



SRX4100



SRX4200

# Fiche technique du pare-feux SRX4100 et SRX4200

## Description du produit

Les SRX4100 et SRX4200 de Juniper Networks sont des pare-feu haute performance de nouvelle génération (NGFW) avec accélération matérielle qui protègent les réseaux de datacenter critiques, les campus d'entreprise et le siège régional. Les SRX4100 et SRX4200 font partie intégrante du cadre [de sécurité connecté de Juniper](#), qui étend la sécurité à chaque point de connexion du réseau pour protéger les utilisateurs, les données et l'infrastructure contre les menaces avancées.

Les SRX4100 et SRX4200 intègrent la mise en réseau et la sécurité dans une seule plateforme pour offrir une prévention des intrusions et une protection contre les logiciels malveillants de pointe avec un débit haute performance, un VPN IPsec et une gestion facile des politiques pour sécuriser le réseau de manière fiable. L'identification et la classification avancées des applications permettent une meilleure visibilité, application, contrôle et protection du trafic réseau, de l'accès aux applications et des données. Ces NGFW fournissent des analyses détaillées du volume et de l'utilisation des applications, des politiques de contrôle des applications précises et une hiérarchisation du trafic basée sur les informations et le contexte des applications afin de réduire la complexité des réseaux de cloud traditionnel, cloud et hybride.

Les pare-feu SRX4100 et SRX4200 offrent une automatisation complète aux entreprises et aux fournisseurs de services. Leurs hautes performances et leur évolutivité permettent aux SRX4100 et SRX4200 d'agir comme des hubs VPN, mettant fin aux connexions VPN/overlay sécurisées dans diverses topologies [SD-WAN](#).



Les pare-feu SRX4100 et SRX4200 sont gérés par [Juniper Security Director Cloud](#), une expérience de gestion unifiée qui connecte les déploiements actuels de l'organisation aux futurs déploiements architecturaux. Security Director Cloud utilise un cadre à politique unique permettant des politiques de sécurité cohérentes dans n'importe quel environnement tout en étendant le zero trust à toutes les parties du réseau, de l'edge au datacenter. Vous bénéficiez ainsi d'une visibilité ininterrompue, d'une configuration des politiques, d'une administration et d'une Threat Intelligence collective, le tout en un seul endroit. Les modèles SRX4100 et SRX4200 sont conformes avec les normes du secteur, offrant l'évolutivité, la facilité de gestion, la connectivité sécurisée et les fonctionnalités avancées d'atténuation des menaces dont les entreprises ont besoin.

## Architecture et composants clés

L'architecture matérielle et logicielle SRX4100 et SRX4200 offre des performances de sécurité rentables dans un petit format 1RU. Ces pare-feu intègrent plusieurs services de sécurité et fonctions réseau en plus du système d'exploitation Junos de pointe de HPE.

Les SRX4100 et SRX4200 reconnaissent plus de 4 800 applications et applications imbriquées dans des transactions en texte brut ou chiffrées SSL. Les pare-feu s'intègrent également à Microsoft Active Directory et combinent les informations utilisateur aux données des applications afin d'étendre la visibilité et le contrôle des applications et des utilisateurs sur l'ensemble du réseau.

## Présentation du produit

Les pare-feu [SRX4100](#) et [SRX4200](#) de Juniper offrent une protection contre les menaces, des performances, une évolutivité, une haute disponibilité et des services de sécurité intégrés de pointe. Conçus pour un débit haute performance tout en empêchant les exploits, les logiciels malveillants et le trafic malveillant, les SRX4100 et SRX4200 sont les mieux adaptés aux datacenters d'entreprise, aux campus et aux sièges régionaux axés sur l'adoption d'une architecture zero trust.

Les SRX4100 et SRX4200 intègrent de manière transparente le réseau et la sécurité dans un pare-feu à facteur de forme fixe et plateforme unique. Les deux pare-feu sont optimisés par le [système d'exploitation Junos \(Junos OS\)](#) et gérés par [Security Director Cloud](#), qui aide les organisations à opérationnaliser le zero trust et à permettre la transformation architecturale grâce à une expérience de gestion unifiée et cadre de politique unique.

## Caractéristiques et avantages

Tableau 1. Fonctionnalités et avantages des SRX4100 et SRX4200

Exigences opérationnelles	Fonctionnalité/solution	Avantages de la gamme SRX4100/SRX4200
<b>Hautes performances</b>	Pare-feu hautes performances	<ul style="list-style-type: none"> <li>— Idéal pour les déploiements de périphérie de centre de données et de campus d'entreprise</li> <li>— Idéal pour les déploiements de pare-feux de nouvelle génération au siège social</li> <li>— L'évolutivité et la capacité des fonctionnalités répondent aux besoins futurs</li> </ul>
<b>Extrémité de haute qualité expérience utilisateur</b>	Contrôle et visibilité des applications	<ul style="list-style-type: none"> <li>— Mises à jour continues des applications fournies par HPE Juniper Networking Threat Labs</li> <li>— Contrôle et hiérarchise le trafic en fonction du rôle de l'application et de l'utilisateur</li> <li>— Inspecte et détecte les applications à l'intérieur Trafic chiffré SSL</li> </ul>
<b>Détection avancée des menaces</b>	IPS, antivirus, antispam, filtrage Web amélioré, sandboxing Juniper Advanced Threat Prevention Cloud, informations sur le trafic chiffré et flux SecIntel Threat Intelligence	<ul style="list-style-type: none"> <li>— Fournit des fonctionnalités IPS et des mises à jour en temps réel des signatures qui protègent efficacement contre les exploits, ce qui s'est avéré le plus efficace du secteur par le passé cinq ans confirmés par plusieurs tiers entreprises de test</li> <li>— Protège contre les programmes malveillants et le trafic Web malveillant</li> <li>— Fournit une plateforme ouverte de Threat Intelligence qui fournit un point unique à tous les opérateurs flux d'informations</li> <li>— Protège contre les attaques de type Zero-day</li> <li>— Empêche les appareils malveillants et compromis de diffuser des logiciels malveillants</li> <li>— Restaure la visibilité perdue en raison du chiffrement, sans les désavantages d'un déchiffrement TSL/SSL complet</li> </ul>
<b>Prévention Zero-day</b>	Prévention prédictive des menaces par l'IA	<ul style="list-style-type: none"> <li>— Prévoit et prévient les logiciels malveillants en temps réel en utilisant l'IA pour identifier de manière efficace les menaces à partir d'extraits de paquets</li> <li>— Élimine les infections à plusieurs phases</li> <li>— Fournit une protection réseau tout au long du cycle de vie de l'attaque, empêchant la réinfection des attaques ultérieures, plutôt que la première 24 heures d'attaque</li> </ul>
<b>Services réseau avancés</b>	Routage, sécurité, fil	<ul style="list-style-type: none"> <li>— Prend en charge le routage avancé de classe opérateur et la qualité de service (QoS)</li> </ul>
<b>Sécurité élevée</b>	VPN IPSec, accès à distance/ VPN SSL	<ul style="list-style-type: none"> <li>— Fournit un VPN IPSec haute performance avec un moteur crypto dédié</li> <li>— Offre diverses options VPN pour diverses conceptions de réseau, y compris l'accès à distance et la dynamique communications de site à site</li> <li>— Simplifie les déploiements VPN de grande envergure avec VPN automatique</li> <li>— Inclut une accélération crypto basée sur le matériel</li> <li>— Accès à distance SSL VPN sécurisé et flexible avec HPE Juniper Networking Secure Connect</li> </ul>
<b>Sécurité intégrée dans la fabric du datacenter</b>	Routes EVPN-VXLAN de type 5	<ul style="list-style-type: none"> <li>— Améliore l'inspection de tunnel pour le trafic encapsulé VXLAN avec des services de sécurité de couche 4 à couche 7</li> <li>— Facilite les opérations grâce à la prise en charge du type 5 par BGP</li> <li>— Ne nécessite pas de décapsulation du trafic EVPN-VXLAN</li> </ul>

Exigences opérationnelles	Fonctionnalité/solution	Avantages de la gamme SRX4100/SRX4200
<b>Très fiable</b>	Cluster de châssis, redondant blocs d'alimentation	<ul style="list-style-type: none"> <li>— Fournit une configuration dynamique et une synchronisation de l'état de la session</li> <li>— Prend en charge les fonctions active/active et active/de sauvegarde scénarios de déploiement</li> <li>— Offre du matériel hautement disponible avec une unité d'alimentation redondante (PSU) et des ventilateurs redondants</li> <li>— Offre un contrôle dédié et une liaison de structure avec une haute disponibilité transparente</li> </ul>
<b>Facile à gérer et à faire évoluer</b>	Interface graphique intégrée, Juniper Security Director Cloud	<ul style="list-style-type: none"> <li>— Permet une gestion centralisée à partir de l'expérience de gestion unifiée HPE avec une visibilité ininterrompue, un provisionnement sans intervention, une gestion et une évolutivité intelligentes des politiques de pare-feu, une traduction d'adresses réseau (NAT) et des déploiements VPN IPSec</li> <li>— Inclut une interface graphique intégrée simple et facile à utiliser pour gestion locale</li> </ul>
<b>Faible coût total de possession</b>	Junos OS	<ul style="list-style-type: none"> <li>— Intégration du routage et la sécurité sur un seul équipement</li> <li>— Réduction des dépenses d'exploitation grâce aux capacités d'automatisation de Junos OS</li> </ul>

## SRX4100 et SRX4200

### Spécifications du pare-feu

#### Spécifications logicielles

##### Services de pare-feu

- Services de pare-feu dynamique
- Pare-feu basé sur zone
- Écrans et déni de service distribué Protection (DDoS)
- Protection contre les anomalies de protocole et de trafic
- UAC (Unified Access Control)

##### Traduction d'adresses réseau (NAT)

- NAT source avec la traduction d'adresses de ports (PAT)
- NAT statique bidirectionnelle 1:1
- NAT de destination avec PAT
- NAT persistante
- Traduction des adresses IPv6

##### Fonctionnalités VPN

- Tunnels : Sur site, réseau en étoile, point de terminaison dynamique, AutoVPN, ADVPN, Group VPN (IPv4/ IPv6/ double pile)
- Juniper Secure Connect : Accès à distance/VPN SSL
- Charge utile de configuration : Oui
- Algorithmes de chiffrement IKE : Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, Suite B
- Algorithmes d'authentification IKE : MD5, SHA-1, SHA-128, SHA-256, SHA-384

- Authentification : Clé pré-partagée et infrastructure à clés publiques (PKI) (X.509)
- IPSec : Protocole Authentication Header (AH)/ Encapsulating Security Payload (ESP)
- Algorithmes d'authentification IPSec : hmac-md5, hmac-sha-196, hmac-sha-256
- Algorithmes de chiffrement IPSec : Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, Suite B
- Confidentialité de transmission parfaite, anti-réponse
- Internet Key Exchange : IKEV1, IKEV2
- Surveillance : Prise en charge de la norme Dead Peer Detection (DPD), supervision VPN
- VPN GRE, IP-in-IP et MPLS

##### Fonctionnalités de haute disponibilité

- Protocole de redondance de routeur virtuel (VRRP) - IPv4 et IPv6
- Haute disponibilité à états
  - Mise en cluster de deux boîtiers
  - Actif/passif
  - Actif/Actif
  - Synchronisation de la configuration
  - Synchronisation de sessions de pare-feu
  - Détection d'appareils/de liens
  - ISSU (Mise à niveau de logiciels en service)
  - HA multinœuds (MNHA)
- Surveillance IP avec basculement de route et d'interface

## Services de sécurité des applications<sup>1</sup>

- Contrôle et visibilité des applications
- QoS des applications
- Routage avancé basé sur des stratégies applicatives (APBR)
- Qualité de l'expérience applicative (AppQoE)
- Routage multichemin basé sur les applications
- Pare-feu basé sur l'utilisateur

## Services de défense contre les menaces et de renseignement<sup>1</sup>

- Système de prévention des intrusions
- Antivirus
- Antispam
- Filtrage d'URL basé sur des catégories/la réputation
- Proxy SS/inspection
- Protection contre les botnets (commande et contrôle)
- Mise en application adaptative basée sur GeoIP
- Juniper Advanced Threat Prevention, une offre SaaS basée sur le cloud, permettant de détecter et de bloquer les attaques de type Zero-day
- Profilage adaptatif des menaces
- Encrypted Traffic Insights
- Renseignements sur les menaces SecIntel
- L'appliance virtuelle Juniper ATP, une solution distribuée solution de prévention avancée des menaces sur site pour détecter et bloquer les attaques zero-day
- Prévention prédictive des menaces par l'IA

## Protocoles de routage

- IPv4, IPv6, routes statiques, RIP v1/v2
- OSPF/OSPF v3
- BGP avec réflecteur de route
- EVPN-VXLAN
- SI-SI
- Multicast : Protocole de gestion de groupe Internet (IGMP) v1/v2, mode clairsemé (SM) indépendant du protocole (PIM)/multidiffusion spécifique à la source (SSM), protocole de description de session (SDP), protocole de routage multidiffusion vectoriel à distance (DVMRP), multidiffusion Protocole de découverte de source (MSDP) ; transfert de chemin inverse (RPF)
- Encapsulation : VLAN, protocole PPPoE (Point-to-Point Protocol over Ethernet)
- Routeurs virtuels

- Routage basé sur la stratégie, routage basé sur les sources
- Routage multichemin à coût égal (ECMP)

## Fonctionnalités de QoS

- Prise en charge de 802.1p, point de code DiffServ (DSCP), EXP
- Classification basée sur VLAN, liaison de données identifiant de connexion (DLCI), interface, bundles, ou filtres multichamps
- Marquage, contrôle et mise en forme
- Classification et planification
- Détection précoce et aléatoire pondérée (WRED)
- Bande passante garantie et maximale
- Contrôle du trafic entrant
- Canaux virtuels

## Services réseau

- Client/serveur/relais DHCP (Dynamic Host Configuration Protocol)
- Proxy DNS (Domain Name System), DDNS (Dynamic DNS)
- Surveillance des performances (RPM) et IP en temps réel HPE
- Surveillance des flux HPE Juniper Networking (J-Flow)

## Services de routage avancés

- Mode paquet
- MPLS (RSVP, LDP)
- Connexion croisée de circuit (CCC), translationnelle connexion croisée (TCC)
- VPN MPLS L2/L2, Pseudo-wire
- Service de réseau local privé virtuel (VPLS), VPN multicast nouvelle génération (NG-MVPN)
- Ingénierie de trafic MPLS et re-direction rapide MPLS

## Gestion, automatisation, journalisation et production de rapports

- SSH, Telnet, SNMP
- Téléchargement d'images intelligent
- CLI et interface utilisateur Web HPE Juniper Networking
- HPE Juniper Networking Security Director Cloud
- Python
- Événements Junos et scripts de commit et d'OP
- Rapports sur l'utilisation des applications et de la bande passante
- Outils de débogage et de dépannage

<sup>1</sup> Proposé sous forme de licence d'abonnement à la sécurité avancée.

## Spécifications matérielles

Tableau 2. Spécifications matérielles SRX4100 et SRX4200

Spécifications	SRX4100	SRX4200
<b>La connectivité</b>		
Nombre total de ports embarqués	8x 1 GbE/10 GbE	8x 1 GbE/10 GbE
Ports d'émetteur-récepteur plus (SFP+) (Small Form-Factor Pluggable)	8x 1 GbE/10 GbE	8x 1 GbE/10 GbE
Ports de gestion hors bande (OOB)	1 x 1 GbE	1 x 1 GbE
Ports haute disponibilité (HA) dédiés	2x1 GbE/10 GbE (SFP/SFP+)	2x1 GbE/10 GbE (SFP/SFP+)
Console (RJ-45)	1	1
Ports USB 2.0 (type A)	2	2
<b>Mémoire et stockage</b>		
Mémoire système (RAM)	64 Go	64 Go
Stockage secondaire (SSD)	240 Go avec 1+1 RAID	240 Go avec 1+1 RAID
<b>Dimensions et puissance</b>		
Format	1 U	1 U
Taille (L x H x P)	17,48 x 1,7 x 25 pouces (44,39 x 4,31 x 63,5 cm)	17,48 x 1,7 x 25 pouces (44,39 x 4,31 x 63,5 cm)
Poids (appareil et bloc d'alimentation)	Châssis avec deux alimentations CA fournitures : 13,15 kg (29 lb)  Châssis avec deux blocs d'alimentation CC : 13,06 kg (28,9 lb)  Châssis avec pack pour expédition : 21,54 kg (47,5 lb)	Châssis avec deux blocs d'alimentation CA : 13,15 kg (29 lb)  Châssis avec deux blocs d'alimentation CC : 13,06 kg (28,9 lb)  Châssis avec emballage pour l'expédition : 21,54 kg (47,5 lb)
Blocs d'alimentation redondants	1+1	1+1
Module d'alimentation	2x 650 W redondant AC-DC/DC-DC PSU	2x 650 W redondant AC-DC/DC-DC PSU
Consommation électrique moyenne	200 W	200 W
Dissipation moyenne de la chaleur	685 BTU/heure	685 BTU/heure
Consommation de courant maximale	4A (pour alimentation 110 V CA)  2A (pour une alimentation 220 V CA)  9A (pour une alimentation CC de -48 V)	4A (pour alimentation 110 V CA)  2A (pour une alimentation 220 V CA)  9A (pour une alimentation CC de -48 V)
Appel de courant maximal	50 A par cycle CA 1	50 A par cycle CA 1
<b>Conformité environnementale et réglementaire</b>		
Niveau sonore	70 dBA	70 dBA
Flux d'air/refroidissement	De l'avant vers l'arrière	De l'avant vers l'arrière
Température de fonctionnement	32 °F à 104 °F (0 °C à 40 °C)	32 °F à 104 °F (0 °C à 40 °C)
Taux d'humidité en fonctionnement	5 à 90% (sans condensation)	5 à 90% (sans condensation)
Temps moyen entre défaillances (MTBF)	221 729 heures (environ 25,3 ans)	221 729 heures (environ 25,3 ans)
Classification FCC	Classe A	Classe A
Conformité RoHS	RoHS 2	RoHS 2

Spécifications	SRX4100	SRX4200
<b>Performance et évolutivité</b>		
Débit de pare-feu (IMIX) Gbit/s <sup>2</sup>	25	Les 50 premières entreprises
Débit de pare-feu (1 518 B) Gbit/s <sup>2</sup>	40	80
Débit VPN IPSec (IMIX) Gbit/s <sup>2</sup>	13	26
Débit VPN IPSec (1400B) <sup>2</sup>	17,5	35
Performances de sécurité des applications (TPS#/CPS**) en Gbit/s	35/16	70/32,5
pare-feux nouvelle génération (TPS#/CPS**) en Gbit/s <sup>3</sup>	30/8	60/16
pare-feux Secure Web Access (CPS**) en Gbit/s <sup>4</sup>	7	14,5
Menace avancée (CPS) <sup>5</sup>	3,5	7,5
Connexions par seconde (64 O)	275 000	550 000
Connexions SSL par seconde	6 000	12.000
Nombre maximal de sessions simultanées (IPv4 ou IPv6)	5 millions	10 millions
Taille de la table de routage (RIB/FIB) (IPv4)	2 millions/1,2 million	2 millions/1,2 million
Tunnels VPN IPSec	4 075	4 075

## Juniper Mist WAN Assurance et Opérations d'IA

Les pare-feu SRX4100 et SRX4200 peuvent également être exploités et orchestrés via Juniper [Mist Cloud](#). Mist AI offre une automatisation sans précédent grâce à une combinaison d'intelligence artificielle, d'algorithmes de machine learning et de techniques de science des données pour gagner du temps, maximiser la productivité informatique et fournir meilleure expérience pour les utilisateurs numériques.

[Juniper Mist WAN Assurance](#) s'appuie sur Juniper Mist Cloud et assure une gestion et des opérations complètes du cycle de vie, notamment des informations [IA natives](#), des tests de vitesse automatisés, la capture dynamique de paquets (dPCAP), la détection des anomalies et l'identification des causes racines qui se concentrent sur l'expérience des utilisateurs finaux. Pour les opérations du jour 0 et du jour 1, WAN Assurance fournit également l'orchestration, l'administration et le ZTP pour SRX4100 et SRX4200. Consultez la [fiche technique WAN Assurance](#) pour plus d'informations.

<sup>2</sup> Chiffres de débit basés sur les paquets UDP et la méthodologie de test RFC2544

<sup>3</sup> Les performances des pare-feux de nouvelle génération ont été mesurées avec parepare-feux, sécurité des applications et IPS activés

<sup>4</sup> Les performances du pare-feu Secure Web Access sont mesurées avec le pare-feu, la sécurité des applications, l'IPS, SecIntel et le filtrage des URL activés

<sup>5</sup> Les performances des menaces avancées sont mesurées avec les fonctionnalités Pare-feu, Sécurité des applications, IPS, SecIntel, Filtrage des URL et Protection contre les logiciels malveillants activés

\*\* Méthode TPS : Performances de débit des sessions HTTP moyennes

\*\* Méthode CPS : Sessions de courte durée

## Informations de commande

Pour commander les pare-feu HPE Juniper Networking [SRX Series](#), et pour accéder aux informations sur les licences logicielles, veuillez consulter la page Comment acheter à l'adresse [juniper.net/us/en/how-to-buy/form.html](https://juniper.net/us/en/how-to-buy/form.html).

## 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 des possibilités, 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://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

## [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.

Active Directory et Microsoft sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Toutes les marques de tiers sont la propriété de leurs propriétaires respectifs.

a00150838FRE

HEWLETT PACKARD ENTERPRISE

[hpe.com](http://hpe.com)

