

DONNER DAVANTAGE D'AUTONOMIE AUX TÉLÉTRAVAILLEURS GRÂCE À LA SOLUTION SANS TUNNEL SESSION SMART SD-WAN

Le télétravail ne s'est pas seulement banalisé, il s'est littéralement imposé aux entreprises comme une nécessité en temps de crise

Déf

Traditionnellement, les solutions VPN reposent sur une tunnelisation IPsec ou SSL. Ces technologies sont à la fois complexes et difficiles à faire évoluer, pour la simple raison qu'elles s'appuient sur un modèle rigide qui rend difficiles les perspectives de télétravail.

Solution

La solution Session Smart SD-WAN crée une structure orientée services qui permet de déployer une architecture « work from anywhere » idéale pour offrir agilité et sécurité tout en proposant aux utilisateurs distants une expérience de qualité.

Avantages

- Amélioration de l'expérience utilisateur et des performances réseau
- Réduction des risques pour la sécurité et respect des obligations de conformité
- Visibilité étendue et détaillée sur les réseaux et les services
- Simplicité d'une architecture orientée services et sans tunnel

La pandémie de COVID-19 a permis aux entreprises de prendre réellement conscience de leur incapacité à fournir des environnements de télétravail à la fois flexibles, sécurisés et productifs. Et ces insuffisances se vérifient tout particulièrement pour les VPN, qui font partie intégrante des environnements de télétravail et autres espaces situés en dehors des murs du bureau. Nous assistons aujourd'hui à une très forte demande autour de solutions de réseau hautement distribuées et sécurisées, capables d'offrir le degré de qualité, de fiabilité et d'agilité indispensable pour bien accompagner cette nouvelle main-d'œuvre distante. La solution Juniper® Session Smart™ SD-WAN offre une structure zero trust qui assure un niveau inégalé de contrôle et d'accès aux ressources stratégiques indispensables aux télétravailleurs, avec un système de routage qui s'adapte en toute transparence aux performances applicatives et aux exigences du trafic.

La problématique

Face à l'intensification de la demande autour des espaces de télétravail, les services IT des entreprises du monde entier s'intéressent aujourd'hui en priorité à la disponibilité et à la sécurité des services VPN. Dans leur version classique et pour des raisons de sécurité, les VPN acheminent l'ensemble du trafic via un tunnel jusqu'au réseau de l'entreprise. Ce trafic englobe aussi bien les applications SaaS (Software as a Service) publiques sécurisées (comme Microsoft Teams, Salesforce et Google Suites), que l'accès Internet standard ou les services hébergés sur les sites client.

Traditionnellement, les solutions VPN reposent sur une tunnelisation IPsec ou SSL. Ces types de VPN sont complexes et difficiles à faire évoluer, et n'offrent aucun contrôle, ni aucune visibilité sur les applications. Dans un contexte marqué par une adoption massive du cloud, par un développement de l'Internet des objets (IoT), par une mobilité croissante des utilisateurs et par la nécessité d'améliorer la réactivité des applications, le modèle de routage rigide fourni par ces technologies de tunnelisation n'est guère favorable à la promotion du télétravail. Les coûts élevés du VPN/WAN ne font que frustrer les entreprises, qui sont de plus en plus nombreuses à vouloir moderniser ces services. En profitant de cette occasion pour transformer leurs réseaux en parallèle, les entreprises peuvent véritablement rentabiliser leurs investissements dans le WAN.

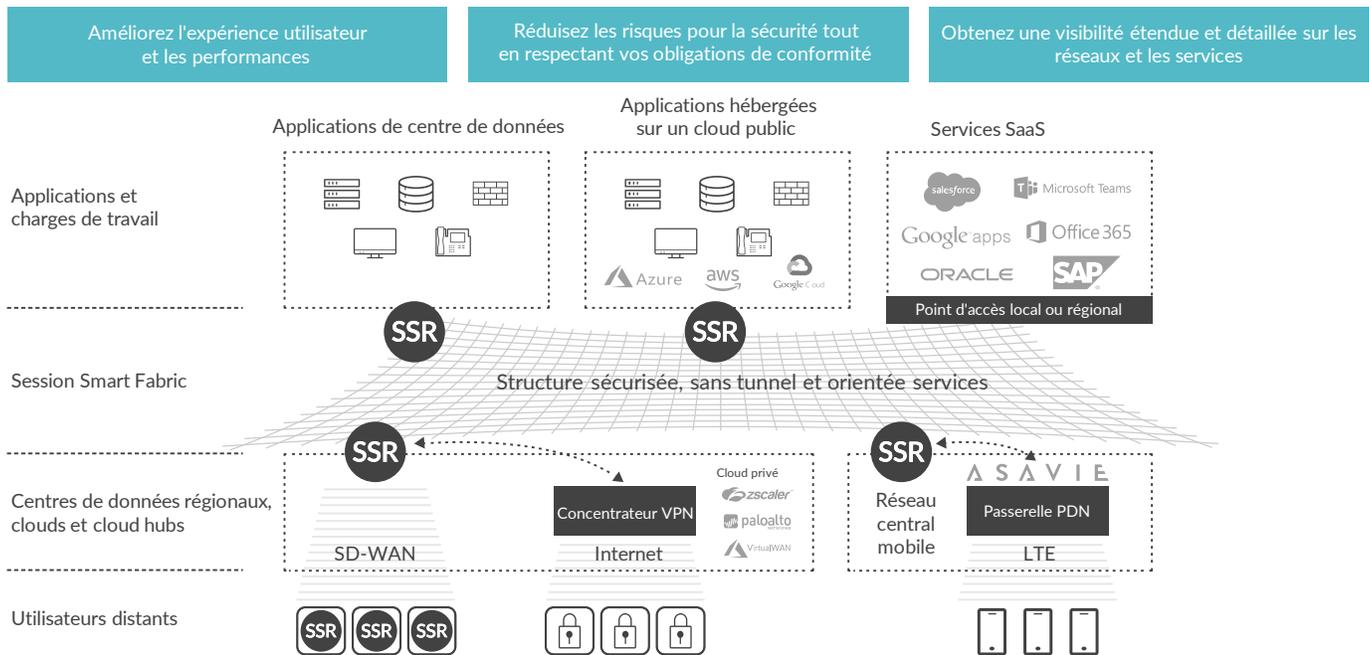


Figure 1 – Session Smart SD-WAN pour utilisateurs distants

La solution Session Smart SD-WAN de Juniper

Les réseaux n'ont jamais joué un rôle aussi important dans notre quotidien et nos moyens de subsistance ; ce qui explique pourquoi les entreprises recherchent plus que jamais des solutions réseau hautement distribuées et sécurisées. La structure orientée services de la solution Juniper Session Smart SD-WAN simplifie l'architecture « work from anywhere » pour offrir agilité et sécurité tout en proposant aux utilisateurs une expérience de qualité.

Composant essentiel de la solution, le routeur Juniper Session Smart s'adapte dynamiquement aux besoins de performances des applications et achemine le trafic en conséquence. Cette approche sans tunnel réduit la latence des applications tout en augmentant la bande passante disponible pour les applications vidéo et autres applications qui consomment d'importantes ressources réseau. L'optimisation des sessions en mode natif permet d'améliorer la rapidité et la fiabilité des applications, de même que tous les aspects liés à la qualité, à la sécurité et à la conformité.

Le monde actuel hautement dispersé, où l'espace de travail n'a plus de frontières physiques, remet définitivement en cause l'ancienne approche de sécurisation du périmètre en faveur d'une sécurité réellement intégrée au cœur des réseaux. La solution Session Smart SD-WAN offre une structure zero trust qui assure un contrôle d'accès inégalé sur les ressources et données stratégiques indispensables aux collaborateurs, avec un mécanisme de routage conçu pour acheminer ces ressources au bon endroit et au bon moment.

L'avantage du routeur Session Smart

Le routeur Juniper Session Smart évite d'avoir à recourir à des tunnels VPN inefficaces et donne du contexte au réseau en associant des sessions transitoires aux applications et services qu'elles prennent en charge. Cette technologie simplifie la manière dont les entreprises répondent aux besoins d'une main-d'œuvre distante, en offrant un mécanisme de gestion centralisé, un contrôle détaillé, des flux individualisés et des fonctions intégrées, le tout complété par une sécurité intrinsèque et une gestion dynamique du trafic. Les fonctionnalités intelligentes intégrées à la solution Session Smart SD-WAN aident les entreprises à offrir un degré inégalé de qualité, de fiabilité et d'évolutivité aux applications et services qui leur permettent de prospérer, et cela même lorsque les télétravailleurs sont nombreux et leur activité intensive.

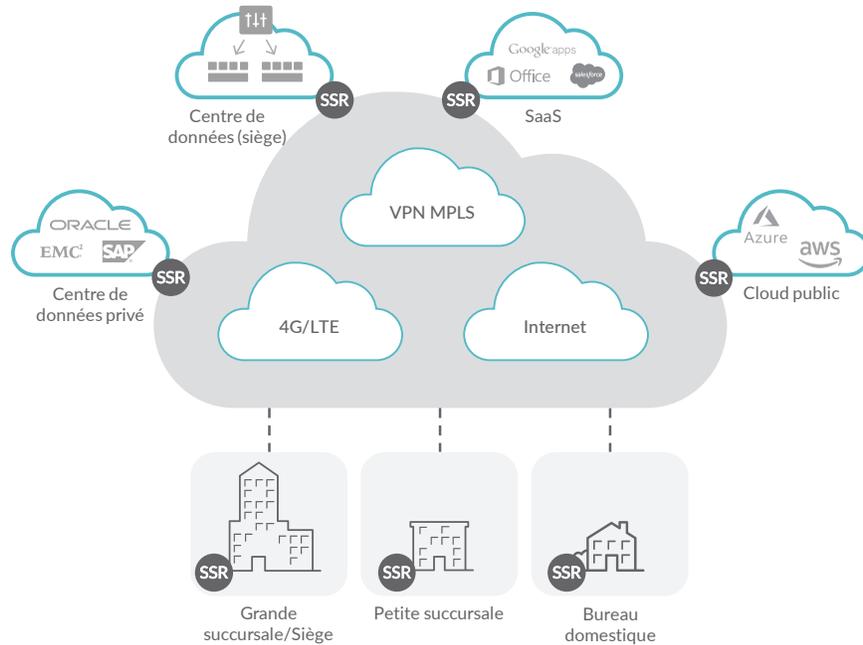


Figure 2 - Session Smart SD-WAN, connectivité sans tunnel

En plus d'éviter les réseaux de superposition et les tunnels, la solution Session Smart SD-WAN centralise les informations sur les services, les locations et les stratégies. Cette approche évite d'avoir à recourir à des outils d'automatisation, limite la complexité, améliore la visibilité et

réduit les coûts. Cette approche sensible au contexte permet également de mieux répondre aux besoins des entreprises et de les guider vers la réussite, en particulier à l'heure où elles sont confrontées à des difficultés inédites et où il devient essentiel pour elles d'accompagner efficacement leur personnel en télétravail.



Figure 3 - Session Smart SD-WAN est sensible au contexte

Fonctionnalités et avantages

Routage en fonction des applications

Les services IT peuvent améliorer les performances de leurs réseaux grâce à un routage qui s'adapte aux applications. Par exemple, le routeur Session Smart reconnaît les applications telles que Microsoft Office 365, Google Suites ou d'autres services SaaS et délègue directement ce trafic sur le WAN. Seules les applications hébergées par l'entreprise sont acheminées vers le centre de données. Par ailleurs, la gestion dynamique des sessions et la reconnaissance des applications permettent d'équilibrer les charges et d'acheminer le trafic en fonction de règles de session définies et de l'état du réseau ; des fonctionnalités qui deviennent indispensables quand des centaines de collaborateurs sont subitement contraints de passer en télétravail.

Certification FIPS 140-2

La norme américaine de sécurité informatique FIPS 140-2 est utilisée pour approuver les modules cryptographiques et préserver la confidentialité. La solution Session Smart SD-WAN, certifiée conforme à cette norme, permet aux entreprises de créer un réseau qui respecte les exigences des normes PCI (Payment Card Industry) et HIPAA (Health Insurance Portability and Accountability Act). En outre, le routeur Session Smart possède la certification ICSA Labs Network Firewall et a obtenu l'attestation PCI. Les entreprises peuvent avoir la garantie que leurs réseaux (et leurs données) restent constamment protégés, partout où se trouvent leurs collaborateurs.

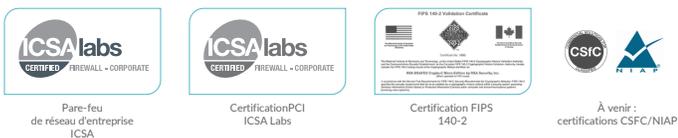


Figure 4 – Certifications FIPS-140-2 et ICSA Labs Network Firewall

Sécurité Zero Trust

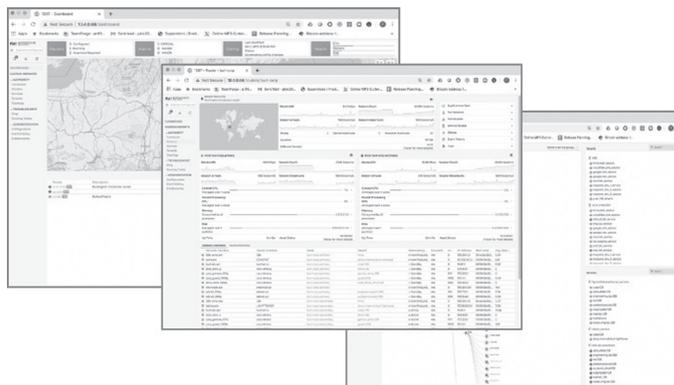
La solution Session Smart SD-WAN permet aux entreprises de déployer un réseau fondé sur une sécurité zero trust, avec la garantie que chaque flux est chiffré et authentifié compte tenu des règles de sécurité associées. Ainsi, même avec des collaborateurs en télétravail, les chefs d'entreprise peuvent avoir la certitude qu'ils seront en mesure d'offrir des connexions microsegmentées ou des VPN individualisés pour leurs différents services, y compris dans une grande organisation.



Figure 5 – Fonctionnalités de la solution Session Smart SD-WAN

Visibilité renforcée

Le conducteur Juniper Session Smart centralise l'orchestration, l'administration, le provisionnement sans intervention, la surveillance et l'analyse des routeurs Session Smart distribués. Ces outils procurent une visibilité unifiée sur l'ensemble du réseau et améliorent les statistiques de sessions, deux aspects de plus en plus importants dans les environnements de télétravail. Les administrateurs peuvent utiliser ces outils pour produire des graphiques personnalisés à partir des indicateurs de performances clés (KPI) qu'ils ont identifiés, et pour générer des rapports sur les événements de sécurité et la situation du trafic. Même avec une main-d'œuvre dispersée, les entreprises peuvent ainsi détecter et prévenir les attaques réseau, tout en respectant leurs obligations de conformité.



Cas d'usage de la solution Session Smart SD-WAN

Session Smart SD-WAN à domicile

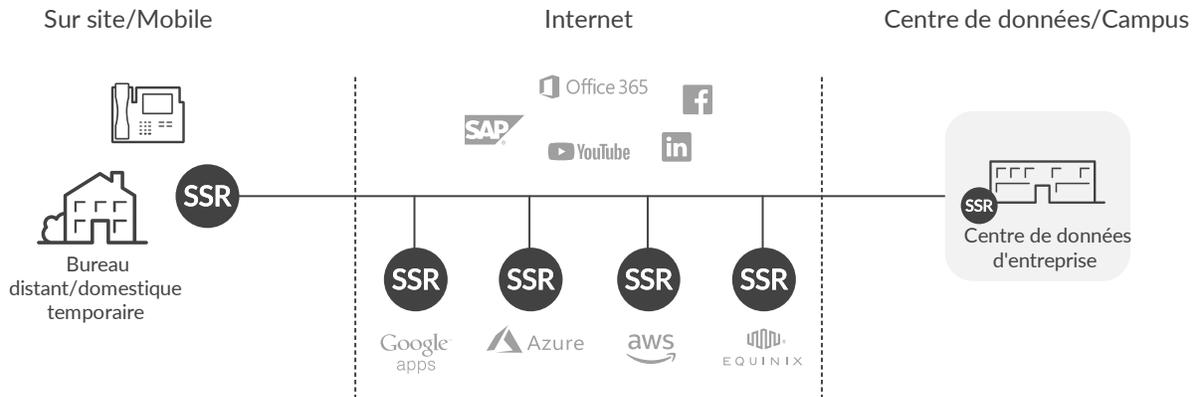


Figure 6 – Session Smart SD-WAN à domicile

Avantages pour le client

| Expérience utilisateur | Sécurité et conformité | Visibilité |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Simplicité de connexion à l'appliance | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Audit par session |
| <ul style="list-style-type: none"> • Faible latence, débit élevé | <ul style="list-style-type: none"> • Connectivité aux environnements internes/externes | <ul style="list-style-type: none"> • Performances des locations/services |
| <ul style="list-style-type: none"> • Provisionnement sans intervention | <ul style="list-style-type: none"> • Accès microsegmenté | <ul style="list-style-type: none"> • Analyse entièrement distribuée |

Dans ce cas d'usage, une instance du routeur Session Smart est déployée à domicile, et une autre dans le centre de données ou le cloud. Les applications sont ensuite acheminées de façon intelligente en fonction de leur destination. Par exemple, alors que les applications SaaS sont délestées directement sur le WAN, les applications d'entreprise qui nécessitent un traitement de gestion des menaces unifiée (UTM) plus poussé peuvent être acheminées vers le centre de données d'entreprise.

Session Smart SD-WAN dans le cloud

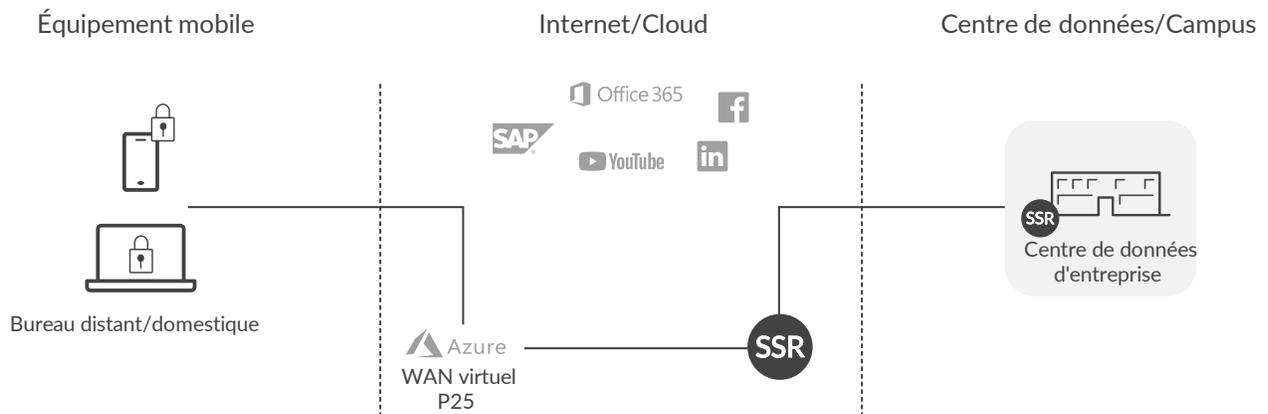


Figure 7 – Session Smart SD-WAN dans le cloud

Avantages pour le client

| Expérience utilisateur | Sécurité et conformité | Visibilité |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Expérience client d'un VPN (portail/connexion) | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Audit par session |
| <ul style="list-style-type: none"> • Évolutivité dans le cloud | <ul style="list-style-type: none"> • Connectivité aux environnements internes/externes | <ul style="list-style-type: none"> • Performances des locations/services |
| <ul style="list-style-type: none"> • Connectivité transparente | <ul style="list-style-type: none"> • Accès microsegmenté | <ul style="list-style-type: none"> • Analyse entièrement distribuée |

Dans ce cas d'usage, un collaborateur distant se connecte à la passerelle VPN cloud à l'aide d'une technologie standard, puis transfère le trafic vers le routeur Session Smart pour qu'il achemine les paquets de façon intelligente jusqu'à leur destination. Le routeur Session Smart est capable de distinguer le trafic des réseaux RFC1918, qui est acheminé vers le réseau d'entreprise, de tous les autres types de trafic (y compris les services cloud) qui sont acheminés directement jusqu'aux services ou via une solution UTM.

Session Smart SD-WAN dans le centre de données avec accès LTE privé

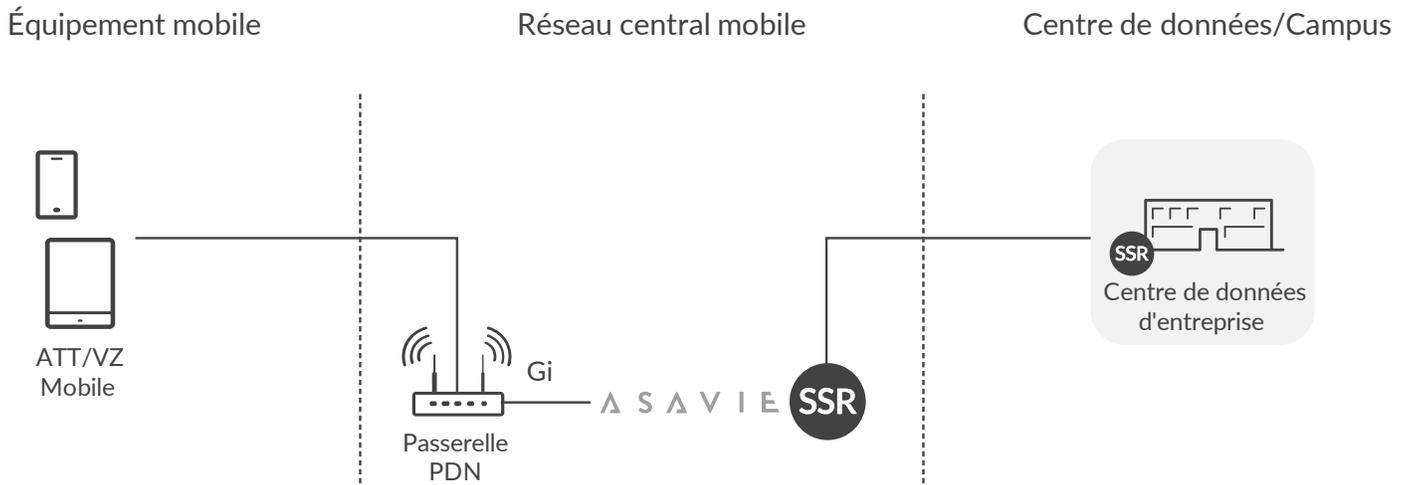


Figure 8 – Session Smart SD-WAN dans le centre de données avec accès LTE privé

Avantages pour le client

| Expérience utilisateur | Sécurité et conformité | Visibilité |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Expérience client (portail/connexion) | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Audit par session |
| <ul style="list-style-type: none"> • Évolutivité dans le cloud | <ul style="list-style-type: none"> • Connectivité aux environnements internes/externes | <ul style="list-style-type: none"> • Performances des locations/services |
| <ul style="list-style-type: none"> • Connectivité transparente | <ul style="list-style-type: none"> • Accès microsegmenté | <ul style="list-style-type: none"> • Analyse entièrement distribuée |

Ce cas d'usage bénéficie d'un partenariat avec Asavie, qui établit des connexions LTE privées de bout en bout afin de faciliter l'utilisation de connexions domestiques. La solution Session Smart SD-WAN est déployée dans le réseau central LTE et dans le centre de données d'entreprise, de manière à garantir la conformité, la sécurité du réseau et le contrôle d'accès au réseau, tout en assurant un routage en fonction des applications.

Session Smart SD-WAN avec Wireguard

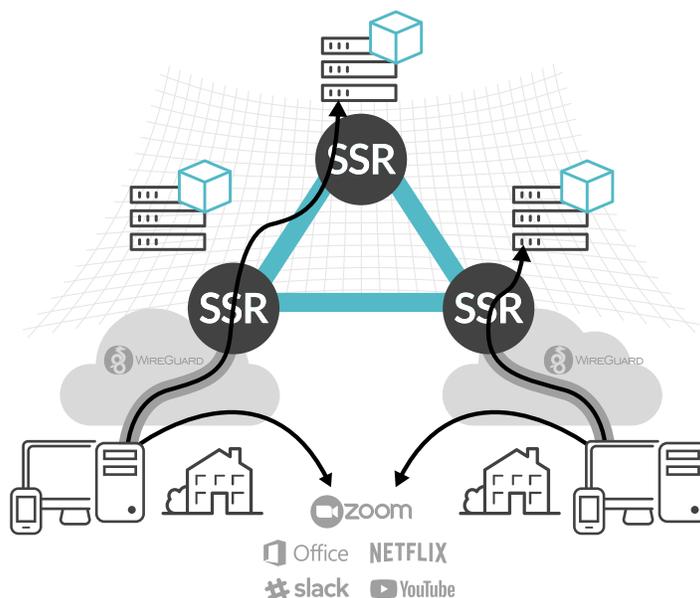


Figure 9 – Session Smart SD-WAN avec Wireguard

Avantages pour le client

| Expérience utilisateur | Sécurité et conformité | Visibilité |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Expérience sans intervention (connexion au Wi-Fi) | <ul style="list-style-type: none"> • FIPS 140-2 | <ul style="list-style-type: none"> • Audit par session |
| <ul style="list-style-type: none"> • Évolutivité dans le cloud | <ul style="list-style-type: none"> • Connectivité aux environnements internes/externes | <ul style="list-style-type: none"> • Performances des locations/services |
| <ul style="list-style-type: none"> • Provisionnement sans intervention | <ul style="list-style-type: none"> • Accès microsegmenté | <ul style="list-style-type: none"> • Analyse entièrement distribuée |

Dans ce dernier scénario de déploiement, les équipements d'entreprise conçus pour être utilisés en dehors du bureau sont dotés d'un client léger Wireguard (une solution VPN open source gratuite) qui s'apparie avec un (ou plusieurs) routeur(s) Session Smart dans la topologie d'entreprise. Par des mécanismes sélectifs et intelligents, la solution Wireguard envoie des sessions sécurisées à ses homologues de routage Session Smart d'où les services sont accessibles, et délègue les services SaaS sécurisés et grand public directement sur le réseau haut débit. Wireguard, associé au routeur Session Smart, étend le périmètre d'accès réseau de l'entreprise aux utilisateurs situés en dehors de leur environnement de bureau.

Résumé : la solution Session Smart SD-WAN favorise la réussite des équipes en télétravail

La solution Juniper Session Smart SD-WAN centralise le contrôle et simplifie le déploiement de réseaux sensibles au contexte ; elle offre un mécanisme de routage intelligent basé sur des signaux intrabandes, une microsegmentation extrêmement précise et une sécurité intrinsèque fondée sur un modèle zero trust. Cet ensemble de fonctionnalités dépasse très largement les offres de routeur traditionnelles en apportant une solution à divers problèmes réseau sous-jacents qui limitent les chances de réussite du télétravail.

Résultat : un réseau sensible au contexte, capable de s'affranchir des frontières de façon simple, dynamique et sécurisée, pour permettre aux organisations de déployer des infrastructures adaptées à leurs applications et suffisamment flexibles pour répondre aux besoins d'employés dispersés.

Perspectives

Pour savoir comment la solution Session Smart SD-WAN peut aider votre organisation à donner aux télétravailleurs les moyens de rester productifs, contactez votre représentant commercial Juniper ou rendez-vous sur www.juniper.net.

À propos de Juniper Networks

Juniper Networks simplifie les réseaux avec 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 déployons beaucoup d'efforts pour concevoir des 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 : 888.JUNIPER
(888.586.4737)
ou +1.408.7452000
Fax: +1.408.745.2100
www.juniper.net

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

