



Fiche technique du pare-feu SRX4600

Description du produit

Le pare-feu SRX4600 de Juniper Networks protège les réseaux stratégiques des datacenters et des campus pour les entreprises, les fournisseurs de services et les fournisseurs de cloud. Ce pare-feu nouvelle génération (NGFW) fait partie intégrante du cadre de [sécurité connectée de Juniper](#), qui étend la sécurité à chaque point du réseau pour protéger les utilisateurs, les données et l'infrastructure contre les menaces avancées. Le pare-feu SRX4600 intègre la mise en réseau et la sécurité dans une plateforme unique pour offrir une prévention des intrusions et une protection contre les logiciels malveillants de pointe avec un débit haute performance, un VPN IPSec, une évolutivité élevée 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. Le pare-feu fournit une analyse détaillée du volume et de l'utilisation des applications, ainsi que des stratégies de contrôle des applications précises pour autoriser ou refuser le trafic en fonction des noms d'applications dynamiques ou des noms de groupes. Le trafic est hiérarchisé en fonction des informations et du contexte des applications pour réduire la complexité des réseaux traditionnels, cloud et cloud hybride.

Le SRX4600 fournit également un [SD-WAN](#) entièrement automatisé aux entreprises et aux fournisseurs de services. En raison de ses hautes performances et de son évolutivité, la passerelle SRX4600 peut agir comme un concentrateur VPN et être un point de terminaison VPN/overlay sécurisé dans les diverses topologies de SD-WAN.



Le pare-feu est géré par Juniper Security Director Cloud, une expérience de gestion unifiée qui relie les déploiements actuels de l'organisation aux futurs déploiements architecturaux. Security Director cloud utilise un cadre de politique unique, permettant des politiques de sécurité cohérentes dans n'importe quel environnement et étendre le zero trust à toutes les parties du réseau de l'edge au datacenter. Cela offre une visibilité continue, une configuration des politiques, une administration et une Threat Intelligence collective en un seul endroit, permettant aux organisations de garantir des architectures et des expériences sécurisées.

Le SRX4600 est alimenté par [Junos](#), le système d'exploitation leader du secteur chargé de protéger les plus grands réseaux stratégiques d'entreprise et de fournisseurs de services au monde.

Architecture et composants clés

L'architecture matérielle et logicielle SRX4600 offre une sécurité économique dans un petit format 1 RU. Le pare-feu spécialement conçu protège les environnements réseau et fournit un débit de pare-feu Internet Mix (IMIX) allant jusqu'à 400 Gbit/s, et il intègre plusieurs services de sécurité et fonctions réseau en plus du système d'exploitation Junos. Les meilleures fonctionnalités de sécurité et d'atténuation des menaces avancées du SRX4600 sont proposées avec des fonctionnalités de système de prévention des intrusions (IPS) et un VPN IPSec dans les déploiements de datacenters, de campus d'entreprise et de sièges régionaux avec des modèles de trafic IMIX.

Présentation du produit

Le [SRX4600](#) est un [pare-feu nouvelle génération](#) de protection contre les menaces de pointe qui répond aux besoins changeants des entreprises, du cloud et pare-feux les [réseaux de fournisseurs de services](#). Le SRX4600 convient mieux aux organisations qui se concentrent sur l'architecture zero trust. Il est conçu pour un débit haute performance tout en empêchant les exploits, les logiciels malveillants et le trafic malveillant.

Le SRX4600 intègre de manière transparente le réseau et la sécurité au sein d'une seule plateforme. Il est géré 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 un cadre de politique unique.

Caractéristiques et avantages

Tableau 1. Fonctionnalités et avantages du SRX4600

Exigence commerciale	Fonctionnalité/solution	Avantages de la SRX4600
Hautes performances	Chemin express +	<ul style="list-style-type: none"> — Fournit un déchargement automatique de tous les flux éligibles pour le transfert à débit linéaire sans configuration supplémentaire — Fournit des services d'inspection complets à tous les flux, quelle que soit leur taille — Ne nécessite aucun compromis entre performances et sécurité — Répond aux exigences pour les déploiements de campus d'entreprise et de périphérie de datacenter — Répond à divers besoins et s'adapte aux déploiements des fournisseurs de services.
Haute qualité, expérience utilisateur	Contrôle et visibilité des applications	<ul style="list-style-type: none"> — Mises à jour continues des applications fournies par HPE Juniper Networking Laboratoires de menaces — Contrôle et hiérarchise le trafic en fonction du rôle de l'application et de l'utilisateur — Inspecte et détecte les applications dissimulées dans le trafic SSL chiffré
Détection avancée des menaces	IPS, antivirus, antispam, filtrage Web amélioré, sandboxing cloud Juniper Advanced Threat Prevention, informations sur le trafic chiffré, flux SecIntel et Threat Intelligence	<ul style="list-style-type: none"> — Fournit des fonctionnalités IPS et des mises à jour en temps réel des signatures qui protègent efficacement contre les exploits, dont l'efficacité a été prouvée dans le secteur par plusieurs entreprises de test tierces — Protège contre les programmes malveillants et le trafic Web malveillant — Fournit une plateforme ouverte de Threat Intelligence qui fournit un point unique pour tous les flux d'intelligence opérationnelle — Protège contre les attaques de type Zero-day — Empêche les appareils malveillants et compromis de diffuser des logiciels malveillants — Restaure la visibilité perdue grâce au chiffrement sans le fardeau lourd de la visibilité totale Déchiffrement TLS/SSL
Prévention Zero-day	Prévention prédictive des menaces par l'IA	<ul style="list-style-type: none"> — 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 — Élimine les infections à plusieurs phases — Fournit une protection qui dure tout au long du cycle de vie des attaques, et pas seulement 24 heures, afin que le réseau ne soit pas réinfecté par des attaques ultérieures
Services réseau de niveau professionnel	Routage, sécurité, fil	<ul style="list-style-type: none"> — Prend en charge le routage avancé de classe opérateur (BGP, OSPF v2/3, IS-IS, RIP v1/2/NG, ICMP multidiffusion, PIM, BFD, plusieurs instances de routage) et la qualité de service (QoS)
Sécurité élevée	VPN IPSec, accès distant/VPN SSL	<ul style="list-style-type: none"> — Fournit un VPN IPSec haute performance avec un moteur crypto dédié — Offre des options VPN différentes pour diverses conceptions réseau, notamment un accès à distance et des communications dynamiques sur le site — Simplifie les déploiements VPN de grande envergure avec VPN automatique — Inclut une accélération crypto basée sur le matériel — Accès distant sécurisé et flexible, IPSec et VPN SSL avec Juniper Connexion sécurisée
Sécurité intégrée dans la fabric du datacenter	Routes EVPN-VXLAN de type 5	<ul style="list-style-type: none"> — Améliore l'inspection des tunnels pour le trafic encapsulé VXLAN avec des services de sécurité de la couche 4 à la couche 7 — Facilite les opérations grâce à la prise en charge du type 5 par BGP — Ne nécessite pas de décapsulation du trafic EVPN-VXLAN
Très fiable	Cluster de châssis, alimentations redondantes	<ul style="list-style-type: none"> — Fournit une configuration dynamique et une synchronisation des états de session — Prend en charge des scénarios de déploiement actif/actif et actif/de secours — Offre du matériel hautement disponible avec une unité d'alimentation redondante (PSU) et des ventilateurs
Facile à gérer et à faire évoluer	Interface graphique intégrée, Juniper Security Director Cloud, Security Director, CLI puissante et automatisation	<ul style="list-style-type: none"> — Permet une gestion centralisée à partir de l'expérience de gestion unifiée de HPE avec une visibilité ininterrompue, un provisionnement sans intervention, une gestion intelligente des politiques de pare-feu et une évolutivité — Prend en charge la traduction d'adresses réseau (NAT) et les déploiements VPN IPSec — Comprend une interface utilisateur graphique intégrée facile à utiliser pour la gestion locale
Faible coût total de possession	Junos OS	<ul style="list-style-type: none"> — Intégration du routage et la sécurité sur un seul équipement — Réduction des dépenses d'exploitation grâce aux capacités d'automatisation de Junos OS

Spécifications logicielles

Services de pare-feu

- Services de pare-feux dynamique
- Pare-feu basé sur zone
- Protection contre les attaques par déni de service (DDoS) sur les écrans et les attaques par déni de service distribué
- 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
- Méthode d'allocation de bloc de port pour NAT de niveau opérateur
- NAT déterministe
- Surcharge de port, appairage de pool, NAPT, NAT44, NAT66, NAPT, NAP-PT, NAT46, NAT64, Dual Stack Lite

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, SHA-512
- 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, hmac-sha-512
- Algorithmes de chiffrement IPSec : Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, Suite B
- Confidentialité de transmission parfaite, anti-réponse
- Groupes Diffie Hellmann du groupe14 au groupe24
- 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 haute disponibilité

- Protocole de redondance virtuelle (VRRP) : IPv4 et IPv6
- Haute disponibilité à états
 - mise en cluster HA
 - Actif/Actif
 - Actif/passif
 - Deux ports de contrôle HA compatibles MACsec (10 GbE)
 - Deux ports de structure HA compatibles MACsec (10GbE)
 - Synchronisation de la configuration
 - Synchronisation de sessions de pare-feu
 - Détection d'appareils/de liens
 - Mise à niveau logicielle en service unifié (ISSU unifiée)
 - HA multinœuds (MNHA)
- Surveillance IP avec basculement de route et d'interface

Services de sécurité des applications¹

- 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 Threat Defense et de renseignement¹

- IPS
- 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 ATP Cloud, une offre SaaS basée sur le cloud, détecte et bloque les attaques zero-day
- Profilage adaptatif des menaces
- Encrypted Traffic Insights
- Renseignements sur les menaces SecIntel
- L'appliance virtuelle Juniper ATP, solution de prévention avancée des menaces sur site pour détecter et bloquer les attaques zero-day
- Prévention prédictive des menaces par l'IA

¹ Proposé sous forme de licence d'abonnement de sécurité avancée

Protocoles de routage

- IPv4, IPv6, routes statiques, RIP v1/v2
- OSPF/OSPF v3
- BGP avec réflecteur de route
- BFD pour une détection rapide
- [EVPN-VXLAN](#)
- SI-SI
- Multicast : Internet Group Management Protocol (IGMP) v1/v2 ; Protocol Independent Multicast (PIM) Sparse Mode (SM)/Dense Mode (DM)/source-specific multicast (SSM) ; Session Description Protocol (SDP) ; Distance Vector Multicast Routing Protocol (DVMRP) ; Multicast Source Discovery Protocol (MSDP) ; Reverse Path Forwarding (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 QoS

- Assistance pour la 802.1p, le point de code DiffServ (DSCP)
- Classification basée sur l'interface, les paquets ou les filtres multichamps
- Marquage, contrôle et mise en forme
- Classification et planification
- Détection précoce et aléatoire pondérée (WRED)
- Bande passante garantie et maximale

Services réseau

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

Gestion, automatisation, journalisation et production de rapports

- SSH, Telnet, SNMP
- Téléchargement d'images intelligent
- CLI et interface utilisateur Web Juniper
- Juniper Security Director Cloud
- Python

- Scripts Junos OS d'évènements, de commit et OP
- Rapports sur l'utilisation des applications et de la bande passante
- Télémétrie gRPC
- Outils de débogage et de dépannage

Spécifications matérielles

Tableau 2. Spécifications matérielles du SRX4600

Spécification	SRX4600
Total à bord Ports d'E/S	Jusqu'à 24x1GbE/10GbE (SFP+) 4x40GbE/100GbE (QSFP28)
Ports de gestion hors bande (OOB)	RJ-45 1 Gbit/s
Ports haute disponibilité (HA) dédiés	Contrôle 2x1GbE/10GbE (SFP+) Données 2x1GbE/10GbE (SFP+)
Console	RJ-45 (RS232)
Ports USB 2.0 (Type A)	1
Mémoire et stockage	
Mémoire système (RAM)	256 Go
Stockage secondaire (SSD)	2 To M.2 SSD
Dimensions et puissance	
Format	1 U
Taille (L x H x P)	44,19 x 4,32 x 67,31 cm (17,4 x 1,7 x 26,5 po) Avec PEM CA : 44,19 x 4,32 x 69,32 cm (17,4 x 1,7 x 27,29 po) Avec PEM CC : 44,19 x 4,32 x 74,17 cm (17,4 x 1,7 x 29,20 po)
Poids (système et 2 puissances modules d'entrée)	Avec PEM CA : 17,24 kg (38 lb) Poids à l'expédition : 20,62 kg (45,47 lb) Avec PEM CC : 18,14 kg (40 lb) Poids à l'expédition : 21,53 kg (47,47 lb)
Blocs d'alimentation redondants	1+1
Module d'alimentation	2 blocs d'alimentation CA-CC redondants 1 600 W 2 blocs d'alimentation CC-CC redondants 1 100 W
Consommation électrique moyenne	650 W
Dissipation moyenne de la chaleur	2218 BTU/heure
Consommation de courant maximale	12A (pour une alimentation 110V CA) 6A (pour une alimentation 220V CA) 24A (pour alimentation -48V CC)

Spécification	SRX4600
Ports de synchronisation de protocole de temps de précision	
Heure de la journée – RS-232 (EIA-23)	1xRJ-45
Horloge BITS	1xRJ-48
Connecteur de synchronisation 10 MHz (GNSS)	1xInput (COAX) 1xOutput (COAX)
Connexion par impulsion par seconde (1-PPS)	1xInput (COAX) 1xOutput (COAX)
Conformité environnementale et réglementaire	
Niveau sonore	69 dBA à la vitesse normale du ventilateur, 87 dBA à pleine vitesse de ventilation
Flux d'air/ refroidissement	De l'avant vers l'arrière
Température de fonctionnement	De 0 °C à 40 °C (32 °F à 104 °F)
Taux d'humidité en fonctionnement	5 % à 90 % sans condensation
Temps moyen entre défaillances (MTBF)	111 626 heures (12,75 ans)
Classification FCC	Classe A
Conformité RoHS	RoHS 2
Conformité NEBS	Conçu pour les NEBS de Niveau 3
Performance	
Débit de pare-feu (IMIX) en Gbit/s ²	400
Débit de pare-feu (1 518 B) en Gbit/s ²	400
Débit VPN IPSec (IMIX) en Gbit/s ²	44
Débit VPN IPSec (1 400 B) en Gbit/s ²	71
Performances de sécurité des applications (TPS##/ CPS**) en Gbit/s ³	92/41

² Il y a huit ports 1GbE/10GbE dédiés. Les quatre ports 40GbE/100GbE peuvent utiliser des câbles de dérivation pour créer 4x10GbE (SFP+) chacun, totalisant 24x10GbE.

³ Chiffres de débit basés sur les paquets UDP et la méthodologie de test RFC2544

⁴ Les performances du pare-feu de datacenter de nouvelle génération sont mesurées avec les fonctionnalités Pare-feu, Sécurité des applications et IPS activées

⁵ Les performances du pare-feu Secure Web Access sont mesurées avec le filtrage des pare-feu, de la sécurité des applications, des IPS, des SecIntel et des URL activé

⁶ Les performances des menaces avancées sont mesurées avec 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

Spécification	SRX4600
pare-feu nouvelle génération (TPS##/ CPS**) en Gbit/s ⁴	90/21
pare-feu Secure Web Access (CPS**) en Gbit/s ⁵	19
Menace avancée (CPS**) Gbit/s ⁶	10,5
Connexions par seconde (64 O)	570 000
Connexions SSL par seconde	16 000
Nombre maximal de sessions simultanées (IPv4 ou IPv6)	60 millions
Taille de la table de routage (RIB/FIB) (IPv4)	4 millions/1,2 million
Tunnels VPN IPSec	7 500

Security Director cloud

[Security Director Cloud](#) est l'expérience de gestion simple et transparente de HPE fournie dans une seule interface utilisateur pour connecter les déploiements actuels des clients à leurs futurs déploiements architecturaux. La gestion est au cœur de la stratégie de sécurité connectée de Juniper et aide les organisations à sécuriser chaque point de connexion sur leur réseau pour protéger les utilisateurs, les données et l'infrastructure.

Les organisations peuvent sécuriser leur architecture avec des politiques de sécurité cohérentes dans n'importe quel environnement : sur site, basé sur le cloud, fourni dans le cloud et hybride. Dans le même temps, ils peuvent étendre le zero trust de l'edge jusqu'au datacenter, aux applications et aux microservices. Avec Security Director Cloud, les entreprises disposent d'une visibilité, d'une configuration des politiques, d'une administration et d'une Threat Intelligence collective ininterrompues, le tout au même endroit.

HPE rencontre les clients là où ils en sont dans leur parcours, les aide à tirer parti de leurs investissements existants et leur permet de passer à leur architecture préférée à un rythme optimal pour l'entreprise en automatisant leur transition avec Security Director Cloud.

Juniper Mist WAN Assurance et Opérations d'IA

Le pare-feu SRX4600 peut également être exploité et orchestré via Juniper [Mist Cloud](#). Mist AI offre une automatisation sans précédent en combinant l'intelligence artificielle, des algorithmes de machine learning et des techniques de science des données pour gagner du temps, maximiser la productivité informatique et offrir la meilleure expérience aux 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 SRX4600. Consultez la [fiche technique WAN Assurance](#) pour plus d'informations.

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.

a00150837FRE

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

Informations de commande

Pour commander les pare-feu SRX Series de Juniper Networks et accéder aux informations sur les licences logicielles, rendez-vous sur la page Comment acheter à l'adresse 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](#).

