Juniper Networks | Engineering Simplicity

Livre blanc

L'ESSOR DU ZERO TRUST

Démêler le vrai du faux

TABLE DES MATIÈRES

SYNTHÈSE

Aujourd'hui, les entreprises ne doivent pas seulement se prémunir contre les cyberattaques et les compromissions de données sensibles. Elles doivent aussi prouver que toutes les mesures sont en place. C'est pourquoi la plupart d'entre elles optent pour ce qui apparaît comme le concept le plus viable : le Zero Trust. Que vous soyez RSSI, ingénieur ou dirigeant, vous devez impérativement comprendre à quel point le Zero Trust est devenu indispensable à toute stratégie de sécurité.

Dans ce livre blanc, nous ferons toute la lumière sur les mythes et les idées reçues entourant les architectures de sécurité Zero Trust. Nous verrons également comment Juniper Connected Security vous aide à déployer une architecture réseau résolument Zero Trust plus rapidement et en toute simplicité.

Introduction : le modèle qui révolutionne la sécurité

L'approche Zero Trust conquiert peu à peu le monde des entreprises, chamboulant sur son passage la manière dont nous abordons la sécurité en général, et les architectures réseau en particulier. Un changement plus que bienvenu dans un contexte marqué par la recrudescence des cybermenaces. Nos modèles actuels, qui accordent une confiance implicite aux utilisateurs, réseaux et systèmes internes, ont fait leur temps. En témoigne la succession sans fin de compromissions causées par ces règles trop permissives.

Si les avantages du Zero Trust ne sont plus à démontrer, le déploiement de ces architectures suscite encore de nombreuses réticences et interrogations parmi les équipes réseau et de sécurité. Devront-elles faire table rase de leur infrastructure réseau existante ? Une microsegmentation du réseau est-elle vraiment envisageable ? Les architectures Zero Trust sont-elles compatibles avec le cloud ?

Dans ce livre blanc, nous démonterons un à un les mythes et les idées reçues entourant les architectures de sécurité Zero Trust. Nous verrons également comment Juniper Connected Security vous aide à déployer une architecture réseau résolument Zero Trust plus rapidement et en toute simplicité.

Protection des environnements : nouveau périmètre, nouveaux enjeux

Auparavant, les points de terminaison étaient intégralement détenus, gérés et sécurisés par l'entreprise. De fait, chaque utilisateur ou appareil présent dans son périmètre pouvait être considéré comme fiable. Quant aux applications de l'entreprise, elles étaient exécutées dans un datacenter sécurisé, et s'accordaient en toute logique une confiance mutuelle.

Aujourd'hui, le périmètre réseau ne cesse de s'étendre à mesure que les workloads migrent vers le cloud. Les appareils mobiles non gérés, autrefois utilisés à titre exceptionnel, deviennent omniprésents au sein des entreprises. Applications, utilisateurs et équipements de travail : plus rien n'est statique, tout est dynamique. Les données de l'entreprise ne sont plus confinées dans l'enceinte de ses datacenters. Mais à force de s'étirer dans toutes les directions, les organisations perdent en visibilité. Leurs défenses se fissurent et leur surface d'attaque s'accroît, obligeant les RSSI à accumuler toujours plus d'outils non intégrés pour tenter d'assurer leur sécurité.

De leur côté, les cybercriminels redoublent d'inventivité pour trouver de nouvelles façons de contourner les systèmes de sécurité les plus avancés, y compris en latéralisant leurs attaques. Et pour leur simplifier la tâche, ils ont désormais à leur disposition des toolkits ultra-sophistiqués décrivant étape par étape comment exploiter des vulnérabilités dont le nombre augmente de façon exponentielle. C'est ainsi qu'en 2018, la National Vulnerability Database recensait 14 760 vulnérabilités connues, soit deux fois plus qu'en 2016.

Que faut-il en retenir ? Tout simplement que la sécurité des réseaux, des utilisateurs, des applications et des données ne passe plus par un renforcement constant du périmètre.

La naissance du Zero Trust

En 2009, le cabinet d'études Forrester Research présente un nouveau modèle de sécurité de l'information basé sur les principes du Zero Trust. Protection renforcée, conformité, simplicité, réduction des coûts… cette approche deviendra rapidement LA référence en matière d'architecture de sécurité des entreprises.

Source : « No More Chewy Centers: The Zero Trust Model of Information Security », Forrester research, Inc., mars 2016

Changement de paradigme dans la sécurité

C'est là que le Zero Trust entre en scène pour s'imposer de plus en plus comme le modèle garant d'une plus grande protection face aux menaces actuelles. Le mot d'ordre ? « Ne jamais faire confiance, toujours vérifier ». Autrement dit, considérer chaque élément d'un réseau comme un vecteur potentiel d'attaque, au même titre que n'importe quelle ressource Internet, et traiter les demandes d'accès en conséquence.

Plébiscité par un grand nombre d'experts, le concept de Zero Trust relègue la confiance implicite au rang de vulnérabilité critique. Faire confiance à tout ce qui se trouve au sein de l'organisation revient en effet à donner aux acteurs malveillants (internes ou externes) toute la latitude nécessaire pour se déplacer latéralement au sein d'un réseau. De simples identifiants détournés leur permettront ainsi d'accéder sans encombre aux données de leurs cibles et de les exfiltrer tout aussi facilement.

L'importance du Zero Trust

Les entreprises identifiées comme « précurseurs de la cybersécurité » dans une récente étude Forbes Insights considèrent toutes les initiatives Zero Trust comme un élément « extrêmement important » de leur stratégie de sécurité.

Source : « Cybersecurity Trailblazers Make Security Intrinsic to Their Business », Forbes Insights, 2019

La solution ? Établir des micropérimètres de sécurité autour des données, applications et services critiques afin de garantir que seuls les utilisateurs et applications autorisés peuvent accéder à ces précieuses ressources. Avec le Zero Trust, vous seul décidez qui peut franchir ou non ces micropérimètres. Les contrôles s'opèrent au plus près de la ressource. Impossible d'y accéder sans autorisation. Vos données sensibles sont ainsi protégées contre le risque d'exfiltration.

Cette approche ne couvre certes pas tous les scénarios d'attaque, mais elle offre aux entreprises des avantages considérables :

- Prévention des menaces sophistiquées et du risque de compromission grâce au blocage des mouvements latéraux et des accès non autorisés
- Détection et réponse accélérées
- Amélioration de la visibilité
- Conformité aux exigences réglementaires (HIPAA, PCI-DSS, FISMA, etc.)

Les fondamentaux du Zero Trust

Au cours des années qui ont suivi son apparition, l'approche Zero Trust est passée sous le microscope des plus grands experts et analystes de la cybersécurité. Parmi eux, le cabinet d'études Forrester, qui a d'ailleurs donné forme à sa dernière itération, baptisée Zero Trust eXtended (ZTX)[1].

Pour faire simple, le Zero Trust est un modèle architectural et conceptuel définissant de façon claire « la manière dont les équipes de sécurité doivent repenser leurs réseaux, en établissant des micropérimètres de sécurité et en employant des techniques d'obfuscation visant à renforcer la protection de leurs données, en limitant les risques liés à des droits d'accès trop permissifs et en améliorant leurs capacités de détection et de réponse grâce à l'automatisation et aux analyses. »

Le framework ZTX donne corps à cette théorie en énumérant les processus et les technologies requis pour créer un environnement orchestré et automatisé, gage de visibilité et d'analyses approfondies sur toutes les composantes de votre infrastructure : données, workloads, réseaux, appareils, collaborateurs (voir figure 1 à la page suivante).

L'approche Zero Trust s'impose peu à peu comme LA référence en matière de sécurité. Pour preuve, à l'échelle mondiale, 60 % des entreprises formalisent ou déploient actuellement une telle stratégie[2]. Contrairement à d'autres, ces précurseurs ont su distinguer parmi les mythes et les idées reçues le véritable potentiel de ce modèle novateur. Il est temps de démêler le vrai du faux.

Les avantages du Zero Trust

« Le Zero Trust fournit une solution mature, sans complexité opérationnelle ni changements architecturaux majeurs. Au contraire, il simplifie les opérations tout en renforçant la sécurité pour mieux protéger vos ressources les plus précieuses. »

Source : « Zero Trust Cybersecurity Current Trends », American Council for Technology-Industry Advisory Council (ACT-IAC), avril 2019

[1] « The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook », Forrester Research, Inc., juillet 2019
[2] « The Digital Enterprise Report: How the World's Largest Organizations Are Evolving with Technology, », Okta, 2019

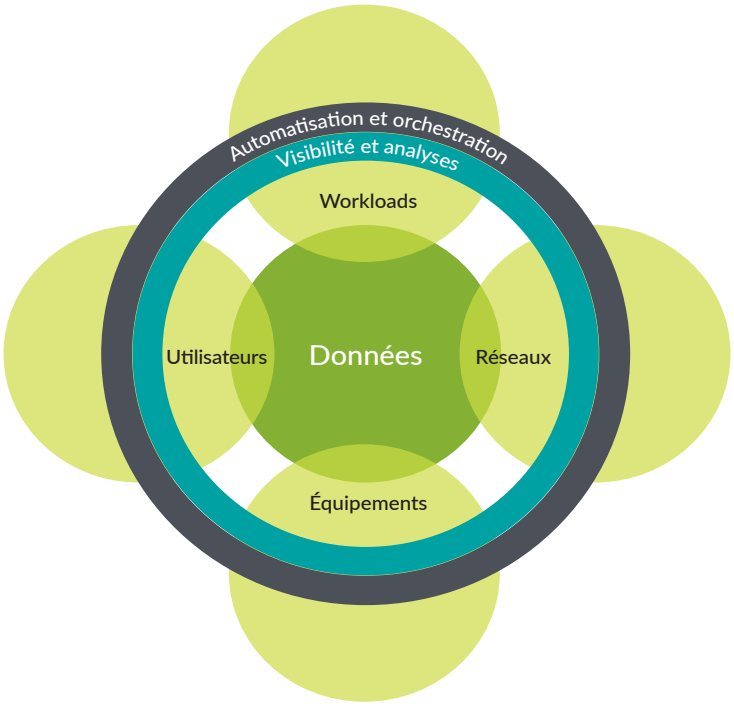

Figure 1 – L'écosystème Zero Trust eXtended (ZTX), pensé par Forrester Research, Inc.

Idée reçue n° 1 : le déploiement d'une approche Zero Trust coûte trop cher

Bon nombre d'entreprises pensent, à tort, que le Zero Trust est un luxe que seules les plus grandes structures peuvent s'offrir. Rien d'étonnant à cela quand on sait que les adeptes du Zero Trust comptent dans leurs rangs des géants comme Google et Coca-Cola. On peut alors en tirer des conclusions hâtives quant aux budgets requis.

La réalité est toute autre. Le Zero Trust est un modèle flexible qui s'adapte à toutes les bourses, des plus petites start-ups aux plus grandes entreprises multinationales. Deux raisons à cela :

1. Le Zero Trust n'est pas un projet avec un début et une fin. C'est un cheminement permanent. Certes, les entreprises dotées d'un budget illimité et vivant dans le collimateur des cyberattaquants auront toutes les raisons de bâtir leur architecture Zero Trust de A à Z. Mais pour la majorité des autres, la stratégie à adopter devra être plus réaliste et surtout échelonnée dans le temps. En misant sur une approche itérative, les budgets plus modestes peuvent étaler leurs efforts et leurs investissements dans la durée, sans avoir à débourser des sommes faramineuses d'entrée de jeu.
2. Parce qu'il améliore l'efficacité opérationnelle et simplifie les processus, le Zero Trust est souvent synonyme d'une réduction des dépenses de sécurité. Autre avantage souligné par Forrester : « en centralisant la gestion de la sécurité, le Zero Trust réduit les coûts »[3].

Juniper Connected Security aide les entreprises à s'appuyer sur leurs outils existants pour concevoir des stratégies optimisées et planifier un déploiement progressif de leur architecture Zero Trust. L'objectif ? Accroître leur visibilité et leur contrôle tout en maîtrisant le flux d'alertes qu'elles reçoivent. Dans cette optique, Juniper a conçu un framework détaillant les cinq étapes à suivre pour accroître la sécurité de votre réseau. Vous pouvez ainsi faire le point sur votre progression et identifier vos prochains objectifs (voir figure 2 à la page suivante).

[3] « The Eight Business and Security Benefits of Zero Trust », Forrester Research, septembre 2019

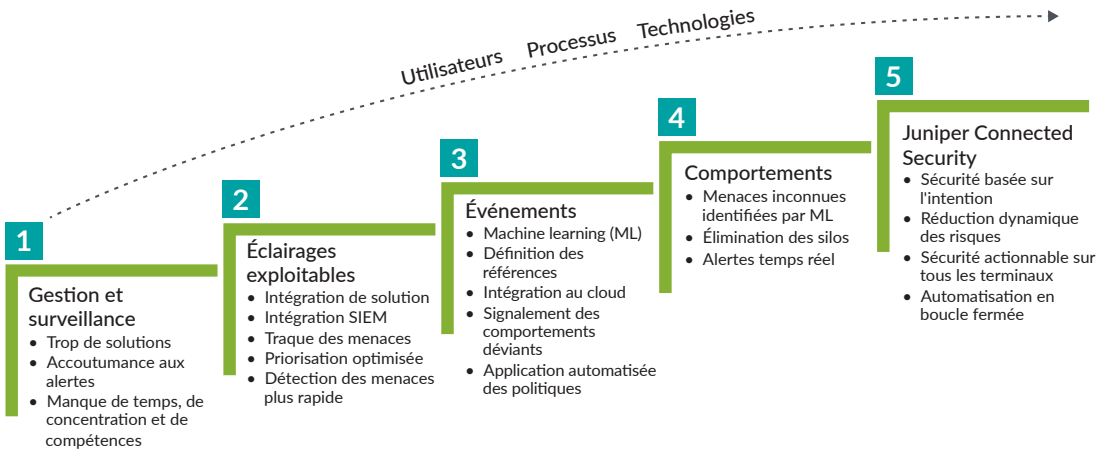

Figure 2 – Les 5 étapes du déploiement Zero Trust selon Juniper Connected Security

Idée reçue n° 2 : la microsegmentation est trop complexe pour être mise en œuvre

La microsegmentation est l'une des chevilles ouvrières du Zero Trust. Comme son nom l'indique, elle consiste à segmenter les périmètres monolithiques d'autrefois en micropérimètres faisant office de « sas » de sécurité soumis à des contrôles d'accès granulaires, stoppant ainsi toute propagation des attaques (voir figure 3 à la page suivante). Malgré son efficacité, bon nombre d'experts réseau et de sécurité préfèrent encore faire l'impasse, pour des raisons parfois injustifiées.

Au début, la microsegmentation était jugée trop complexe et trop chronophage pour être déployée sur les environnements existants. L'implémentation et la gestion de micropérimètres faisaient alors figure d'épouvantail, compte tenu de la multitude d'utilisateurs, de services, d'applications et de dépendances applicatives à prendre en compte. Si ces réserves s'avèrent encore justifiées pour les entreprises employant des outils de sécurité et des solutions réseau disparates, incapables de leur fournir une visibilité de bout en bout sur leur réseau et leur environnement, ce n'est pas le cas pour d'autres.

Certaines technologies s'attachent en effet à faciliter le déploiement des architectures réseau Zero Trust, réduisant par là même la complexité et les coûts liés à la création et au maintien de ces micropérimètres. Comment ? En dotant directement les équipements de fonctions de sécurité qui peuvent ensuite être gérées et contrôlées à l'aide de politiques de sécurité centralisées.

Juniper Connected Security propose par exemple toutes les fonctionnalités nécessaires au déploiement des composants clés d'une architecture Zero Trust et à la mise en place de micropérimètres :

- **Passerelle de segmentation réseau** : la passerelle de segmentation de Juniper Connected Security réunit au sein d'un noyau centralisé tous les services de sécurité et les équipements autrefois isolés. Aussi performante qu'économique, cette plateforme associe routage, commutation, pare-feu nouvelle génération, gestion des menaces unifiées (UTM) et chiffrement complet basé sur les standards IPSec.
- **Micropérimètres parallèles et sécurisés** : une zone de commutation liée à une interface ultra-rapide crée un segment sécurisé, baptisé MCAP (Microcore and Permeter) par Forrester. Les MCAP désignent les différents micropérimètres parallèles, agrégés dans la fabric de la passerelle de segmentation unifiée. Juniper Connected Security permet aux entreprises de segmenter leurs réseaux en microcores selon des attributs de sécurité prédéfinis. À la clé, une meilleure visibilité sur toute leur activité réseau (par rôle, utilisateur ou application) et un contrôle d'accès draconien au niveau de chaque MCAP. Ce n'est pas tout. Juniper va plus loin en étendant la sécurité à l'ensemble des couches réseau (incluant les commutateurs, routeurs et points d'accès Wi-Fi) afin d'endiguer les attaques et d'éviter qu'elles ne se propagent à d'autres composants, y compris aux commutateurs de marque Juniper ou autre.
- **Gestion centralisée** : Juniper Connected Security permet aux équipes IT de gérer l'ensemble des MCAP en toute simplicité et transparence, à partir d'une console centralisée faisant office de fond de panier. Un système qui accroît l'efficacité et l'évolutivité des processus. Quant aux équipes de sécurité, elles n'ont plus besoin d'accumuler règles et politiques pour sécuriser le réseau. Quelques politiques globales suffisent pour garantir une protection optimale à chaque MCAP, sur toute l'infrastructure, et assurer un contrôle plus granulaire au niveau de chaque instance de la passerelle de segmentation.

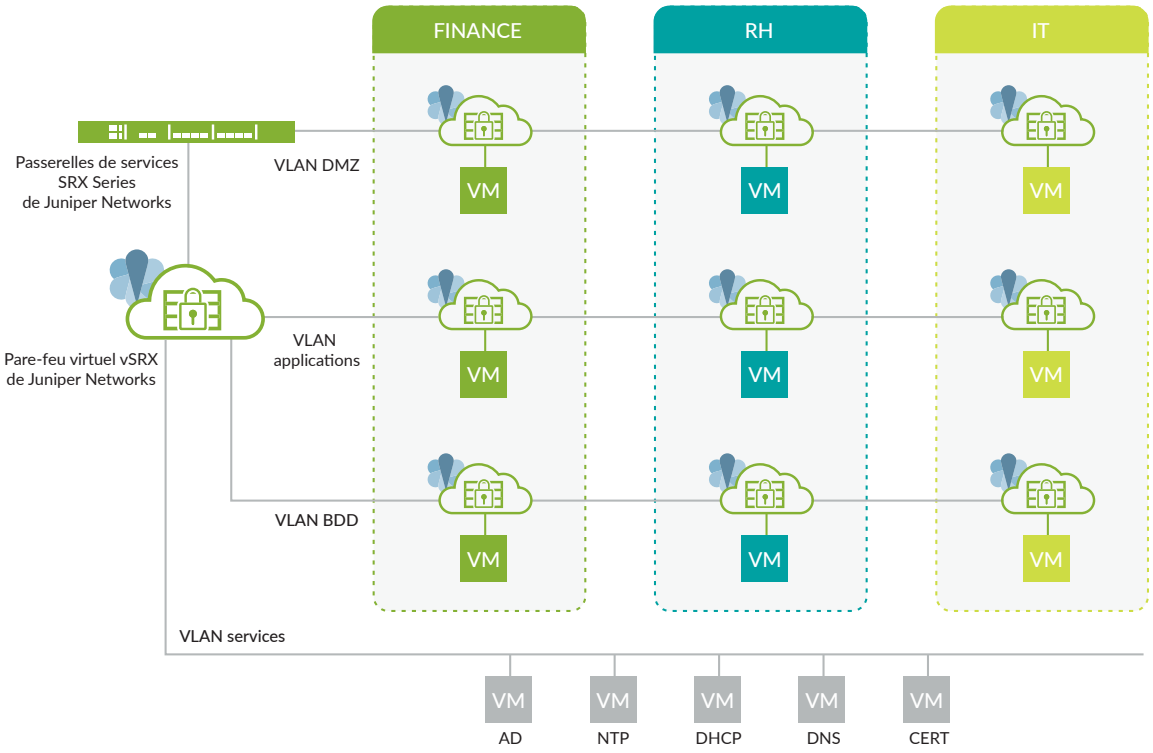

Figure 3 – Exemple de microsegmentation dans un datacenter

Idée reçue n° 3 : le Zero Trust nécessite de faire table rase des infrastructures existantes

Bon nombre d'entreprises continuent de croire que le modèle Zero Trust doit être déployé ex nihilo. Qu'il nécessite de tout reprendre à zéro, de se départir de l'existant pour faire place à une plateforme unique.

Si certaines organisations peuvent se le permettre, d'autres n'ont ni le temps ni les moyens nécessaires pour adopter une approche si radicale du Zero Trust. Qu'elles se rassurent, rien ne les y oblige. Une architecture Zero Trust peut tout à fait être déployée de manière progressive, sur la base de leur réseau existant.

La clé consiste à élaborer une stratégie échelonnée dans le temps, conçue pour accroître votre maturité de façon graduelle. La réussite de cette stratégie passe par des solutions capables de s'intégrer à vos outils existants pour déployer progressivement de nouvelles fonctionnalités Zero Trust sur tout votre réseau.

Aucun fournisseur ne peut prétendre protéger à lui seul tout un réseau d'entreprise. C'est pourquoi Juniper propose des solutions ouvertes et des produits interopérables, capables de fournir à ses clients une vue à 360° sur l'ensemble de leurs moyens de défense. Juniper Connected Security s'inscrit dans cette vision pour améliorer vos capacités de détection et contrer les menaces les plus sophistiquées grâce à une Threat Intelligence de pointe, et ce en toute simplicité.

Idée reçue n° 4 : le Zero Trust ne sécurise que les environnements sur site

Le concept du Zero Trust peut se résumer en un impératif : nous devons cesser d'accorder une confiance implicite à tout ce qui se trouve sur notre réseau. Face à l'apparente simplicité d'un tel argument, bon nombre d'entreprises ont conclu quelque peu précipitamment que le Zero Trust ne pouvait protéger que leurs data centers. S'il est vrai que les cybercriminels exploitent cette confiance implicite avant tout pour infiltrer vos infrastructures, ils savent aujourd'hui se projeter bien au-delà de vos environnements sur site.

Autre raison pour laquelle les entreprises pensent, à tort, que l'approche Zero Trust se limite principalement – voire exclusivement – à leurs data centers : elles ont tendance à croire que leur fournisseur de services cloud (CSP) est responsable de leur sécurité dans l'environnement dématérialisé. C'est même l'un des plus grands malentendus dans le monde du cloud computing. En réalité, cette responsabilité est généralement partagée entre d'une part le fournisseur, qui est chargé de protéger l'infrastructure cloud, et d'autre part le client, à qui il incombe de sécuriser ses workloads, données et utilisateurs. En d'autres termes, non, le Zero Trust ne se limite pas aux infrastructures sur site. Il est d'ailleurs indispensable pour défendre les ressources de l'entreprise dans les environnements cloud et multicloud.

Avec Juniper Connected Security, vos politiques de sécurité s'appliquent aussi dans le cloud. Vous couvrez ainsi les modèles de livraison de services les plus récents tout en protégeant les workloads et les données, du point de terminaison jusqu'à la périphérie de votre réseau, en passant par tous les clouds intermédiaires. Votre entreprise peut ainsi renforcer sa posture de sécurité, sur site comme dans le cloud. Vos workloads conteneurisés bénéficient également de la sécurité Zero Trust, gage d'une visibilité et d'une protection renforcées jusqu'aux communications entre les différents microservices composant chaque application.

Idée reçue n° 5 : le Zero Trust est incompatible avec une approche multi-fournisseurs

Nous l'avons vu, l'approche Zero Trust a rapidement su conquérir les professionnels de la sécurité. Face à cet engouement, de nombreux vendeurs ont pris le train en marche, déclarant que seule une solution mono-fournisseur pourrait soutenir un tel modèle. Selon eux, pour garantir la cohérence de leur architecture Zero Trust, les entreprises doivent se tourner vers un partenaire unique, capable de leur offrir toutes les solutions dont elles auront besoin.

Le problème, c'est qu'aucun fournisseur ne peut prétendre à l'heure actuelle sécuriser l'intégralité d'un réseau basé sur une architecture Zero Trust. Forrester assure même que l'intégration de fonctionnalités complémentaires, issues de différents domaines de la sécurité, est primordiale, arguant que « l'ergonomie et le contrôle des ressources réparties sur divers systèmes de données, réseaux et infrastructures sont essentiels pour garantir l'efficacité du Zero Trust ».

Dans cette optique, nous avons conçu notre solution Juniper Connected Security autour d'un écosystème mondial de partenaires, travaillant ensemble à la conception et à l'implémentation de réseaux porteurs d'une réelle valeur ajoutée pour l'entreprise. Grâce à leurs solutions et à leur expertise de pointe, nous pouvons étendre la portée de nos offres et répondre à un plus grand nombre de cas d'usage.

Cap sur le Zero Trust avec Juniper Connected Security

Maintenant que nous avons dissipé les malentendus entourant le Zero Trust et ses architectures, voyons comment Juniper Connected Security peut vous aider à tirer le meilleur parti de cette approche innovante.

Tout d'abord, Juniper s'impose comme un leader de la sécurité et de la performance réseau. Nous aidons de grandes structures à construire les réseaux les plus vastes et les plus sophistiqués de toute la planète. Nous comptons parmi nos clients 97 entreprises du Fortune Global 100 et les cinq plus grands réseaux sociaux du web. Plus de 86 % du trafic smartphone aux États-Unis transitent sur nos réseaux.

Juniper Networks investit massivement dans la recherche et le développement pour mettre au point des innovations qui révolutionnent tous les aspects des technologies réseau : circuits intégrés, systèmes, logiciels et sécurité. Pare-feu nouvelle génération, commutation, protection anti-malware renforcée, politiques intelligentes, déploiement flexible… toutes nos offres s'inscrivent dans l'approche Juniper Connected Security pour aider les entreprises du monde entier à réussir le déploiement de leur stratégie Zero Trust (voir figure 4 à la page suivante).

[4] « The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook », Forrester Research, Inc., juillet 2019

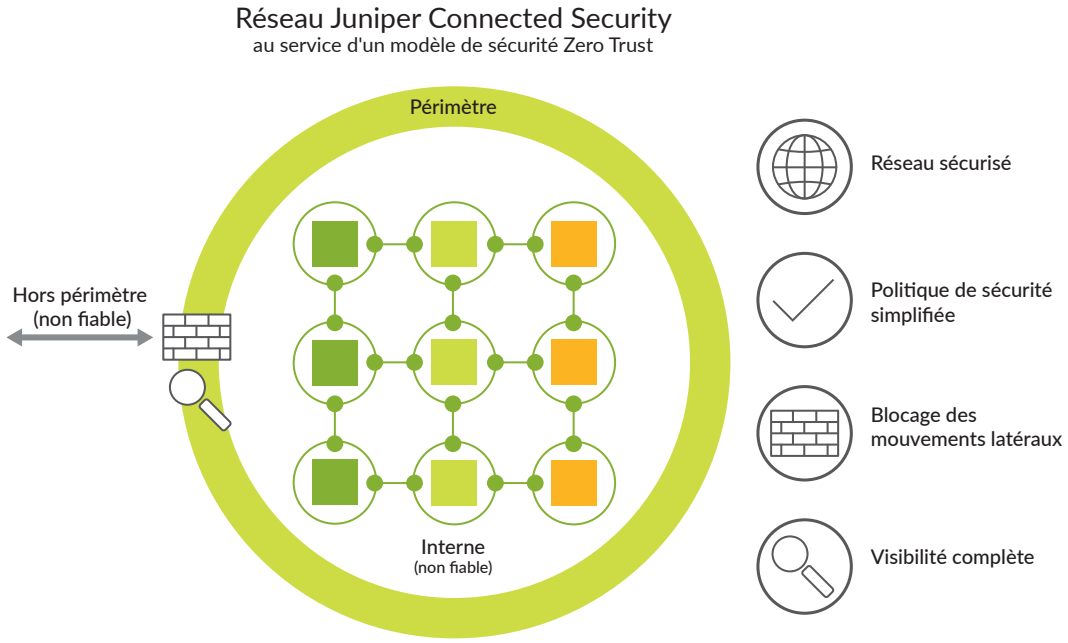

Figure 4 – Une architecture Zero Trust déployée avec Juniper Connected Security

Tableau 1 – Juniper Connected Security offre une solution pour chaque pilier du modèle Zero Trust

Pilier	Offre Juniper
Données	• Chiffrement complet, basé sur les standards IPSec, pour sécuriser le transfert des données de l'entreprise d'un réseau à l'autre • Prise en charge de la microsegmentation
Réseaux	• Visibilité, protection et automatisation du réseau, géré comme une seule et même entité • Sécurité étendue à tous les points de terminaison du réseau, y compris aux produits tiers • Passerelle de segmentation robuste pour la mise en place de micropérimètres de sécurité
Utilisateurs	• Contrôle granulaire pour la gouvernance et la gestion des accès utilisateurs • Interactions utilisateurs sécurisées
Équipements	• Prise en charge de politiques utilisateurs basées sur l'intention pour faciliter le partage de ressources et d'informations entre les équipements réseau (commutateurs, routeurs, pare-feu et autres équipements de sécurité), mais aussi déclencher et coordonner des actions de remédiation dès la détection d'une menace
Workloads	• Systèmes de défense avancés, au plus près de la ressource à protéger, dans le cloud public et partout où vos workloads sont appelés à s'exécuter dans le cadre de vos modèles de service actuels • Contrôle granulaire des politiques
Visibilité et analyses	• Visibilité accrue sur le trafic réseau, y compris pour l'identification des utilisateurs et des applications • Analyse des données de session en temps réel et envoi de captures de paquets vers un référentiel centralisé via un port SPAN
Automatisation et orchestration	• Protection unifiée, basée sur l'automatisation, le machine learning et une Threat Intelligence en temps réel • Gestion simplifiée grâce à une plateforme dédiée à la création, au déploiement et à la réplication de politiques de sécurité communes, facilitant ainsi l'implémentation de nouveaux services et applications

Conclusion

À l'heure où les environnements IT évoluent et où la menace s'intensifie à un rythme sans précédent, il est grand temps pour les entreprises de toutes tailles de repenser leur sécurité autour du modèle Zero Trust. En s'obstinant à renforcer la protection de leur périmètre, elles ne font qu'inviter des cyberattaques toujours plus redoutables et répétées à déferler sur leurs environnements cloud et sur site.

Pour tout savoir sur les nombreux avantages de l'approche Juniper Connected Security, rendez-vous sur www.juniper.net/fr/fr/security.

À propos de Juniper Networks

Juniper Networks simplifie les réseaux avec des produits, des solutions et des 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/fr/fr/

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