Prisma Access

Le travail hybride et les architectures « direct-to-app » ont rendu obsolètes les architectures de sécurité traditionnelles, tout en élargissant considérablement notre surface d'attaque. Dans le sillage de cette transformation sont nées des offres de sécurité cloud qui n'offrent cependant qu'une protection incomplète et hétérogène, sans parler de la médiocrité des expériences utilisateurs.

C'est là que Palo Alto Networks entre en scène avec Prisma Access, un produit de sécurité ZTNA 2.0 simple et unifié qui protège vos collaborateurs hybrides tout en leur offrant une expérience d'exception. Résolument cloud-native, Prisma Access offre la seule solution ZTNA 2.0 du marché dotée de fonctionnalités capables de sécuriser l'ensemble du trafic applicatif et de protéger les accès et les données pour réduire considérablement le risque de compromission. Grâce à son référentiel de politiques commun et à sa gestion centralisée, la solution assure la protection des collaborateurs hybrides, tout en leur offrant une performance optimale garantie par des SLA.

La différence Prisma Access

Prisma Access permet aux collaborateurs d'accéder en toute sécurité aux applications dont ils ont besoin, où qu'ils se trouvent et quel que soit l'appareil qu'ils utilisent, réduisant ainsi considérablement les risques. Cette solution cloud-native unifiée protège les entreprises et les équipes hybrides grâce à des fonctionnalités de sécurité de pointe, avec en prime une évolutivité dynamique et des performances maximales qui améliorent l'expérience utilisateur. Prisma Access facilite la protection des collaborateurs hybrides et des entreprises cloud-first en leur offrant :

- **Une sécurité renforcée grâce au ZTNA 2.0**, associant d'une part un contrôle granulaire des accès et des inspections de sécurité permanentes basés sur le principe du moindre privilège, et d'autre part une DLP d'entreprise performante afin de protéger tous les utilisateurs, appareils, applications et données.
- **Un produit de sécurité unifié** offrant des protections complètes rassemblées en un seul et même outil garant d'une visibilité centralisée, de politiques homogènes et de données partagées pour tous les utilisateurs et applications.
- **La meilleure expérience utilisateur** reposant sur une architecture cloud-native conçue pour sécuriser les entreprises à l'échelle du cloud et offrir une performance sans compromis, le tout garanti par des engagements SLA leaders.

Prisma Access vous offre le meilleur de la sécurité au sein d'une plateforme SSE cloud-native. Combinée à Prisma SD-WAN, elle permet aux entreprises de transformer leur réseau et leur sécurité avec la solution SASE (Secure Access Service Edge) la plus complète qui soit.

Couche SECaaS (Security-as-a-Service)

Prisma Access offre des fonctionnalités de sécurité complète consolidées au sein d'une plateforme SSE unifiée facilitant le déploiement du ZTNA 2.0 et garantissant la meilleure expérience utilisateur possible.

Pare-feu « as-a-service »

Le pare-feu « as-a-service » (FWaaS) de Prisma Access fournit toutes les fonctionnalités des pare-feu nouvelle génération (NGFW) de Palo Alto Networks : protection du trafic entrant et sortant, authentification utilisateur et contrôle d'accès natifs, inspection « single pass » des couches L3 à L7 pour protéger les sites distants, etc.

Passerelle web sécurisée dans le cloud (Cloud SWG)

Prisma Access propose Cloud SWG, une passerelle web sécurisée dans le cloud conçue pour protéger les utilisateurs distants des menaces lorsqu'ils accèdent aux applications web et non-web, où qu'ils se trouvent dans le monde. Pour plus de flexibilité, ces derniers peuvent choisir entre plusieurs options de connectivité (avec agent, sans agent, VPN IPsec ou proxy explicite) qui facilitent la transition depuis les solutions SWG traditionnelles basées sur des proxys. Cloud SWG s'intègre en natif au CASB nouvelle génération et prend en charge toutes les protections web de Prisma Access, y compris Threat Prevention, WildFire®, URL Filtering, Advanced URL Filtering, DNS Security et DLP. Enfin, l'intégration de l'architecture CloudBlades dans Prisma Access rend possible l'isolation de navigateur à distance (RBI).

Zero Trust Network Access (ZTNA) 2.0

Les contrôles d'accès granulaires du ZTNA 2.0 assurent une sécurité optimale des connexions des utilisateurs à leurs applications. Une fois la connexion effectuée, leur comportement est contrôlé en permanence pour détecter tout écart. À elle seule, cette vérification réduit considérablement la surface d'attaque. Des inspections de sécurité extrêmement poussées sont effectuées sur tous les types d'applications (sur site, Internet, propriétaires, SaaS, cloud-native) pour les protéger contre toute forme de menace. Le trafic applicatif est parfaitement sécurisé, sans aucune concession sur les performances et l'expérience utilisateur. Le ZTNA 2.0 de Prisma Access, c'est aussi une protection des données et des accès basée sur une politique DLP unique, gage d'une visibilité complète sur toute l'entreprise.

Cloud Access Security Broker nouvelle génération

Prisma Access offre le seul CASB nouvelle génération du marché capable de garder le rythme face à l'explosion du SaaS. Il s'appuie pour cela sur des fonctionnalités natives et automatisées combinant gestion de la posture de sécurité (SSPM) SaaS, visibilité proactive, sécurité de pointe et protection des données en temps réel (y compris des secrets difficilement détectables dans les applications collaboratives). Le CASB Prisma Access intègre des fonctionnalités multimodes

basées sur une sécurité inline et par API, tant pour les applications SaaS approuvées que non approuvées, afin d'aider les entreprises cloud-first à :

- Détecter et bloquer les activités émanant de comptes compromis et d'utilisateurs malveillants avant qu'elles ne provoquent des dégâts.
- Détecter les activités suspectes symptomatiques d'une compromission de compte ou de la présence d'un utilisateur malveillant.
- Renforcer leur protection au-delà des contrôles de conformité standards à l'aide d'un moteur de politiques de sécurité leader sur le marché.
- Éliminer le risque de compromission et de perte de données lié aux erreurs de configuration.
- Corriger en un clic les erreurs de configuration critiques et réduire ainsi considérablement le temps de remédiation.

Couche NWaaS (Network-as-a-Service)

Prisma Access assure un accès sécurisé et homogène à toutes les applications – dans le cloud, en data center ou sur Internet.

Fonctionnalités réseau pour les utilisateurs hybrides et mobiles

Connectez vos utilisateurs hybrides et mobiles à l'aide de l'application GlobalProtect dans différentes configurations : User-Based Always-on, Pre-Logon Always-on ou à la demande. Prisma Access prend en charge un « split tunneling » basé sur l'itinéraire d'accès, le type, les risques associés et la consommation de bande passante des applications.

Fonctionnalités réseau pour les sites distants

Utilisez des équipements de base compatibles IPsec (routeurs, appliance SD-WAN, etc.) pour connecter vos sites distants à Prisma Access via un tunnel VPN IPsec standard. Vous pouvez utiliser le protocole BGP (Border Gateway Protocol) ou un routage statique depuis le site en question, ainsi que le routage ECMP (Equal-Cost Multipath) pour gagner en performance et en redondance sur de multiples liaisons.

Suivi des expériences numériques

L'option Autonomous Digital Experience Management (ADEM) pour Prisma Access offre une visibilité complète SASE-native. Elle fournit des éclairages par segment sur tout le parcours de livraison des services, avec en prime une analyse du trafic réel et synthétique qui permet d'automatiser la résolution des problèmes d'expérience numérique (y compris en self-service grâce à l'outil ADEM Self-Serve). Le module Prisma Access Insights offre gratuitement aux utilisateurs Prisma Access une visibilité à la demande sur l'état de fonctionnement de leur déploiement Prisma Access.

Gestion centralisée

Prisma Access peut être géré de deux manières :

- **Prisma Access Cloud Management** pour rationaliser la gestion des configurations de Prisma Access autour de quatre axes : intégration transparente (avec configuration préprogrammée selon les bonnes pratiques), évaluation continue de la sécurité, suivi de l'expérience numérique, et expérience cloud unifiée pour le reporting.
- **Console de gestion de la sécurité réseau Panorama** pour centraliser la gestion des politiques de Prisma Access et de tous les pare-feu nouvelle génération de Palo Alto Networks. En gérant la sécurité du réseau en central, Panorama permet de gagner du temps et de réduire la complexité.

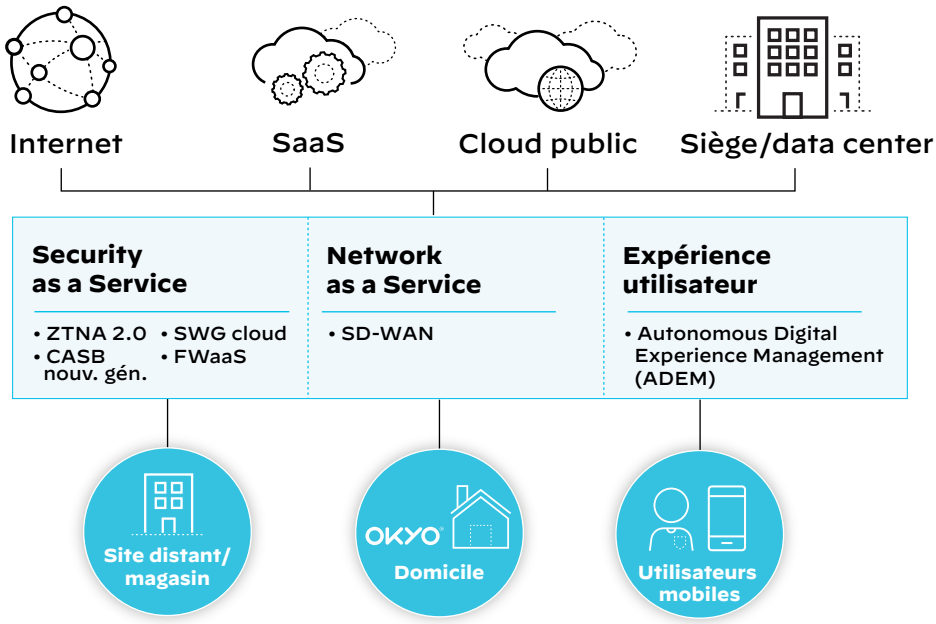

Figure 1 : Architecture Prisma Access

Tableau 1 : Caractéristiques et fonctionnalités de Prisma Access

	Prisma Access pour les réseaux	Prisma Access pour les utilisateurs	Prisma Access pour Clean Pipe
Points de présence	Plus de 100 dans 77 pays	• Plus de 100 dans 77 pays (GlobalProtect) • 25 points de présence (proxy explicite)	17 points de présence
Type de connexion	Tunnel IPsec	• IPsec/SSL de l'application GlobalProtect • VPN sans client GlobalProtect • Proxy explicite	Peering via Partner Interconnect (interconnexion VLAN par tenant)
Application GlobalProtect Plateformes prises en charge	n/a	• Apple iOS • Apple macOS • Google Android • Application Android pour Chromebook • CentOS Linux • Red Hat Enterprise Linux • Ubuntu • Windows 10 et UWP	n/a
		Plateformes IoT • Raspberry Pi OS • Windows IoT Enterprise • Ubuntu • Google Android	
Accords de niveau de service			
Disponibilité	99,999 % par mois calendaire		
Connectivité	99,99 % à 10 ms sur une heure		

Tableau 2 : Fonctionnalités de Prisma Access	
Fonctionnalité	**Description**
App-ID	Classifie en permanence toutes les applications indépendamment du port, du chiffrement TLS/SSL ou de la technique d'attaque utilisée pour contourner le système de détection. Contrairement aux solutions d'ancienne génération qui s'appuient sur les couches L3 et L4 comme premier niveau de contrôle avant classification des applications, Prisma Access exécute App-ID en même temps que d'autres contrôles en couche L7 (fonctionnalité User-ID, par exemple).
User-ID	S'intègre à un large éventail de référentiels d'identité (contrôleurs WLAN, VPN, serveurs d'annuaire, portails captifs basés sur les navigateurs, proxys, etc.) pour que vos politiques puissent s'appliquer à vos utilisateurs et vos groupes, où qu'ils se trouvent.
Device-ID*	Permet de créer des politiques qui s'appliquent systématiquement à un appareil donné, indépendamment de l'endroit du réseau d'où il est connecté. Des politiques basées sur les attributs d'un appareil (version du système d'exploitation, par exemple) donnent aux équipes de sécurité la possibilité d'opérer un contrôle plus strict de la surface d'attaque. Les journaux Device-ID fournissent du contexte et offrent une visibilité supplémentaire. Combinés aux données App-ID et User-ID, ils permettent d'obtenir des éclairages approfondis sur les comportements au sein du réseau.
Déchiffrement SSL	Inspecte et applique une politique de sécurité au trafic TLS/SSL chiffré, entrant et sortant, ainsi qu'au trafic utilisant le protocole HTTP/2. URL, source, destination, utilisateur, groupe d'utilisateurs, port… vous pouvez activer ou désactiver le déchiffrement selon différents critères pour répondre à vos exigences de confidentialité et de conformité.
Surveillance des DUG (Dynamic User Groups)	Propose des actions de sécurité dynamiques basées sur le comportement des utilisateurs pour limiter la marge de manœuvre des utilisateurs suspects ou malveillants. Cette fonctionnalité permet de définir des DUG dans Prisma Access pour enclencher des actions de sécurité rapides sans attendre que des modifications aient été effectuées sur les annuaires d'utilisateurs.
Détection par ML/IA	Permet une détection inline et sans signature des attaques et une prévention des exploits zero-day. Prisma Access fournit une protection en temps réel, marquant ainsi la fin des mises à jour planifiées. Jusqu'à 95 % des menaces inconnues sont bloquées instantanément, avec des signatures émises en moins de 10 secondes, ce qui réduit de 99,5 % le nombre de systèmes infectés.
IoT Security*	Combine le machine learning à notre technologie App-ID et à une télémétrie collective pour profiler tous les appareils. Objectif : rechercher les menaces, évaluer les risques, analyser les vulnérabilités, détecter les anomalies et recommander des politiques basées sur le niveau de confiance. Cette fonctionnalité permet de neutraliser les menaces IoT, IoMT et OT connues et inconnues, et d'appliquer nativement des politiques de sécurité via un NGFW Palo Alto Networks piloté par ML ou via orchestration avec des solutions tierces.
Intégration des proxys explicites	Permet de choisir le mode proxy où le client (navigateur) est configuré pour utiliser un serveur proxy. Cette option offre aux utilisateurs mobiles une manière alternative de se connecter à Prisma Access et de sécuriser leur trafic Internet et SaaS (HTTP/HTTPS). Les fichiers PAC sont pris en charge pour la configuration du navigateur.
PAN-OS Policy Optimizer	Fournit un workflow simple pour migrer des règles basées sur les ports vers des règles App-ID. Vous réduisez ainsi votre surface d'attaque et augmentez l'efficacité de vos politiques de sécurité.
Isolation de navigateur à distance (RBI)	Exploite les fonctionnalités de réécriture et de catégorisation d'URL présentes dans les NGFW pour s'intégrer à des clouds RBI tiers via CloudBlades. Vous pouvez ainsi transférer tout ou partie du trafic Internet vers le cloud RBI. Cette fonctionnalité fluidifie l'expérience utilisateur tout en transférant certains trafics (inconnus ou à haut risque) vers le cloud RBI à des fins d'inspection supplémentaire. Le trafic restant peut être inspecté par Prisma Access et dirigé directement vers Internet.
Reporting	Inclut par défaut un rapport détaillé et personnalisable d'utilisation des applications SaaS pour vous livrer un aperçu sur tout le trafic SaaS – autorisé ou non – de votre réseau. Vous pouvez également créer des rapports personnalisés en fonction de vos besoins, et les planifier, les télécharger et les partager en toute simplicité avec d'autres membres de votre organisation.
Authentification des utilisateurs	Compatibilité avec toutes les méthodes d'authentification PAN-OS (Kerberos, RADIUS, SAML, LDAP, certificats clients, base de données utilisateur locale, etc.). Une fois l'utilisateur authentifié par GlobalProtect, cette fonctionnalité fournit instantanément une mise en correspondance utilisateur-adresse IP pour User-ID sur Prisma Access.
Advanced DNS Security	Assure une protection en temps réel et intègre des capacités de machine learning inline pour bloquer les rappels CnC et les attaques DNS. Intégré en natif à Prisma Access, Advanced DNS Security automatise votre protection, empêche les attaquants de contourner vos systèmes de sécurité et élimine le besoin de recourir à d'autres outils ou de modifier le routage DNS.
Advanced URL Filtering	Offre une sécurité renforcée contre les menaces web (phishing, malware, CnC, etc.) en s'appuyant sur des bases de données complètes et un moteur de sécurité web ML capable de répertorier et de bloquer les URL malveillantes en temps réel. Son système anti-phishing de pointe vous protège contre les sources de compromission les plus courantes. Il vous aide ainsi à reprendre le contrôle total du trafic web à l'aide de vérifications et de politiques granulaires permettant d'automatiser les actions de sécurité en fonction des utilisateurs, des scores de risque et des catégories de contenu.
Prévention des pertes de données (DLP)*	Comprend un ensemble d'outils et de processus destinés à protéger vos données sensibles de tout partage, extraction, utilisation abusive ou accès non autorisé. Le service DLP sur Prisma Access favorise l'application de politiques de sécurité des données et prévient la perte des données sensibles pour les utilisateurs mobiles et les réseaux distants.
Monitoring de l'expérience numérique (DEM)*	Avec le module supplémentaire ADEM SASE, les entreprises bénéficient d'une meilleure visibilité sur les performances applicatives et réseaux, que ce soit pour leurs utilisateurs mobiles ou sur les réseaux distants. L'ADEM fournit des éclairages par segment sur tout le parcours de livraison des services, avec en prime une analyse du trafic réel et synthétique qui permet d'automatiser la résolution des problèmes d'expérience numérique (y compris en self-service grâce à l'outil ADEM Self-Serve).
Profil d'informations sur l'hôte (HIP)	Procède à l'inspection du terminal pour établir un bilan de sa configuration, puis crée un profil HIP. Prisma Access se sert ensuite de ce profil pour appliquer des politiques qui n'autorisent l'accès aux applications que lorsque le terminal est correctement configuré et sécurisé.

Tableau 2 : Fonctionnalités de Prisma Access (suite)	
Fonctionnalité	**Description**
Mise en quarantaine des appareils	Empêche des appareils compromis d'accéder aux données confidentielles. Vous pouvez ajouter ces appareils à une liste de mise en quarantaine, de façon manuelle ou automatique, et utiliser GlobalProtect pour empêcher les utilisateurs de s'en servir pour se connecter au réseau. Vous pouvez également restreindre l'accès aux applications à partir de ces appareils compromis.
Qualité de service (QoS)	Vous permet de préserver les performances du trafic et des applications ultra-prioritaires avec une capacité réseau limitée. La fonctionnalité QoS donne la priorité au trafic critique ou au trafic nécessitant une faible latence (VoIP, vidéoconférence, etc.). Vous pouvez également définir un seuil minimal de bande passante réservé aux applications métiers critiques.
Trafic interne IPv6	Sécurise l'ensemble du trafic interne IPv6 entre les terminaux et les applications privées. Cette fonctionnalité est disponible pour les utilisateurs mobiles, GlobalProtect, les réseaux distants et les connexions au service.
IPsec VPN site-à-site	Prend en charge les tunnels site-à-site sur IPv4 et IKEv1/IKEv2 pour en assurer la compatibilité. Dans un environnement comportant de nombreux sites de connexion, le routage ECMP équilibre les sessions sur les connexions Internet disponibles pour fournir une redondance et des économies supplémentaires.
Journalisation	Affiche les journaux du trafic, des applications, des utilisateurs, des menaces, des URL et des filtres de données pour faciliter l'organisation des données par le biais de Cortex Data Lake dans le cloud.
Automatisation des politiques	Permet d'exploiter des informations provenant de sources tierces pour actualiser dynamiquement les politiques de sécurité via l'API XML et une combinaison de groupes d'adresses dynamiques (DAG).
Système de prévention des intrusions (IPS)	Neutralise les exploits, les dépassements de tampon et les analyses de ports. D'autres fonctionnalités (blocage de paquets invalides ou mal formés, défragmentation IP, réassemblage TCP, etc.) vous protègent contre les techniques d'obfuscation de contournement des attaquants. Les signatures basées sur les vulnérabilités sont mises à jour en permanence à partir du service WildFire de prévention des malwares. Les signatures personnalisées peuvent également être importées manuellement, y compris à partir de formats connus comme Snort et Suricata.
Protection antimalware	Utilise un moteur basé sur les flux qui effectue un blocage inline à très haute vitesse pour détecter les malwares connus et les variantes inconnues des familles de malwares connus. Les fonctionnalités IPS et anti-malware s'attaquent à plusieurs vecteurs de menaces avec une seule licence, éliminant ainsi le besoin d'acheter et de maintenir des produits IPS et proxy spécialisés auprès d'autres fournisseurs.
Protection anti-CnC	Bloque les communications malveillantes sortantes résultant d'infections de malwares, analyse passivement les requêtes DNS, et identifie les schémas uniques de botnets. Cette fonctionnalité permet d'identifier les utilisateurs infectés et empêche les téléchargements secondaires et les données de quitter votre organisation.
Détection des menaces inconnues avec analyses avancées	Identifie les menaces inconnues grâce aux données issues de la plus grande communauté mondiale d'analyse des malwares, fruit de remontées d'informations des réseaux, terminaux, environnements cloud et autres partenaires externes. WildFire exploite notre hyperviseur personnalisé avec analyse bare metal, et utilise divers moteurs d'analyse complémentaires capables de détecter les attaques contournant les environnements de sandboxing.
Protection contre les menaces inconnues	Génère automatiquement des protections tout au long du cycle d'attaque lorsqu'une nouvelle menace est détectée pour la première fois (blocage des fichiers malveillants, accès aux URL malveillantes, trafic CnC, etc.), puis applique ces protections à tous les abonnés WildFire en quelques secondes pour la plupart des nouvelles menaces.
Analyse du comportement des fichiers	Effectue une analyse détaillée des comportements pour vous aider à comprendre le fonctionnement de malwares récemment détectés. Les journaux intégrés permettent d'identifier rapidement les utilisateurs infectés et d'investiguer les compromissions potentielles grâce à une analyse détaillée et une visibilité sur les évènements liés à des menaces inconnues.
Prévention orientée cloud	Utilise une architecture modulaire basée dans le cloud pour offrir une prévention automatique pilotée par CTI, sans avoir à mettre en œuvre et à gérer des appareils distincts pour le web et la messagerie électronique à chaque point d'entrée/de sortie de votre réseau.
Analyse multi-vectorielle et visibilité	Combine l'évolutivité cloud de WildFire à une analyse avancée des fichiers et à l'indexation d'URL pour fournir une analyse récursive multivectorielle (solution unique et complète de protection contre les attaques multi-étapes). Contrairement aux autres solutions, WildFire peut suivre plusieurs étapes d'une attaque, ce même si l'exécution échoue à une étape donnée. Lorsque WildFire inspecte des liens incorporés ou des liens d'e-mails dans le cadre de son analyse, il met à jour URL Filtering si les pages web correspondantes hébergent des exploits ou révèlent une activité de phishing.
Exécution complète des fichiers	Exécute simultanément des fichiers inconnus dans plusieurs versions de systèmes d'exploitation et d'applications pour cerner pleinement l'étendue d'une menace. L'analyse multi-version garantit une analyse WildFire approfondie, contrairement aux sandboxes requérant des images gold et risquant par conséquent de considérer un fichier malveillant comme inoffensif du simple fait que le système d'exploitation ou la version de l'application cible n'a pas été spécifié dans l'image gold.

Remarque : Des différences régionales peuvent s'appliquer. Pour plus de détails, reportez-vous au contrat de niveau de service (SLA) de Prisma Access.

* Nécessite une licence supplémentaire.

paloalto NETWORKS

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