



CINQ RAISONS D'ADOPTER LES PARE-FEU DE NOUVELLE GÉNÉRATION SRX300

Sécurisez tous les points de votre réseau pour protéger les utilisateurs, les applications et l'infrastructure.

Problématique

Les clients recourant à des pare-feu obsolètes exposent l'ensemble de leur entreprise à un très grand risque de cyberattaque.

Solution

En adoptant la nouvelle gamme de passerelles de services Juniper SRX300, les entreprises peuvent renforcer leur protection face aux attaques les plus avancées.

Avantages

- Identifiez et bloquez les menaces en temps réel avec une sécurité de pointe
- Consolidez la sécurité et le réseau sur une seule et même plateforme
- Simplifiez les opérations de sécurité pour résoudre plus rapidement les problèmes signalés
- Limitez les perturbations des opérations de sécurité

À en croire le flot incessant de révélations sur les piratages informatiques, la cybersécurité est plus que jamais un sujet d'actualité. Le Forum économique mondial estime ainsi que les cyberattaques sont la rançon de notre cyberdépendance croissante. D'après eux, la menace d'un vol ou d'une compromission de données de grande ampleur figure parmi les cinq grands défis de notre époque.¹ C'est pourquoi les entreprises doivent apprendre à détecter, isoler et contrer les cybermenaces pour éviter toute fuite de données ou infraction à la réglementation.

La problématique

À l'ère du mobile, du cloud et de l'IoT, le vieux modèle de sécurité périmétrique ne suffit plus à protéger votre entreprise. Hormis la sophistication et la prolifération éclair des cybermenaces, votre surface d'attaque a aussi augmenté de manière significative. Les infrastructures de sécurité d'ancienne génération ne parviennent plus à tenir le rythme face à des réseaux à très haut débit et des attaques furtives qui sévissent au quotidien. Et les anciens pare-feu et solutions vieillissantes ne font qu'aggraver le problème. Non seulement ils créent des brèches exploitables par des attaquants en tout genre (cybermafias, acteurs étatiques, etc.), mais leur complexité et leur maintenance laborieuse peuvent également éroder l'efficacité opérationnelle des équipes de sécurité et détourner les talents de missions plus stratégiques.

Migrer vers la nouvelle génération de pare-feu avec Juniper Networks

Les entreprises équipées de pare-feu d'ancienne génération peuvent facilement migrer vers la gamme de passerelles de services SRX300 de Juniper Networks® pour bénéficier d'une protection intégrale et simplifiée. Les clients peuvent opter pour les modèles SRX300, SRX320, SRX340 et SRX345, tous équipés de fonctionnalités réseau, SD-WAN, de sauvegarde LTE et de sécurité avancée, sur une seule et même plateforme. Idéales pour les sites distants et les infrastructures distribuées, les passerelles de services SRX Series facilitent votre migration. Vous pouvez ainsi bénéficier de l'expertise et des processus de sécurité Juniper, moderniser rapidement votre réseau et déployer des pare-feu complets conçus pour lutter contre les menaces avancées.

Cinq raisons d'adopter les pare-feu de nouvelle génération SRX300

Qui dit pare-feu dépassés, dit risques de sécurité. En migrant vers les toutes dernières passerelles de services SRX300, vous renforcez la sécurité de votre entreprise.

¹The Global Risks Report : 2018, Forum économique mondial, http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

En fait, il existe cinq bonnes raisons d'adopter la nouvelle gamme SRX300 pour protéger votre entreprise distribuée. Découvrons-les une à une.

- 1. Cybersécurité avancée et simplifiée.** Les passerelles SRX300 agissent comme un point de contrôle essentiel sur la plateforme Juniper de sécurité connectée, ce qui non seulement simplifie les opérations mais protège aussi les utilisateurs, les applications et l'infrastructure. Associée à Juniper Sky™ Advanced Threat Prevention (ATP), SRX300 détecte les ransomwares et autres malwares furtifs tout en adaptant continuellement vos cyber-défenses à des risques en perpétuelle mutation. La gestion et le contrôle automatiques des politiques utilisent des données sur le réseau et les menaces pour mettre à jour les politiques et unifier leur mise en application sur toute l'infrastructure.
- 2. Prévention en temps réel.** L'intégration des passerelles de services SRX300 à Juniper Sky ATP dote votre entreprise d'une nouvelle couche de protection qui détecte et bloque les malwares inconnus avant qu'ils n'atteignent leur cible. Juniper Sky ATP s'appuie sur une technologie de machine learning, alimentée par des informations temps réel issues du cloud, pour analyser en continu les fichiers web et e-mail à la recherche de ransomwares ou autres menaces furtives. Cette intégration permet aux pare-feu SRX300 d'assurer des analyses approfondies, un blocage inline et des alertes immédiatement exploitables.
- 3. Sécurité renforcée, expertise opérationnelle préservée.** La gamme SRX300 propose la sécurité la plus puissante du marché pour les entreprises distribuées. En migrant vers les toutes dernières plateformes de nouvelle génération, votre entreprise capitalise sur son expertise opérationnelle de la sécurité Juniper tout en profitant de la puissance et de la performance de la dernière version du système d'exploitation Juniper Networks Junos®. En clair, vos équipes réseau et sécurité n'ont pas à se former sur un nouvel OS, ce qui non seulement améliore leur efficacité opérationnelle mais leur permet aussi de se consacrer à des missions d'innovation.
- 4. Déploiements pour entreprises distribuées.** Les entreprises ont besoin d'une plateforme combinant des fonctionnalités de sécurité et de SD-WAN pour sites distants et distribués à des fonctions ZTP (Zero Touch Provisioning), de qualité de l'expérience (QoE) et de routage basé sur les applications.
- 5. Routage sécurisé.** Afin d'offrir la plus grande connectivité WAN possible, la gamme de passerelles de services SRX300 intègre des ports de fibre optique et de Media Access Control Security (MACsec), et gère les sauvegardes LTE sans fil. Vous répondez ainsi aux différents besoins de connexion pour vos sites distants et distribués.

Choisir le bon pare-feu SRX300

La gamme de passerelles de services SRX300 a été conçue pour répondre à tous les besoins des entreprises distribuées. Les clients utilisant des pare-feu Juniper d'ancienne génération peuvent déployer les modèles SRX300 suivants pour migrer vers les technologies de pare-feu nouvelle génération. Quelques exemples :

- Si vous utilisez le SSG-5 ou le SRX100, vous pouvez migrer vers le SRX300.
- Si vous utilisez le SSG-20 ou le SRX210/SRX220, vous pouvez migrer vers le SRX320.
- Si vous utilisez le SSG-140 ou le SRX240, vous pouvez migrer vers le SRX340 ou SRX345.

Idéale pour sécuriser les magasins ou sites distants de petite taille, la gamme SRX300 offre sécurité, routage, SD-WAN et connectivité WAN, le tout sur un équipement de bureau compact. Le pare-feu SRX320 assure la sécurité et la connectivité des sites distribués de petite taille. Il s'appuie pour cela sur des fonctionnalités de sécurité, de routage, de SD-WAN et de connectivité WAN sur un petit appareil de bureau équipé de ports Ethernet PoE+ en option. Le SRX340 sécurise la connectivité des sites distribués de taille moyenne en consolidant protection, routage, SD-WAN et connectivité WAN dans un format 1U. Il propose également des options de gestion unifiée des menaces (UTM) et de sauvegarde LTE sans fil pour une sécurité renforcée et une sauvegarde WAN assurée pour chaque site. Enfin, les passerelles de services SRX345, plus adaptées aux sites distants de taille moyenne à grande, regroupent des fonctions de sécurité, de routage, de SD-WAN et de connectivité WAN dans un format 1U. Elles affichent des débits de pare-feu de 5 Gbits/s et des débits VPN IPsec de 800 Mbits/s.



SRX300



SRX320



SRX340



SRX345

Synthèse – Une cybersécurité simplifiée et renforcée

Face à un paysage de la cybersécurité de plus en plus complexe, les pare-feu d'ancienne génération ne peuvent plus protéger les entreprises contre les vols et compromissions de données. Avec la plateforme de sécurité connectée de Juniper et la gamme de passerelles de services SRX300, vous pouvez simplifier et renforcer considérablement votre sécurité en rationalisant l'intégration de défenses adaptées à votre écosystème.

Prochaines étapes

Retrouvez toute la gamme SRX300 de pare-feu de nouvelle génération sur notre site www.juniper.net/us/en/products-services/security/srx-series/srx300/.

Pour en savoir plus sur les parcours de migration vers SRX300, contactez votre conseiller Juniper Networks.

À propos de Juniper Networks

Juniper Networks simplifie le réseau grâce à des produits, solutions et 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 inventons des méthodes de conception de 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
<https://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

