LE CAMPUS PILOTÉ PAR L'IA

L'intelligence artificielle, pilier des réseaux de campus de la prochaine décennie

Livre blanc

SOMMAIRE

Introduction 3
Juniper AI-Driven Campus Network : le réseau de campus Juniper piloté par l'IA 3
Plateforme AIOps moderne de microservices cloud 4
Commutation Wi-Fi et filaire pilotée par l'IA 4
Fabrics de campus 5
Commutateurs Ethernet de campus cloud-ready 6
Déploiement d'une fabric de campus pilotée par l'IA 7
Gestion opérationnelle d'une fabric de campus pilotée par l'IA 8
Points d'accès Wi-Fi d'entreprise 9
Juniper Connected Security 9
Junos OS : Pilier des réseaux haute-performance 12
Télémétrie Junos 12
Conclusion 13
À propos de Juniper Networks 13

SYNTHÈSE

Le réseau de la prochaine décennie a pour double vocation d'améliorer l'expérience utilisateur et de simplifier les opérations informatiques. Seulement voilà, face aux défis actuels et à la diversité des besoins des entreprises, les solutions LAN filaires et sans fil traditionnelles ne sont plus à la hauteur. Évolutivité, fiabilité, sécurité, performances, agilité… tout leur fait défaut.

C'est là que le campus piloté par l'IA fait toute la différence en exploitant la puissance de l'intelligence artificielle (IA) à l'ère du cloud, du mobile et de l'IoT. La solution campus de Juniper allie un portefeuille d'équipements robustes à la puissance de Mist AI™ pour simplifier les opérations réseau, améliorer les expériences utilisateurs et permettre aux équipes IT de se recentrer sur les initiatives stratégiques. Découvrez dans ce livre blanc les différentes composantes d'un réseau de campus piloté par l'IA de Mist AI.

Introduction

Les réseaux d'entreprise connaissent une véritable métamorphose en réponse aux exigences croissantes du cloud et à la prolifération des équipements mobiles et IoT. Le problème, c'est que la complexité tend à augmenter avec le nombre d'équipements. Côté métiers, les applications cloud ouvrent la voie à de nouveaux business models, offrent une plus grande flexibilité et favorisent l'adoption de technologies clés telles que les communications unifiées, la vidéo et d'autres applications sensibles à la latence. Côté IT, les avancées technologiques et l'adoption généralisée du machine learning (ML) et de l'IA peuvent améliorer considérablement les opérations et les expériences des équipes informatiques et des utilisateurs.

Face à ces nouvelles exigences, les architectes réseau doivent repenser la conception de leurs réseaux pour prendre en charge les composantes data, voix et vidéo des applications cloud. Pour ce faire, ils font appel à des standards réseau ouverts et à des plateformes de gestion logicielles qui leur permettent de réduire les coûts opérationnels. Au final, tout l'enjeu est d'exploiter le potentiel de fonctions d'automatisation, de télémétrie et d'IA simplifiées pour concevoir le réseau de la décennie à venir.

Juniper AI-Driven Campus Network : le réseau de campus Juniper piloté par l'IA

Le portefeuille Juniper Networks de services cloud, de logiciels et d'équipements offre des solutions de réseau de campus de bout en bout. WAN, LAN, Wi-Fi, sécurité… il couvre tous ces domaines et prend en charge des standards réseaux ouverts, notamment EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN), dans un souci permanent de simplicité architecturale, d'évolutivité et de performances.

Le réseau de campus piloté par l'IA de Juniper se compose des éléments suivants :

- Plateforme AIOps moderne de microservices cloud
- Commutation Wi-Fi et filaire pilotée par l'IA
- Fabrics de campus sur une architecture EVPN-VXLAN
- Commutateurs Ethernet de campus cloud-ready
- Points d'accès d'entreprise avec Wi-Fi, Bluetooth LE et IoT
- Juniper Connected Security et segmentation du réseau
- Système d'exploitation Junos®
- Télémétrie Junos

Plateforme AIOps moderne de microservices cloud

L'architecture de Juniper® Mist Cloud repose sur des microservices garants d'une agilité, d'une évolutivité et d'une résilience inégalées. Les services cloud peuvent monter ou descendre en charge selon les besoins, sans les coûts ni la complexité caractéristiques des équipements monolithiques. À la clé, le déploiement quasi hebdomadaire de nouvelles améliorations et de correctifs sans aucune perturbation du réseau. Entièrement programmable, cette plateforme s'appuie sur des API ouvertes permettant une automatisation complète et une intégration transparente à des produits tiers complémentaires. Cette approche innovante des réseaux d'entreprise, nous la devons à l'architecture Juniper Mist Cloud combinant l'IA, le ML et la science des données avec la toute dernière technologie de microservices pour offrir une solution incomparable.

Commutation Wi-Fi et filaire pilotée par l'IA

Juniper applique Mist AI aux réseaux de campus pour optimiser l'expérience utilisateur et simplifier la gestion IT opérationnelle à l'aide d'une solution filaire et sans fil unifiée. Vieilles de plus de 15 ans, les solutions traditionnelles s'appuient sur des bases de code monolithiques difficiles à gérer, sujettes aux bugs et très coûteuses à faire évoluer. Or, la disponibilité n'est plus le seul mot d'ordre. Désormais, l'expérience utilisateur s'impose comme le principal critère de mesure de la performance d'une infrastructure réseau. Penchons-nous sur la méthode Juniper.

Juniper Mist Wi-Fi Assurance remplace les tâches manuelles de dépannage par des opérations sans fil automatisées, avec à la clé un Wi-Fi prévisible, fiable, mesurable et doté d'une visibilité totale sur les niveaux de service côté utilisateurs. La fonction de détection des anomalies déclenche automatiquement une capture de paquets pour corréler les événements, ce qui permet d'enrichir l'intelligence réseau avec la gestion des ressources radio (RRM) au niveau du client et de bénéficier d'une visibilité sans précédent sur l'expérience utilisateur du réseau sans fil.

Quant aux équipements filaires, ils bénéficient de l'automatisation pilotée par l'IA de Juniper Mist Wired Assurance (voir Figure 1). Ce service exploite la télémétrie détaillée de Junos, issue des commutateurs Ethernet EX Series de Juniper Networks®, pour simplifier les opérations, raccourcir le temps moyen de réparation (MTTR) et accroître la visibilité sur les expériences utilisateurs à travers différents types d'équipements (IoT, serveurs, imprimantes, etc.). Juniper Mist Wired Assurance simplifie tous les aspects de la commutation EX Series, de l'intégration jusqu'au provisionnement, en passant par la gestion de l'architecture de Juniper Mist Cloud.

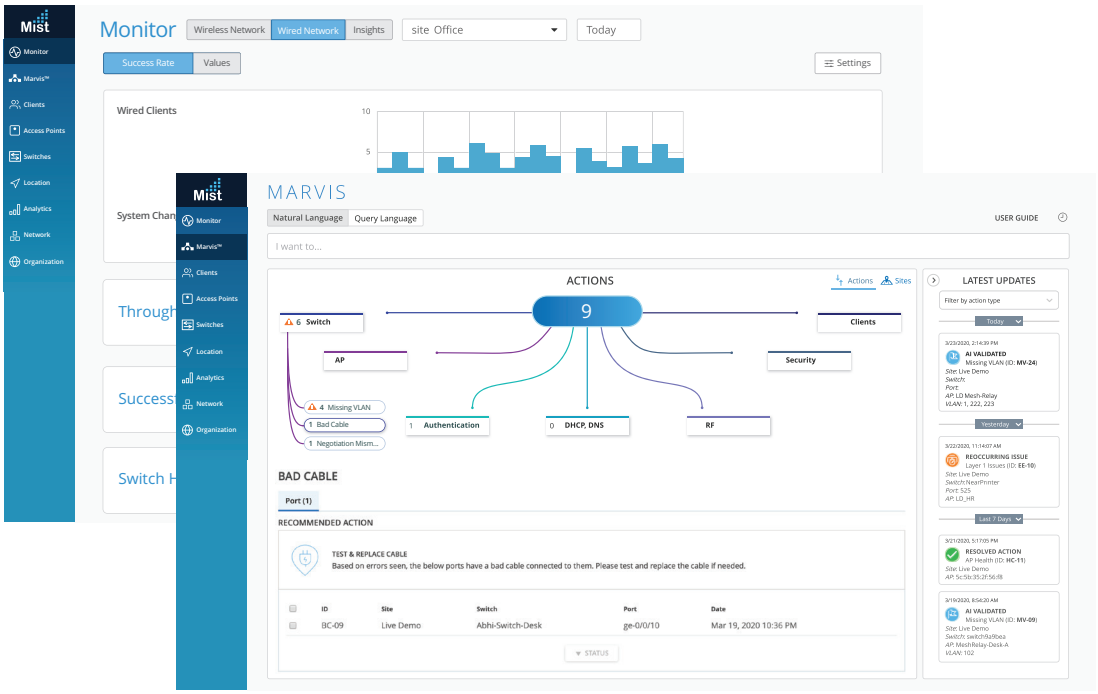

Figure 1. Wired Assurance et Assistant de réseau virtuel Marvis

L'assistant de réseau virtuel Marvis (Figure 1) est conçu spécialement avec Mist AI pour les réseaux WLAN, LAN et WAN d'entreprise. Grâce à sa compréhension du langage naturel, il permet aux utilisateurs d'interagir directement avec le moteur de Mist AI. Quant à ses capacités d'action autonomes, elles transforment en profondeur les opérations réseau, passant d'un dépannage réactif à une remédiation proactive. Résultat, Marvis renforce l'efficacité des équipes IT, réduit les tickets de support et raccourcit le temps moyen de résolution. À l'heure où l'adoption de l'IA appliquée aux opérations IT (AIOps) continue de s'accélérer, Marvis aide les entreprises à gérer leurs vastes environnements informatiques avec efficacité et précision.

Fabrics de campus

La généralisation des équipements IoT sur le campus impose aux réseaux de pouvoir rapidement monter en charge, sans pour autant ajouter de la complexité. En raison de leurs capacités réseau limitées, ces appareils requièrent une contiguïté sur la couche L2 entre les bâtiments ou les campus. Le problème, c'est que les réseaux de couche L2 créent des boucles (looping), ralentissent la convergence en cas de défaillance et engendrent des problèmes de sécurité liés au flooding du plan de données. Traditionnellement, les VLAN privés propriétaires ont permis de combler cette faille de sécurité. Reste toutefois à régler les problèmes de boucles et de lenteur de la convergence propres à la couche L2. De même, cette approche s'avère inefficace et difficile à gérer : inefficace en raison de la consommation excessive de la bande passante ; difficile à gérer, car les VLAN doivent être étendus à de nouveaux ports réseau.

EVPN-VXLAN

L'architecture de campus pilotée par l'IA dissocie le réseau overlay (superposé) du réseau underlay (sous-jacent) grâce à des technologies basées sur des standards ouverts, comme Ethernet VPN (EVPN) et Virtual Extensible LAN (VXLAN). Non seulement cette approche élimine les boucles et accélère la convergence, mais elle répond aussi aux besoins des réseaux d'entreprise d'aujourd'hui en permettant aux administrateurs réseau de créer des réseaux L2 logiques sur différents réseaux de couche L3. Autre avantage de la technologie EVPN-VXLAN : la microsegmentation du trafic entre les équipements IoT, gage d'une sécurité renforcée. Juniper prend en charge les fabrics de campus EVPN-VXLAN validées suivantes :

- **Multihébergement EVPN (sur cœur réduit ou distribution)** : le multihébergement EVPN au niveau de la distribution du réseau permet aux commutateurs d'accès d'agréger les liens sur une paire d'équipements de distribution. Grâce à ses capacités de multihébergement – de la couche d'accès à la couche de distribution – le protocole STP (Spanning Tree Protocol) n'est plus nécessaire sur les réseaux de campus. Cela permet également de réduire les couches de distribution et du cœur.
- **Distribution centrale des fabrics de campus** : une paire de commutateurs centraux ou de distribution EX Series interconnectés assure la prise en charge des passerelles EVPN L2 et VXLAN L3. Le réseau IP Clos entre les couches de distribution et de cœur de réseau offre deux modes : superposition à pont central ou à routage périphérique.
- **Fabric de campus IP Clos :** l'architecture de la fabric de campus IP Clos pousse la fonctionnalité de passerelle VXLAN L2 vers la couche d'accès, activant ainsi la microsegmentation standardisée à l'aide de politiques basées sur des groupes.

Grâce à cette architecture EVPN-VXLAN de bout en bout, vous pouvez gérer votre campus et votre datacenter comme une seule et même fabric IP, avec une politique et un contrôle OTT (over-the-top) fournis par Juniper. Le recours aux politiques de groupes pour l'ensemble du réseau simplifie également l'application des politiques. Un nombre illimité de commutateurs peuvent être connectés dans un réseau Clos ou une fabric IP : le réseau EVPN-VLAN étend la fabric et relie plusieurs bâtiments tandis que le réseau VXLAN étire la couche L2 à travers le réseau.

Pour en savoir plus, rendez-vous sur https://www.juniper.net/content/dam/www/assets/solution-briefs/fr/fr/evpn-vxlan-campus-fabrics.pdf.

Outre les architectures basées sur EVPN-VXLAN, Juniper prend également en charge la technologie Virtual Chassis. Son principe : permettre à un maximum de 10 commutateurs interconnectés de fonctionner comme un seul dispositif logique avec une seule adresse IP. Résultat, les entreprises peuvent séparer la topologie physique des regroupements logiques d'équipements, pour une utilisation plus efficace des ressources.

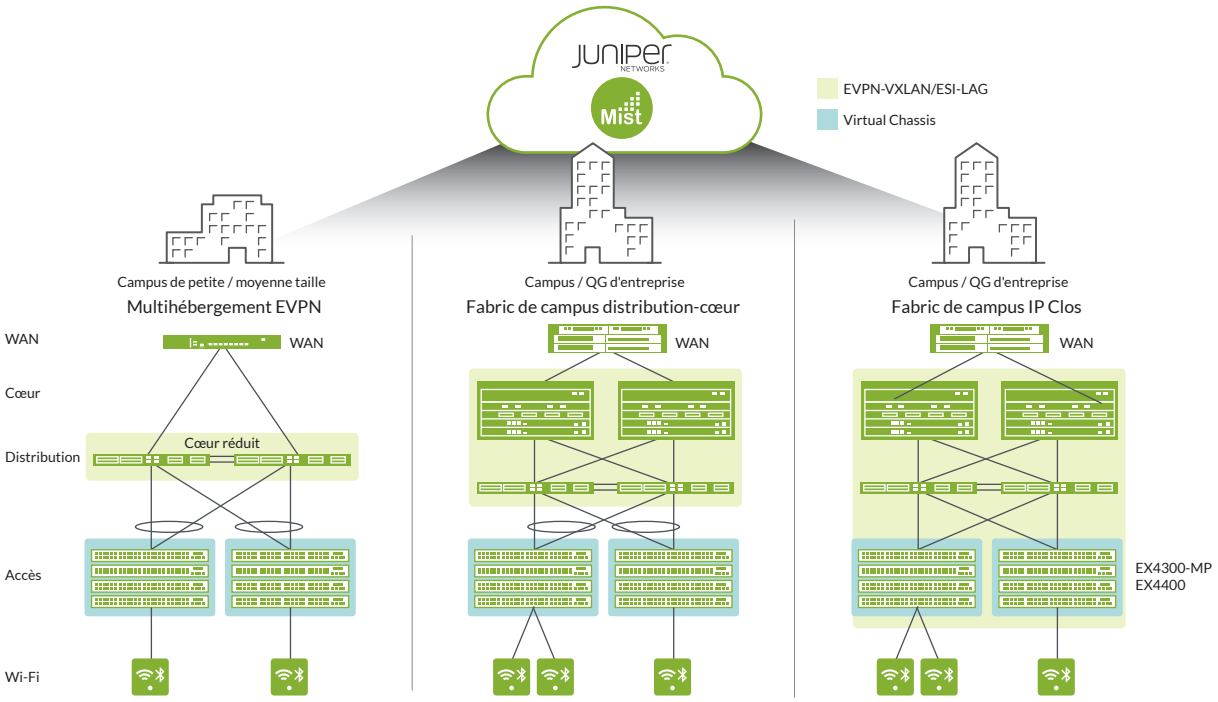

Figure 2. Fabrics de campus présentant des architectures basées sur Virtual Chassis et EVPN-VXLAN

Commutateurs Ethernet de campus cloud-ready

Juniper propose un portefeuille ouvert, programmable et piloté par l'IA de commutateurs d'accès et de cœur/distribution pour les réseaux de campus des entreprises. Ces commutateurs d'accès cloud-ready prennent en charge Juniper Mist Wired Assurance, ce qui permet d'intégrer l'AIOps aux commutateurs sur la couche d'accès. Les commutateurs répondent à un certain nombre d'exigences des réseaux de campus, parmi lesquelles :

- Capacités cloud-ready et gestion par l'architecture Juniper Mist Cloud
- Capacités multigigabits
- Media Access Control Security (MACsec) AES256
- Power over Ethernet (PoE/PoE+/PoE++)
- Évolutivité des architectures de fabric grâce à Virtual Chassis et EVPN-VXLAN
- Prise en charge multifournisseur
- Microsegmentation standardisée à l'aide de politiques basées sur des groupes (GBP)
- Télémétrie basée sur les flux

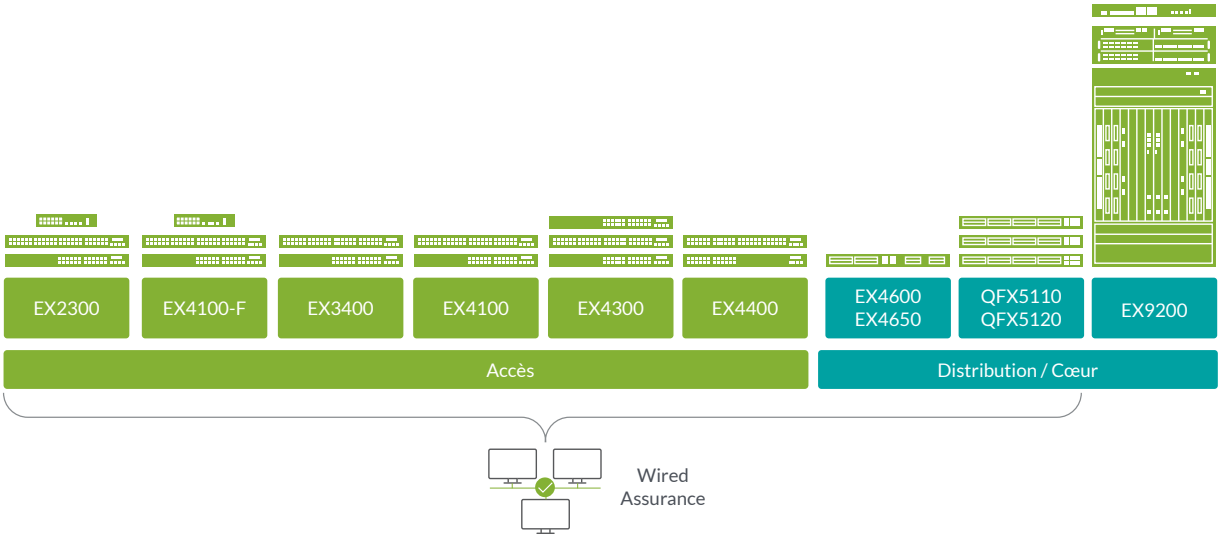

Figure 3. Le portefeuille de campus des commutateurs EX Series et QFX Series

Déploiement d'une fabric de campus pilotée par l'IA

Force est de constater que la configuration manuelle des fabrics de campus peut engendrer des incohérences et des erreurs imprévues dans les déploiements. Pour pallier ce problème opérationnel, la solution Juniper Mist Cloud simplifie la gestion des fabrics de campus EVPN-VXLAN. Plus précisément, les administrateurs peuvent choisir une topologie (multihébergement EVPN, distribution-cœur ou IP Clos) et laisser le logiciel faire le reste (voir Figure 4). Cette approche orientée IA unifie la gestion des environnements LAN, WLAN et WAN sur le campus et les sites distants, tout en garantissant une expérience utilisateur hors pair sur le réseau filaire et sans fil du campus.

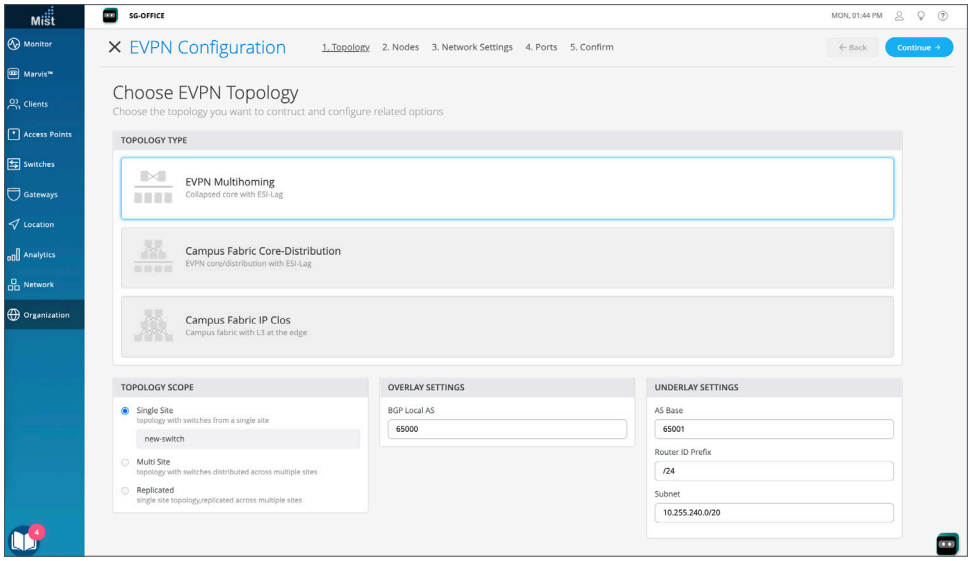

Figure 4. Conception de fabric de campus avec Juniper Mist Wired Assurance

*Multihébergement EVPN initialement pris en charge, architectures supplémentaires prises en charge dans les futures versions.

Gestion opérationnelle d'une infrastructure de campus pilotée par l'IA

Juniper Mist™ Wired Assurance active, configure, gère et dépanne les commutateurs Ethernet EX Series gérés dans le cloud. Ce service cloud offre une automatisation et des niveaux de service pilotés par l'IA, garants d'une meilleure expérience sur les appareils connectés. Juniper Mist Wired Assurance exploite la télémétrie de commutation détaillée de Junos® pour simplifier les opérations, raccourcir le temps moyen de réparation et améliorer la visibilité. Tour d'horizon des principales caractéristiques des opérations, de la conception (jour 0) à la gestion (jour 2) :

- **Opérations du jour 0** : intégration transparente des commutateurs, soit par l'activation d'un nouveau commutateur, soit par le transfert d'un commutateur existant, avec un code d'activation unique pour offrir toute la simplicité du plug-and-play.
- **Opérations du jour 1** : configuration basée sur des modèles pour permettre le déploiement en masse de fabrics traditionnelles et de campus, tout en conservant la flexibilité et le contrôle nécessaires pour appliquer des attributs personnalisés aux sites ou aux commutateurs. Les profils de ports dynamiques permettent le provisionnement automatique des ports.
- **Opérations du jour 2** : l'IA de Juniper Mist Wired Assurance aide à satisfaire les exigences de niveau de service (débit, connexions réussies, intégrité des commutateurs), grâce à une série de métriques clés avant et après la connexion (voir Figure 5). À cela s'ajoutent les nombreuses capacités de pilotage autonome de Marvis Actions : détection des boucles, ajout des VLAN manquants, réparation des ports mal configurés, identification des câbles défectueux, isolation des ports instables, et détection des clients défaillants (voir Figure 6). Enfin, Juniper Mist Cloud simplifie les mises à niveau logicielles.

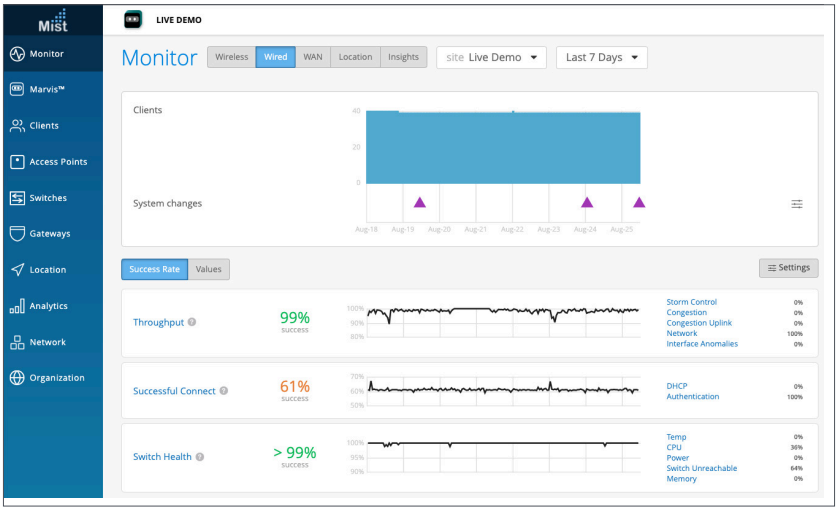

Figure 5. Niveaux de service garantis de Juniper Mist Wired Assurance

Figure 6. Marvis Actions pour les commutateurs filaires

En savoir plus sur Juniper Mist™ Wired Assurance.

Points d'accès Wi-Fi d'entreprise

Avec sa gamme de points d'accès d'entreprise, Juniper s'impose comme le chef de file de la convergence du Wi-Fi, du Bluetooth Low Energy (BLE) et de l'IoT. Les capacités de ML et de corrélation des événements de ces produits facilitent la collecte et l'analyse des données, ainsi que l'application des politiques. Les points d'accès haute-performance des séries AP43 et AP45 de Juniper sont dotés d'une batterie brevetée d'antennes dynamiques vBLE à 16 éléments, qui assure les services de géolocalisation les plus précis et les plus évolutifs du marché. Les points d'accès Juniper sont spécialement conçus pour collecter des métadonnées sur plus de 150 états entrant dans le moteur Mist AI.

Fonctionnalité	AP45	AP34	AP43	AP63	AP33	AP32	AP12
Norme Wi-Fi	Wi-Fi 6E 802.11ax (Wi-Fi 6) 4x4 : 4SS	Wi-Fi 6E 802.11ax (Wi-Fi 6) 2x2 : 2SS	802.11ax (Wi-Fi 6) 4x4 : 4SS	802.11ax (Wi-Fi 6) 4x4 : 4SS	802.11ax (Wi-Fi 6) ; 5 GHz : 4x4 : 4SS 2,4 GHz : 2x2 : 2SS	802.11ax (Wi-Fi 6) ; 5 GHz : 4x4 : 4SS 2,4 GHz : 2x2 : 2SS	802.11ax (Wi-Fi 6) 2x2 : 2SS
Options d'antenne	Interne/ Externe	Interne	Interne/ Externe	Interne/ Externe	Interne	Interne/ Externe	Interne
BLE virtuel	✓	–	✓	✓	✓	–	–

Juniper Connected Security

Selon ZDNet, en 2020, le FBI a enregistré une hausse de 69 % des plaintes pour cyberattaques par rapport à l'année précédente. Face à cette explosion, il est plus crucial que jamais que les entreprises, petites ou grandes, se dotent d'une stratégie de sécurité efficace. Or, la protection de leur réseau passe d'abord par une visibilité totale, tant sur les ressources à protéger que sur les menaces en présence. Tout angle mort pourrait leur être fatal. Malgré la forte dynamique d'innovation de ces dix dernières années, les acteurs de la sécurité réseau n'ont pas réussi à infléchir la courbe des compromissions. Pour cela, il leur faudrait sécuriser chaque point de connexion sur l'ensemble du campus. Avec le renfort de l'IA, le réseau pourrait ainsi mettre en place une défense efficace pour neutraliser plus rapidement les attaques.

Cette approche de la sécurité réseau, c'est celle de Juniper® Connected Security. Elle étend la visibilité, la Threat Intelligence et les contrôles à chaque point de connexion – du client jusqu'au workload. En s'appuyant d'une part sur chaque point de connexion pour savoir qui se trouve sur le réseau de campus, et d'autre part sur l'IA pour déterminer les risques à l'instant t, les entreprises peuvent réduire leur exposition et sécuriser le campus sans pour autant bloquer l'accès aux ressources.

La sécurité se doit de protéger deux choses : les données du datacenter et leur accès en périphérie. L'approche Zero Trust a pour vocation de protéger les données et leur accès. Or, la protection des données passe par une triple exigence : le chiffrement des données en transit, le chiffrement des données au repos et une connexion sécurisée.

- Le protocole Secure Vector Routing (SVR) permet une segmentation basée sur le vecteur de routage, compliquant ainsi toute tentative par les attaquants d'intercepter les données en transit.
- La solution Juniper Secure Connect établit un accès Zero Trust Network Access (ZTNA) pour toutes les connexions réseau, quelle que soit leur provenance, et les encapsule dans un tunnel privé.
- Les contrôles de sécurité basés sur l'intention automatisent l'application des politiques de sécurité dans les environnements de cloud public, et ce grâce aux capacités d'automatisation de Junos. Par exemple, toutes les données au sein de nouveaux compartiments Amazon S3 sont chiffrées au repos. Nul besoin de configurer les règles manuellement pour appliquer l'autorisation d'accès aux données.

Le réseau

Les paquets transitant d'un point à un autre du réseau doivent remplir les conditions suivantes : être légitimes, être dépourvus d'exploits ou de malwares et être autorisés à aller d'un point A à un point B. Le trafic doit donc être passé au crible pour détecter tout contenu malveillant.

Les pare-feu nouvelle génération (NGFW) s'imposent comme la solution idéale d'inspection du trafic. Si l'on tend à appliquer des signatures aux en-têtes et aux corps de paquets, ainsi qu'aux groupes de paquets, pour repérer tout trafic malveillant, l'IA pour sa part évalue rapidement les fichiers inconnus, les comportements systèmes et les schémas de trafic pour repérer les signes d'une tentative d'attaque en cours.

Les passerelles de services SRX Series de Juniper Networks assurent visibilité et contrôle sur le trafic réseau, mais pas seulement : leurs services de sécurité pilotés par l'IA permettent également de mieux lutter contre les menaces connues et inconnues. Au menu :

- Prévention contre les nouveaux malwares : Juniper ATP Cloud s'appuie sur le machine learning pour évaluer rapidement les fichiers inconnus et détecter les malwares ou graywares en analysant leurs comportements dans l'environnement d'exécution.
- Visibilité et contrôle sans déchiffrement : Juniper ATP Cloud évalue aussi les risques provenant du trafic réseau chiffré et des appareils connectés (dont l'IoT) en analysant les composants essentiels des certificats utilisés et des comportements du trafic.

Utilisateurs

Sur le campus, vos utilisateurs accèdent aux ressources internes, mais aussi à celles exposées à Internet. En ce sens, ils constituent un vecteur d'attaque potentiel. Pour limiter le risque, leur accès doit donc être contrôlé et authentifié.

C'est dans cette optique que les passerelles SRX Series de Juniper appliquent des politiques basées sur les utilisateurs pour assurer des contrôles d'accès granulaires à toutes les ressources internes et externes. La gamme SRX Series s'intègre à toutes les solutions IAM du marché ; elle permet ainsi aux politiques de sécurité et d'accès sécurisé de suivre les utilisateurs partout dans leurs déplacements. Par ailleurs, Juniper ATP Cloud détermine si le compte utilisateur a été compromis, adapte de manière dynamique la politique de sécurité ou le VLAN, et applique des niveaux d'authentification supplémentaires si nécessaire.

Workloads

Les workloads sont les éléments parfois éphémères qui sous-tendent les applications. En protégeant vos workloads contre les exploits applicatifs et en les séparant des autres workloads et applications, vous dressez un dernier rempart autour des précieuses données qu'abrite votre datacenter.

- Sur site ou dans le cloud, la solution Juniper Cloud Workload Protection protège les applications contre les exploits zero-day, et ce dès leur apparition. Elle veille constamment à la protection des applications de production contre les exploits de vulnérabilités, garantissant ainsi la connectivité et la résilience des services stratégiques. Son arme ? La microsegmentation automatique qui met à l'abri les bases de données individuelles, les collecteurs de données, et toutes les autres ressources, à l'aide notamment de sa solution de protection des applications en cours d'exécution.
- Le pare-feu de conteneurs cSRX de Juniper Networks protège les applications via un pare-feu conteneurisé. Pour cela, il segmente et contrôle le trafic à destination et en provenance de chaque application.

Équipements et appareils

Appareils utilisateurs, serveurs occasionnels, objets connectés (IoT)… la diversité des équipements et appareils du campus se connectant au réseau représente un véritable casse-tête en termes de visibilité. En effet, les équipements IoT sont légion sur le campus – du distributeur automatique de snacks à l'imprimante, en passant par la machine à café connectée. À la différence des appareils utilisateurs, les dispositifs IoT ne sont pas toujours équipés d'agents. Il est donc difficile d'évaluer le niveau d'accès réseau approprié et leur posture de sécurité actuelle.

- Juniper ATP Cloud, le hub de Threat Intelligence appliquée au réseau, évalue les risques qui pèsent sur les appareils connectés, identifie les différents types d'équipements (dont l'IoT), et orchestre les interventions nécessaires en cas de compromission d'un appareil connecté.

Petit aperçu des fonctionnalités d'ATP Cloud pour la protection des appareils dans un réseau Zero Trust :

Profilage des risques piloté par Mist AI

Cette fonction protège les accès réseau en périphérie (campus, site distant ou télétravail) en offrant aux équipes IT une visibilité détaillée sur le réseau et des contrôles de sécurité à chaque point de connexion, ce qui leur permet de mieux défendre leur infrastructure. Les réseaux de campus jouent ainsi une part active dans la mise en place d'un réseau orienté sécurité.

Système de sécurité intelligent pour Mist

Les alertes détectées par les passerelles SRX Series et ATP Cloud aident à évaluer rapidement les risques de sécurité lorsque des utilisateurs et équipements se connectent aux réseaux sans fil, puis à prendre les mesures qui s'imposent (par exemple, mise en quarantaine ou application de politiques).

Service SecIntel pour les commutateurs EX Series

En cas de compromission d'un appareil, ATP Cloud en informe les commutateurs EX pour qu'ils bloquent ou confinent l'équipement en question. Vous maintenez ainsi un contrôle sur chaque appareil, même en l'absence d'agents sur les terminaux.

Analyses et automatisation

En matière de sécurité, la visibilité sur les activités de votre réseau ne constitue que la première moitié du chemin. La deuxième consiste à exploiter ces informations et d'autres données CTI pour appliquer des politiques Zero Trust. Vous réduirez ainsi davantage les risques, tout en favorisant la montée en capacité des équipes réseau et sécurité. Les outils garants d'une plus grande visibilité :

- Security Director Cloud : gérez tous les contrôles de sécurité (sur site, dans le cloud et depuis le cloud) sur une seule et même console. Avec Security Director Cloud, les politiques de sécurité accompagnent les utilisateurs, les appareils et les applications dans tous leurs déplacements, sans aucun compromis sur la visibilité ou les mesures de protection contre les menaces. En clair, vous pouvez créer une politique de sécurité et l'appliquer à n'importe quel utilisateur, appareil et application, quels que soient ses mouvements et pérégrinations.
- Security Director Insights : cette fonctionnalité de Security Director ingère les données CTI et les détections issues d'outils de sécurité tiers pour dévoiler les attaques en cours et les comparer au référentiel du framework Mitre ATT&CK. Security Director prend ensuite le relais pour définir les actions qui s'imposent (directement ou via l'automatisation Ansible) et les orchestrer sur les différents outils du réseau.
- Fonctions d'automatisation Junos : doté d'un solide ensemble d'API et d'autres éléments d'automatisation natifs, le système d'exploitation Juniper Junos optimise l'automatisation du réseau. Grâce à lui, les entreprises peuvent contrôler et configurer la quasi-totalité des processus et capacités sur l'ensemble des plateformes Juniper, et en auditer les performances. Cette capacité d'accès programmatique à Junos simplifie la gestion opérationnelle et réduit vos dépenses d'investissement (CapEx) et d'exploitation (OpEx). Ainsi, vous automatisez le traitement des tickets et les demandes de changements de vos clients tout en gardant un œil sur l'intégrité globale de l'architecture.

Segmentation dans les réseaux de campus

Pour sécuriser les données et les ressources, les architectes réseau peuvent combiner les techniques de micro et macrosegmentation. Ainsi, une architecture EVPN-VXLAN universelle peut s'étendre aux campus et aux datacenters afin d'assurer la segmentation cohérente et de bout en bout des terminaux et des applications sur le réseau. Elle permet également de minimiser le flooding en couche L2 pour réduire les menaces de sécurité et simplifier le réseau.

- La macrosegmentation sépare le réseau de manière logique au sein même des équipements réseau partagés et sur les liens partagés. Dans un réseau EVPN-VXLAN, elle est assurée à l'aide de VLAN au niveau de la couche L2 et du VRF (Virtual Routing and Forwarding) au niveau de la couche L3. Le VRF assure l'isolation en maintenant le trafic IP entre deux dispositifs VRF isolés l'un de l'autre.

- La microsegmentation répond aux problèmes critiques de protection des réseaux en réduisant les risques et en s'adaptant aux exigences de sécurité. Juniper aide à mettre en œuvre une microsegmentation basée sur des listes de contrôle d'accès (ACL) ou des filtres de pare-feu pour contrôler le trafic intra-virtuel.

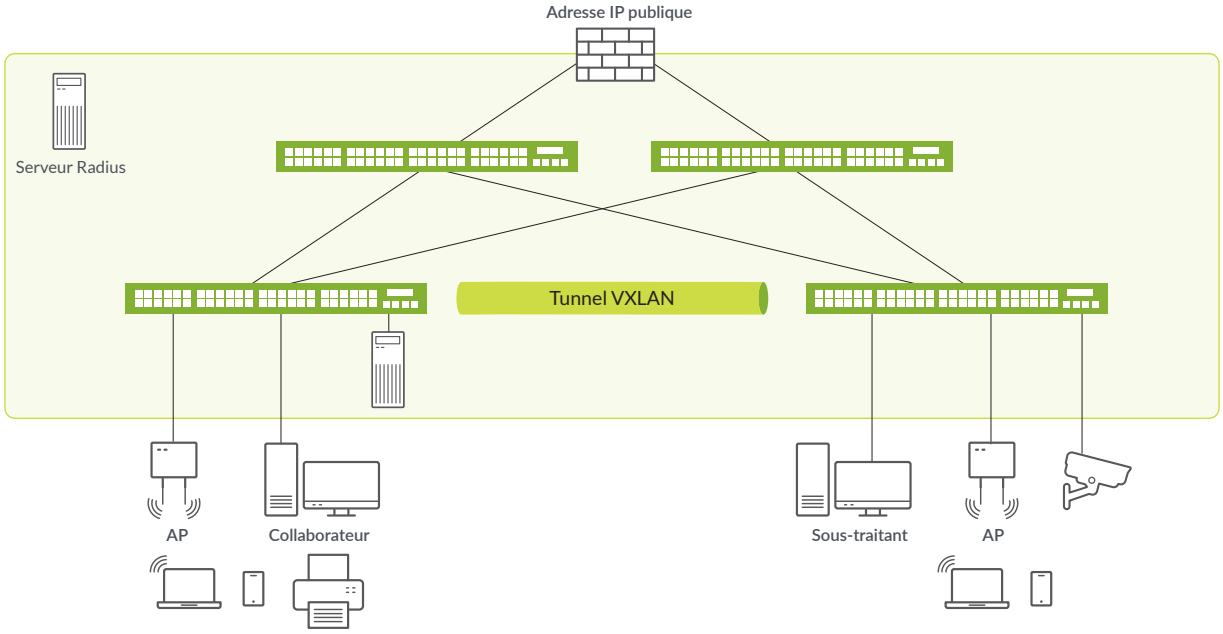

Figure 7. Segmentation du réseau en fonction des collaborateurs ou des équipements IoT

Junos OS : pilier des réseaux haute-performance

Le système d'exploitation Junos® fournit un langage commun à tous les dispositifs de routage, de commutation et de sécurité de Juniper. La puissance de Junos OS simplifie les réseaux haute-performance pour augmenter leur disponibilité et accélérer le déploiement des services, avec à la clé un coût total de possession réduit. L'expérience utilisateur homogène et l'ensemble d'outils automatisés offerts par Junos OS facilitent la planification et la formation, améliorent l'efficacité des opérations quotidiennes et permettent d'implémenter les changements plus rapidement sur le réseau.

Ce qui distingue Junos OS des autres systèmes d'exploitation réseau, c'est la façon dont il est construit : un seul système d'exploitation avec une seule architecture modulaire au sein d'un ensemble linéaire de versions logicielles. Principaux avantages :

- Un système d'exploitation unique, couvrant tout type et toute taille de plateformes, permet de réduire le temps et les efforts de planification, de déploiement et d'exploitation de l'infrastructure réseau.
- Son système linéaire de mises à jour logicielles est éprouvé et offre de nouvelles fonctionnalités à une cadence stable et régulière.
- Enfin, son architecture logicielle modulaire unique assure sécurité, évolutivité et haute disponibilité, tout en s'ouvrant à l'automatisation et à l'intégration d'innovations de partenaires.

Télémétrie Junos

Les modèles de données traditionnels qui recueillent des statistiques sur l'état opérationnel ont atteint leurs limites d'échelle et d'efficacité. L'interface de télémétrie Junos lève ces freins en s'appuyant sur un modèle push qui fournit des données de manière asynchrone, ce qui élimine tout besoin d'attente active (polling) et lui confère toute l'évolutivité nécessaire pour surveiller des milliers d'objets au sein d'un réseau.

L'interface de télémétrie Junos vous permet de provisionner des capteurs visant à collecter et exporter des données liées à une variété de ressources système, telles que les interfaces physiques et les filtres de pare-feu. Deux modèles de données sont pris en charge :

- Un modèle de données ouvert et extensible défini par Juniper Networks. Son architecture distribuée lui permet de monter en charge de manière transparente.
- Un modèle de données OpenConfig qui génère des données sous forme de messages structurés Google protocol buffer (gpb) dans un format universel clé/valeur. Les appels de procédure à distance gRPC étant basés sur TCP et acceptant le chiffrement SSL, ce modèle est considéré comme sûr et fiable.

Conclusion

Le réseau de campus piloté par l'IA de Juniper est pensé pour fournir aux clients une architecture moderne, flexible et standardisée, parfaitement en phase avec un avenir placé sous le signe du cloud. Il répond aux exigences strictes actuelles sans transiger sur la fiabilité, la sécurité et l'agilité. Les composants de base communs, les workflows d'automatisation préintégrés et les toolkits d'automatisation personnalisés étendent les avantages de l'analyse prédictive du datacenter vers le campus et au-delà.

Autres ressources

- Centre de conception du campus
- Site web gamme EX Series
- Services Juniper Mist Cloud
- Juniper Connected Security
- Démo en direct : Wired and Wireless Wednesdays
- Démo en direct : L'entreprise augmentée par l'IA
- Juniper Connected Security

À propos de Juniper Networks

Chez Juniper Networks, nous nous engageons à simplifier considérablement les opérations réseau et à offrir une expérience utilisateur incomparable. Analyses, automatisation, sécurité et IA : nos solutions de pointe sont porteuses de résultats tangibles pour votre entreprise. Car pour Juniper Networks, la connectivité, outre son pouvoir fédérateur, nous donne les moyens de résoudre les grands défis de ce monde en matière de bien-être, de développement durable et d'égalité.

Siège EMEA et APAC
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 207 125 700
Fax : +31 207 125 701

Siège social et commercial
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : 888.JUNIPER (888 586 4737)
ou +1 408 745 2000 | Fax : +1 408 745 2100
www.juniper.net/fr

2000752-006-FR juillet 2022