Contacts presse :
Carine Currit / Charles Catherinot
Edelman pour Juniper Networks
01 56 69 72 96 / 75 23
carine.currit@edelman.com / charles.catherinot@edelman.com

JUNIPER NETWORKS AMÉLIORE LES SOLUTIONS DE PARE-FEU DE NOUVELLE GÉNÉRATION POUR SIMPLIFIER ET RENFORCER LA SÉCURITÉ A LA PÉRIPHÉRIE DU RÉSEAU D'ENTREPRISE

Pour les entreprises, l'optimisation des passerelles de services SRX de Juniper Networks est un gage de sécurité et de contrôle, mais aussi d'efficacité et de souplesse

PARIS, France, le 26 juin 2014 - Juniper Networks (NYSE : JNPR), leader de l'innovation réseau, annonce l'ajout de nouvelles fonctionnalités à ses solutions de pare-feu de nouvelle génération (NGFW) afin de protéger la périphérie du réseau entreprise, mais aussi de renforcer la sécurité, le contrôle et l'efficacité, tout en simplifiant le déploiement et la gestion.

Les cybermenaces étant de plus en plus sophistiquées et ciblées, les entreprises ont besoin de pare-feu permettant de multiplier les couches de sécurité sans pour autant se compliquer la tâche. Or, aujourd'hui, la plupart d'entre elles commencent seulement à étudier les avantages potentiels des pare-feu de nouvelle génération. Selon Gartner, moins de 20 % des connexions Internet des entreprises sont actuellement sécurisées par des pare-feu de nouvelle génération (NGFW). D'ici la fin 2014, ce chiffre passera à 35 % de la base installée, les NGFW représentant 70 % des achats de services de périphérie réseau en entreprise[1].

Les nouvelles fonctionnalités de la solution de pare-feu de nouvelle génération de Juniper Networks permettent aux grandes entreprises de gérer une multitude de déploiements et de cas d'utilisation, en simplifiant les procédures administratives. Par ailleurs, la solution de Juniper facilite et centralise l'administration, et offre une plate-forme de services ouverte pour les fonctions de sécurité indispensables : prévention des intrusions (IPS), gestion unifiée des menaces (UTM) et visibilité sur les applications. Enfin, elle optimise les ressources de l'entreprise pour les activités stratégiques en déterminant qui a accès à telle ou telle application et quelles applications sont prioritaires sur le réseau.

Les points à retenir
Juniper Networks optimise ses passerelles de services SRX dont les fonctions de sécurité de nouvelle génération aident les clients à contrer les menaces et à contrôler leur réseau, sans alourdir le travail d'administration.

- **Gestion simplifiée :**
  - La gestion centralisée des pare-feu SRX et virtuels Firefly Perimeter est facilitée par le logging et le reporting intégrés, et par le contrôle d'accès basé sur les rôles de Junos Space Security Director qui administre les nouveaux services de sécurité (pare-feu utilisateur, sécurité applicative avec AppSecure et gestion unifiée des menaces). Désormais, tous les pare-feu de Juniper Networks sont gérés par une seule et même plate-forme d'administration centralisée qui permet de gagner en simplicité et en rapidité.
  - Directement intégrée avec Active Directory, la gamme SRX de Juniper Networks applique les règles de pare-feu basées sur les rôles utilisateurs sans coûts, ni périphériques supplémentaires. Cette solution intégrée simplifie le déploiement des fonctions de pare-feu basées sur les rôles

[1] « Magic Quadrant for Enterprise Network Firewalls » de Gartner, par Greg Young, Adam Hils et Jeremy D'Hoinne, 15 avril 2014.

lorsqu'une entreprise n'a pas besoin d'une solution de sécurité complète de bout en bout telle que le service de contrôle d'accès unifié de Juniper.
    - Pour les entreprises cherchant à combiner la sécurité du datacenter et celle de la périphérie du réseau dans une brique unique, AppID fournit une gestion granulaire de la visibilité des applications et du contrôle basée sur la politique de confidentialité de l'entreprise. Ces contrôles permettent d'utiliser AppID pour protéger le trafic en périphérie de réseau, là où c'est nécessaire, sans l'appliquer sur le datacenter, ce qui évite d'ajouter un niveau de complexité inutile.
- **Meilleure protection :**
    - AppID est un moteur heuristique optimisé pour l'identification des applications évasives ou cachées dans d'autres applications (tunnel). Il joue un rôle important dans le blocage des applications à risque, comme celles de Peer-To-Peer, ou dans le contrôle des applications vidéo, sociales et de communication telles que Skype ou BitTorrent. AppID est, par ailleurs, en mesure d'identifier près de deux fois plus d'applications qu'auparavant.
    - Le pare-feu virtuel de Juniper, Firefly Perimeter prend désormais en charge les fonctionnalités des pare-feu de nouvelle génération telles que la prévention des intrusions et la gestion unifiée des menaces. Les utilisateurs de Firefly Perimeter peuvent ainsi ajouter des couches de sécurité à leur réseau pour se prémunir contre les attaques tentant d'exploiter les failles de sécurité des applications, mais aussi contre les logiciels malveillants, les spams et autres menaces orientées sur les contenus.
- **Solution de personnalisation ouverte :**
    - La solution de pare-feu de nouvelle génération de Juniper Networks peut être personnalisée par les clients en fonction de leurs contraintes de sécurité spécifiques. Les signatures AppID et IPS utilisent un langage ouvert permettant aux clients de créer leurs propres signatures, lesquelles ne sont pas forcément stockées dans la base de données standard. Les entreprises ont ainsi la possibilité d'insérer des signatures pour leurs applications personnalisées ou d'ajouter des signatures IPS pour contrer les exploitations qu'elles auraient identifiées. Elles sont alors à même d'exercer un contrôle plus étroit sur le trafic applicatif au sein de leur réseau, tout en étant mieux protégées contre les attaques ciblant ces applications personnalisées. L'ajout de signatures IPS et de signatures pour les applications personnalisées est très fréquent dans les établissements financiers et les administrations.

Témoignages

« Juniper Networks s'engage à fournir aux entreprises les technologies de sécurité leur permettant de déployer la performance, la flexibilité et le contrôle nécessaire pour se prémunir contre les attaques en constante évolution qu'elles rencontrent. Les nouvelles fonctionnalités de nos solutions de nouvelle génération de pare-feu donnent à nos clients plus d'options pour gérer et sécuriser la périphérie de leur réseau, en améliorant le contrôle et l'efficacité. »

- *Nawaf Bitar, senior vice-président et general manager de la business unit Sécurité chez Juniper Networks*

« Pour répondre aux besoins de l'entreprise, les responsables de la sécurité informatique n'ont d'autres choix que de se prémunir contre les cybermenaces, tout en accélérant et en augmentant le retour sur les investissements IT. Les pare-feu de nouvelle génération de Juniper Networks sont conçus pour fournir des solutions efficaces et performantes, avec une entrée de gamme accessible s'adaptant aux exigences de leur environnement. »

- *Sébastien Kher, fondateur et PDG de Nomios France*

Ressources complémentaires

- Passerelles de services SRX de Juniper
- Blog Juniper : Qui est premier ? Qui est second ? Avec la nouvelle génération de pare-feu
- Communauté Juniper.net
- Juniper sur Twitter
- Juniper sur Facebook

A propos de Juniper Networks
Juniper Networks (NYSE : JNPR) propose des solutions de routage, de commutation et de sécurité innovantes. Des datacenters aux équipements grand public, les innovations de Juniper Networks, les logiciels, les processeurs et les systèmes, transforment l'expérience des réseaux et le modèle économique associé. Pour en savoir plus, rendez-vous sur Juniper Networks (www.juniper.net) ou rapprochez-vous de Juniper via Twitter et Facebook.

###

Les déclarations contenues dans le présent communiqué de presse et portant sur les perspectives de Juniper Networks, sur ses produits futurs ainsi que sur les avantages à venir en faveur des clients constituent des déclarations prospectives impliquant un certain nombre d'incertitudes et de risques. Les résultats ou événements réels sont susceptibles de varier significativement par rapport aux résultats et événements anticipés dans ces déclarations prospectives en raison de plusieurs facteurs, parmi lesquels des retards dans la disponibilité prévue des produits, l'incapacité de la société à prévoir avec précision les tendances technologiques émergentes, ainsi que d'autres facteurs énumérés dans les plus récents rapports de Juniper Networks sur formulaire 10-K et formulaire 10-Q, déposés auprès de la Securities and Exchange Commission. Toutes les déclarations formulées dans le présent communiqué de presse ne valent qu'à la date dudit communiqué de presse. Juniper Networks n'est nullement tenue de mettre à jour les informations contenues dans ce communiqué de presse dans le cas où les faits ou circonstances de l'événement évolueraient par la suite, après la date du présent communiqué de presse. Tout produit futur, fonctionnalité, amélioration ou spécification connexe susceptible d'être évoqué(e) dans ce communiqué de presse se destine uniquement à des fins d'information, étant susceptible de changer à tout moment sans préavis, et ne constitue nullement un engagement en faveur de la délivrance de tout produit futur, fonctionnalité, amélioration ou spécification connexe. Les informations contenues dans le présent communiqué de presse ont pour objectif de souligner l'orientation générale des produits de Juniper Networks, et ne sauraient fonder la prise d'une décision d'achat.