Enterprise Strategy Group | Getting to the bigger truth.™

LIVRE BLANC ESG

# SD-WAN nouvelle génération : les 10 points essentiels

Par Bob Laliberte, Analyste senior ESG, et Leah Matuson, Chargée d'étude

Mars 2021

Ce livre blanc ESG a été rédigé pour Palo Alto Networks.
Il est diffusé sous licence d'ESG.

## Sommaire

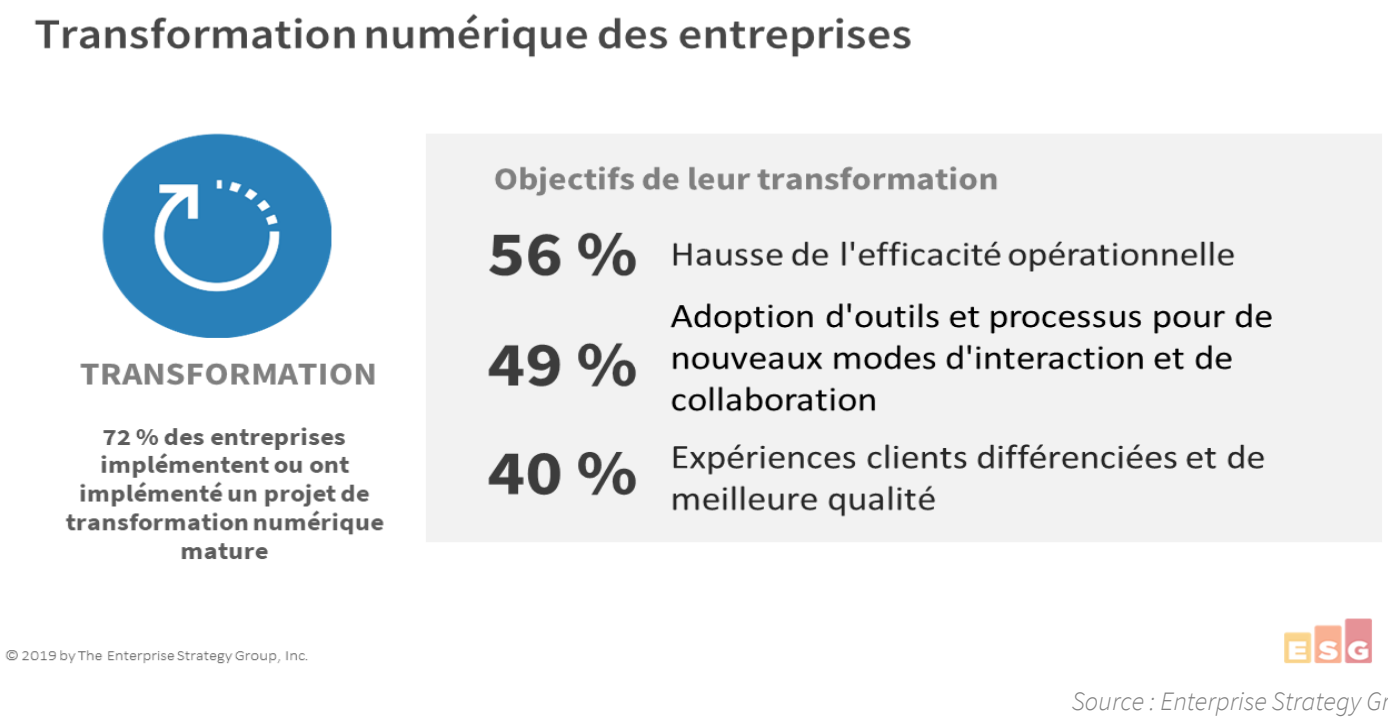
## Le réseau face aux nouvelles réalités d'un environnement cloud distribué

De tout temps, les entreprises ont dû s'adapter à l'évolution de leur environnement. Toutefois, le rythme de cette évolution a changé. Désormais, les acteurs de tous les secteurs doivent composer avec un environnement IT et applicatif en mutation perpétuelle. Pandémie oblige, le rythme du changement s'est en effet accéléré avec l'adoption massive du télétravail et la prolifération d'applications de nouvelle génération dans les data centers d'entreprise, de multiples clouds publics et, de plus en plus souvent, des sites en périphérie. Ce qui accroît la complexité informatique.

Il n'y a donc rien d'étonnant à ce que les entreprises aient mis les bouchées doubles sur leurs projets de transformation numérique. D'après une étude d'ESG, 22 % d'entre elles qualifient cette transformation de mature (plusieurs projets déjà implémentés et optimisés), tandis que 50 % affirment qu'elle suit son cours (implémentation et exécution de projets).[1] Par comparaison, un an plus tôt, 19 % des entreprises étaient matures et seulement 39 % avaient des projets en cours.

Il est également important de noter les raisons qui incitent ces entreprises à entamer leur transformation numérique. D'après notre étude, elles cherchent avant tout à améliorer leur efficacité opérationnelle (56 %), à adopter des outils et processus compatibles avec de nouveaux modes d'interaction et de collaboration (49 %) et à offrir des expériences clients différenciées et de meilleure qualité (40 %). Il est clair que tous ces objectifs (cf. Figure 1) doivent permettre aux entreprises de s'adapter et de renforcer leur résilience.

**Figure 1. Transformation numérique**




*Source : Enterprise Strategy Group*

### Besoin de connectivité des environnements hautement distribués

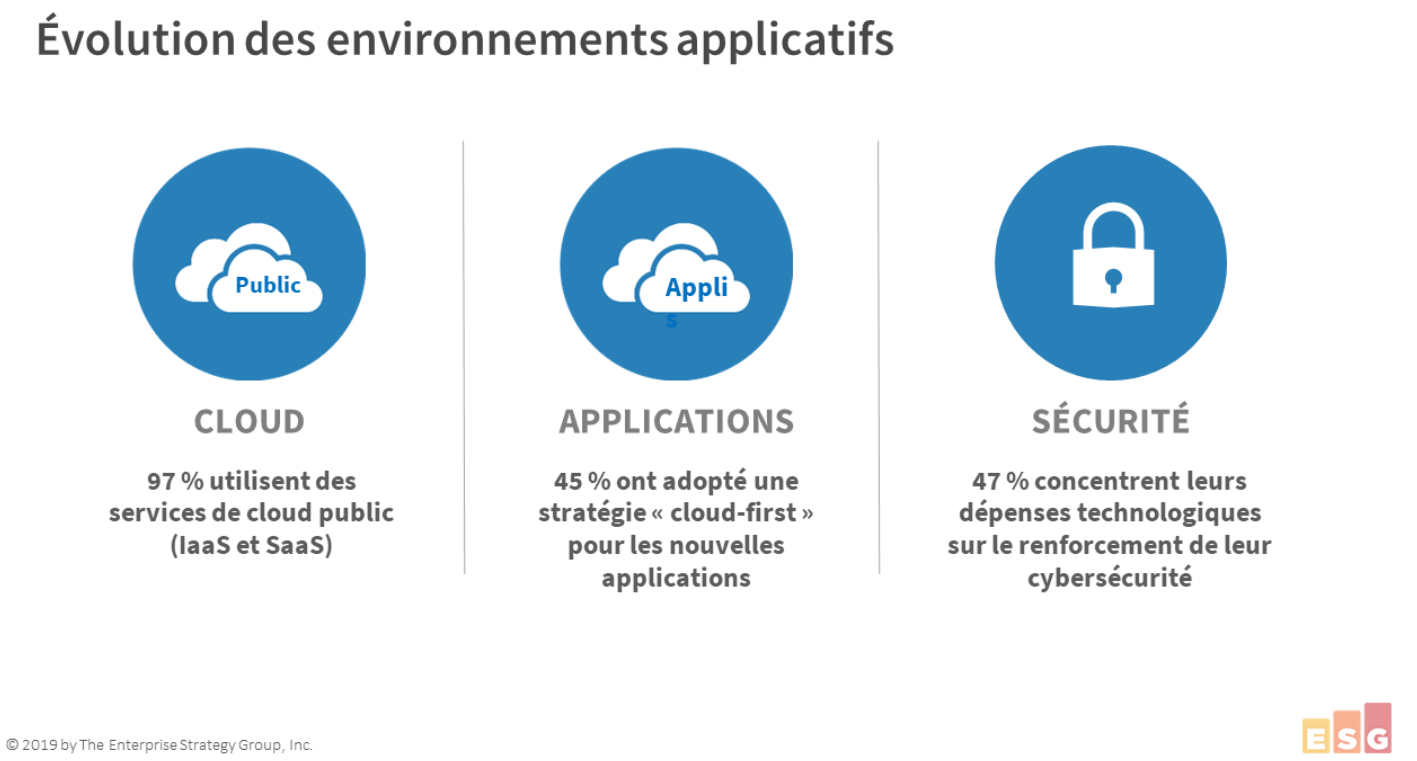
Outre le passage au télétravail, la pandémie a accéléré la migration des applications vers le cloud. D'après l'étude d'ESG, la hausse du taux d'adoption des applications cloud fera en effet partie des principaux effets durables de cette crise sanitaire

[1] Source : Rapport d'étude ESG, *Enquête 2021 sur les intentions d'achat technologique*, janvier 2021. Sauf indication contraire, l'ensemble des graphiques et des références à des études ESG contenus dans le présent eBook proviennent de ce rapport.

(24 %). En outre, près de la moitié des sondés (45 %) déclarent que leur entreprise a adopté une stratégie « cloud-first » du déploiement de nouvelles applications, contre seulement 38 % l'année dernière.

Pour ces environnements hautement distribués, les entreprises ont non seulement besoin de connectivité, mais aussi de sécurité. Les données et les applications stratégiques ne sont plus uniquement hébergées dans des data centers sur site. Les salariés peuvent travailler depuis n'importe où, sur presque n'importe quel appareil. C'est pourquoi il est essentiel de protéger les applications et les utilisateurs, où qu'ils se trouvent. Dans un contexte de fluidification du périmètre et d'expansion de la surface d'attaque, la plupart des entreprises (47 %) concentrent leurs dépenses technologiques sur le renforcement de leur cybersécurité (cf. Figure 2).

**Figure 2. Priorité au cloud et à la sécurité**




*Source : Enterprise Strategy Group*

Pour connecter et protéger leur environnement hautement distribué, les entreprises doivent implémenter des solutions réseau équipées de fonctionnalités de sécurité parfaitement intégrées, tout en garantissant des niveaux élevés de performance et d'expérience client. D'après l'étude ESG, les sommes investies dans la mise en œuvre de stratégies technologiques à long terme devraient augmenter, le but étant de bénéficier d'une infrastructure plus flexible et résiliente en cas de nouveau choc pour leur activité (53 %). Par ailleurs, les entreprises plus avancées dans leur transformation numérique investiront davantage dans les solutions IT (une hausse de 4,33 % des dépenses, contre seulement + 0,15 % dans les entreprises sans projet). Par conséquent, les entreprises vont devoir opter pour une nouvelle génération de technologies et solutions innovantes, garantes de déploiements applicatifs fluides et sécurisés à travers leur environnement hautement distribué.

## Limites des architectures réseau et de sécurité traditionnelles

Malheureusement, la plupart des solutions traditionnelles n'on ni les capacités, ni la dimension nécessaires pour soutenir la transformation numérique à l'œuvre aujourd'hui. Les limites architecturales freinent l'innovation, nuisent aux

performances et coûtent souvent cher en maintenance et en exploitation. Parmi ces solutions traditionnelles figurent les architectures réseau hub-and-spoke et les architectures de sécurité périmétrique (castle and moat), mais aussi certaines solutions SD-WAN de première génération (des solutions basées exclusivement sur le réseau et les paquets).

## Les architectures réseau traditionnelles incompatibles avec les environnements hautement distribués

### Conception réseau hub-and-spoke

Les réseaux hub-and-spoke – qui renvoient à l'image d'une roue dont les rayons convergent tous vers le moyeu central – ont d'abord été conçus pour les data centers internes qui hébergeaient la plupart des applications d'entreprise, et non pour les environnements applicatifs complexes et hautement distribués d'aujourd'hui. Dans ce modèle, le trafic réseau d'un site distant passe obligatoirement par le data center avant d'accéder à une application cloud, voire à un autre site distant. Les premières solutions de télétravail reprenaient souvent ce modèle. Elles utilisaient des VPN avec des pare-feu et des concentrateurs en data center pour diriger le trafic vers les applications cloud. Or, si cette approche a permis de répondre temporairement à un besoin, elle n'est pas viable à long terme. Les trois grandes lacunes de ces architectures réseau traditionnelles :

- Coût de la solution. Les solutions réseau traditionnelles reposent généralement sur les lignes fixes coûteuses et rigides des opérateurs télécoms. Dans des configurations haute disponibilité en particulier, les liaisons MPLS nécessitent parfois de mettre soi-même en place le dernier kilomètre, ce qui occasionne des dépenses qui viennent s'ajouter à un prix déjà élevé.

- Manque d'agilité. Les réseaux MPLS à ligne fixe nécessitent souvent des installations supplémentaires, ce qui pourra retarder le raccordement. Avec ce type de connexions, l'ajout et le déplacement de liaisons s'avèrent également laborieux. À l'heure où de plus en plus d'entreprises doivent migrer leurs applications vers la périphérie, beaucoup peinent à trouver des lignes fixes qui desservent ces sites.

- Impact sur les performances. Les entreprises qui s'appuient encore sur une architecture réseau traditionnelle font passer le trafic réseau par leur data center (hairpinning), ce qui rallonge inutilement les temps de latence et peut nuire aux performances applicatives. Ces environnements réseau traditionnels mettent tout le trafic applicatif sur un pied d'égalité, puisque toutes les applications (Wi-Fi invité et SAP) sont traitées de la même manière : en cas de défaillance, tout le trafic bascule vers la liaison de secours. Cela implique souvent un processus manuel chronophage. Enfin, les fonctions de sécurité s'exécutent dans le data center, ce qui nuit aux performances réseau.

## Les SD-WAN traditionnels créent des obstacles de taille

### SD-WAN traditionnels

Bien qu'elles fassent mieux que l'architecture réseau traditionnelle, de nombreuses solutions SD-WAN de première génération freinent également la création d'un environnement applicatif moderne et hautement distribué. Axées sur le trafic réseau uniquement, elles génèrent les problématiques suivantes :

Visibilité exclusivement sur la couche réseau : Parce que ces solutions utilisent essentiellement des informations de trafic basées sur les paquets en couche 3, elles offrent peu de visibilité sur la couche applicative. Par conséquent, elles permettent d'assurer la qualité du service réseau, mais côté applicatif, les équipes réseau peinent parfois à respecter leurs engagements SLA. Pour les applications dans le cloud et en périphérie, certaines entreprises devront faire appel à d'autres solutions de visibilité.

Sécurité hétérogène : La plupart des fournisseurs de solutions de première génération s'associaient à des spécialistes de la sécurité dont les produits venaient se greffer à leurs solutions sur les sites distants, ce qui mobilisait du temps et de l'énergie pour l'installation et la gestion. Cela pouvait également se solder par des niveaux de protection irréguliers selon les solutions de sécurité déjà en place sur la périphérie. Évidemment, les environnements de télétravail hautement distribués n'arrangent rien. De fait, pour les entreprises interrogées par ESG, la principale difficulté liée au développement du télétravail tient dans l'augmentation du nombre de vulnérabilités de cybersécurité dont les collaborateurs à distance sont à l'origine.[2]

Procédures et processus manuels : À l'heure où les entreprises se retrouvent de plus en plus sous pression pour assurer des expériences de qualité dans un environnement toujours plus complexe et distribué, les équipes opérationnelles ne peuvent répondre aux exigences à l'aide de procédures et processus manuels. Or, si les activités de provisionnement ont beaucoup progressé, les tâches opérationnelles et de gestion du cycle de vie restent souvent manuelles.

Quelle que soit leur solution réseau existante, presque toutes les entreprises peinent à éliminer la complexité liée aux environnements applicatifs et de travail hautement distribués. D'après l'étude d'ESG, 75 % des entreprises trouvent leur environnement IT plus complexe qu'il y a deux ans. Reste à savoir d'où vient cette complexité. Les cinq principaux facteurs cités par les sondés mettent en lumière les défis à relever pour connecter un environnement distribué sans aucun compromis sur la sécurité. Les professionnels interrogés mentionnent avant tout le développement du télétravail pour cause de pandémie (49 %), les nouvelles règlementations relatives à la sécurité et à la confidentialité des données (38 %), la croissance des volumes de données (38 %), l'évolution du champ des cybermenaces (35 %), ainsi que la multiplication et la diversification des terminaux (32 %).

## Checklist : les 10 éléments à inclure dans votre cahier des charges pour une solution durable

Beaucoup d'entreprises se lancent actuellement dans le déploiement de solutions durables afin de garantir des connexions à la fois sécurisées et centrées sur les applications pour les télétravailleurs et les environnements cloud hautement distribués. Pour leurs équipes opérationnelles, il est donc essentiel d'ajouter les points suivants à leur cahier des charges.

Les critères d'une bonne solution SD-WAN de nouvelle génération :

1. Focalisation sur les applications : Les projets de transformation numérique et les applications de nouvelle génération donnent naissance à des environnements applicatifs hautement distribués. Pour les équipes IT, tout l'enjeu consiste à garantir des expériences utilisateurs de qualité, quel que soit le lieu d'hébergement de l'application. Les solutions SD-WAN de nouvelle génération doivent donc intégrer des fonctions de visibilité et de contrôle sur la couche applicative (couche 7). Cela permettra aux entreprises d'accélérer la migration des applications vers un ou plusieurs clouds publics (IaaS et SaaS compris), avec l'assurance que les politiques et décisions de chemins réseau sont fondées sur le respect des engagements SLA ayant trait aux applications, et non uniquement au réseau.

2. Simplicité d'utilisation : Compte tenu de la complexité des environnements, les entreprises ont besoin de solutions SD-WAN de nouvelle génération faciles à déployer et à exploiter. Elles doivent pouvoir déployer et provisionner rapidement une solution sur leurs sites distants, sans avoir à détacher des techniciens sur chaque site. En somme, il leur faut des solutions plug-and-play que n'importe quel utilisateur lambda peut aisément brancher à une prise électrique et raccorder au réseau. Dans un contexte de convergence des fonctions réseau et sécurité, toute solution

[2] Source : Rapport d'étude ESG, *Impact de la pandémie de Covid-19 sur le télétravail, dépenses IT 2020 et futures stratégies technologiques*, juin 2020.

doit offrir des accès basés sur les rôles afin de permettre aux équipes réseau et de sécurité de consulter et créer des politiques.

3. Automatisation accrue : Les environnements hautement distribués deviennent si complexes que les équipes opérationnelles ont du mal à les gérer efficacement par le simple biais de tâches manuelles. Les entreprises ont donc besoin de solutions intégrant des fonctions d'automatisation intelligentes pour le provisionnement (Zero Touch Provisioning), mais aussi pour des tâches opérationnelles comme l'auto-optimisation et l'auto-réparation de l'environnement SD-WAN. Il est en effet préférable de pouvoir déterminer rapidement si le problème vient du réseau ou de l'application afin d'en accélérer la résolution. Des technologies comme l'intelligence artificielle et le machine learning s'avèrent essentielles à l'automatisation intelligente.

4. Déploiement/gestion dans le cloud : Avec la pandémie, les effectifs des entreprises sont aujourd'hui éparpillés un peu partout. Or, étant donné l'importance de maintenir la productivité de tous ces collaborateurs, les solutions de nouvelle génération doivent impérativement se fonder sur une architecture de gestion dans le cloud. En effet, les équipes opérationnelles doivent pouvoir accéder facilement à la console de gestion pour créer des politiques applicatives, de sécurité et de conformité. Une gestion dans le cloud permet de centraliser les politiques et de les appliquer de façon distribuée sur tous les sites. C'est un pilier de la gestion du cycle de vie puisqu'elle garantit l'installation automatique de tous les correctifs de sécurité, avec à la clé une protection homogène sur l'ensemble de l'entreprise. Enfin, lorsque ces solutions de gestion dans le cloud sont conçues sur des architectures applicatives modernes, il est possible d'intégrer rapidement de nouvelles fonctionnalités produits et des mises à jour de sécurité à l'environnement, au lieu de se contenter de MAJ annuelles ou biannuelles.

5. Convergence des fonctions réseau et de sécurité : L'émergence du framework SASE (Secure Access Service Edge) accentue le besoin d'intégration des fonctions (et des équipes) réseau et de sécurité. Un SD-WAN nouvelle génération avec accès sécurisé constitue un excellent point de départ. Toutefois, les entreprises désireuses d'appliquer l'intégralité de ce framework doivent s'assurer que d'autres fonctionnalités de sécurité sont ou seront parfaitement intégrées à la solution. De fait, elles doivent pouvoir tout provisionner depuis la console cloud de gestion centralisée : pare-feu nouvelle génération, accès réseau Zero Trust (ZTNA), passerelles web sécurisées (SWG), Cloud Access Security Brokers (CASB), services d'isolement de navigateur à distance (RBI), etc. Comme nous l'avons déjà mentionné, les accès basés sur les rôles contribuent grandement à cette convergence. Les entreprises doivent décider entre une approche mono- et multifournisseur, et cerner les avantages et les inconvénients de chacun de ces choix.

6. Haute performance : Quel que soit le réseau utilisé, les solutions SD-WAN de nouvelle génération doivent pouvoir exploiter et optimiser le trafic sur presque n'importe quelle connexion réseau, y compris les liaisons MPLS, les connexions Internet haut débit et les réseaux mobiles (notamment 4G et bientôt 5G), mais aussi utiliser cette connectivité mobile comme troisième connexion de secours. Il est essentiel de pouvoir exploiter plusieurs liaisons pour garantir la haute disponibilité, y compris des lignes fixes comme solution primaire et de basculement. Toutefois, avec le déploiement de la 5G, les entreprises devraient également étudier la viabilité de la connectivité mobile comme liaison primaire dans un avenir proche. N'importe quelle solution SD-WAN doit être capable d'exploiter toute la bande passante disponible afin d'optimiser le trafic et de sélectionner automatiquement le meilleur chemin en fonction du niveau de priorité de l'application. Pour y parvenir, elle doit bénéficier d'une bonne visibilité sur les couches 3 (réseau) et 7 (application).

7. Visibilité de bout en bout : Pour mieux cerner et optimiser l'expérience, les solutions doivent bénéficier d'une visibilité complète de bout en bout, des terminaux jusqu'aux applications, où qu'ils se trouvent. Cela pourra aller des capteurs IoT sur les sites en périphérie et au domicile des salariés, jusqu'aux applications hébergées dans les data centers

d'entreprise, les sites en périphérie ou le cloud public. Cette visibilité granulaire sur les couches 3 et 7 accélèrera l'isolement et la résolution des problèmes réseau et applicatifs. En prime, toutes les informations obtenues sur ces deux environnements permettront aux entreprises de développer des politiques parfaitement optimisées pour leurs cas particuliers.

8. Réduction des coûts : En dépit de la complexité croissante, les budgets IT restent limités. Heureusement, les solutions SD-WAN de nouvelle génération peuvent remplacer les liaisons MPLS coûteuses par des connexions haut débit plus économiques et ainsi considérablement réduire les coûts réseau. Pour les entreprises qui utilisent de multiples liaisons MPLS pour la haute disponibilité, ces économies ne sont pas négligeables. C'est d'autant plus vrai sur les architectures réseau traditionnelles (hub-and-spoke) dont la liaison secondaire sert uniquement de connexion de secours. Les solutions SD-WAN peuvent quant à elles exploiter les deux en mode actif-actif. En plus des coûts réseau, les solutions de nouvelle génération qui intègrent des fonctions de sécurité peuvent réduire la quantité de matériels et logiciels nécessaires sur chaque site, ainsi que les coûts de maintenance associés.

9. Amélioration de l'agilité : Pendant la pandémie mondiale, la capacité à se connecter rapidement à de nouveaux lieux géographiques s'est révélée essentielle. En ce sens, les solutions SD-WAN de nouvelle génération doivent pouvoir gérer les salariés tant au bureau qu'à leur domicile. Le fait de pouvoir utiliser à la fois les liaisons MPLS, les lignes fixes haut débit et les connexions mobiles permet de déployer la technologie presque n'importe où. Le SD-WAN de nouvelle génération doit également pouvoir s'appuyer sur des déploiements asymétriques – c'est-à-dire se connecter au cloud et optimiser le trafic à l'aide d'un seul équipement sur le site de l'entreprise (contrairement aux déploiements symétriques qui nécessitent un équipement à chaque extrémité de la connexion ou à proximité de ces extrémités dans le cas des environnements SaaS).

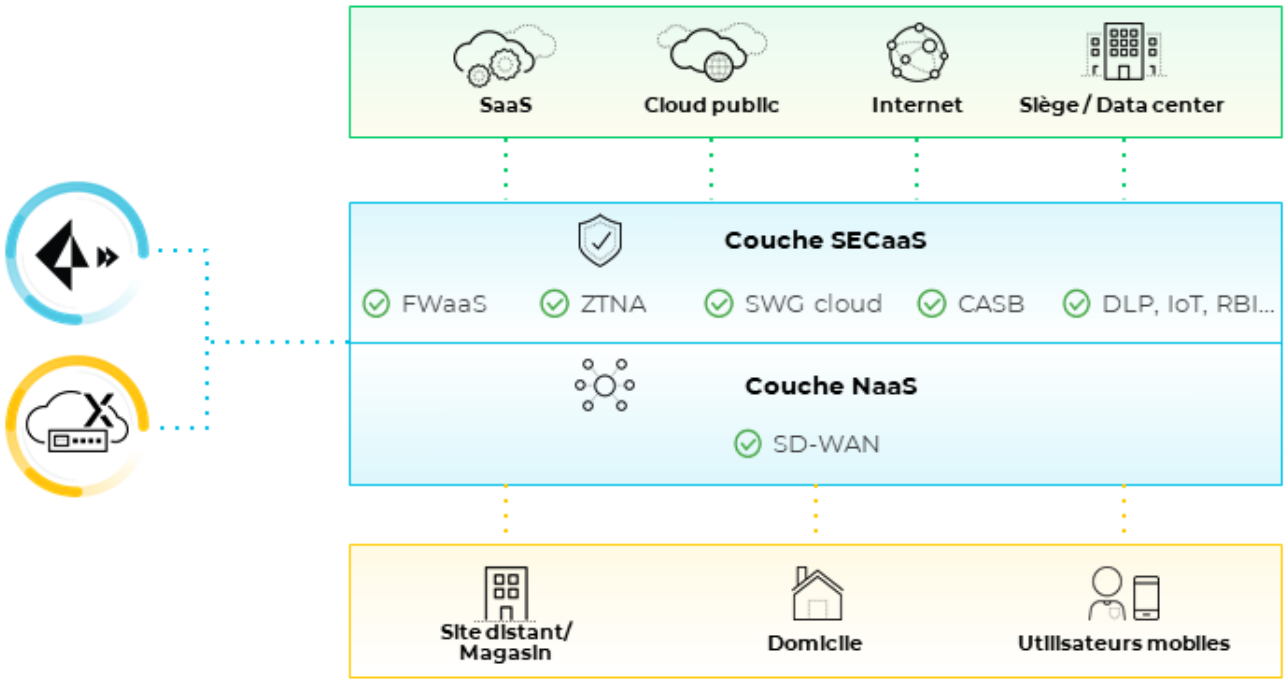
10. Accélération de l'innovation : Ce critère est très important. Les solutions SD-WAN de nouvelle génération permettent de réduire les coûts réseau et d'ajouter de la bande passante, ce qui ne peut être que positif. Toutefois, ce qui fait vraiment la différence, ce sont les possibilités que cette bande passante supplémentaire offre aux entreprises. Ces dernières devraient réfléchir aux possibilités qu'elle entrouvre en termes d'expérience client et de lancements de services innovants (comme des applis vocales ou vidéo gourmandes en bande passante). Les solutions SD-WAN de nouvelle génération peuvent également permettre la consolidation d'autres services en périphérie. En somme, les entreprises devraient voir plus loin que le SASE et envisager l'intégration d'autres services à cette solution pour en libérer tout le potentiel.

## Palo Alto Networks accélère le SD-WAN de nouvelle génération

### Des solutions conçues pour accélérer l'adoption des environnements applicatifs distribués et sécurisés

Pionnier des technologies de nouvelle génération, Palo Alto Networks a intégré le SD-WAN à sa gamme Prisma en rachetant CloudGenix en avril 2020. Prisma SD-WAN (anciennement CloudGenix SD-WAN) permet aux entreprises d'utiliser le SD-WAN de nouvelle génération pour connecter les utilisateurs en tout lieu (sur leur campus, leur site distant ou à domicile) à des applications distribuées à travers des data centers, de multiples clouds publics et des sites en périphérie, et ce en toute sécurité. Associée à Prisma Access, cette solution les aide à accélérer l'implémentation d'un framework SASE complet (cf. Figure 3).

**Figure 3. Solution SASE complète de Palo Alto Networks**




*Source : Palo Alto Networks*

## Palo Alto Networks Prisma SD-WAN

Palo Alto Networks Prisma SD-WAN est une solution orientée applications de nouvelle génération, capable d'utiliser des connexions haut débit économiques, mais aussi les réseaux 4G et 5G comme liaison de secours, voire comme connexion principale. En conjonction avec Prisma Access, elle offre une solution SASE robuste. Les trois grands atouts de Prisma SD-WAN :

### Orienté applications

Pour optimiser l'expérience en entreprise dans un contexte d'effectifs et d'applications distribués, Prisma SD-WAN mise sur la visibilité sur les couches 3 (réseau) et 7 (applications). Lorsqu'elles ont accès à des informations comme les codecs et les scores MOS (Mean Opinion Score) sur les flux de données audio et vidéo, les entreprises peuvent créer des politiques à même d'optimiser le trafic en fonction des SLA applicatifs, et non uniquement des SLA réseau. Ce niveau de visibilité garantit une bonne expérience aux salariés qui accèdent à des outils collaboratifs comme Zoom et Teams à partir des sites distants et de leur domicile. En prime, le fait de pouvoir isoler le trafic réseau et applicatif raccourcit considérablement les délais de résolution puisque les équipes opérationnelles peuvent concentrer leurs efforts et travailler plus efficacement.

La visibilité sur les applications permet à Prisma SD-WAN de répondre aux besoins des entreprises avec un seul équipement sur les sites en périphérie (déploiement asymétrique). À la clé : une hausse de l'agilité et un retour sur investissement plus rapide.

### Hautement automatisé

Pour améliorer l'efficacité opérationnelle, Prisma SD-WAN automatise non seulement les déploiements, mais aussi les tâches d'exploitation et de maintenance. Quant aux entreprises qui veulent gagner en agilité et déployer rapidement des

solutions SD-WAN sur leurs sites distants, Prisma SD-WAN leur offre des fonctionnalités de déploiement Zero Touch. Ainsi, nul besoin d'être un technicien pour raccorder des appareils aux branchements électriques et au réseau sur les sites distants (dans les filiales et à la maison avec ION 1000). En outre, la console de gestion centralisée dans le cloud peut provisionner chaque équipement en fonction de politiques prédéfinies.

Quant à l'automatisation des tâches d'exploitation et de maintenance, elle comprend des fonctionnalités d'auto-réparation et d'auto-optimisation. Les fonctionnalités d'auto-réparation permettent de corréler des évènements afin d'identifier la cause racine d'un problème et de le résoudre sans aucune intervention humaine. Pour les problèmes qui nécessitent toutefois une intervention, Palo Alto Networks a rationalisé le workflow en intégrant ServiceNow et en fournissant des informations réseau et applicatives détaillées. Capable d'exploiter à la fois les lignes fixes et les connexions mobiles, Prisma Access est synonyme de haute disponibilité et de résilience. L'autre fonctionnalité post-déploiement à retenir, c'est l'auto-optimisation. La solution maintient automatiquement les niveaux de service des applications qui traversent les liaisons WAN en fonction des politiques qui s'appliquent à elles. Plus important encore, Prisma SD-WAN dirige automatiquement le trafic vers le chemin le mieux adapté. Il peut notamment utiliser la dorsale native cloud de Palo Alto Networks au lieu d'Internet afin de garantir des performances optimales.

### Mode cloud

Prisma SD-WAN embarque une console cloud de gestion simple d'utilisation qui permet aux équipes opérationnelles (NetOps, SOC) d'accéder à des informations et de créer des politiques, soit depuis les locaux de leur entreprise, soit depuis chez elles grâce aux accès basés sur les rôles. Ainsi, les entreprises réduisent la quantité de matériels déployés tout en accélérant la gestion du cycle de vie. Prisma SD-WAN peut déployer les correctifs de sécurité et de nouvelles fonctionnalités en toute transparence, ce qui élimine le besoin de fenêtres de maintenance et d'interruptions de service.

La console de gestion centralisée dans le cloud permet également aux équipes opérationnelles de créer facilement des politiques et de les appliquer instantanément sur tous les sites en périphérie. Grâce à une parfaite intégration à Prisma Access, les entreprises peuvent homogénéiser leur sécurité.

Prisma SD-WAN intègre également la technologie CloudBlades pour favoriser l'innovation sur les sites en périphérie. CloudBlades utilise des API pour intégrer des services tiers déployables en périphérie. Outre les services de sécurité, cette plateforme permet de déployer des services vocaux ou opérationnels sans ajouter de matériels ni de logiciels. Actuellement, CloudBlades prend en charge Prisma Access, ServiceNow, Microsoft, Slack, Equinix, Amazon, RingCentral, PagerDuty, et plus encore. Enfin et surtout, les entreprises peuvent développer leurs propres applications à connecter avec CloudBlades via un programme pour développeurs.

## Palo Alto Networks Prisma Access, solution de sécurité complète en mode cloud

Leader reconnu des solutions de sécurité innovantes, Palo Alto Networks a développé Prisma Access pour permettre aux entreprises d'étendre leurs systèmes de sécurité aux sites distants et aux télétravailleurs. Gestion dans le cloud, réseaux de nouvelle génération, services de sécurité réseau... cette solution offre un éventail complet de fonctionnalités de sécurité pour accélérer le passage des entreprises au framework SASE. Elle fournit également une visibilité de bout en bout, des terminaux (y compris les capteurs IoT) jusqu'aux applications hébergées dans le cloud.

Prisma Access intègre de multiples fonctions de sécurité cloud, notamment le ZTNA pour le contrôle des accès aux applications et la protection contre les menaces. Basé sur une architecture NGFW, le pare-feu sous forme de service (FWaaS) détecte les menaces pour protéger les sites distants. La passerelle web sécurisée (SWG) bloque les sites malveillants et prévient les pertes de données grâce au machine learning (ML). Quant au Cloud Access Security Broker (CASB), il veille à l'application des politiques de sécurité de votre entreprise sur le trafic réseau entre les appareils sur site et les fournisseurs cloud (IaaS et SaaS). La prévention des pertes de données (DLP) empêche les compromissions et renforce

la conformité et la confidentialité des données. L'isolement de navigateur/navigateur à distance (BI/RBI) tient les activités de navigation à l'écart des terminaux afin de rétrécir leur surface d'attaque. Enfin, la sécurité IoT (Internet des objets) aide les entreprises à se prémunir contre les cyberattaques lancées à partir des équipements IoT connectés à leur réseau afin de prévenir les interruptions de service, la baisse de productivité et la perte de chiffre d'affaires.

## Conclusion

Aujourd'hui, les entreprises doivent se projeter sur le long terme en investissant dans des solutions de résilience qui garantissent leur sécurité et leurs performances dans des environnements hautement distribués (applicatifs et utilisateurs). Selon l'étude ESG, l'adoption des applications cloud est en pleine accélération. C'est pourquoi une connectivité sécurisée, performante et hautement disponible s'avère essentielle afin de maintenir la productivité et d'offrir des expériences utilisateurs de qualité – sans avoir à trancher entre performance et sécurité.

Pour les entreprises, tout l'enjeu se situe au niveau des applications. Par conséquent, elles ont besoin de solutions technologiques de nouvelle génération qui fournissent une bonne visibilité sur l'environnement applicatif. Les solutions innovantes qui convergent les fonctions réseau et sécurité permettent de combler diverses lacunes des environnements traditionnels. C'est par elles que les entreprises pourront accélérer leur transition vers un framework SASE robuste. En portant leur choix sur un seul et même fournisseur comme Palo Alto Networks, elles pourront simplifier l'intégration des technologies réseau et de sécurité, rationaliser le support et résoudre efficacement les problèmes.

En clair, Prisma SD-WAN et Prisma Access de Palo Alto Networks vous donnent toutes les clés pour optimiser vos performances en fonction des applications et du réseau. Côté protection, la sécurité est parfaitement intégrée afin de favoriser l'innovation dans les environnements utilisateurs et cloud hautement distribués, première étape essentielle d'une transition vers le SASE.



**Enterprise Strategy Group** est un cabinet de conseil, d'études et de stratégie dont les études, analyses et enquêtes livrent des éclairages concrets à la communauté IT mondiale.

www.esg-global.com contact@esg-global.com +1 508 482 0188