

PARE-FEU VIRTUEL VSRX DE JUNIPER NETWORKS POUR GOOGLE

Présentation du produit

Le pare-feu virtuel vSRX de Juniper Networks offre un pare-feu virtuel cloud-native complet pour Google Cloud Platform™, avec une sécurité avancée et une sécurité pare-feu SD-WAN, mise en réseau robuste et gestion automatisée du cycle de vie des machines virtuelles pour les fournisseurs de services et les entreprises. Pour activer une version d'essai du vSRX pour Google Cloud Platform, rendez-vous sur le [marché GCP™](#).

Description du produit

À mesure que les charges de travail migrent vers le cloud public, elles posent des défis pour sécuriser les données et la communication entre les charges de travail exécutées dans le cloud et d'autres emplacements.

Les professionnels du réseau et de la sécurité doivent effectuer un acte d'équilibrage délicat, en offrant les avantages des technologies cloud sans compromettre la sécurité de l'organisation. Ce défi ne peut être relevé que par une solution qui suit le rythme des menaces en constante évolution tout en répondant à l'agilité et à l'évolutivité des environnements cloud, sans sacrifier la fiabilité, la visibilité et le contrôle.

HPE Juniper Networking relève ces défis de front en étendant les fonctionnalités des pare-feu primés [Juniper Networks SRX Series](#) en tant que pare-feu virtuel cloud-native pour Google Cloud Platform (GCP), permettant aux professionnels de la sécurité de déployer et de faire évoluer la protection par pare-feu pour les charges de travail exécutées dans GCP. Le pare-feu virtuel vSRX de Juniper Networks offre une sécurité pare-feu (NGFW) de nouvelle génération inégalée qui comprend un système de prévention des intrusions (IPS), une protection contre les logiciels malveillants, un contrôle des applications et une détection des menaces à la demande. [pare-feu](#) Le vSRX prend également en charge les communications sécurisées avec le SD-WAN, les réseaux virtuels GCP et le SD-LAN pour une segmentation sécurisée entre les charges de travail.

Les fonctionnalités de provisionnement automatisé vSRX pour GCP permettent aux administrateurs réseau et de sécurité de provisionner et de faire évoluer rapidement et efficacement la protection par pare-feu pour répondre aux besoins dynamiques des environnements cloud. En combinant le vSRX avec la puissance de [Junos Space Security Director](#) ou Contrail® Service Orchestration, les administrateurs peuvent améliorer considérablement la configuration, la gestion et la visibilité des politiques sur les actifs physiques et virtuels à partir d'une plateforme centralisée commune.

HPE s'engage à aider ses clients à réaliser la valeur de leurs investissements existants et s'est engagée à interopérabilité pour tous ses pare-feu SRX Series. Outre Security Director et Contrail Service Orchestration, le vSRX prend en charge OpenContrail et d'autres solutions de gestion tierces. Le vSRX peut également s'intégrer à d'autres outils d'orchestration cloud de nouvelle génération tels qu'OpenStack, directement ou via des API riches.

Outre les cas d'utilisation de cloud public et de virtualisation traditionnelle, le vSRX permet aux fournisseurs de services et aux entreprises de déployer une fabric SD-WAN sécurisée avec des défenses de périphérie. La fabric SD-WAN sécurisée s'adapte aux besoins individuels de n'importe quel site tout en offrant la flexibilité nécessaire pour défendre les applications virtualisées et orientées services partout où elles existent sur le réseau.

Security Director peut gérer jusqu'à 25 000 Les pare-feu SRX Series, qu'ils soient physiques, virtuels, ou conteneurisés, à partir d'une seule instance de gestion. Cet outil permet aux organisations de gérer, d'automatiser et d'orchestrer la sécurité réseau, la virtualisation et l'interconnectivité du point de terminaison à l'edge et à tous les clouds intermédiaires, à partir d'une plateforme unique.

Le pare-feu virtuel vSRX peut également utiliser plusieurs options de connectivité pour connecter les sites en toute sécurité. Qu'elle soit virtuelle ou physique à la fabric WAN de l'entreprise, l'extension de la connectivité sécurisée à d'autres datacenters (comme la collocation de déploiements cloud tiers) peut nécessiter de communiquer avec les charges de travail cloud.

SD-WAN sécurisé

Pour accéder aux applications hébergées dans Google Cloud, les succursales exploitent traditionnellement les connexions via les sites de campus d'entreprise pour accéder aux applications GCP. Dans cette situation, le SD-WAN sécurisé peut être déployé dans l'agence et utiliser vSRX on GCP pour activer une solution plus optimisée pour la connectivité qui va directement à GCP, évitant ainsi la nécessité d'accéder aux applications cloud via le réseau du campus.

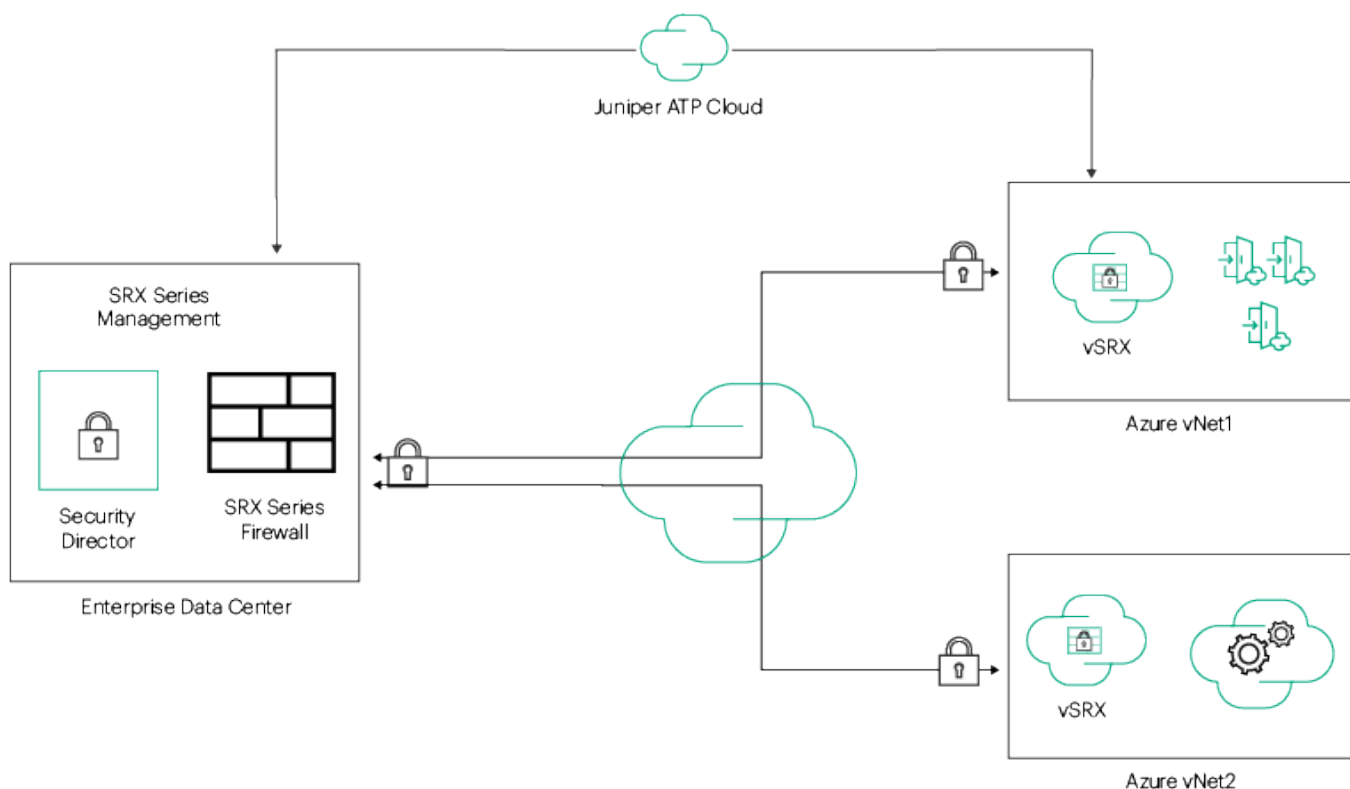


Figure 1. vSRX pour sécuriser les charges de travail dans GCP

Architecture et composants clés

Connectivité sécurisée

Le vSRX sur GCP peut sécuriser les communications entre les charges de travail exécutées sur différents réseaux virtuels et/ou un datacenter sur site. La fonctionnalité VPN vSRX permet une connectivité sécurisée entre l'appariement de réseau virtuel dans la même région GCP et l'appariement de réseau virtuel global entre les régions GCP. La fonctionnalité VPN permet au vSRX d'offrir une connectivité sécurisée entre les réseaux virtuels GCP sans envoyer de flux de données sur Internet, ce qui minimise les problèmes de coût, de latence et de disponibilité.

Un vSRX déployé dans GCP peut agir comme un hub SD-WAN, prenant en charge un accès sécurisé entre les campus et les succursales et GCP directement dans le cadre d'un déploiement SD-WAN plus important. Il peut également servir de hub SD-WAN, où il fournit un accès sécurisé aux ressources cloud hébergées dans GCP, devenant ainsi le point central des sessions Internet régionales. Ce point central permet au vSRX sur GCP de sécuriser les charges de travail et de fournir une connectivité SD-WAN sécurisée qui s'adapte à l'évolution des besoins de l'entreprise.

Protection des charges de travail

Les pare-feu protègent les charges de travail, mais tous les pare-feu ne sont pas créés égaux. Avec vSRX on GCP, les clients peuvent s'assurer que les politiques sont déployées de manière cohérente sur l'ensemble de leur réseau, que ces charges de travail fonctionnent sur site, dans le cloud public ou à l'edge. Les clients qui utilisent déjà des pare-feu SRX Series sur leurs réseaux peuvent facilement étendre ces politiques à n'importe quel pare-feu virtuel vSRX fonctionnant dans le cloud public ou ailleurs.

Le vSRX prend en charge la création et le déploiement de politiques de pare-feux à l'aide de balises de métadonnées, facilitant ainsi l'automatisation de la sécurité et réduisant le nombre de règles requises lors de la mise en œuvre initiale ou de la maintenance continue. Ces métadonnées offrent aux administrateurs de sécurité une meilleure visibilité en fournissant une vue réseau complète basée sur les balises de métadonnées, ce qui signifie qu'elles ne sont plus limitées à la gestion et au filtrage des règles basées sur l'adresse IP.

En plus de l'application des politiques, le vSRX fournit des services de sécurité avancés, notamment IPS, antivirus et antimalware, pour identifier et bloquer les menaces avancées ciblant les charges de travail hébergées dans le cloud GCP.

Segmentation des charges de travail

Le vSRX peut sécuriser la communication et assurer la segmentation de la charge de travail sur GCP en appliquant des politiques concernant les communications qui doivent être autorisées entre les segments de charge de travail. Le vSRX facilite la segmentation et le contrôle granulaires du réseau en appliquant des politiques de sécurité au niveau de la charge de travail virtualisée. Du point de vue de la sécurité, plus le niveau de blocage de la menace est granulaire, plus le confinement de la propagation de la menace est efficace.

Caractéristiques et avantages

Services de sécurité avancés

La mise en œuvre de systèmes hérités non intégrés construits autour de pare-feu traditionnels et d'appliances et de logiciels autonomes individuels ne suffit plus pour se protéger contre les attaques sophistiquées d'aujourd'hui.

La suite de sécurité avancée HPE permet aux utilisateurs de déployer plusieurs technologies pour répondre aux besoins uniques et évolutifs des organisations modernes et du paysage des menaces en constante évolution. Les mises à jour en temps réel garantissent que les technologies, les politiques et les autres mesures de sécurité sont toujours à jour.

Le vSRX for GCP fournit un ensemble polyvalent et puissant de services de sécurité avancés, notamment l'IPS, la protection contre les logiciels malveillants, le contrôle des applications et la sécurité du contenu.

Système de prévention des intrusions

L'IPS pour vSRX pour GCP contrôle l'accès aux réseaux informatiques, protégeant les systèmes en inspectant les données et en prenant des mesures telles que le blocage des attaques au fur et à mesure qu'elles se développent ou la création d'une série de règles dans le pare-feu. IPS intègre étroitement les fonctionnalités de sécurité des applications HPE à l'infrastructure réseau pour atténuer davantage les menaces et se défendre contre un large éventail d'attaques et de vulnérabilités.

Juniper Advanced Threat Prevention

[Juniper® Advanced Threat Prevention](#) s'intègre au vSRX for GCP pour fournir une protection dynamique et automatisée contre les logiciels malveillants connus et les menaces zero-day avancées, ce qui entraîne des réponses quasi instantanées.

Visibilité et contrôle des applications avec AppSecure Juniper Secure Connect

Juniper Networks AppSecure est une suite de sécurité des applications de nouvelle génération, offrant visibilité, protection, application et contrôle des menaces. Cette fonctionnalité en option offre une visibilité puissante et un suivi continu des applications. Avec des signatures ouvertes, des ensembles d'applications uniques peuvent être surveillés, mesurés et contrôlés pour s'aligner étroitement sur les priorités commerciales de l'organisation.

[Juniper Secure Connect](#) est une application VPN SSL hautement flexible qui fournit un accès sécurisé aux ressources de l'entreprise et du cloud aux employés qui s'éloignent des ressources protégées. Cette application VPN SSL est disponible pour les systèmes d'exploitation les plus courants. Il offre une connectivité adaptable à n'importe quel appareil, où qu'il soit, réduisant les risques en étendant la visibilité et l'application des règles des utilisateurs au cloud.

Sécurité du contenu

Le vSRX pour GCP comprend une sécurité complète du contenu contre les logiciels malveillants, les virus, les attaques de phishing, les spams et d'autres menaces avec les meilleures fonctionnalités antivirus, antispam, de filtrage Web et de filtrage de contenu.

Tableau 1. Fonctionnalités et avantages de vSRX pour GCP

| Fonctionnalité | Description du service | Avantage |
|---|--|---|
| Prise en charge matérielle évolutive | Vous permet de démarrer avec 2 cœurs de processeur et 7,5 Go de mémoire, et d'évoluer jusqu'à 16 cœurs et 60 Go de mémoire | Fournit une empreinte matérielle flexible et évolutive pour répondre à vos besoins actuels et futurs, à mesure que le trafic augmente |
| Licence flexible | Prend en charge le paiement à l'utilisation (PAYG) et options d'apport de licence (BYOL) | Fournit des options flexibles de licence et d'achat pour sécuriser les charges de travail dans GCP et la connectivité entre votre datacenter et GCP |

Spécifications

Tableau 2. vSRX sur les types d'instances GCP

| Type d'instance GCP | vCPU dans le type d'instance | Mémoire dans le type d'instance (Go) |
|---------------------|------------------------------|--------------------------------------|
| N1-standard-2 | 2 | 7,5 |
| N1-standard-4 | 4 | 15 |
| N1-standard-8 | 8 | 30 |
| N1-standard-16 | 16 | 60 |

Pour obtenir la liste complète des types d'instance Azure pris en charge, rendez-vous sur juniper.net/documentation/en_US/vsrx/topics/topic-map/security-vsrx-google-system-requirements.html.

Informations de commande

Pour plus d'informations sur le pare-feu virtuel vSRX BYOL de Juniper Networks pour GCP, rendez-vous sur juniper.net/us/en/productsservices/security/srx-series/vsrx ou contactez votre représentant commercial HPE.

Pour activer une version d'essai du vSRX pour GCP, rendez-vous sur GCP Marketplace à l'adresse console.cloud.google.com/marketplace/details/juniper-marketplace/vsrx-next-generation-firewall?q=vsrx&id=de0a15a3-968e-4bed-8eca-e892b06e8701.

| Produit | Description |
|---|--|
| Pare-feu virtuel vSRX | <ul style="list-style-type: none">— pare-feux central avec VPN IPSec, traduction d'adresses réseau (NAT), coût de service et services de routage enrichis— AppSecure avec AppID, AppFW, AppQoS et AppTrack— Services de sécurité de contenu incluant IPS |
| Pare-feu virtuel vSRX avec protection anti-virus | <ul style="list-style-type: none">— Fonctionnalités de pare-feux de base, VPN IPSec, NAT, coût de service et services de routage enrichis— AppSecure avec AppID, AppFW, AppQoS et AppTrack— Services de sécurité de contenu, notamment IPS, antivirus, anti-spam, web et filtrage de contenu |

À propos de HPE

HPE est un leader en matière de technologie d'entreprise essentielle, combinant la puissance de l'IA, du cloud et du réseau pour aider les organisations à atteindre davantage. En tant que pionniers de la possibilité, notre innovation et notre expertise font progresser la façon dont les gens vivent et travaillent. Nous permettons à nos clients de tous les secteurs d'optimiser les performances opérationnelles, de transformer les données en prévisions et d'optimiser leur impact. Libérez vos ambitions les plus audacieuses avec HPE. Pour en savoir plus, rendez-vous sur [HPE.com](https://www.hpe.com).

Clause de non-responsabilité : Cette fiche technique a été traduite par une machine à l'aide de l'intelligence artificielle en allemand/français/italien/espagnol/japonais/coréen pour votre information. Notez que cette traduction n'a pas fait l'objet d'une révision ni d'une vérification par des traducteurs humains. Il se peut par conséquent, qu'elle comporte des erreurs ou de légères distorsions par rapport au texte d'origine. Pour obtenir des informations plus précises et plus fiables, veuillez vous référer à la version en anglais de la fiche technique.

Visiter [HPE.com](https://www.hpe.com)

Live Chat

© Copyright 2025 Hewlett Packard Enterprise Development LP. Les informations figurant dans ce document sont susceptibles d'être modifiées sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune partie du présent document ne saurait être interprétée comme offrant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité en cas d'erreurs ou d'omissions de nature technique ou rédactionnelle dans le présent document.

GCP et Google Cloud Platform sont des marques déposées de Google LLC. Azure est une marque commerciale ou déposée de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Toutes les marques de tiers sont la propriété de leurs propriétaires respectifs.

a00151271FRE, Rév. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

