez de nouvelles solutions de surveillance et de sécurité quelles que soient les contraintes liées aux informations personnelles identifiables	• Délivrez des solutions de surveillance conformes aux réglementations sur la confidentialité • Réduisez les risques de l'entreprise liés aux solutions de surveillance réseau • Appliquez et gérez des masques de données de manière centralisée avant de transmettre les informations aux outils de sécurité et de surveillance multiples. • Configurez et gérez des masques de données au moyen d'une interface graphique par glisser déposer conviviale • Utilisez tout décalage souhaité, et des options préconfigurées, pour les formats courants tels que les numéros de carte de crédit.

Rendre le trafic inter-VM visible :
Lorsque le trafic demeure dans l'environnement virtuel

SITUATION

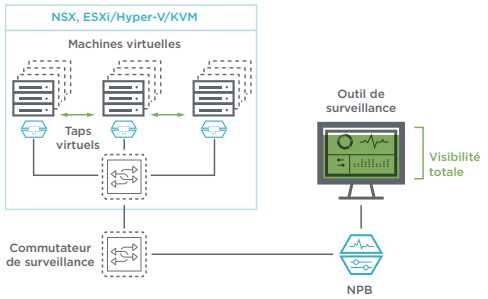
Pour tirer parti de la souplesse et de la puissance des environnements virtualisés tout en gardant le contrôle de l'infrastructure physique, les entreprises ont recours à des solutions cloud privées. Cependant, la visibilité limitée du trafic réseau virtualisé se traduit par des angles morts pour les outils de surveillance des centres de données virtuels ou physiques.

SANS LA VISIBILITÉ IXIA



L'outil n'a aucune visibilité du trafic est-ouest entre les machines virtuelles

AVEC LA VISIBILITÉ IXIA



Visibilité complète dans les environnements virtuels via tout hyperviseur majeur

SOLUTION

La plate-forme CloudLens™ d'Ixia permet d'accéder aux données circulant entre les machines virtuelles, procurant ainsi une visibilité complète des environnements cloud privés. Compatible avec tous les principaux hyperviseurs, CloudLens transmet des données aussi bien aux outils physiques qu'à ceux de type cloud. Les processeurs de paquets virtuels ou les NPB physiques agrègent le réseau virtuel, le filtrent et équilibrent sa charge, tout en appliquant des traitements avancés tels que la déduplication, le packet trimming et la technologie Netflow pour fournir les données appropriées à l'outil voulu. CloudLens prend en charge une architecture intégralement cloud uniquement.

RÉSULTAT

Le trafic virtuel est rendu visible par les outils de surveillance.

Prestataire de solutions	Clients
• Étendez votre entreprise de systèmes de surveillance ou de sécurité à l'échelle du cloud • Utilisez la visibilité des centres de données virtuels et des réseaux cloud comme point de départ de vos argumentations sur les avantages d'une architecture de visibilité • Déployez une architecture qui favorise les ventes additionnelles et complémentaires pour tous les modèles de déploiement (sur site, cloud privé ou cloud public)	• Obtenez une visibilité complète du trafic dans les environnements virtuels • Optimisez le trafic et la bande passante de sorte que les outils puissent opérer avec un maximum d'efficacité • Choisissez n'importe quelle option de déploiement cloud ou hybride • Tirez parti des NPB d'Ixia pour amener les données cloud dans une structure semblable à celle d'un centre de données afin de constituer un flux unique

Décharger le décryptage SSL sur la couche Visibilité :

Lorsque le décryptage a un impact sur les performances de la solution

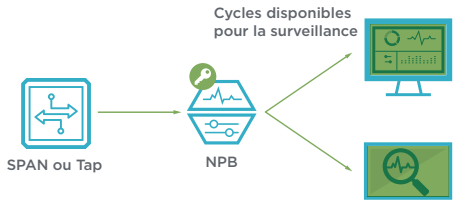
SITUATION

Pour gérer le trafic crypté, il est essentiel de maintenir un niveau de sécurité élevé mais les solutions de sécurité ne sont aptes à traiter que le texte en clair. Certaines solutions contournent cette contrainte en proposant une fonction de décryptage facultative. Mais le décryptage étant une fonction fortement axée sur les processus, les performances de la solution peuvent s'en trouver considérablement réduites. Les solutions de sécurité ne décryptent en outre le trafic que pour leurs propres inspections internes et ne peuvent pas partager celui-ci avec d'autres solutions de sécurité. De plus, l'utilisation d'appliances sur des segments séparés alourdit l'administration et limite la flexibilité quant à ce qu'il s'agit de décrypter ou de filtrer

SANS LA VISIBILITÉ IXIA

Traiter le décryptage sur chaque outil en ligne monopolise de précieux cycles de traitement, entrainant des mises à niveau d'outils

AVEC LA VISIBILITÉ IXIA



La fonction Active SSL du NPB décrypte/crypte une fois les données pour décharger les outils et les rendre plus efficaces

SOLUTIONS

L'ajout d'une matrice NPB dotée de la fonctionnalité de décryptage SSL active permet de réaliser le décryptage une seule fois et de rendre simultanément le texte en clair disponible pour toutes les solutions de surveillance. Les outils de surveillance peuvent alors dédier tous leurs cycles de traitement à leur fonction principale, ce qui renforce leur efficacité. Un filtrage supplémentaire des données décryptées est également possible pour que seules les données pertinentes soient transmises à un outil de surveillance donné. Les NPB d'Ixia font appel à un processeur cryptographique permettant un décryptage actif beaucoup plus rapide qu'avec les outils de surveillance et sans perte de paquets.

RÉSULTAT

Déchargées du décryptage SSL les solutions de sécurité peuvent concentrer leur action sur l'inspection en profondeur des paquets.

Prestataire de solutions	Clients
• Créez un nouveau cycle de vente pour la surveillance du trafic crypté - un segment de marché en pleine expansion • Démarrez les échanges de données conformément aux spécifications de la norme TLS 1.3 • Augmentez la capacité et les performances de la solution de surveillance en la déchargeant du décryptage • Déployez une architecture qui favorise les ventes additionnelles et complémentaires d'outils de sécurité et de surveillance	• Réduisez les risques pour la sécurité globale en analysant le trafic crypté • Augmentez la capacité et les performances des solutions de surveillance • Partagez à un coût réduit le trafic crypté avec tous les outils de sécurité et de surveillance souhaités • Assurez un dimensionnement économique de la capacité de décryptage via les NPB

SOMMAIRE

SÉCURITÉ EN LIGNE CAS D'UTILISATION

Protéger la disponibilité du réseau:

Lorsque le système de sécurité en ligne est en panne ou exige une maintenance

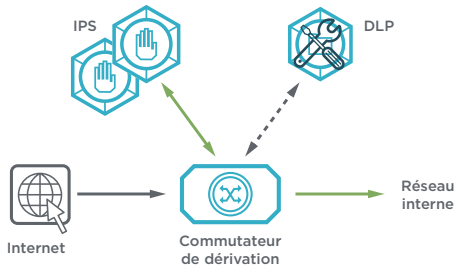
SITUATION

Les appliances de sécurité déployées en ligne sur le réseau actif doivent opérer à leurs performances maximales sans la moindre défaillance. Le temps de fonctionnement individuel peut en effet avoir un impact direct sur la disponibilité des applications réseau. Une fois en ligne sur le réseau, chaque appliance est un point de défaillance potentiel dont le déploiement peut prendre des heures et dont la mise à niveau, le dépannage ou la reconfiguration peut nécessiter un temps d'arrêt. L'attente d'une fenêtre de maintenance disponible augmente en outre le risque de ne pas repérer une menace ou une attaque.

SANS LA VISIBILITÉ IXIA

Chaque outil en ligne est un point de défaillance unique sur le réseau

AVEC LA VISIBILITÉ IXIA



En cas de défaillance ou de maintenance, Ixia protège automatiquement la disponibilité du réseau

SOLUTION

La fiabilité du réseau et des systèmes de sécurité est augmentée en déployant des commutateurs de dérivation externes (bypass) devant les appliances de sécurité, pour un fonctionnement en mode en ligne, Tap ou dérivation, Les commutateurs iBypass d'Ixia sont préconfigurés pour surveiller les appliances de sécurité au moyen de la fonction « Heartbeat » la plus rapide du marché et s'installent en quelques minutes. Les solutions peuvent être pilotées hors bande puis, plus tard, passer en ligne sans temps d'arrêt. Ixia procure également le basculement automatique entre deux appliances redondantes pour garantir la résilience de la sécurité en ligne.

RÉSULTAT

Une réduction des temps d'arrêt et des solutions résilientes.

Prestataire de solutions	Clients
• Vendez de nouvelles appliances de sécurité, installez-les sans temps d'arrêt et avec un retour sur investissement plus rapide • Différentiez votre offre en mettant en avant la possibilité de mise à jour sans fenêtre de maintenance et la prise en charge du basculement automatique • La mise à niveau simplifiée réduit vos coûts d'assistance et les problèmes liés à des configurations obsolètes	• Les commutateurs de dérivation se déploient en quelques minutes et les déploiements suivants de nouvelles appliances de sécurité ne requièrent pas l'arrêt du réseau • Le réseau est protégé de toute défaillance matérielle, logicielle ou de port • Plus besoin d'une fenêtre de maintenance pour mettre à jour la solution • Le basculement automatique entre deux appliances actives assure un fonctionnement ininterrompu de la solution

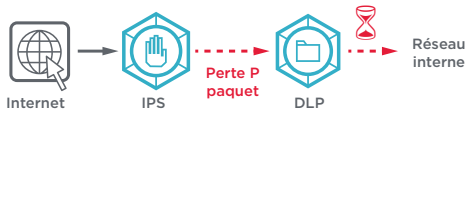
Maintenir une sécurité haute performance :

Lorsqu'un volume croissant entraîne un engorgement et des pertes de paquets

SITUATION

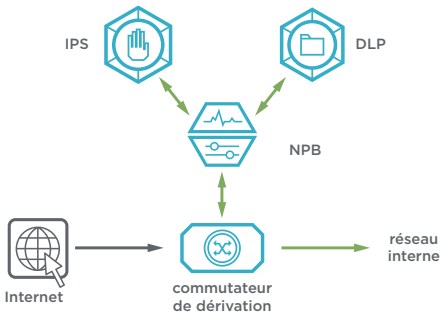
La croissance exponentielle des données peut mettre les solutions de surveillance de la sécurité à rude épreuve, en particulier celles qui sont déployées en ligne pour l'inspection de tout trafic entrant ou sortant. Les appliances submergées risquent alors de ralentir, de perdre des paquets, voire même de cesser de fonctionner, Ceci peut engendrer des temps d'arrêt et les risques de faille de sécurité peuvent s'en trouver augmentés.

SANS LA VISIBILITÉ IXIA



Le trafic non filtré peut engorgé les outils, allonger le temps de réponses et causer des pertes paquets

AVEC LA VISIBILITÉ IXIA



Le filtrage à la vitesse de ligne supprime les paquets en double et non pertinants pour accroitre l'efficacité des outils

SOLUTION

Le déploiement d'une matrice NPB (en plus du commutateur de dérivation externe) peut contribuer à réduire l'engorgement du réseau en exfiltrant les paquets en double ou non pertinents avant l'acheminement du trafic vers les solutions de sécurité à des fins d'inspection. Enlever du trafic des paquets tels que données vocales, vidéos ou musiques peut réduire celui-ci dans des proportions pouvant atteindre 35 % ou davantage. Avec moins de paquets à inspecter, les solutions de sécurité peuvent gérer la croissance du trafic avec un risque d'engorgement ou de perte de paquets revu à la baisse. Le portefeuille de matrices NPB Vision d'Ixia est géré à l'aide d'une interface graphique par glisser déposer conviviale qui simplifies la création des filtres.

RÉSULTAT

Le filtrage du trafic rend les solutions de sécurité plus efficaces en réduisant l'engorgement du réseau.

Prestataire de solutions	Clients
• Augmentez le retour sur investissement de vos solutions en prenant en charge les segments réseau de volume plus élevé • Délivrez des solutions de sécurité plus performantes en réduisant les engorgements et les risques de perte de paquets • La visibilité auto-maintenue avec le compilateur de filtre dynamique élimine les chevauchements de filtre et réduit les risques de perte de paquets • Augmentez votre compétitivité grâce aux NPB « zéro perte de paquets » d'Ixia	• Gérez au moindre coût le volume croissant du trafic • Réduisez les risques de perte de paquets, responsables d'incidents de sécurité • Allégez la surcharge des solutions de sécurité en filtrant le trafic • La gestion de filtres dynamique élimine les chevauchements de filtres, réduisant ainsi le risque de perte de paquets

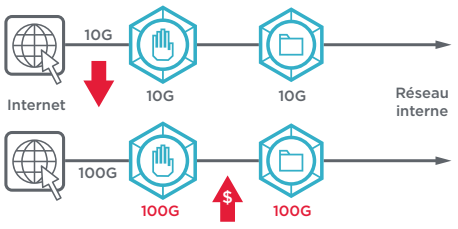
Étendre la durée de vie des solutions de sécurité :

Lorsqu'une mise à niveau réseau cause des conflits d'interfaces

SITUATION

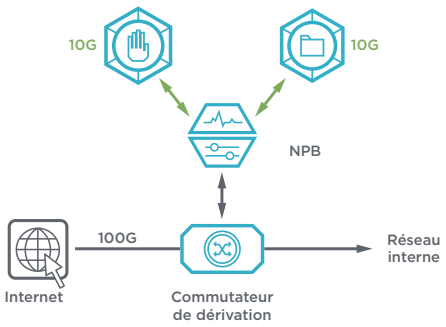
Les mises à niveau de vitesse de réseau engendrent également des changements dans les interfaces réseau. Ceci peut empêcher l'utilisation continue des solutions de sécurité en ligne existantes, voire rendre la mise à niveau de ces solutions inévitable alors même que les dispositifs actuels offrent encore des capacités et fonctions utiles. Pour financer ces mises à niveau, des entreprises sont parfois contraintes de retarder l'achat de solutions plus avancées pour contrer les cyber-attaques et menaces émergentes sur Internet.

SANS LA VISIBILITÉ IXIA



La mise à niveau des liens réseau exige une mise à niveau simultanée des outils de sécurité en ligne

AVEC LA VISIBILITÉ IXIA



Un NPB transmet le trafic à la vitesse désignée de l'outil afin détendre sa durée de vie

SOLUTION

L'ajout d'une matrice NPB permet d'agréger les données de divers types de liens réseau. Le trafic peut alors être transmis simultanément aux solutions de sécurité à diverses vitesses de connexion, étendant ainsi leur durée de vie. Les NPB d'Ixia peuvent être facilement déployés et gérés depuis un point central pour assurer la transmission des données correctes à l'outil adéquat. Le portefeuille de NPB Vision d'Ixia inclut une interface graphique par glisser déposer conviviale qui, en un simple clic, permet la connexion aisée des outils de surveillance aux sources de trafic appropriées.

RÉSULTAT

Étend la durée de vie des solutions existantes et libère un budget pour des solutions avancées.

Prestataire de solutions	Clients
• Surmontez vos contraintes budgétaires en séparant le cycle de vente des outils de sécurité et de surveillance du cycle de mise à niveau du réseau • Augmentez votre valeur aux yeux du client en étendant la durée de vie des solutions de sécurité existantes • Déployez une architecture qui favorise les ventes additionnelles et complémentaires de solutions de surveillance	• Maximisez la valeur à long terme de vos investissements en solutions de sécurité en ligne • Permettez à un ensemble de plates-formes diverses d'opérer conjointement quelles que soient leurs interfaces • Libérez un budget pour l'achat de solutions plus avancées qui renforcent votre protection contre les menaces et attaques émergentes

Assurer une surveillance garantissant une sécurité résiliente :

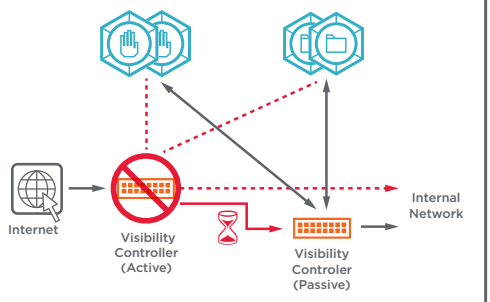
Lorsque le basculement nécessite l'utilisation d'un dispositif redondant

SITUATION

Pendant le basculement automatique d'un système de sécurité en ligne, le trafic peut continuer à transiter afin de ne pas interrompre l'activité de l'entreprise. Pour les solutions de visibilité qui ne peuvent être configurées qu'en mode actif-passif, restaurer le traitement complet et relancer la distribution des données prendra au moins une minute. Or beaucoup de choses peuvent se produire en 60 secondes et le risque accru lié aux cyber-attaques, logiciels malveillants et fuites de données peut s'avérer trop élevé dans certains secteurs d'activité.

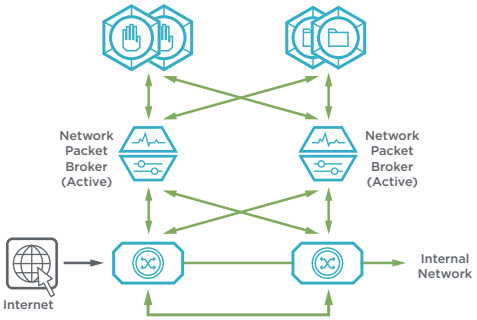
SOLUTION

SANS LA VISIBILITÉ IXIA



A redundant packet broker in passive must boot up, leaving your network exposed.

AVEC LA VISIBILITÉ IXIA



Ixia NPBs in active-active mode share the load and enable near-instant recovery.

Des négociateurs de paquets réseau redondants configurés en mode actif-actif et agissant de manière parfaitement synchronisée agrègent, filtrent, traitent et transmettent les données à toutes les solutions de sécurité en ligne. Ceci leur permet d'opérer plus efficacement, de gérer les pics de trafic périodiques et de basculer automatiquement (en une seconde maximum) pour que l'inspection de sécurité se poursuive de façon ininterrompue. Les outils qui reçoivent un flux réseau permanent sont ceux qui assurent la surveillance de sécurité la plus résiliente. La configuration actif-actif d'Ixia prévient les temps d'arrêt à tous les niveaux de défaillance (outil, NPB ou dérivation), garantissant ainsi un temps de fonctionnement maximal. Ixia est le seul fournisseur à permettre une restauration quasi-instantanée de la surveillance en ligne, un avantage d'une importance capitale dans les secteurs comme les services financiers et la santé.

RÉSULTAT

Les composants de visibilité en mode actif-actif assurent une surveillance ininterrompue de la sécurité.

Prestataire de solutions	Clients
• Vendez sur les segments de marché où le besoin d'une sécurité résiliente est le plus essentiel (services financiers, santé) • Augmentez votre valeur aux yeux du client en lui démontrant la quasi instantanéité du basculement de l'architecture de sécurité • Respectez vos accords de niveau de service (SLA) et différenciez votre offre d'architecture de sécurité	• Maximisez la résilience de la sécurité et minimisez les risques grâce au basculement quasi-instantané du système de sécurité en ligne • Augmentez le retour sur investissement lié aux NPB redondants en confiant à ceux-ci l'équilibrage de la charge pendant les opérations normales. • Nos solutions sont conçues de telle sorte que même les NPB sont protégées des défaillance

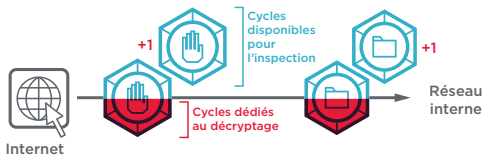
Décharger le décryptage SSL sur la couche Visibilité :

Lorsque le décryptage a un impact sur les performances de la solution

SITUATION

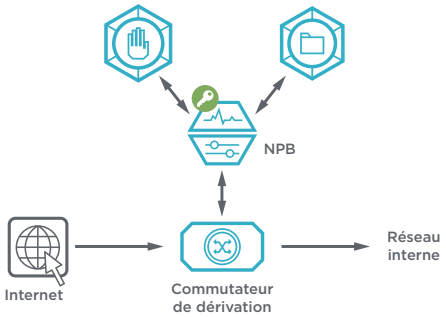
Pour gérer le trafic crypté, il est essentiel de maintenir un niveau de sécurité élevé mais les solutions de sécurité ne sont aptes à traiter que le texte en clair. Certaines solutions contournent cette contrainte en proposant une fonction de décryptage facultative. Mais le décryptage étant une fonction fortement consommatrice de CPU, les performances de la solution peuvent s'en trouver considérablement réduites. Les solutions de sécurité ne décryptent en outre le trafic que pour leurs propres inspections internes et ne peuvent pas partager celui-ci avec les autres solutions de sécurité.

SANS LA VISIBILITÉ IXIA



Traiter le décryptage sur chaque outil en ligne monopolise de précieux cycles de traitement, entrainant des mises à niveau d'outils

AVEC LA VISIBILITÉ IXIA



La fonction Active SSL du NPB décrypte/crypte une fois les données pour décharger les outils et les rendreplus efficaces

SOLUTION

L'ajout d'une matrice NPB avec permet de réaliser le décryptage une seule fois et de rendre simultanément le texte en clair disponible pour toutes les solutions de surveillance. Les appliances de sécurité peuvent alors dédier tous leurs cycles de traitement à leur fonction principale, ce qui renforce leur efficacité. Un filtrage supplémentaire des données décryptées est également possible pour que seules les données pertinentes soient transmises à un outil de surveillance donné. Le trafic est de plus réencrypté avant son retour sur le réseau. Les NPB d'Ixia font appel à un processeur cryptographique permettant un décryptage actif beaucoup plus rapide qu'avec les outils de surveillance et sans perte de paquets.

RÉSULTAT

Déchargées du décryptage SSL les solutions de sécurité peuvent concentrer leur action sur l'inspection en profondeur des paquets.

Prestataire de solutions	Clients
• Créez un nouveau cycle de vente pour la surveillance du trafic crypté - un segment de marché en pleine expansion • Augmentez la capacité et les performances des solutions de sécurité en les déchargeant du décryptage • Déployez une architecture qui favorise les ventes additionnelles et complémentaires d'outils de sécurité et de surveillance	• Réduisez les risques pour la sécurité globale en analysant le trafic crypté et en le réencryptant de façon fiable. • Augmentez la capacité et les performances des solutions de surveillance • Réduisez vos coûts de surveillance en partageant les données de trafic avec tous les outils d'analyse et de surveillance voulus • Assurez un dimensionnement économique de la capacité de décryptage via les NPB

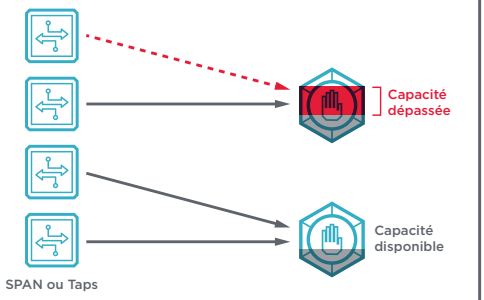
Équilibrer la charge pour prévenir les engorgements :

Lorsque les rafales de données ou le volume varient selon les liens réseau

SITUATION

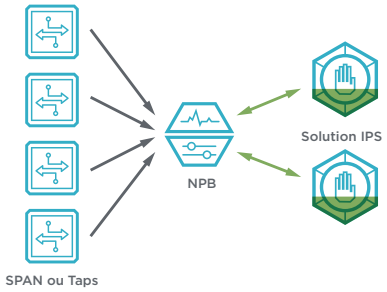
Les rafales de données ou les variations de croissance d'un lien réseau à l'autre peuvent amener certaines appliances de sécurité au-delà des limites de leur capacité alors que d'autres appliances sont sous-utilisées. L'engorgement de ces appliances peut entraîner des défaillances de dispositifs ou des pertes de paquets. L'ajout et la configuration d'une capacité d'outil supplémentaire peut alors perturber la disponibilité du réseau ou la surveillance de la sécurité, augmentant ainsi les risques pour l'entreprise.

SANS LA VISIBILITÉ IXIA



La croissance en volume ou les rafales peuvent engorger une appliance alors que la capacité de certaines autres est sous-utilisé

AVEC LA VISIBILITÉ IXIA



Le NPB équilibre automatiquement la charge entre les solutions disponibles, sans intervention manuelle

SOLUTION

L'ajout d'une matrice permet d'agréger le trafic côté réseau et d'équilibrer automatiquement la charge entre les outils de surveillance multiples côté inspection. Les NPB d'Ixia peuvent être facilement déployés et gérés depuis un point central pour assurer la transmission des données correctes à l'outil adéquat. Le portefeuille de NPB Vision d'Ixia inclut une interface graphique par glisser déposer conviviale qui, en un simple clic, permet la connexion aisée des outils de surveillance aux sources de trafic appropriées.

RÉSULTAT

L'équilibrage de la charge réduit les risques associés à l'engorgement et aux pertes de paquets.

Prestataire de solutions	Clients
• Augmentez votre valeur aux yeux du client en augmentant facilement l'évolutivité et la fiabilité des solutions via l'équilibrage automatique de la charge • Augmentez votre compétitivité en améliorant les performances et la viabilité de vos solutions de sécurité • Déployez une architecture qui favorise les ventes additionnelles et complémentaires de solutions de surveillance	• Optimisez l'utilisation de vos outils de sécurité et de surveillance multiples en équilibrant la charge de données entre ces derniers, afin de prévenir toute surcharge des systèmes individuels • Déployez une stratégie de « capacité de survie N + 1 » peu coûteuse et réductrice de risque pour les solutions de surveillance • Augmentez la fiabilité de la surveillance, au niveau sécurité, et réduisez les risques liés aux pertes de paquets

À propos d'Ixia

Société filiale de Keysight, Ixia fournit des solutions de test, de visibilité et de sécurité pour renforcer les réseaux et les environnements cloud des entreprises, prestataires de services et fabricants de matériel réseau. Ixia procure aux organisations des environnements sûrs dans lesquels ils peuvent développer, déployer et opérer en toute confiance. Dans le monde entier, des clients s'appuient sur les solutions Ixia pour vérifier leurs conceptions, optimiser leurs performances et assurer la protection. Le résultat : des applications plus performantes, une sécurité plus résiliente, un meilleur retour sur investissement et des clients satisfaits.

IXIA
26601 AGOURA ROAD
CALABASAS, CA 91302, ÉTATS-UNIS

(NUMÉRO GRATUIT EN AMÉRIQUE DU NORD)
1.877.367.4942

(POUR LES AUTRES PAYS)
+1.818.871.1800
(FAX) 1.818.871.1805
www.ixiacom.com

IXIA EUROPE
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
ROYAUME-UNI

SERVICE COMMERCIAL :
+44.1628.408750
(FAX) +44.1628.639916

IXIA ASIE-PACIFIQUE
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SERVICE COMMERCIAL :
+65.6332.0125
(FAX) +65.6332.0127