Logo partenaire ici

ZTNA 2.0 : nouveau standard de sécurisation des accès

Sécuriser les collaborateurs dans un monde où le travail n'est plus un lieu où l'on se rend mais une activité que l'on pratique

Sommaire

Introduction

Deux ans auront suffi pour transformer de façon radicale nos modes et nos environnements de travail. Au cours de ces quelques mois, les projets entrepris dans cette direction (télétravail, migration vers le cloud…) auront connu un véritable coup d'accélérateur pour faire face aux nouvelles réalités et à leurs nouveaux enjeux. Car désormais, le travail ne désigne plus un lieu où l'on se rend, mais bel et bien une activité que l'on pratique.

Dans ce nouveau paradigme, le routage de tout le trafic via les data centers (backhauling) laisse peu à peu la place aux connexions direct-to-app. Résultat : les surfaces d'attaque augmentent de manière exponentielle.

Une situation aggravée par la permissivité excessive des architectures traditionnelles qui fournissent des droits d'accès trop étendus, doublés de capacités de détection de menaces et de vulnérabilités insuffisantes, voire inexistantes. En clair, toutes les conditions sont réunies pour la compromission de comptes à privilèges.

En parallèle, les cyberattaques continuent de progresser à un rythme effréné, tant en volume qu'en sophistication. Les attaques par ransomware ont été particulièrement nombreuses – et lucratives – au cours de la pandémie.

Les méthodes traditionnelles de sécurisation des accès distants et les architectures d'ancienne génération (y compris la première itération du Zero Trust Network Access, ou ZTNA 1.0) ne font plus le poids face à la multiplication et à la sophistication des attaques. Une nouvelle approche s'impose.

Les applications n'ont plus de frontières

80 % des entreprises suivent une stratégie cloud hybride.[1]

Chaque entreprise utilise en moyenne 110 applications SaaS.[2]

Les cinq failles du ZTNA 1.0

Les solutions ZTNA de première génération, aussi appelées ZTNA 1.0, ont été créées il y a près d'une décennie. Le champ des menaces, les réseaux d'entreprise et les modes de travail étaient alors bien différents de ceux que nous connaissons aujourd'hui. Car le monde a changé et le ZTNA 1.0 n'est désormais plus en phase avec les enjeux actuels. Les acteurs malveillants l'ont bien compris et ils n'ont d'ailleurs pas tardé à trouver de nouveaux moyens d'en exploiter les failles.

Mais avant toute chose, opérons un retour en arrière pour voir de quelles problématiques est né le ZTNA 1.0.

Le Zero Trust Network Access de première génération a été conçu pour limiter l'exposition et réduire la surface d'attaque des entreprises. Il agit en tant que « broker d'accès » sécurisant les connexions aux applications. Lorsqu'un utilisateur cherche à accéder à une application, la solution ZTNA vérifie que ce dernier dispose des droits suffisants à cet effet. Si c'est le cas, alors l'accès est autorisé et la connexion établie.

À partir de cet instant, l'outil ZTNA n'intervient plus. L'utilisateur bénéficie d'un accès total et permanent à l'application et ses actions ne font l'objet d'aucune surveillance.

C'est sur ce modèle architectural que repose l'approche ZTNA 1.0. Un modèle non seulement insuffisant, mais surtout dangereux compte tenu de la physionomie des menaces actuelles. Voici cinq bonnes raisons d'abandonner le ZTNA 1.0 au profit d'une approche mieux adaptée aux nouveaux enjeux de cybersécurité.

Les utilisateurs travaillent où ils veulent

76 % des salariés veulent maintenir une alternance présentiel/distanciel.[3]

1. Le ZTNA 1.0 va à l'encontre du principe du moindre privilège

Le premier défaut du ZTNA 1.0 est qu'il ne respecte par le principe du moindre privilège. La notion même de Zero Trust implique une vérification systématique des connexions. Le but est de s'assurer que les utilisateurs disposent uniquement des droits requis pour accéder à une application. Ni plus ni moins.

C'est le principe du moindre privilège, dont se targuent de nombreux fournisseurs de solutions ZTNA 1.0, soutenant que des droits d'accès aux applications trop étendus exposent inutilement de larges portions du réseau. Or, ces solutions gèrent l'accès aux applications au niveau des couches 3 (réseau) et 4 (transport) du modèle OSI, sur la seule base des adresses IP et des ports TCP/UDP.

Un réseau et une application sont deux choses bien différentes. Pourtant, les solutions ZTNA 1.0 se basent sur des informations réseau pour accorder des accès aux applications. Cette méthode axée sur les couches 3 et 4 pose un certain nombre de problèmes. Par exemple, si l'application

Une année 2021 marquée par les ransomwares

Explosion de 518 % des attaques par ransomware par rapport à 2020.[4]

La rançon moyenne payée par les entreprises aux États-Unis, au Canada et en Europe a augmenté de 171 % par rapport à 2020.[5]

1. *Flexera 2021 State of the Cloud Report*, 9 mars 2021, Flexera, https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report.
2. "Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2021," Statista, 16 février 2022, https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/.
3. *Sécurité du travail hybride : état des lieux 2021*, Palo Alto Networks, 15 août 2021, https://start.paloaltonetworks.fr/state-of-hybrid-workforce-security-2021.
4. *Unit 42 Ransomware Threat Report*, Unit 42, 24 mars 2022, https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.
5. Ibid.

emploie des ports ou des adresses IP dynamiques, vous devez étendre les droits d'accès au-delà du nécessaire pour couvrir les plages utilisées. Autre désagrément : il vous est impossible d'accorder des droits pour une seule fonctionnalité ou un seul élément sous-applicatif. L'utilisateur accède à l'application dans son intégralité. Enfin, les malwares qui écoutent derrière les adresses IP et ports autorisés peuvent communiquer librement et se propager latéralement au sein du réseau. En bref, les solutions ZTNA 1.0 accordent des droits d'accès beaucoup trop étendus, contrevenant ainsi au principe du moindre privilège.

2. Le ZTNA 1.0 s'appuie sur le principe de vérification unique

Il s'agit là d'une autre faille des solutions ZTNA 1.0. Le modèle de vérification unique, ou « allow and ignore », est particulièrement risqué.

Pourquoi ? Parce qu'une fois la connexion autorisée et établie entre l'utilisateur et l'application, celle-ci est réputée sûre pour toute la durée de la session, et les comportements de l'utilisateur ou de l'appareil ne sont soumis à aucun contrôle ultérieur.

Un modèle qui se contente d'une seule vérification vous mènera tout droit au désastre. Car beaucoup de choses peuvent se produire après que l'accès initial a été accordé. L'utilisateur ou l'appareil peuvent changer de comportement, et l'application peut être compromise.

Une intrusion signifie forcément que quelqu'un ou quelque chose a pu, d'une manière ou d'une autre, entrer sur votre réseau à un moment donné. De fait, bon nombre d'attaques se dissimulent au sein du trafic légitime pour échapper aux contrôles de sécurité.

3. Des inspections de sécurité inexistantes

Outre cet excès de confiance, les solutions ZTNA 1.0 présentent une autre faille : le trafic applicatif n'y est soumis à aucune inspection de sécurité. Une fois la connexion établie, le ZTNA 1.0 accorde une confiance implicite à la session active et s'abstient donc d'effectuer tout contrôle supplémentaire. Si l'appareil est compromis, et un malware est introduit dans la session, ces solutions n'ont aucun moyen de détecter le trafic malveillant qui en découle, ni d'y répondre de manière appropriée. Le ZTNA 1.0 devient alors un instrument de la sécurité par l'obscurité, ce principe qui expose les entreprises, leurs utilisateurs, leurs applications et leurs données à tous les risques.

4. Des données sans protection

Avec le ZTNA 1.0, les données, en particulier celles contenues dans les applications privées, ne sont pas protégées. La grande majorité du trafic des entreprises se retrouve donc à la merci des acteurs malveillants, internes ou externes. Pour éviter toute exfiltration des données sensibles sur les applications SaaS, les entreprises doivent déployer des solutions DLP (Data Loss Prevention) distinctes. Ce foisonnement d'outils imposé par le ZTNA 1.0 complexifie leur environnement et accroît le risque de compromission.

5. Toutes les applications ne sont pas sécurisées

Les solutions ZTNA 1.0 ne protègent pas toutes les applications. Parmi les laissées-pour-compte, on retrouve les applications cloud, celles utilisant des ports dynamiques ou encore celles basées sur des connexions initiées par un serveur vers des appareils distants, comme les applications d'assistance informatique. Les applications SaaS sont également exclues du périmètre.

Et face aux applications cloud-native modernes, composées d'une multitude de containers de microservices et utilisant des ports et adresses IP dynamiques, les contrôles d'accès ZTNA 1.0 se révèlent totalement inefficaces. En effet, cette approche requiert d'étendre les accès à une large plage d'adresses et de ports, une méthode qui va à l'encontre des principes du Zero Trust.

Or, à l'heure où les entreprises poursuivent leur migration cloud, elles deviennent de plus en plus dépendantes de leurs applications cloud-native. Le ZTNA 1.0 doit donc laisser la place à une nouvelle approche.

Les avantages du ZTNA 2.0

Les entreprises poursuivent leur transformation numérique dans le but d'optimiser leurs performances et de mettre à la disposition de leurs collaborateurs tous les outils dont ils ont besoin, où qu'ils soient.

Cette évolution transparaît surtout dans la manière dont ils accèdent à ces outils. Le backhaul laisse désormais la place à des connexions directes. À domicile, sur la route, au bureau… quel que soit l'endroit où ils travaillent, les collaborateurs doivent pouvoir accéder aux applications indispensables à leur mission, sans compromettre la sécurité de l'entreprise.

Face à ce changement de paradigme, la cybersécurité doit se réinventer autour d'une nouvelle approche. Son nom : le ZTNA 2.0.

Les principes fondamentaux du ZTNA 2.0

Le ZTNA 2.0 repose sur cinq principes élémentaires.

1. Le ZTNA 2.0 applique le principe du moindre privilège dans sa forme la plus stricte, opérant un contrôle des accès basés sur les informations recueillies depuis la couche 3 (réseau) jusqu'à la couche 7 (application).
2. Le ZTNA 2.0 procède à une vérification continue du niveau de confiance. Les solutions Zero Trust modernes doivent contrôler en permanence le niveau de confiance octroyé pour pouvoir réagir en temps réel au moindre changement de comportement (utilisateur, application, appareil…).
3. Le ZTNA 2.0 inspecte l'intégralité du trafic de manière constante afin de protéger l'entreprise contre les menaces et les attaques de toutes sortes.
4. Le ZTNA 2.0 protège l'ensemble des données de façon homogène, sur toutes les applications, qu'elles soient exécutées sur les mainframes existants ou qu'il s'agisse de la nouvelle génération d'applications de collaboration cloud-native.
5. Le ZTNA 2.0 sécurise toutes les applications (privées, cloud, SaaS…), sur l'intégralité du réseau.

Ces cinq principes viennent combler les lacunes des solutions ZTNA 1.0. Ils permettent aux entreprises de renforcer leur sécurité et de répondre aux exigences des modes de travail hybrides actuels, tout en donnant un nouvel élan à leur transformation numérique. Analysons dans le détail chacune de ces fonctionnalités.

1. Principe du moindre privilège

Palo Alto Networks a mis au point App-ID™, User-ID™ et Device-ID™. Ensemble, ces trois outils vous permettent d'accroître votre visibilité et d'opérer un contrôle granulaire sur l'octroi des droits d'accès à vos applications. Fidèles aux principes du ZTNA 2.0, nos solutions ne se contentent pas de vérifier de façon ponctuelle l'identité de l'utilisateur et son interaction avec le FQDN ou le port. Elles vont plus loin que cela.

De fait, à l'ère du ZTNA 2.0, les fonctionnalités doivent être « à états ». C'est pourquoi notre solution App-ID est capable de mémoriser une multitude d'informations relatives à la session TCP (Transmission Control Protocol), à l'établissement de la connexion avec l'application (handshake), au comportement de cette dernière, aux protocoles à états, et bien plus encore. En parallèle, les outils User-ID et Device-ID réunissent à chaque contrôle tous les renseignements nécessaires à propos des utilisateurs et de l'appareil employé.

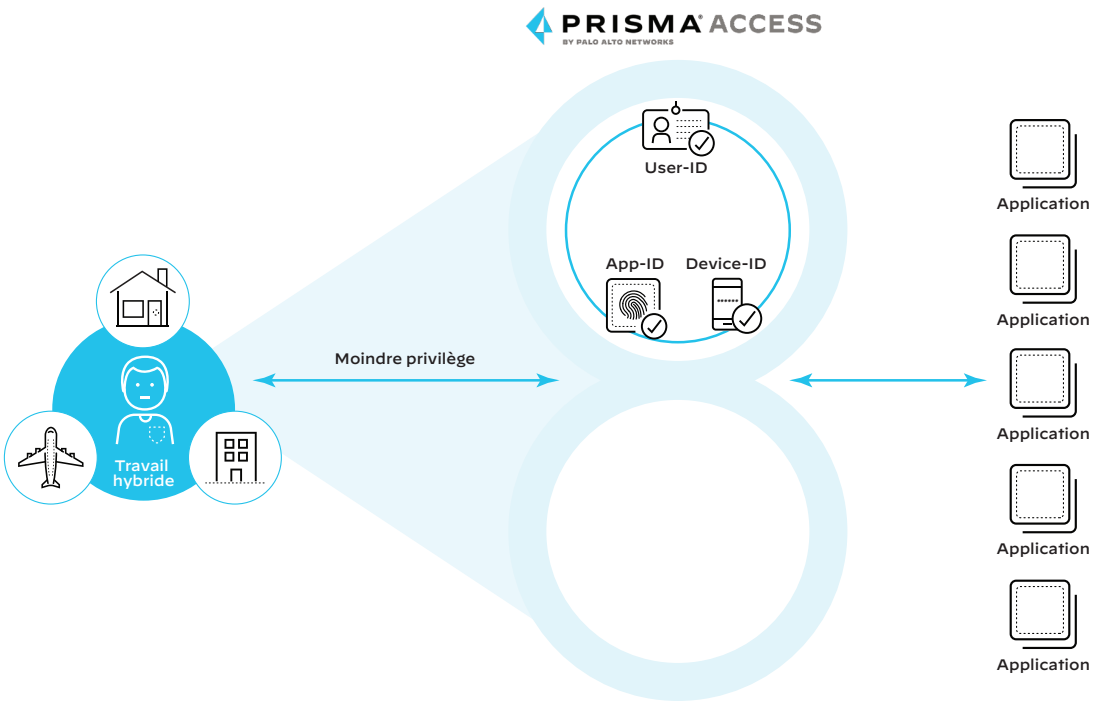

Figure 1 : Palo Alto Networks utilise App-ID, User-ID et Device-ID pour garantir le respect du principe du moindre privilège

Le triptyque App-ID, User-ID et Device-ID vous permet d'aller au-delà des vérifications uniques et d'accéder à une mine d'informations contextuelles, gage de décisions mieux éclairées. Vous pouvez octroyer des droits d'accès à un utilisateur ou à un appareil spécifique pour l'application demandée, puis recueillir en permanence de nouvelles données afin de pouvoir réagir en temps réel en cas de changement de comportement.

2. Vérification continue du niveau de confiance

Prisma Access vous permet de procéder à une vérification continue du niveau de confiance, même après que les droits d'accès à l'application ont été accordés. La solution contrôle en permanence l'état de l'appareil et réagit en temps réel à toute variation, y compris à tout changement dans le comportement de l'utilisateur ou de l'application.

L'approche Zero Trust exclut par nature toute confiance implicite. Or, sans vérification continue du niveau de confiance, le système ne remet plus en doute la fiabilité de l'utilisateur ou de l'application une fois la connexion établie. Beaucoup de choses peuvent pourtant se produire après ce premier contrôle (changement de comportement, compromission…).

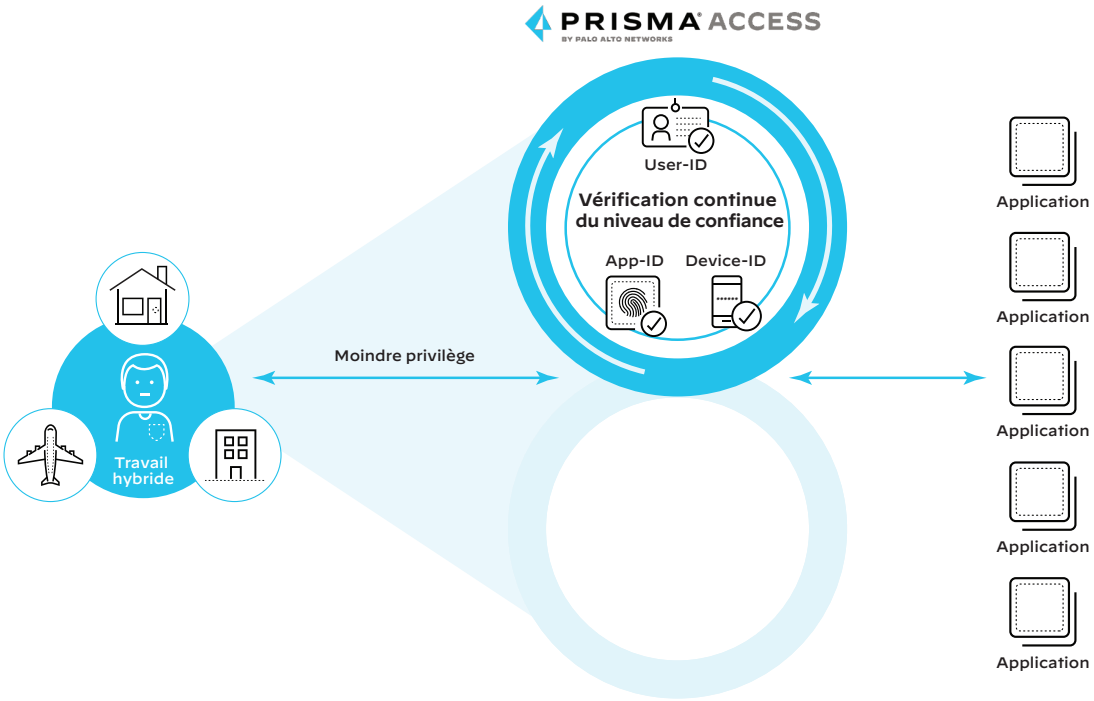

Figure 2 : La vérification continue du niveau de confiance permet un contrôle permanent du comportement des appareils, des applications et des utilisateurs, même après l'autorisation d'accès

3. Inspection de sécurité permanente

Prisma Access intègre les solutions WildFire®, Advanced URL Filtering, Threat Prevention, SaaS Security, DNS Security et bien d'autres encore, pour une inspection de sécurité continue. Elle procède également à des contrôles de sécurité approfondis et réguliers pour l'identification des connexions autorisées et la détection des attaques zero-day. Nos technologies de prévention des menaces pilotées par l'IA et le machine learning nous permettent ainsi de neutraliser 95 % des attaques zero-day inline. Résultat, votre environnement est instantanément protégé. Vous n'avez plus besoin d'attendre que l'attaque ait fait une première victime ou que les signatures aient été mises à jour.

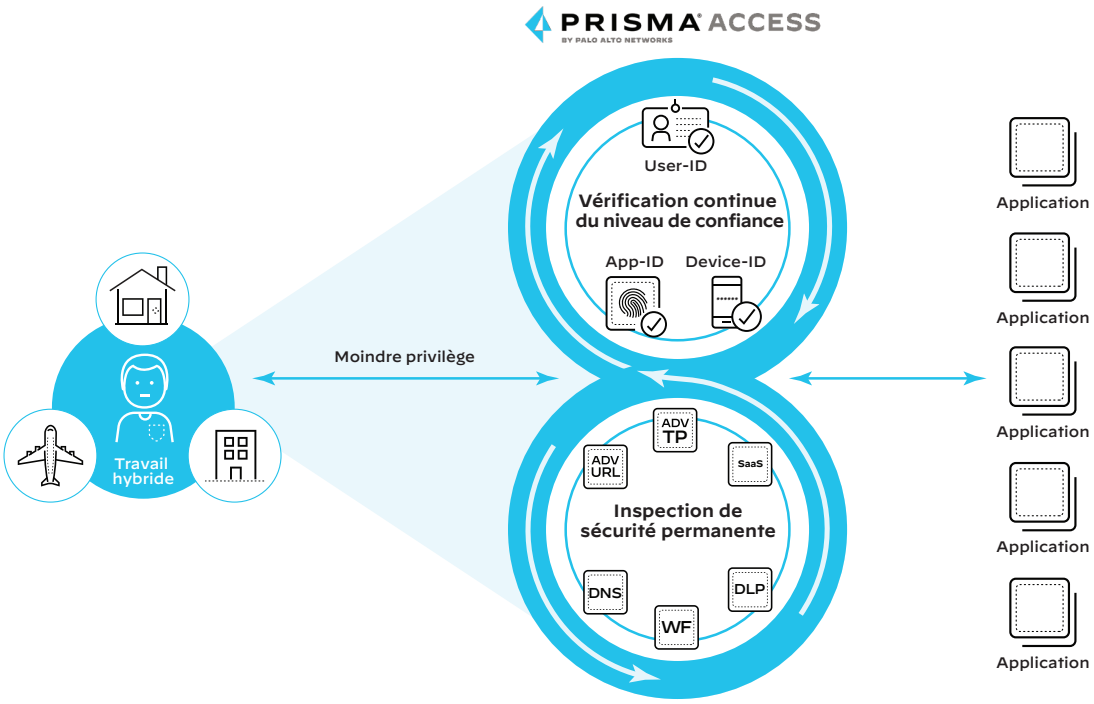

Figure 3 : Inspection de sécurité permanente pour une surveillance continue et une protection ininterrompue contre les menaces

4. Protection homogène de toutes les données

Prisma Access intègre des fonctionnalités DLP avancées pour sécuriser l'ensemble de vos données. Vos applications SaaS et privées sont protégées à l'aide d'une politique DLP unique qui garantit une cohérence parfaite et élimine toute incertitude. Vous pouvez ainsi optimiser la protection de vos données et le déploiement de vos politiques de sécurité sur tout votre parc applicatif à partir d'une seule et même solution.

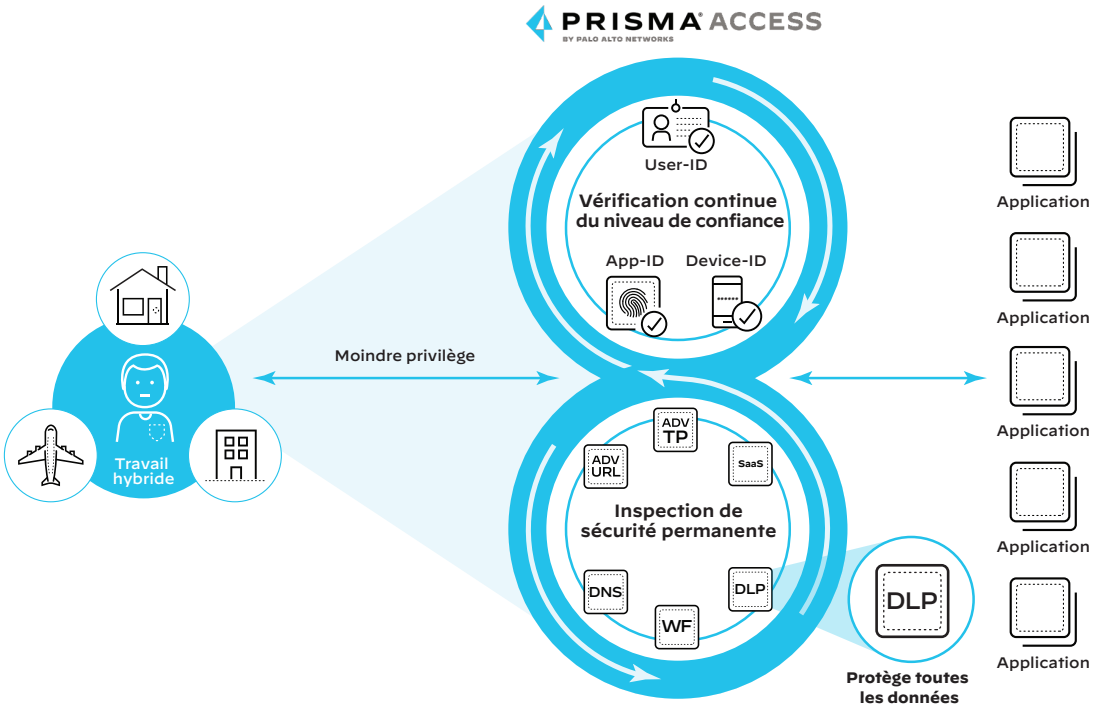

Figure 4 : Protection homogène des données sur tout votre environnement grâce à des politiques de sécurité renforcées et cohérentes

5. Sécurisation complète de toutes les applications

Privées, traditionnelles, SaaS, ancienne ou nouvelle génération, cloud-native, microservices avec adresses IP et ports dynamiques… Prisma Access protège toutes vos applications, quelles que soient leurs spécificités.

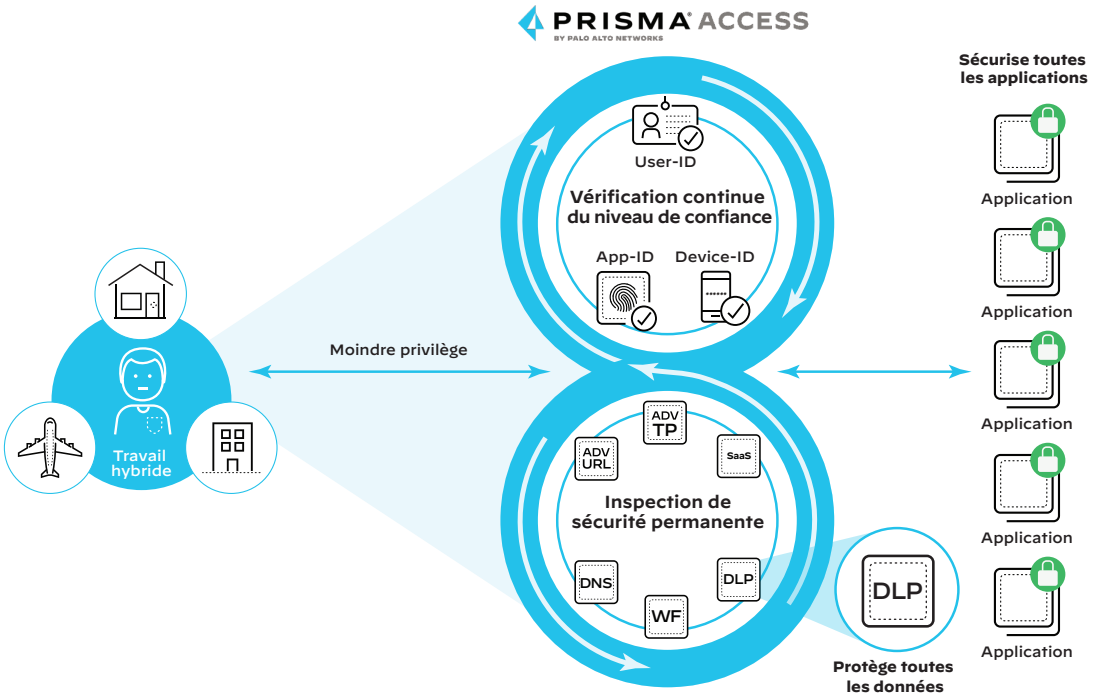

Figure 5 : Privée, cloud-native, ancienne génération… Prisma Access protège toutes les applications, quelles que soient leurs spécificités

Prisma Access : la solution ZTNA 2.0 par excellence

Prisma® Access est la seule solution cloud ZTNA 2.0 du marché, conçue pour conjuguer sécurité unifiée, simplicité d'utilisation et expérience utilisateur d'exception. Là où les outils traditionnels échouent, Prisma Access associe des fonctionnalités de pointe (ZTNA 2.0, SWG, CASB nouvelle génération, FWaaS, DLP…) pour former une solution SASE inédite, ultra complète et performante. Au menu :

- **Des contrôles d'accès granulaires** pour une sécurité optimale des connexions entre utilisateurs et applications et une réduction significative de la surface d'attaque
- **Une vérification continue du niveau de confiance** basée sur les comportements, même après la connexion
- **Des inspections de sécurité régulières et poussées** pour un trafic parfaitement sécurisé, sans compromis sur les performances et l'expérience utilisateur
- **Une protection des données et des accès** basée sur une politique DLP unique assurant une visibilité complète de la sécurité
- **Une sécurisation de toutes les données et applications** (sur site, Internet, propriétaires, SaaS, cloud-native) à partir d'une solution centralisée

Résolument cloud-native, la solution Palo Alto Networks offre une gestion multi-tenant de la sécurité à l'échelle du cloud, tout en garantissant une parfaite isolation des clients grâce à une architecture unique en son genre.

Elle s'appuie sur les niveaux d'élasticité et de disponibilité des plus grands CSP, ainsi que sur des réseaux fibres dédiés de premier plan, pour proposer des opérations de sécurité et des performances applicatives garanties par des engagements SLA leaders.

Autre avantage, le module ADEM (Autonomous Digital Experience Management) permet une identification et une résolution proactive des problèmes potentiels avant même qu'ils ne se manifestent Résultat : **des performances et une expérience utilisateur optimales** garanties.

ZTNA 2.0 : par où commencer ?

L'implémentation du ZTNA 2.0 ne doit pas être un fardeau. Elle doit se faire de façon simple, intuitive et sans compromis. Cela requiert d'établir un cahier des charges en phase avec les problématiques auxquelles votre entreprise est confrontée, tout en évitant une refonte complète de votre architecture ou des perturbations majeures de vos activités.

Voici trois points de départ potentiels pour donner l'impulsion à votre stratégie ZTNA 2.0 :

- **Remplacement du VPN**. Départissez-vous des concentrateurs VPN sur site, des architectures de backhauling peu performantes, des chemins réseau inefficaces et des infrastructures trop coûteuses à gérer.
- ***Remplacement de la SWG***. Abandonnez les architectures physiques et proxy traditionnelles au profit d'une approche cloud moderne, garante de la sécurité de vos utilisateurs lorsqu'ils accèdent à Internet ou aux outils web.
- **Sécurité avancée pour les applications SaaS ou CASB nouvelle génération**. Modernisez vos outils pour faire face à l'explosion du SaaS. Limitez votre exposition au risque, renforcez la sécurité de vos applications SaaS et de vos données sensibles, et reprenez le contrôle sur le Shadow IT.

Point de départ n° 1 : Remplacement du VPN

Remplacez vos technologies d'accès distant VPN vieillissantes par une solution ZTNA 2.0 moderne qui optimisera l'accès réseau de vos utilisateurs en télétravail ou en mode hybride, réduira les goulets d'étranglement et simplifiera les opérations de gestion.

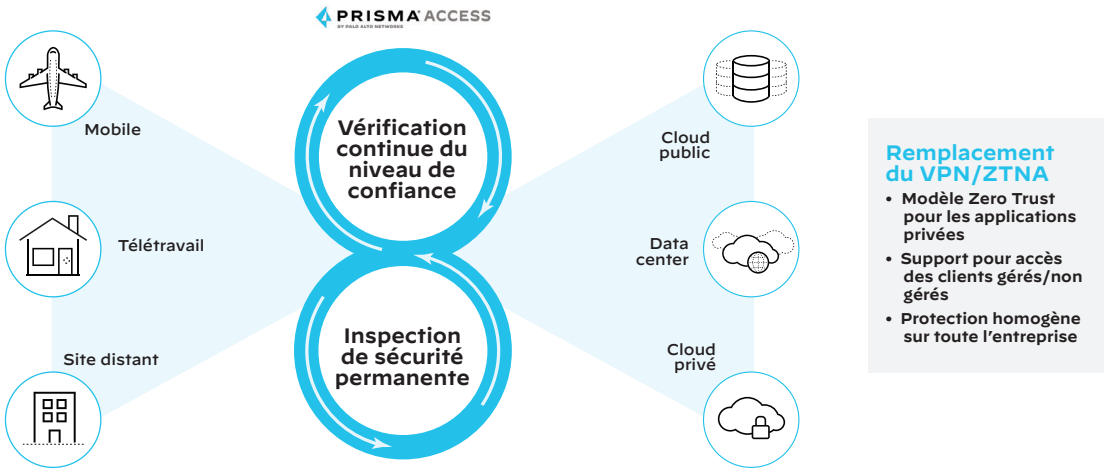

Figure 6 : Le ZTNA 2.0 comble les lacunes des VPN traditionnels pour renforcer la sécurité du travail distant et hybride

Plusieurs facteurs vont dans le sens d'un remplacement du VPN :

- Migration des applications vers un modèle hybride pour exploiter tout le potentiel des environnements cloud, multi-cloud et sur site. Les technologies VPN traditionnelles qui redirigent le trafic vers un concentrateur sur site, via un backhaul ou un cheminement tortueux, sont peu évolutives et offrent une expérience utilisateur bien inférieure au potentiel du ZTNA 2.0.
- Évolution des exigences régissant l'accès aux applications d'entreprise. Pour faire leur travail, les collaborateurs utilisent généralement des appareils gérés par l'entreprise. Pourtant, un nombre croissant d'appareils non gérés accèdent aux réseaux – et aux applications – des entreprises.
- Un modèle de protection cohérent et universel qui couvre toutes les applications et ne se limite pas aux applis web ou d'ancienne génération.

Il existe plusieurs solutions capables de répondre à ces besoins. Pourtant, seule Prisma Access vous permet de moderniser votre réseau et vos outils de sécurité pour contrôler à la fois les appareils gérés et non gérés, tout en assurant une protection homogène de l'ensemble de vos environnements.

Des milliers de collaborateurs protégés partout dans le monde

Grâce à Prisma Access, notre client a pu connecter 350 000 utilisateurs dans 158 pays tout en garantissant un accès direct à Internet pour ses centaines de sites distants répartis dans le monde entier. Prisma Access lui a également permis de sécuriser de façon homogène l'accès à toutes ses applications, y compris d'ancienne génération, sur plus de 30 data centers et emplacements cloud.

- Pour connecter ses sites et utilisateurs distants aux ressources de l'entreprise, ce cabinet de conseil du Fortune 100 utilisait une solution VPN multifournisseurs vieillissante et rigide.
- Son hétérogénéité, associée au nombre astronomique de collaborateurs et de sites distants à protéger, privait l'entreprise de toute visibilité sur ses environnements et nuisait à leur sécurité.
- Problèmes de connectivité, manque de fiabilité, expériences inégales d'un site à l'autre… les collaborateurs étaient tout sauf satisfaits de cette solution. L'objectif premier était donc de la remplacer.

Point de départ nº 2 : Remplacement de la SWG

Bon nombre d'entreprises cherchent à optimiser l'accès de leurs collaborateurs aux applications web. Le backhauling, qui consiste à rediriger le trafic web via le data center de l'entreprise avant de livrer le contenu demandé jusqu'au lieu de connexion, implique des temps de latence extrêmement longs. Prisma Access supprime cette latence tout en renforçant la sécurité.

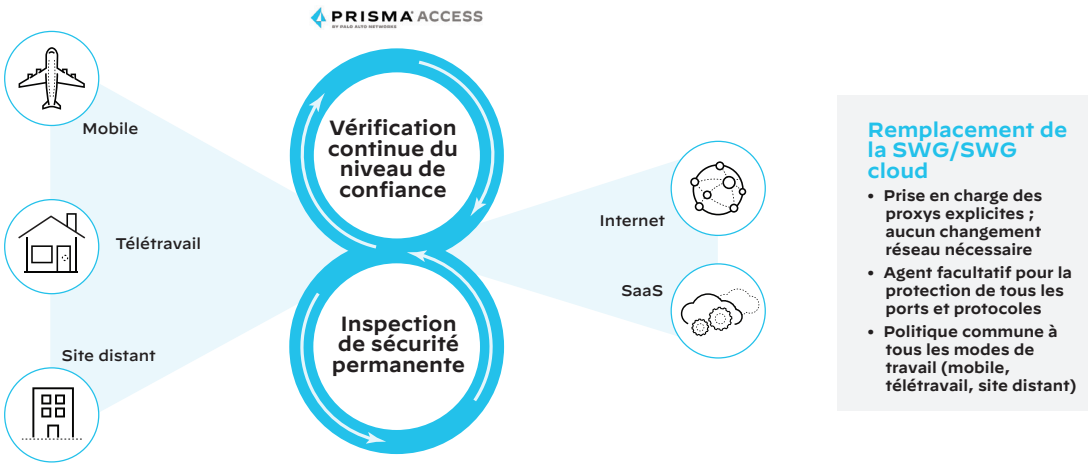

Figure 7 : Avec Prisma Access, l'approche ZTNA 2.0 permet également de supprimer les latences liées aux SWG traditionnelles

Avec Prisma Access, préparez votre entreprise au ZTNA 2.0. Vous pouvez déployer à tout moment les agents qui sécuriseront l'ensemble de vos ports, protocoles et applications. Prisma Access offre de nombreux avantages :

- De multiples méthodes de connexion proposées (proxy explicite, avec agent, sans client) pour implémenter une SWG capable de prendre en charge les collaborateurs hybrides et les sites distants
- Migration simplifiée depuis les proxys d'ancienne génération vers les solutions d'accès sécurisé en mode cloud. Une simple mise à jour des fichiers PAC existants suffit. Aucun changement nécessaire au niveau du réseau
- Intégration transparente à Prisma SD-WAN pour assurer une protection homogène sur tous les sites distants

Vers une sécurité cloud-native

Les solutions de notre client ne parvenaient plus à suivre le rythme face à la migration de ses outils et applications vers le cloud. Confrontés à des expériences erratiques et des problèmes de performance, les collaborateurs n'ont pas tardé à exprimer leur mécontentement.

Pour résoudre le problème, cette entreprise pharmaceutique du Fortune 100 a choisi de moderniser son infrastructure, en limitant les déploiements matériels multifournisseurs sur site au profit d'une solution de sécurité en mode cloud.

Grâce à Prisma Access et à son proxy explicite, trois mois ont suffi à l'entreprise pour migrer 100 000 utilisateurs vers le cloud, sans effort et sans aucune réorganisation de son architecture.

La nouvelle solution cloud-native lui a permis de consolider et d'éliminer ses équipements proxy physiques avec, à la clé, une sécurité renforcée sur tous ses sites et pour tous ses utilisateurs. Autre avantage, le module ADEM (Autonomous Digital Experience Management) de Prisma Access offre désormais à ses collaborateurs une expérience optimale sur les environnements hybrides.

Point de départ nº 3 : Sécurité avancée pour les applis SaaS

Prisma Access facilite le déploiement des CASB nouvelle génération pour garantir une protection complète de toutes les applications, sur site ou dans le cloud. Les entreprises peuvent ainsi reprendre le contrôle sur le Shadow IT et établir des workflows simplifiés qui sécurisent l'accès aux applications SaaS et leur permettent de faire face à l'explosion du « Software as a Service ».

Prisma Access offre la protection API la plus étendue du marché pour les applications SaaS et collaboratives approuvées.

Doté de capacités DLP avancées, adaptées aux applis privées comme publiques, Prisma Access offre un CASB nouvelle génération qui étend la protection des données à tous vos environnements : SaaS, réseau, sites distants, travail hybride. Il s'accompagne également de fonctionnalités d'auto-remédiation et facilite la gestion des réponses aux incidents.

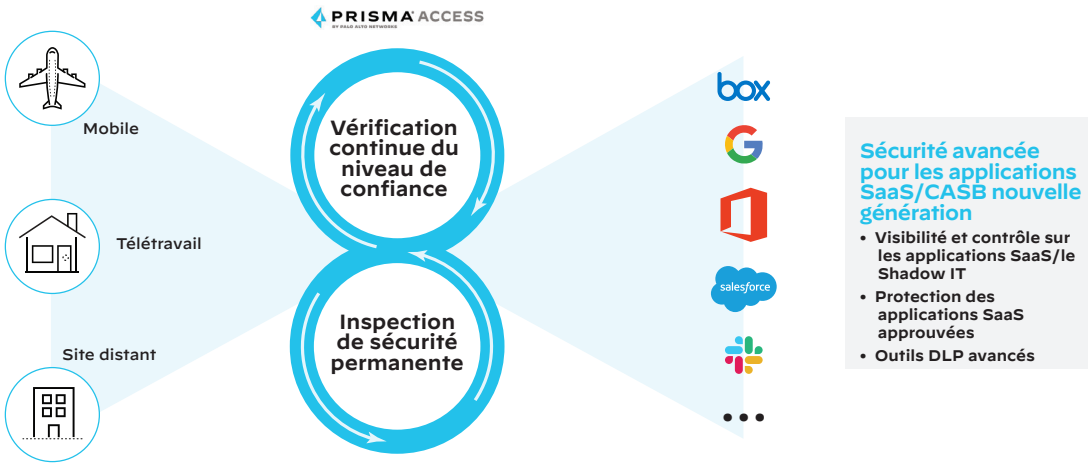

Figure 8 : Prisma Access offre un CASB nouvelle génération qui protège toutes les applications, sur site ou dans le cloud

Applications SaaS : visibilité, contrôle et sécurité des données

Une entreprise leader dans le domaine des technologies automobiles, employant 180 000 collaborateurs répartis dans 124 usines, 12 centres techniques et 44 pays, avait choisi de migrer ses applications vers le cloud. Elle avait besoin d'une meilleure visibilité et d'un contrôle granulaire des accès sur ses applications SaaS connues et inconnues. Elle cherchait également à consolider la gestion de ses multiples fournisseurs et produits, tout en adoptant un outil d'inspection des menaces.

Autre objectif : simplifier l'élaboration et le déploiement des politiques et éliminer le besoin de recourir à un proxy ou agent ou de synchroniser les risques, les politiques et les objectifs sur les différentes couches de sa stack. Grâce au CASB nouvelle génération de Prisma Access, l'entreprise n'a plus besoin de mettre à jour/configurer ses agents pour l'inspection et la protection inline des terminaux non gérés.

Conclusion

Comment une approche aussi faillible que le ZTNA 1.0 a-t-elle seulement pu voir le jour ? Face à ses nombreux défauts, on est en droit de se poser la question. N'oublions pas toutefois que cette solution a été créée pour répondre à des problématiques de cybersécurité qui ne sont plus les nôtres. Car le paysage des menaces a évolué, les acteurs cyber perfectionnent leurs techniques et les surfaces d'attaque sont plus étendues que jamais. La raison ? Des réseaux hybrides qui permettent aux collaborateurs de s'affranchir des limites physiques de leur entreprise. Le travail est désormais une activité que l'on pratique et non plus un lieu où l'on se rend.

Le ZTNA 2.0 fait entrer la sécurité des accès dans une nouvelle ère. Prisma Access, la seule solution de sécurité ZTNA 2.0 du marché, mise sur des outils simplifiés, unifiés et spécialisés pour vous accompagner sur cette voie.

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr

parent_wp_ztna-2.0:-the-new-standard-for-securing-access_051022-fr