

JUNIPER SECURE CONNECT

Présentation du produit

[Juniper® Secure Connect](#) est une application VPN SSL et IPSec hautement flexible qui offre aux télétravailleurs un accès sécurisé aux ressources de l'entreprise et du cloud, offrant une connectivité fiable et une sécurité cohérente sur n'importe quel appareil, n'importe où. Juniper Secure Connect est disponible pour les appareils de bureau et mobiles, notamment Windows, Apple macOS, iOS, iPadOS et Android. Associé au pare-feu [SRX Series](#), il aide les organisations à atteindre rapidement des performances et une connectivité optimales du client au cloud, réduisant ainsi les risques en étendant la visibilité et l'application aux utilisateurs et aux appareils, où qu'ils se trouvent.

Description du produit

Les organisations sont de plus en plus distribuées, principalement en raison du travail à distance et de l'expansion des succursales. La sécurisation de ce trafic distribué nécessite une visibilité approfondie du réseau et la possibilité d'appliquer des politiques à chaque point de connexion.

Juniper Secure Connect permet aux organisations de fournir un accès sécurisé aux utilisateurs finaux en tirant parti de la connectivité IP. En travaillant avec les pare-feu Juniper Networks® SRX Series comme point de terminaison SSL VPN et IPSec de tête de réseau, déployés sur le campus, dans un datacenter ou dans le cloud, Juniper Secure Connect permet un accès sécurisé aux ressources vitales à partir des appareils utilisateurs exécutant Windows, Apple macOS, iOS, iPadOS et Android™. Le déploiement de Secure Connect est simple : L'application client doit s'assurer que la politique la plus récente est utilisée à chaque connexion. Aucune interaction entre l'utilisateur final et l'administrateur n'est nécessaire pour réduire le temps de déploiement et un dépannage continu.

Architecture et composants clés

Proposé sous forme de licence complémentaire pour les pare-feu SRX Series, Juniper Secure Connect exploite la connectivité IP pour fournir un accès sécurisé aux utilisateurs de n'importe où. Juniper Secure Connect fonctionne avec les pare-feu SRX Series dans des formats physiques, virtuels et as-a-service, offrant une connectivité et une sécurité réseau pour prendre en charge les utilisateurs, les appareils et les données où qu'ils se trouvent.

L'application Juniper Secure Connect offre des fonctionnalités supplémentaires qui améliorent la sécurité et la convivialité. Ces fonctionnalités incluent l'authentification biométrique et la validation automatique des

politiques avant d'établir une connexion. L'application utilise une connexion pré-domaine Windows pour s'assurer que les appareils Windows sont validés et mis à jour avec la dernière politique de groupe Active Directory pendant la connexion, qui utilise des solutions d'authentification multifactorielle externes.

Les politiques de sécurité sont appliquées aux appareils via Juniper Secure Connect. Ces politiques peuvent traiter ce trafic comme s'il n'était pas fiable. Secure Connect exploite Juniper Networks® AppSecure, le système de prévention des intrusions (IPS), la sécurité du contenu et la prévention avancée des menaces pour étendre la sécurité aux appareils distants. Cela garantit une sécurité cohérente sur l'ensemble du réseau et fournit le niveau approprié d'accès sécurisé.

Juniper Secure Connect s'appuie sur des politiques de sécurité cohérentes qui permettent aux organisations d'assurer une protection efficace contre les menaces depuis et vers les succursales, les bureaux à domicile et les employés travaillant à distance depuis d'autres réseaux, ce qui permet aux organisations de garantir des architectures et des expériences sécurisées.

Les flux de données peuvent être identifiés par l'application, l'utilisateur, l'adresse IP et l'URL, ce qui permet aux équipes informatiques de hiérarchiser ou d'inspecter plus en profondeur certains de ces flux de données. Avec Juniper Secure Connect, la politique peut exiger que tout le trafic soit acheminé via Connexion VPN ou configurée pour prendre en charge la tunnelisation fractionnée, garantissant ce trafic peut suivre le chemin le meilleur et le plus sécurisé.

Tableau 1. Caractéristiques et avantages

Fonctionnalité	Description	Avantage
Disponible pour les ordinateurs de bureau et les appareils mobiles	Disponible pour les systèmes d'exploitation Windows, Apple macOS, iOS, iPadOS et Android.	Accès flexible et sécurisé pour les appareils gérés et non gérés.
Configuration sans intervention	Utilise la validation sécurisée et automatique de la politique la plus récente, garantissant que les utilisateurs bénéficient toujours de la bonne politique de sécurité appliquée.	Offre une politique de sécurité toujours à jour, garantissant la sécurité des utilisateurs et l'accès à les bonnes ressources à tout moment.
Authentification multifactorielle et biométrique	Prend en charge l'authentification multifactorielle externe à partir de solutions d'authentification multifactorielle (MFA) de pointe pour renforcer la sécurité. Il prend également en charge l'authentification biométrique intégrée sur les appareils avec prise en charge matérielle.	Améliore la sécurité de l'entreprise en tirant parti d'une deuxième forme d'authentification pour les utilisateurs distants.
Sécurité et visibilité complètes	L'accès des utilisateurs via Juniper Secure Connect doit être soumis à IPS, à Juniper Advanced Threat Prevention et à une sécurité avancée pour identifier et bloquer les menaces inconnues et connues provenant de réseaux non professionnels.	Réduit les risques et fournit les éléments nécessaires visibilité pour s'assurer que les utilisateurs d'accès à distance sont ne pas introduire de menaces connues ou inconnues.

Juniper 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 toutes les environnements : sur site, dans le cloud, cloud et hybride, et étendez le zero trust à toutes les parties du réseau, de la périphérie au datacenter, en passant par les applications et les 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 ses clients là où ils en sont dans leur parcours architectural, 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 la sécurité Directeur Cloud.

Secure Edge

[Juniper Secure Edge](#) sécurise les équipes n'importe où avec l'accès rapide, fiable et sécurisé dont elles ont besoin. Il offre des fonctionnalités SSE complètes, y compris FWaaS, SWG et CASB avec DLP, ZTNA et une protection avancée contre les menaces pour protéger l'accès aux applications Web, SaaS et sur site et fournir aux utilisateurs une sécurité qui les suit où qu'ils aillent.

HPE rencontre les clients où qu'ils se trouvent et les emmène là où ils veulent aller en tirant parti de ce qu'ils ont et en étendant leurs initiatives zero trust à une architecture fournie dans le cloud sans casser la banque ou leur équipe opérationnelle.

Juniper Secure Edge, géré par Security Director Cloud, utilise un cadre de politiques unique qui permet de créer des politiques de sécurité une seule fois pour suivre les utilisateurs, les appareils et les données où qu'ils aillent. Les clients n'ont pas besoin de partir de zéro lors de l'adoption la sécurité fournie par le cloud. Grâce à notre assistant en trois clics, ils peuvent facilement exploiter les politiques de périphérie de campus existantes et les traduire en une politique SSE. Comme il utilise un cadre stratégique unique, quel que soit le modèle de déploiement, Secure Edge applique en quelques clics les politiques de sécurité existantes des déploiements traditionnels à son modèle dans le cloud, réduisant ainsi les erreurs de configuration et les risques.

Qu'il s'agisse de sécuriser les utilisateurs distants, les campus et les succursales, le cloud privé, le cloud public ou les datacenters de cloud hybride, HPE offre une gestion unifiée et une visibilité ininterrompue sur toutes les architectures. Cela permet aux équipes opérationnelles de relier efficacement leurs investissements actuels aux objectifs architecturaux futurs, y compris le SASE. Les clients peuvent gérer la sécurité partout et en tout lieu, sur site, dans et depuis le cloud, avec des politiques de sécurité qui suivent les utilisateurs, les appareils et les données où qu'ils aillent, le tout à partir d'une interface utilisateur unique.

Les utilisateurs disposent d'un accès rapide, fiable et sécurisé aux données et aux ressources dont ils ont besoin, ce qui garantit une expérience utilisateur optimale. Les équipes de sécurité informatique profitent de leur visibilité totale sur l'ensemble du réseau tout en tirant parti de leurs équipements existants, ce qui leur permet de passer à une architecture cloud à leur propre rythme.

Juniper Secure Edge fournit des politiques de sécurité cohérentes qui suivent les utilisateurs, les appareils et les données sans avoir à copier ou recréer des ensembles de règles. Il est facile de déployer le contrôle des applications fournies dans le cloud, la prévention des intrusions, le filtrage du contenu et du Web, et une prévention efficace des menaces sans compromettre la visibilité ou l'application de la sécurité.

Plusieurs tests tiers ont constamment validé HPE Juniper Networking comme la technologie de sécurité la plus efficace du marché au cours des cinq dernières années, avec une efficacité de sécurité de plus de 99 % dans tous les cas d'utilisation.

Tableau 2. Caractéristiques

Fonctionnalités	Windows	MacOS	iOS/iPadOS	Android
Cryptographie de nouvelle génération	Oui	Oui	Oui	Oui
VPN SSL basé sur le client	Oui	Oui	Oui	Oui
Détection des pairs morts (DPD)	Oui	Oui	Oui	Oui
Tunnelisation divisée	Oui	Oui	Oui	Oui
Authentification multifactorielle (MFA)	Oui	Oui	Oui	Oui
Authentification biométrique	Oui	Oui	Oui	Oui
Configuration de l'application sans intervention	Oui	Oui	Oui	Oui
Contrôles de conformité avant connexion	Oui	Oui	Oui	Oui
Licence et durée de support Juniper Secure Connect	1, 3 ou 5 ans			

Informations de commande

Pour commencer à utiliser Juniper Secure Connect et accéder aux informations sur les licences logicielles, utilisez les liens suivants sur le site d'assistance HPE :

- [Fenêtres](#)
- [macOS](#)
- [iOS/iPadOS](#)
- [Android](#)

Pour en savoir plus, rendez-vous sur la [page Comment acheter](#) sur www.juniper.net. Les licences Juniper Secure Connect sont empilables et leur utilisation est basée sur les utilisateurs actuels connectés au pare-feu SRX Series de tête de réseau.

À propos de Hewlett Packard Enterprise

HPE est un leader dans le domaine des technologies d'entreprise essentielles, combinant la puissance de l'IA, du cloud et du réseau pour aider les organisations à en faire plus. 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.

Android est une marque déposée de Google LLC. Active Directory et Windows 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.

a00150844FRE, rév. 1

HEWLETT PACKARD ENTERPRISE

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

