Le Télétravail selon Palo Alto Networks : Aucun compromis de sécurité

Généraliser et sécuriser les besoins en mobilité pour les utilisateurs nomades ou en télétravail est un enjeu crucial. Un utilisateur distant peut accéder grâce à un poste de l'entreprise ou avec son propre device à des ressources de l'entreprise à l'Internet, aux applications SaaS et à tous les cloud publics. Pour sécuriser les flux quel que soit le scenario d'accès, Palo Alto Networks, le leader mondial de la cybersécurité proposent plusieurs solutions.

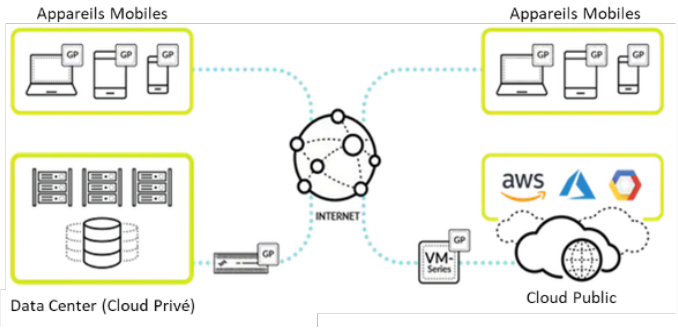
GlobalProtect

Palo Alto Networks GlobalProtect™ se présente sous la forme d'un client installé sur le poste et qui établit automatiquement une connexion sécurisée IPsec/VPN SSL vers le firewall nouvelle génération le plus proche. La plupart des applications Web peuvent également être accédées en clientless. De cette manière, tous les accès des utilisateurs distants bénéficient d'une visibilité et d'un contrôle complets de tous leur trafic réseau, applications, ports et protocoles.

L'App GlobalProtect fonctionne sur des devices mobiles

GlobalProtect Etablit une connexion sécurisée VPN SSL/Ipsec « always-on » vers le firewall nouvelle génération

Les utilisateurs ont un accès sécurisé direct aux données sensibles dans le cloud et le data center



Le client GlobalProtect est natif de la solution Firewall nouvelle génération. Lorsqu'il est utilisé sous forme de souscription rattachée au firewall, il permet d'être utilisé pour n'importe quel device, y compris mobile de type IOS, Android ou Linux. La souscription GlobalProtect permet également de contôler les accès aux ressources d'un utilisateur distant en fonction de l'état de configuration et de sécurisation du poste grâce à une vérification du profil (HIP).

GlobalProtect : Avantages et cas d'usage

VPN Accès distant

- Accès sécurisé aux applications internes et cloud

Prévention avancée contre les menaces

- Sécurise le flux Internet
- Bloque les menaces vers les endpoints
- Protège contre le phishing et le vol d'identifiants

Filtrage URL

- Applique les politiques de filtrage
- Filtre les accès aux domaines malveillants
- Prévient l'utilisation d'outils d'évasion et de contournement
- Contrôle les accès et applique les règles pour les applications SaaS tout en bloquant les apps non autorisées

BYOD

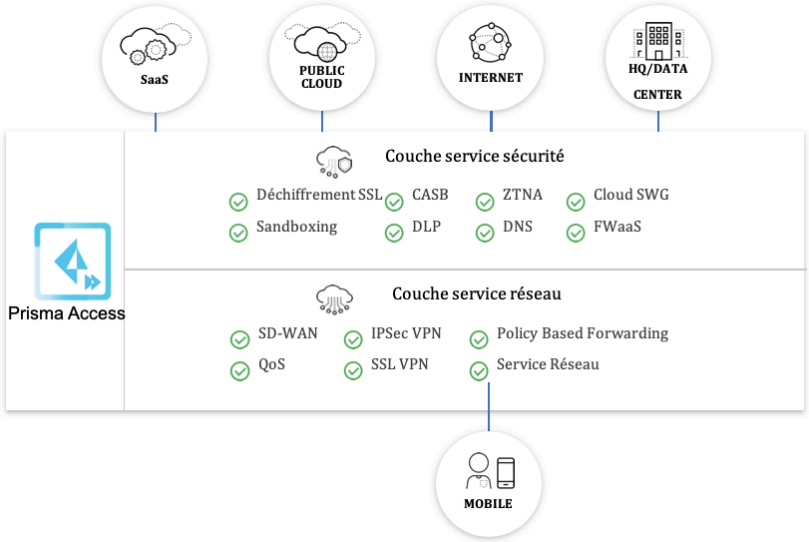
- Support des apps VPN pour la confidentialité des users
- Permet un accès sécurisé sans client pour les partenaires, clients, contractants
- Supporte l'identification automatique des devices non gérés
- Supporte les mécanismes d'authentification sur mesure pour les devices gérés et non gérés

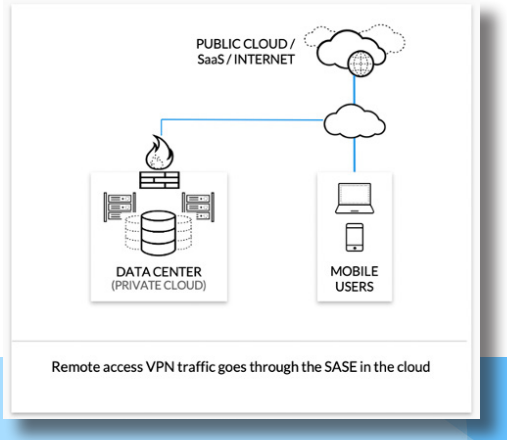
Implémentation Zéro Trust

- Fournit une identification fiable de l'utilisateur
- Fournit un profil d'utilisateur immédiat et précis pour la visibilité et l'application de règles
- Applique une authentification multi-facteurs pour les ressources sensibles

Prisma Access (SASE)

Prisma Access est une offre cloud de « Firewall-as-a-service » qui offre toutes les fonctions et toutes les souscriptions du firewall nouvelle génération Palo Alto Networks, géré de manière centralisée et unifié avec les firewalls physiques si le client en possède. La disponibilité et la montée en charge du service sont gérées et garanties par Palo Alto Networks. Une connexion sécurisée « Always-on » se fait grâce au client GlobalProtect disponible sur **Windows, MacOs, Linux, Android et iOS.**





Prisma Access permet un accès sécurisé à toutes les ressources, qu'elles soient internes, cloud ou en SaaS et ce quel que soit l'emplacement de l'utilisateur. La fonction de filtrage URL remplace le proxy. Les fonctions de sandboxing sont natives.

Tous les mécanismes d'authentification sécurisés sont implémentables. Et la connexion se fait automatiquement vers le point de collecte le plus proche où que soit l'utilisateur dans le monde sans avoir à passer par le site central.