Prisma Access

Avec le développement à l'international, la mobilité des effectifs et l'avènement du cloud computing, les entreprises ne déploient plus leurs applications comme avant. Avec Prisma™ Access, vous bénéficiez de la protection dont vous avez besoin, là où vous en avez besoin. Prisma Access fournit un périmètre de services d'accès sécurisé (*Secure Access Service Edge*, SASE) offrant des fonctionnalités réseau et de sécurité distribuées à l'échelle mondiale pour tous vos utilisateurs et applications.

Au bureau ou en déplacement, vos collaborateurs se connectent à Prisma Access pour accéder en toute sécurité à Internet et à leurs applications hébergées dans le cloud ou en data center.

La différence Prisma Access

Prisma Access a été conçu pour bloquer les cyberattaques, pas uniquement sécuriser le web. Or, la lutte contre les cyberattaques exige d'inspecter tout le trafic. À défaut, des failles béantes apparaissent dans votre système de sécurité.

Prisma Access protège tout le trafic, de toutes les applications et sur tous les ports. Objectif :

- **Prévenir les cyberattaques** grâce à une approche éprouvée de la sécurité et à des données de Threat Intelligence garantes d'une visibilité détaillée et d'un contrôle précis dans toute l'organisation.
- **Inspecter intégralement le trafic applicatif** à double sens et sur tous les ports, y compris le trafic TLS/SSL chiffré, pour les communications avec Internet, avec le cloud ou entre les différentes filiales de l'entreprise.
- **Bénéficier d'une Threat Intelligence complète** alimentée automatiquement par des données issues de Palo Alto Networks et de centaines de sources tierces.

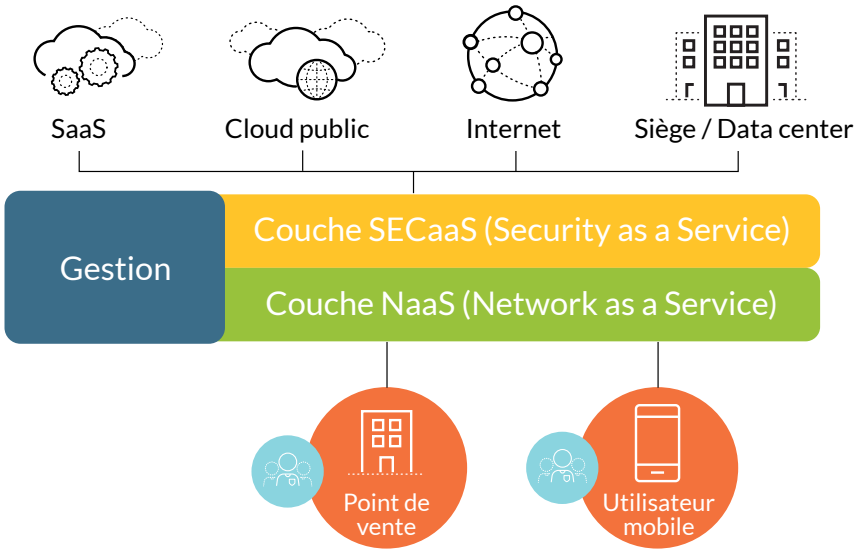

Figure 1 : Architecture Prisma Access

Couche NaaS

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

Tableau 1 : Accès sécurisé aux applications, en tous lieux et à tout moment

	Site distant	Siège social/ régional	Cloud public	Cloud privé / Data center	SaaS	Web	Internet
Site/Réseau distant	✓	✓	✓	✓	✓	✓	✓
Utilisateur mobile	✓	✓	✓	✓	✓	✓	✓

Connectivité des réseaux distants

- Utilisez des équipements de base compatibles IPsec (routeurs, équipements SD-WAN de périphérie, pare-feu tiers, etc.) pour connecter vos sites distants à Prisma Access via un tunnel VPN IPsec standard.
- Routez le trafic depuis les sites distants à l'aide du protocole BGP (Border Gateway Protocol) ou de chemins de routage statiques.
- Misez sur le routage ECMP (Equal Cost Multi-Path) pour améliorer les performances et la redondance sur de multiples liaisons.

Connectivité des utilisateurs mobiles

- Connectez vos utilisateurs mobiles à l'aide de l'application GlobalProtect dans différentes configurations : User-Based Always-on, Pre-Logon Always-on ou à la demande.
- Utilisez un tunnel « always-on » complet pour une sécurité optimale. Prisma Access prend en charge le « split tunneling » basé sur l'itinéraire d'accès, le « split tunneling » VPN par application et le « split tunneling » basé sur les applications à faible risque/large bande passante, comme le streaming vidéo.

Gestion de la bande passante

- Exploitez la technologie App-ID™ pour mettre les applications légitimes sur liste blanche et définir des politiques de blocage, libérant ainsi le réseau des applications inutiles et gourmandes en bande passante.
- Appliquez des règles de qualité de service (QoS) pour prioriser et modeler le trafic géré par Prisma Access.

Journalisation

- Exploitez des systèmes de journalisation automatisés, centralisés et évolutifs dans le cloud.
- Centralisez la gestion et le reporting.
- Transférez les journaux vers votre serveur syslog et/ou système de gestion des informations et événements de sécurité (SIEM).

Couche SECaaS

Pare-feu sous forme de service

- Le pare-feu sous forme de service (FWaaS) de Prisma Access protège les sites distants contre les menaces tout en assurant les services de sécurité caractéristiques d'un pare-feu nouvelle génération : Threat Prevention, URL Filtering, sandboxing, etc.

DNS Security

- Intégré à Prisma Access, notre service DNS Security offre une combinaison d'analyses prédictives, de fonctions d'automatisation et de machine learning pour combattre les menaces dans le trafic DNS. Les organisations peuvent ainsi bloquer les domaines malveillants connus, détecter les domaines malveillants inconnus et bloquer les tentatives de DNS tunneling.

Threat Prevention

- Utiliser Prisma Access pour la prévention des menaces, c'est allier les technologies éprouvées de la plateforme Palo Alto Networks à des fonctions d'automatisation et une Threat Intelligence mondiale pour neutraliser les attaques connues et inconnues.

Passerelle web sécurisée dans le cloud

- La passerelle web sécurisée (SWG, *Secure Web Gateway*) de Prisma Access a été conçue pour maintenir une visibilité sur tous les types de trafic tout en bloquant les techniques de contournement susceptibles de dissimuler des menaces. Nos fonctions de filtrage web permettent également à notre technologie de prévention des vols d'identifiants de bloquer la saisie d'identifiants d'entreprise sur des sites inconnus.

Prévention contre la perte de données

- Prisma Access utilise des contrôles de prévention contre la perte de données (DLP, *Data Loss Prevention*), soit in-line (via Prisma Access), soit par API (via Prisma SaaS). Ces contrôles DLP permettent aux organisations de catégoriser les données et d'établir des politiques de protection contre la perte de données.

Cloud Access Security Broker

- Prisma Access et Prisma SaaS intègrent des contrôles de sécurité in-line, contextuels et basés sur des API, faisant office de CASB (Cloud Access Security Broker) pour définir les accès aux informations sensibles. Ces contrôles s'appliquent à toutes les politiques d'applications cloud.

Gestion

Prisma Access peut être géré de deux manières :

- **Via la solution Panorama™ de gestion de la sécurité du réseau** pour centraliser l'administration de Prisma Access et de tous les pare-feu nouvelle génération de Palo Alto Networks.
- **Dans le cloud** à travers une interface web dotée de profils préconfigurés et de workflows simplifiés, en utilisant l'application Prisma Access du hub.

Tableau 2 : Caractéristiques et fonctionnalités de Prisma Access			
	Prisma Access pour les réseaux	**Prisma Access pour les utilisateurs**	**Prisma Access pour Clean Pipe**

Cas d'usage	• Sites distants / Points de vente
	• Clouds privés virtuels
	• Hub SD-WAN Palo Alto Networks
	• Sécurité SD-WAN tierce
		• Utilisateurs mobiles avec :
		  • Ordinateurs portables
		  • Smartphones
		  • Tablettes
		• Zero Trust Network Access (ZTNA)
			• Environnements de fournisseurs de services / opérateurs télécom multi-tenant
			• Sécurité du trafic sortant vers Internet

Licences			
Base	Mbit/s	Utilisateurs	Mbit/s
	Basé sur un pool de bande passante ; jusqu'à 1 Gbit/s par connexion	Basé sur le nombre total d'utilisateurs uniques	Basé sur un pool de bande passante ; jusqu'à 10 Gbit/s par tenant
Taille de déploiement minimale	Pool de bande passante de 200 Mbit/s	200 utilisateurs	100 Mbit/s par tenant
Tunnels de services			
Tunnels de services de base	Jusqu'à trois tunnels de services inclus		N/A
Tunnels de service supplémentaires	Des tunnels de services supplémentaires (jusqu'à 100) peuvent être créés en allouant 300 Mbit/s du pool de bande passante par tunnel supplémentaire		N/A
Connectivité			
Implantations	Plus de 100 dans 76 pays		17 implantations
Connection type	• Tunnel IPsec • SD-WAN (PAN-OS 9.1 ou ultérieur)	IPsec/SSL de l'application GlobalProtect	Peering via Partner Interconnect (interconnexion VLAN par tenant)
Plateformes compatibles avec l'application GlobalProtect	N/A	Apple iOS Apple macOS Google Android Google Chrome OS Linux CentOS Red Hat Enterprise Linux Ubuntu Windows 7, 8, 10 et UWP	N/A
Gestion			
Panorama	• Licence pour Panorama requise • Pas de licence pour le plugin Panorama de Prisma Access • Prisma Access ne compte pas dans la licence des équipements Panorama		
Gestion cloud	Aucune licence requise pour l'application Prisma Access du hub		
Sécurité			
URL Filtering	Inclus		
Threat Prevention	Inclus		
WildFire	Inclus		
Profil HIP (Host Information Profile)	Inclus		
DNS Security	Abonnement requis		
Data Loss Prevention (DLP)	Abonnement requis		
Cortex XDR	Abonnement requis		
Prisma SaaS	Abonnement requis		
AutoFocus	Abonnement requis		
Journalisation			
Cortex Data Lake	Cortex Data Lake est nécessaire pour la journalisation dans Prisma Access (abonnement requis)		

PRISMA ACCESS
BY PALO ALTO NETWORKS

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

prisma-access-ds-111219-fr