LIVRE BLANC

SD-WAN nouvelle génération : une fabric orientée applications pour une expérience utilisateur incomparable

Comme son nom l'indique, le SD-WAN orienté applications identifie les signatures d'application pour diriger le trafic sur le meilleur chemin possible. Il s'impose ainsi comme un rouage essentiel pour optimiser la performance réseau. Découvrez un système capable de reconnaître les applications pour améliorer l'expérience utilisateur et transformer la gestion réseau à long terme.

PRISMA® SD-WAN
BY PALO ALTO NETWORKS

sdxcentral®

Introduction

La vie tout entière est une succession de performances, tant dans nos loisirs (sports, musiques, etc.) que dans la gestion d'un réseau informatique dont dépendent une multitude d'utilisateurs au quotidien.

Dans ce domaine, la performance repose en grande partie sur les fournisseurs d'accès Internet (FAI). Or, ces derniers doivent obtenir des débits et une disponibilité irréprochables de la part de leurs partenaires technologiques de confiance pour s'engager sur des contrats SLA garantissant un niveau de service irréprochable à leurs clients.

Les SLA réseau des FAI couvrent notamment différentes métriques :

Disponibilité – En général, les FAI garantissent un certain degré de disponibilité, par exemple 99,9 %. En d'autres termes, le réseau doit être opérationnel 99,9 % du temps. Si le réseau est indisponible plus de 0,1 % du temps, le FAI peut être redevable de pénalités vis-à-vis du client.

Temps de réponse – De même, les FAI garantissent généralement un certain temps de réponse de leurs équipes support, par exemple 15 minutes. Dans ce cas, le FAI s'engage à répondre aux demandes d'assistance des clients en moins de 15 minutes. S'il dépasse ce délai, le client peut être en droit de solliciter un remboursement ou une remise.

Bande passante – Les FAI garantissent généralement une certaine bande passante, par exemple 100 Mbit/s. Le client doit donc pouvoir télécharger et charger des données à un débit de 100 Mbit/s. Là encore, si le FAI ne parvient pas à fournir au client la bande passante garantie, le client peut être en droit de réclamer un remboursement ou une remise.

En formalisant toutes ces métriques dans le cadre de contrats SLA, les FAI peuvent garantir à leurs clients une expérience réseau de haute qualité.

Côté IT d'entreprise, comment s'inspirer de l'exemple des FAI pour garantir des niveaux d'intelligence, de réactivité et de sécurité sur les applications ? Ce document vous livre des éléments de réponse.

En quoi consiste la reconnaissance des applications et pourquoi est-elle si déterminante ?

Pour faire simple, la reconnaissance des applications consiste à pouvoir identifier les applications de tous types : applications critiques d'entreprise, SaaS, Internet et cloud. Il s'agit d'une fonctionnalité indispensable pour toute solution qui connecte les utilisateurs aux applications et en assure la gestion et la sécurité. Ce type de fonctionnalité est plutôt rare dans le cadre d'une solution SD-WAN, car il représente une avancée majeure par rapport aux capacités des systèmes d'ancienne génération.

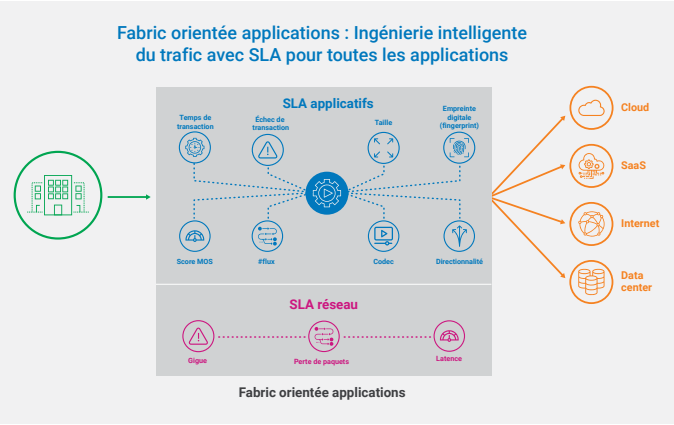
Beaucoup d'administrateurs réseau affirment que leurs réseaux peuvent détecter les applications en cours d'utilisation. C'est un bon début, mais encore faut-il que ces informations soient précises et exploitables pour renforcer les performances applicatives et l'expérience utilisateur. Dès lors qu'ils savent à quels SLA une application est soumise, les administrateurs peuvent définir des règles de routage des applications sur des chemins réseaux qui garantiront une bande passante et des performances suffisantes. Tout ceci est essentiel pour aboutir à une solution réseau orientée applications.

Dès lors que leur réseau peut reconnaître le trafic de chaque application, les administrateurs n'ont pas à surveiller constamment si les applications empruntent le chemin le plus efficace jusqu'à leur destination. Les bonnes pratiques sont systématiquement respectées, même s'il est possible d'intervenir manuellement à tout moment pour modifier des règles ou prendre une décision à titre exceptionnel dans un scénario particulier.

Le comportement des applications peut aussi changer subitement dans les flux réseau

L'autre raison pour laquelle la reconnaissance des applications revêt une importance cruciale est que ces dernières réagissent parfois de manière imprévisible au cours d'une interaction réseau. Ainsi, en plein milieu du flux réseau, les services SaaS et autres applications et sous-applications peuvent changer radicalement de comportement. Quelques exemples :

- **Elles peuvent utiliser des ports et des protocoles différents du réseau sous-jacent.** Par exemple, une application web peut utiliser le port 80 pour le trafic HTTP, tandis qu'une application SaaS peut utiliser un autre port, par exemple 443, pour le trafic HTTPS. Ce comportement peut compliquer les tâches de suivi et de gestion du trafic pour les administrateurs réseau .
- **Elles peuvent introduire d'autres services et fonctionnalités qui altèrent la circulation du trafic sur le réseau.** Une application SaaS peut ainsi proposer un service de chat qui utilise un autre protocole que le réseau sous-jacent. Le trafic peut alors être routé différemment, avec des répercussions potentielles sur la performance et la sécurité.
- **Les applications sont aujourd'hui composées de plusieurs sous-applications.** En général, une application SaaS ou cloud est une suite d'applications parentes et de sous-applications. Pour toute décision de transfert du trafic, il est donc important de savoir comment ces sous-applications sont identifiées et associées à leurs applications parentes.
- **Classification et identification des applications chiffrées.** La plupart des applications sont protégées par un chiffrement qui complique leur identification et leur classification en tant qu'applications SaaS, UCaaS ou cloud, car elles utilisent toutes le protocole SSL pour protéger leur signature.



Attributs fondamentaux de la reconnaissance des applications dans un réseau

La reconnaissance des applications peut renforcer les performances, la sécurité et la fiabilité des réseaux. En basant ses décisions de transfert sur la base des signatures, cette fonctionnalité permet de router le bon trafic vers la bonne application, tout en bloquant le trafic malveillant.

Toutefois, la qualité de la reconnaissance des applications ne vaut que par les éléments qui la composent, parmi lesquels :

Fingerprinting précis – L'empreinte digitale (fingerprinting) est une technique qui consiste à identifier les applications d'après leurs caractéristiques distinctives. Elle peut se faire par l'analyse de leur trafic, par exemple les en-têtes et les payloads des paquets, ou par l'analyse de leur comportement. En ce sens, le fingerprinting peut servir à reconnaître plus précisément la nature des applications.

Différenciation des applications par l'examen de marqueurs suivants :

Numéros de port – Chaque application utilise un ensemble défini de numéros de port. Par exemple, le protocole HTTP utilise le port 80, tandis que le protocole HTTPS utilise le port 443. La fonction de reconnaissance des applications peut se baser sur ces informations pour identifier l'application utilisant un port particulier.

Protocole – Chaque application utilise un protocole particulier. Par exemple, le protocole HTTP est un protocole textuel, tandis que le protocole FTP est binaire.

Comportement des applications – Chaque application présente un comportement qui lui est propre. Par exemple, un navigateur web envoie généralement une série de requêtes à plusieurs serveurs web, tandis qu'un client de messagerie électronique envoie une seule requête à un serveur e-mail. En plus de ces facteurs, la fonctionnalité de reconnaissance des applications peut utiliser le fingerprinting pour identifier les applications.

Schémas de trafic – L'identification des sessions applicatives, complétée par une analyse approfondie des applications et des sous-applications qui la composent, s'avère essentielle pour toute solution orientée applications. De même, la détermination des schémas de trafic SSL pour identifier le serveur d'applications auquel elles accèdent peut aboutir à une classification plus précise des applications.

Une définition flexible des applications permet aux administrateurs réseau de personnaliser les modes d'identification et de classification des applications. Cette capacité peut s'avérer utile dans une variété de situations, notamment pour l'introduction de nouvelles applications ou la mise à jour d'applications existantes. Par exemple, supposons qu'un administrateur réseau veuille définir une nouvelle application que le système de reconnaissance des applications du réseau ne reconnaît pas encore. Pour ce faire, il doit fournir au système des informations sur les caractéristiques du trafic de l'application, comme les ports et les protocoles qu'elle utilise. Une fois l'application définie, le système de reconnaissance sera en mesure d'identifier et de classifier le trafic lié à cette application.

Les métriques SLA des applications, comme les temps de transaction, les échecs de transaction et les scores MOS (Mean Opinion Score) sont également utiles pour identifier les applications, car ils peuvent révéler des indices sur le type d'application en question. Par exemple, un temps de transaction élevé peut être le signe que l'application effectue énormément de traitements, tandis qu'un nombre élevé d'échecs de transaction peut révéler le dysfonctionnement d'une application. Le score MOS est un indicateur de qualité de l'expérience (QoE) d'une application réseau. En ce sens, il peut servir à identifier les applications qui posent problème aux utilisateurs.

Priorisation des applications en fonction de paramètres, comme leur niveau de criticité ou leur nature (SaaS ou cloud), en se basant sur les facteurs suivants :

- **Utilisation –** La reconnaissance des applications peut analyser le volume de trafic généré par une application donnée, révélant ainsi son importance pour l'entreprise.
- **Intention –** La reconnaissance des applications peut observer le comportement d'une application. Par exemple, les applications employées pour les fonctions vitales de l'entreprise, comme l'e-mail ou le système CRM (Customer Relationship Management), ont vraisemblablement plus d'importance que les applications réservées à des tâches moins stratégiques comme la navigation web.

Les décisions de routage basées sur les signatures comparent les signatures du trafic à une base de données d'applications connues. Si le système de reconnaissance des applications détecte une correspondance, il peut alors prendre une décision de routage d'après la classification préétablie de l'application. Par exemple, s'il est avéré que le trafic provient d'une application web, le système de reconnaissance des applications peut transférer le trafic vers le serveur web concerné. Si le trafic provient d'une application de messagerie, le trafic est dirigé vers le serveur de messagerie.

Pour respecter tous ses engagements SLA sur les clients réseaux, Prisma SD-WAN de Palo Alto Networks fait appel à plusieurs fonctionnalités, dont la reconnaissance des applications, l'optimisation des chemins, un niveau de sécurité élevé et une forte scalabilité. Prisma SD-WAN est conçu pour s'adapter aux besoins de n'importe quelle entreprise, petite ou grande.

Rôle de la fabric orientée applications de Prisma SD-WAN dans la reconnaissance des applications

Les solutions SD-WAN d'ancienne génération étant basées sur les paquets, elles acheminent le trafic en fonction de l'adresse IP de destination. Elles exigent pour cela de nombreuses configurations manuelles pour le paramétrage et la gestion du routage. En phase opérationnelle, les utilisateurs doivent en plus configurer et gérer manuellement les équipements SD-WAN. Par leur nature même, ces solutions SD-WAN de première génération sont donc moins efficaces et plus délicates à gérer que les solutions SD-WAN plus récentes, ou de deuxième génération.

La solution Prisma SD-WAN de Palo Alto Networks intègre une fabric orientée applications qui, comme son nom l'indique, est conçue autour des besoins de toutes les applications. Concrètement, le réseau est configuré pour optimiser la performance, la sécurité et la fiabilité des applications métiers les plus critiques.

Une fabric orientée applications définit un chemin autorisé (accès direct à Internet, MPLS direct, VPN, satellite, LTE, etc.) pour chaque application, tout en assurant des performances élevées, une sécurité renforcée et la segmentation du WAN. Elle fournit ainsi un accès « direct-to-app », qui se traduit par une excellente expérience utilisateur sur toutes les applications SaaS, cloud ou on-prem de l'entreprise. Par contraste, une solution « book-ended » applique une architecture centralisée, qui exige une topologie complexe et des changements de contrôle d'accès, tout en produisant une latence importante.

Point important : une solution orientée applications digne de ce nom doit garantir la disponibilité des applications sur la base de SLA applicatifs, contrairement aux solutions d'ancienne génération qui se basent sur les SLA réseau pour effectuer un routage intelligent du trafic.

Caractéristiques spécifiques d'une fabric orientée applications

Une fabric orientée applications peut améliorer les performances des applications en s'assurant que ces dernières disposent de la bande passante suffisante. Côté sécurité, elle contribue également à renforcer leur protection en bloquant le trafic malveillant et en les isolant les unes des autres. Elle accroît également la fiabilité des applications en proposant des fonctions de redondance et de basculement en cas de panne.

Voici quelques-unes des principales caractéristiques d'une fabric orientée applications :

- **Reconnaissance des applications –** Le réseau peut identifier et classifier les applications. Ces informations peuvent servir à optimiser la performance, la sécurité et la fiabilité d'applications particulières.
- **Politiques propres à chaque application –** Il est possible de configurer le réseau en appliquant des politiques spécifiques à chaque application. Ces configurations peuvent contribuer à améliorer la performance, la sécurité et la fiabilité de chaque application.
- **Segmentation par application –** Le réseau peut être segmenté en fonction des applications. Cette segmentation permet d'isoler les applications les unes des autres et d'éviter la propagation d'éventuels problèmes.
- **Transfert basé sur les sessions applicatives –** Le réseau peut être configuré pour router le trafic d'applications spécifiques par des chemins définis. Cette fonctionnalité peut contribuer à améliorer la performance et la sécurité des applications en question. Contrairement à d'autres solutions qui répartissent les paquets (« packet-spraying »), Prisma SD-WAN adopte une stratégie de transfert basée sur les sessions, qui permet de répartir et d'équilibrer le trafic applicatif en mode actif/actif.
- **Monitoring granulaire des applications –** Le monitoring du réseau permet de suivre les performances et l'état de santé d'applications particulières. Ces informations peuvent servir à identifier des problèmes applicatifs et à apporter les changements nécessaires pour améliorer les performances et la fiabilité.

Suite de solutions Prisma SD-WAN

Prisma SD-WAN repose depuis toujours sur une architecture descendante. C'est pourquoi la solution tout entière fonctionne autour du type d'application détecté sur le réseau d'un site distant. Elle se différencie en cela des réseaux conventionnels qui utilisent généralement des protocoles de routage pour identifier les adresses IP et les itinéraires de transmission du trafic aux sites distants connectés.

Prisma SD-WAN analyse le trafic d'un site distant de l'entreprise et le valide étape après étape. De plus, la plateforme connaît les types d'application déployés, tout en offrant suffisamment de flexibilité pour personnaliser ces catégories. Dès lors qu'elle connaît la catégorie et le type de l'application, ainsi que d'autres détails comme sa version, ses derniers correctifs et sa nature (SaaS, internet ou privée), elle fournit des recommandations par défaut et assure un routage spécifique au trafic de cette application.

Une fois qu'un utilisateur a configuré des politiques métiers pour une application donnée, le routage du trafic sortant est défini en conséquence et l'ingénierie du trafic de Prisma SD-WAN prend la relève. La solution vérifie non seulement les adresses IP et la connectivité, mais reconnaît en plus les décisions éventuellement prises antérieurement sur la base des politiques et de la signature de l'application.

Force est de reconnaître que ce niveau de détail et de contrôle n'est pas fréquent dans le monde des réseaux.

Prisma SD-WAN : une analyse approfondie des conditions du réseau

Avant l'envoi du trafic par un chemin particulier, Prisma SD-WAN détermine l'état de santé du réseau sur l'itinéraire choisi, puis surveille ensuite le trafic au niveau applicatif après son envoi. Les administrateurs peuvent ainsi identifier les problèmes non repérables au moyen des seules métriques réseau, par exemple un serveur d'applications sous-performant à la destination. Ces problèmes peuvent accroître les temps de transaction et le taux d'échec, deux indicateurs que Prisma SD-WAN peut surveiller et analyser.

Supposons par exemple que Microsoft Office 365 soit transféré sur un réseau haut débit. Les performances du réseau sont bonnes, mais l'application elle-même est à la peine. Prisma SD-WAN examine les politiques métiers définies, leur apporte de la visibilité, puis recherche immédiatement un autre chemin viable. La solution transfère alors le trafic en basculant complètement le flux vers l'autre chemin disponible, tout en veillant à en informer les administrateurs réseau.

Le scénario est identique si le système doit localiser un autre serveur pour l'application. Dans ce cas de figure, il est possible de conserver le même chemin si le système peut atteindre un autre serveur plus performant. Bref, on voit ici toute la flexibilité qu'apporte la fonctionnalité de reconnaissance des applications de Prisma SD-WAN.

L'ensemble des fonctionnalités offertes par Prisma SD-WAN aboutit à une amélioration des performances réseau globales, avec 1) une accélération des temps de réponse des transactions et des applications et 2) un traitement plus rapide des processus de compression et de décompression de grands volumes de données (les codecs) qui, dans d'autres conditions, pourraient ralentir la transmission des données. Dans le contexte des applications temps réel, les codecs ont pour mission de compresser et décompresser les données suffisamment vite pour un usage immédiat. L'enjeu est particulièrement important pour les applications comme la visioconférence, les jeux en ligne et le streaming en live.

Les éléments de Prisma SD-WAN propulsent les sites distants dans une nouvelle ère

Conceptualisé pour la première fois par le cabinet Gartner en 2019 pour décrire une série de technologies émergentes, le SASE (Secure Access Service Edge) combine un SD-WAN (Software-Defined Wide Area Network) et la sécurité réseau au sein d'un même service cloud.

Dans le réseau d'entreprise de nouvelle génération, les atouts complémentaires du triptyque reconnaissance des applications, SASE intégré et SD-WAN aboutissent à un modèle qui s'impose rapidement comme une infrastructure réseau robuste, sécurisée et efficace. Aucune entreprise ne peut y être insensible !

Le plus gros obstacle est que depuis des décennies, les entreprises déploient des produits « best-of-breed » spécialisés pour chaque fonction de leur dispositif de sécurité réseau. Mais au fil du temps, la maintenance et la gestion de ces produits individuels se compliquent singulièrement. Comme chaque tronçon du réseau est étroitement connecté à tous les autres et en dépend, le moindre ajustement peut prendre des allures de parcours du combattant. Ajoutez à cela une multitude de fournisseurs, et tous les ingrédients sont réunis pour occuper vos soirées et vos week-ends.

En s'affranchissant de tous ces inconvénients, les solutions dites de « plateformes » s'imposent clairement comme une tendance IT de fond en 2023.

Fidèle à son mot d'ordre « better together », Palo Alto Networks capitalise depuis longtemps sur les synergies dans le développement de ses solutions. Progressivement, Prisma SD-WAN a resserré son intégration et sa consolidation pour incorporer à sa solution toutes les composantes de l'accès aux données. Cette architecture permet une configuration centralisée des politiques pour les deux solutions.

Alors que la planète IT poursuit chaque année son inexorable progression, les technologies d'hier sont supplantées par des applications et plateformes plus rapides et plus efficaces, et les produits réseau d'ancienne génération montrent vite leurs limites. En optant pour une plateforme, les administrateurs réseau n'ont plus à gérer et corriger des dizaines de produits opérationnels 24x7, ni à connaître en détail tous les équipements et logiciels de leur parc.

Réunis dans une seule et même solution, la reconnaissance des applications, le SD-WAN et le SASE multiplient les atouts :

Gestion simplifiée – L'intégration de ces éléments ouvre la voie à une centralisation de la gestion et de l'orchestration des fonctions sécurité et réseau, ce qui simplifie l'administration et réduit la complexité opérationnelle.

Performances en hausse – Le SD-WAN optimise les performances applicatives et le trafic réseau par un routage intelligent des données sur plusieurs liaisons WAN. La reconnaissance des applications s'inscrit dans cette approche en fluidifiant le processus. Grâce à une intégration étroite avec le SASE, le SD-WAN peut se connecter aux services de sécurité cloud les plus proches pour garantir des connexions à faible latence pour toutes les applications.

Automatisation des opérations post-déploiement – Grâce à l'intégration native du module ADEM (Autonomous Digital Experience Management), le SD-WAN assure une détection et une analyse prédictives qui permettent de corriger proactivement tout dysfonctionnement. De plus, l'ADEM offre à l'équipe IT une observabilité qui lui permet d'établir un bilan de santé de tout le réseau.

Conclusion

Avec la reconnaissance des applications, les composants SASE et SD-WAN se complètent pour agir en parfaite interopérabilité et former une solution à la fois économique et flexible qui répond à toutes les problématiques réseau et de sécurité des entreprises. Ces synergies ont montré à quel point elles améliorent les performances, l'organisation de la sécurité et la gestion du temps des équipes IT. Les administrateurs réseau ont tout à y gagner.

Le défi que doivent maintenant relever les DSI consiste à concrétiser les bénéfices à long terme d'une telle plateforme pour gérer un réseau d'entreprise.

Rendez-vous sur la page Prisma SD-WAN pour découvrir comment la fonctionnalité de reconnaissance des applications assure une expérience utilisateur incomparable.

PRISMA® SD-WAN
BY PALO ALTO NETWORKS

À propos de Prisma SD-WAN

Prisma SASE de Palo Alto Networks incarne le site distant du futur, hybride, digitalisé et sécurisé avec un SD-WAN de nouvelle génération. Contrairement à la solution SD-WAN de première génération, cette approche offre une connectivité flexible et résiliente pour les engagements SLA relatifs à n'importe quelle application et liaison WAN. De plus, elle applique une sécurité Zero Trust pour les utilisateurs, les applications et les appareils IoT, tout en automatisant les opérations post-déploiement avec AIOps. Ainsi, les entreprises peuvent fournir en toute transparence une excellente expérience utilisateur, sécuriser leur réseau de manière holistique (y compris l'IoT) et simplifier les opérations informatiques complexes.

https://www.paloaltonetworks.fr/sase/sd-wan

sdxcentral®

À propos de SDxCentral

SDxCentral est une société B2B de technologies marketing et de médias. Côté médias, nous capitalisons sur notre expertise pour donner aux professionnels de l'informatique les moyens de mieux conseiller leur entreprise et de faire progresser leur carrière. Nos contenus informent et renseignent les professionnels du cloud, des réseaux et de la sécurité qui occupent des postes opérationnels, de développement et de direction dans des entreprises de premier plan et de grands fournisseurs de services. Côté technologies marketing, nous utilisons l'engagement des acheteurs pour cerner et prédire leurs intentions, et nous connectons nos clients avec les professionnels IT intéressés. Associées à notre contenu personnalisé piloté par les données, nos solutions de technologies marketing proposent aux spécialistes du marketing d'entreprise ou des ventes d'orienter les acheteurs de produits et solutions IT pour les convertir en clients.

www.sdxcentral.com