Juniper Networks | Engineering Simplicity

TechTarget | Custom Media White Paper

Cinq incontournables des solutions SD-WAN de nouvelle génération

AVANT-PROPOS

Chaque entreprise dépend d'Internet. Le problème, c'est que le réseau n'a jamais été conçu pour assurer la sécurité des environnements applicatifs actuels. Au départ, les systèmes Internet hôtes partageaient sans souci des fichiers et des informations avec tous les appareils connectés. Et il n'y avait quasiment aucun protocole de sécurité.

Résultat : aujourd'hui, Internet regorge de cybercriminels qui mettent tout en œuvre pour accéder à des informations protégées, exfiltrer des données sensibles, et infecter les systèmes avec des malwares et des ransomwares afin de paralyser les entreprises.

Ce document revient sur l'évolution des SD-WAN (Software-Defined Wide-Area Network) de première génération et sur les éléments à prendre en compte pour évaluer les offres de nouvelle génération qui permettent de sécuriser les réseaux de demain.

Problématiques du SD-WAN

Les SD-WAN ont parcouru un long chemin depuis leur apparition au début du 21e siècle. Ainsi, deux catégories d'utilisateurs doivent désormais mettre le réseau à niveau.. La première concerne les primo-adoptants du SD-WAN, qui reconnaissent l'impact positif de cette technologie, mais se heurtent désormais aux limites des produits de première génération. La seconde rassemble les nombreuses grandes entreprises qui ne sont toujours pas passées aux environnements SD-WAN et continuent de s'appuyer sur des modèles WAN traditionnels plus statiques.

Au fil du temps, ces entreprises ont créé un véritable patchwork pour sécuriser leur réseau. Face aux menaces émergentes, elles utilisent une multitude de tunnels et des réseaux privés virtuels (VPN), et s'appuient sur de nombreuses solutions spécialisées pour chaque composant de sécurité. Or, une telle approche oblige souvent les équipes IT et NOC (Network Operations Center) à jongler entre plusieurs consoles pour gérer la sécurité des workloads LAN, WAN et cloud. En outre, la sécurité est souvent ajoutée après la conception du réseau, ce qui nuit aux performances des applications et à l'expérience utilisateur. Pire, les entreprises sont la cible d'un nombre toujours croissant de compromissions et d'attaques par malwares capables de paralyser leur activité, voire toute une économie.

Le routage réseau doit évoluer

La plupart des protocoles et méthodologies de routage existants sont basés sur une technologie vieille de plusieurs décennies, dont les inconvénients deviennent chaque jour plus apparents. Quelques exemples :

- Les architectures « hub-and-spoke » ne tiennent pas face aux nouveaux workloads dynamiques et aux flux massifs de données, générés par le cloud et les applications SaaS.
- Les architectes réseau peinent à fournir des accords de niveau de service (SLA) centrés sur les applications qui répondent aux demandes des utilisateurs.
- Beaucoup d'entreprises doivent jongler avec un mix d'appareils et de produits de sécurité spécialisés (routeurs, pare-feu, systèmes IPS, appliances VPN, etc.), ce qui ne fait qu'ajouter aux problématiques opérationnelles et logistiques.

Les SD-WAN d'ancienne génération sont clairement devenus inefficaces et coûteux.

Les SD-WAN d'ancienne génération sont clairement devenus inefficaces et coûteux. Bien qu'ils contribuent à résoudre certains problèmes de gestion, ils sont limités par un manque de service garanti pour les flux de données individuels, une visibilité insuffisante sur les sessions réseau et les données d'application, sans parler du coût élevé des tunnels VPN (IPsec par exemple) qui monopolisent une bande passante précieuse.

Une refonte du routage s'impose. Pourtant, les entreprises frémissent à l'idée d'effectuer une mise à niveau globale qui exige de faire table rase de l'existant afin d'adopter les avantages du SD-WAN nouvelle génération.

L'immobilisme multiplie les risques

Les demandes métier en constante évolution exercent au quotidien une pression croissante sur les équipes IT. Exemples de problématiques :

- Les initiatives de transformation numérique continuent d'augmenter le nombre d'utilisateurs et la quantité de données sur le réseau.
- La multiplication des appareils utilisés pour accéder aux ressources de l'entreprise et aux applications cloud élargit la surface d'attaque.
- La pénurie de compétences technologiques oblige les équipes en place à faire plus avec moins.

Ces demandes croissantes concernent tous les secteurs, avec le même constat : si le réseau ne peut pas suivre, c'est l'expérience client qui en pâtit. Un WAN ne se contente plus d'assurer la connectivité et l'envoi de paquets ; il doit offrir une expérience adéquate aux utilisateurs, où qu'ils se trouvent et quel que soit l'appareil qu'ils utilisent.

Si le réseau ne peut pas s'auto-réparer, ou au moins s'auto-diagnostiquer, l'IT et le NOC seront à jamais condamnés à jouer les équilibristes et à être pointés du doigt en cas de problèmes ou de compromission.

Verdict : un WAN obsolète peut véritablement entraver la compétitivité d'une entreprise.

SD-WAN nouvelle génération : ce que veulent les entreprises

Une manière de résoudre ces problématiques consiste à adopter des solutions SD-WAN nouvelle génération. Ces dernières vous permettent de vous débarrasser d'une grande partie des produits spécialisés d'ancienne génération,, et offrent une évolutivité et une flexibilité à la hauteur des exigences des plus grandes entreprises.

Pour choisir un SD-WAN nouvelle génération, il faut prendre en compte cinq facteurs clés et exiger certaines fonctionnalités :

1. Architecture basée sur les sessions – Ce type d'architecture crée une fabric de routage intelligente basée sur les besoins uniques de chaque session. À la clé : une meilleure visibilité tant sur l'expérience des utilisateurs que sur les performances du réseau.
2. Réseau Zero Trust – Il est temps pour chaque entreprise de passer d'une « confiance généralisée » à une « confiance zéro ».
3. AIOps – La possibilité d'automatiser et d'orchestrer le réseau permet aux entreprises de résoudre les problèmes avant qu'ils n'affectent les opérations ou n'entraînent une perte de données.
4. Réseau sans tunnel – Une telle configuration élimine les VPN et les tunnels IPsec qui monopolisent les ressources.
5. Secure Access Service Edge (SASE) – Les critères d'une architecture SASE (politiques et gestion de la sécurité simples et centralisées, accès basé sur les rôles, etc.) permettent de garantir des performances et une sécurité optimales pour des collaborateurs de plus en plus mobiles.

Toutes ces fonctionnalités, et bien plus, sont rassemblées dans le SD-WAN Session Smart™ de

Juniper.

La différence Session Smart™

Pourquoi Session Smart™ ? Garantir la meilleure expérience réseau possible est indispensable à la réussite de toute entreprise. Un réseau Session Smart™ est le seul capable de combiner l'intelligence, la visibilité et la simplicité nécessaires pour répondre aux exigences strictes de performances et de sécurité des environnements actuels et futurs. Les réseaux Session Smart™ sont basés sur les utilisateurs et contextualisent les données pour offrir un contrôle précis des SLA de sécurité et de performances.

Basés sur un modèle Zero Trust pour garantir les plus hauts niveaux de sécurité, les réseaux SD-WAN Session Smart™ utilisent le Secure Vector Routing (SVR), un concept innovant qui fournit tous les éléments attendus d'un tunnel IPsec sans ses inconvénients (surcharge des en-têtes de paquets, par exemple). Ainsi, tout en réduisant l'encombrement du réseau et en améliorant la bande passante, un tel réseau offre une meilleure visibilité sur chaque flux de trafic et permet de surveiller de bout en bout la qualité de chaque connexion. La sécurité et les performances sont, quant à elles, renforcées par le chiffrement adaptatif, un moyen plus intelligent d'assurer la sécurité tout en améliorant l'expérience utilisateur. Après tout, puisque 90 % du trafic global est déjà chiffré, pourquoi le chiffrer deux fois ?

Parce que ces innovations garantissent des expériences utilisateur de haute qualité et répondent aux normes de conformité internationales, les clients à la recherche d'une solution SD-WAN qui satisfait aux critères SASE n'ont pas besoin de chercher plus loin. (Le SASE est une architecture de cybersécurité moderne conçue pour fournir des services de sécurité plus proches des utilisateurs et leur apporter un niveau d'accès approprié basé sur leur niveau de risque à un moment précis.)

Le SD-WAN Session Smart™ est entièrement logiciel et fonctionne en conjonction avec l'infrastructure déjà en place chez les clients, ce qui permet une transition sans interruption et sans mise à niveau majeure. Une approche logicielle basée sur les sessions contribue également à réduire la complexité en périphérie en stoppant la prolifération de solutions intermédiaires telles que les équilibreurs de charge, les routeurs et la protection anti-DDos. Au lieu de cela, ces fonctionnalités sont regroupées dans un seul routeur Session Smart™ et s'exécutent dans le cadre du SD-WAN sur n'importe quelle plateforme matérielle standard. Elles concourent ainsi à garantir les performances, qu'elles soient déployées sur une machine virtuelle, un serveur whitebox, ou dans le cloud sur Azure ou Amazon Web Services.

Dans de nombreux cas, un routeur Session Smart™ (qui intègre pare-feu L3 et L4 et une protection Zero Trust) placé en périphérie est plus que suffisant d'un point de vue de la sécurité.. Cela réduit le besoin de déployer sur chaque site des pare-feu physiques nouvelle génération coûteux et

potentiellement nuisibles pour les performances.

Avantages d'un SD-WAN Session Smart™ :

- Utilisation de la bande passante 50 % plus efficace en moyenne
- Évolutivité massive (jusqu'à plus de 10 000 sites)
- Pare-feu sur les couches L3 et L4 avec filtrage de paquets, IDP/IPS, protection anti-DoS, DPI, filtrage d'URL, etc.
- Modèle Zero Trust de rejet par défaut
- Surveillance continue des chemins pour déterminer les meilleurs itinéraires disponibles et assurer une expérience utilisateur optimale
- Détection et analyse des utilisateurs et applications sur le réseau ; routage intelligent des sessions conformément à des SLA de performances et de sécurité facilement configurables
- Élimination de l'effet « trombone » ou « hairpin » causé par une redirection de tout le trafic vers le datacenter, et susceptible de ralentir les performances et dégrader l'expérience utilisateur

Les tunnels IPsec et les VPN ne peuvent pas évoluer indéfiniment et connaissent souvent des défaillances lorsque la demande augmente. Avec son architecture sans tunnel qui n'est limitée ni en taille ni en portée sur le LAN, le WAN, le cloud ou l'IoT, un SD-WAN Session Smart™ permet de faire évoluer les réseaux et la sécurité de manière simple et économique, même dans les plus grandes entreprises.

Des niveaux de services personnalisables permettent aux équipes IT de cerner immédiatement l'impact du WAN sur l'expérience utilisateur.

L'expérience, nouveau mot d'ordre du réseau

En introduisant le SD-WAN Session Smart™ dans son portefeuille riche et croissant de solutions (incluant les récentes acquisitions de 128 Technology, d'Apstra et de Netrounds), Juniper concrétise sa vision du réseau complet, de bout en bout et du client jusqu'au cloud. La stratégie est claire : après la disponibilité, c'est désormais l'expérience qu'il faut surveiller.

Les données de télémétrie collectées au niveau des utilisateurs et des applications par le routeur Session Smart™ sont transmises à Mist WAN Assurance et à Marvis, un assistant réseau virtuel optimisé par l'IA. Les équipes IT bénéficient ainsi des insights nécessaires à une résolution proactive des problèmes. Des niveaux de services personnalisables leur permettent également de cerner immédiatement l'impact du WAN sur l'expérience utilisateur. Enfin, l'IA Mist et Marvis effectuent des corrélations sur l'ensemble des réseaux sans fil, filaires et WAN pour favoriser une expérience unique, sans interruption et optimisée dans toute l'entreprise, pour les utilisateurs et les opérateurs.

Prochaines étapes

Le routeur Session Smart™ de Juniper alimente une solution réseau avancée et orientée services qui fait franchir un nouveau cap au routage défini par logiciel. Idéal pour les entreprises numériques d'aujourd'hui, le routeur Session Smart™ permet une connectivité WAN agile, sécurisée et résiliente, avec à la clé des économies et une simplicité exceptionnelles. Pour en savoir plus, rendez-vous sur : https://www.juniper.net/fr/fr

À propos de Juniper Networks

Juniper Networks simplifie les réseaux avec des produits, des solutions et des services qui connectent le monde. Nos capacités d'innovation nous permettent d'écarter les obstacles et de briser la complexité des réseaux à l'ère du cloud pour éliminer les difficultés que connaissent nos clients et partenaires au quotidien. Pour Juniper Networks, le réseau est un moyen de partager des connaissances et de favoriser un progrès au service de l'humain. Pour cela, nous déployons beaucoup d'efforts pour concevoir des réseaux automatisés, évolutifs et sécurisés, capables d'évoluer au rythme des entreprises.

Siège social et commercial
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : +1 888 586 4737
ou +1 408 745 2000
Fax : +1 408 745 2100
www.juniper.net/fr/fr/

Siège EMEA et APAC
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 0 207 125 700
Fax : +31 0 207 125 701

Juniper Networks | Engineering Simplicity

Ce document a été rédigé par TechTarget Inc. à la demande de Juniper Networks.