GLOBALPROTECT

Prévenir les violations et sécuriser la main-d'œuvre mobile

GlobalProtect étend la protection offerte par la plateforme de sécurité nouvelle génération de Palo Alto Networks aux membres de votre main-d'œuvre mobile et ce, où qu'ils aillent.

Scénarios d'utilisation et avantages

VPN et accès à distance

- Assure un accès sécurisé aux applications de l'entreprise internes et à celles basées dans le cloud

Prévention contre les menaces avancées

- Sécurisation du trafic Internet
- Blocage des menaces avant le terminal
- Protection contre le phishing et le vol d'informations d'identification

Filtrage des URL

- Application de politiques d'utilisation acceptables
- Filtrage des accès aux domaines malveillants et aux contenus pour adultes
- Blocage des outils d'évasion et d'évitement

Sécurisation de l'accès aux applications SaaS

- Contrôle de l'accès et application des politiques pour les applications SaaS tout en bloquant les applications non approuvées

BYOD (apportez votre propre appareil)

- Prend en charge le VPN par application pour protéger la confidentialité des utilisateurs
- Offre un accès sécurisé sans client aux partenaires, aux associés et aux sous-traitants

Renforcement de la segmentation réseau interne

- Identification fiable des utilisateurs
- Informations précises sur l'hôte, disponibles immédiatement pour plus de visibilité et une meilleure application des stratégies
- Application de l'authentification multifacteurs renforcée pour l'accès aux ressources sensibles

Dans la mesure où les utilisateurs et les applications sortent désormais du périmètre réseau traditionnel, le cadre à sécuriser est de plus en plus étendu. Les équipes chargées de la sécurité ont des difficultés à avoir une bonne vision du trafic réseau et à faire appliquer les politiques de sécurité pour bloquer les menaces. Les technologies traditionnelles utilisées pour protéger les terminaux mobiles comme les logiciels antivirus des terminaux hôtes et les VPN d'accès à distance, sont incapables de bloquer les techniques avancées qu'emploient aujourd'hui les attaquants plus sophistiqués.

Le client de sécurité réseau Palo Alto Networks® GlobalProtect™ permet aux organisations de protéger leur main-d'œuvre mobile en étendant la plateforme de sécurité nouvelle génération à l'ensemble des utilisateurs, quel que soit l'endroit où ils se trouvent. Il sécurise le trafic en appliquant les capacités de la plateforme à comprendre l'utilisation qui est faite des applications, à associer le trafic aux utilisateurs et aux périphériques, et à appliquer les politiques de sécurité avec les technologies nouvelle génération.

Extension en externe de la protection de la plateforme

GlobalProtect protège la main-d'œuvre mobile en inspectant l'ensemble du trafic à l'aide des pare-feu nouvelle génération de l'organisation. Ceux-ci sont déployés sous la forme de passerelles Internet au niveau du périmètre dans la DMZ ou dans le cloud. Les ordinateurs portables, les smartphones et les tablettes dotés de l'application GlobalProtect bénéficient automatiquement d'une connexion VPN SSL/IPsec sécurisée au pare-feu nouvelle génération. Les performances sont optimales quel que soit le lieu, et l'organisation dispose d'une visibilité complète du trafic réseau pour les applications, et sur les différents ports et protocoles. En supprimant les angles morts dans le trafic de la main-d'œuvre mobile, l'organisation bénéficie d'une bonne vision des applications.

Protection du réseau en interne

Seule une partie des utilisateurs a besoin d'accéder à l'intégralité du réseau. Les équipes chargées de la sécurité adoptent la segmentation réseau pour partitionner leur réseau et appliquer des contrôles d'accès précis aux ressources internes. GlobalProtect fournit des identifications ultrarapides et des plus fiables à la plateforme. Les organisations peuvent ainsi élaborer des politiques précises autorisant ou limitant l'accès en fonction des besoins métier. De plus, GlobalProtect fournit des informations sur l'hôte qui établissent les critères des périphériques associés aux politiques de sécurité. Ces mesures permettent aux organisations de prendre les mesures préventives nécessaires pour sécuriser leur réseau interne adopter des contrôles réseau de type Confiance zéro et réduire la surface d'attaque.

Dans le cadre d'un tel déploiement de GlobalProtect, les passerelles réseau internes peuvent être configurées avec ou sans tunnel VPN.

Inspection du trafic et application des politiques de sécurité

GlobalProtect permet aux équipes de sécurité d'élaborer des politiques dont l'application est homogène, que l'utilisateur soit interne ou externe. Les équipes chargées de la sécurité peuvent appliquer toutes les fonctionnalités de prévention des cyberattaques de la plateforme, notamment :

- **Technologie App-ID™ :** identifie le trafic applicatif indépendamment du numéro de port, et permet aux organisations d'élaborer des politiques pour gérer l'utilisation des applications en fonction des utilisateurs et des appareils.
- **Technologie User-ID™ :** identifie les utilisateurs et appartenances à des groupes pour gagner en visibilité et appliquer des politiques de sécurité réseau basées sur les rôles.
- **Décryptage :** inspecte et contrôle les applications chiffrées avec le trafic SSL/TLS/SSH. Bloque les menaces au sein du trafic chiffré.
- **Service cloud d'analyse des menaces WildFire™ :** automatise l'analyse des contenus afin d'identifier les nouveaux logiciels malveillants, jusque-là inconnus et très ciblés, d'après leur comportement. Elle génère, par ailleurs, des renseignements sur les menaces pour pouvoir arrêter ces dernières quasiment en temps réel.
- **Prévention des menaces pour systèmes IPS et antivirus :** la prévention des intrusions bloque les failles réseau ciblant les systèmes d'exploitation et les applications vulnérables, les attaques par refus de service et les attaques par analyse des ports. Les profils antivirus empêchent les logiciels malveillants et les logiciels espions d'atteindre les terminaux à l'aide d'un moteur basé sur le flux.
- **Filtrage des URL avec PAN-DB :** PAN-DB classe les URL en fonction de leur contenu au niveau du domaine, du fichier ou de la page, et reçoit les mises à jour de WildFire de sorte que les catégorisations évoluent en même temps que les contenus Web.
- **Blocage des fichiers :** arrête le transfert des fichiers dangereux et non demandés tout en surveillant de façon poussée les fichiers autorisés à l'aide de WildFire.
- **Filtrage des données :** ce filtrage permet aux administrateurs de mettre en œuvre des politiques bloquant les mouvements de données non autorisés comme le transfert d'informations client ou d'autres contenus confidentiels.

Conditions d'hôte personnalisées (par exemple, identification des utilisateurs et des appareils)

Authentification utilisateur

GlobalProtect prend en charge toutes les méthodes d'authentification PAN-OS® existantes, y compris Kerberos, RADIUS, LDAP, SAML 2.0, les certificats clients et une base de données utilisateur locale. Dès que GlobalProtect authentifie l'utilisateur, il fournit instantanément au pare-feu nouvelle génération les informations de mappage d'adresses IP-utilisateur servant pour User-ID.

Options d'authentification forte

GlobalProtect prend en charge différentes méthodes d'authentification tierces à plusieurs facteurs, notamment les jetons à usage unique, les certificats et les cartes à puce via l'intégration RADIUS.

Ces options aident les organisations à renforcer la preuve de l'identité pour accéder au data center interne ou aux applications SaaS.

GlobalProtect simplifie encore plus l'utilisation et le déploiement d'une authentification forte :

- **Authentification par cookie :** après l'authentification, une organisation peut utiliser un cookie chiffré pour les accès suivants à un portail ou à une passerelle, pour toute la durée de vie du cookie en question.
- **Prise en charge simplifiée du protocole d'enregistrement de certificat :** GlobalProtect peut automatiser l'interaction avec une infrastructure à clé publique (PKI) d'entreprise pour gérer, émettre et distribuer des certificats aux clients GlobalProtect.

Profil d'informations sur l'hôte

GlobalProtect examine le terminal pour obtenir un inventaire de sa configuration, puis élabore un profil qui est partagé avec le pare-feu nouvelle génération. Le pare-feu utilise ce profil pour appliquer des politiques applicatives qui autorisent l'accès uniquement quand le terminal est correctement configuré et sécurisé. Ces principes favorisent la mise en conformité avec les politiques qui régissent les droits d'accès dont dispose un utilisateur avec un appareil donné.

Les politiques HIP peuvent s'appuyer sur différents attributs, notamment :

- Niveau de correctif (système d'exploitation et application)
- Version et état des systèmes hôtes de lutte contre les logiciels malveillants
- Version et état des pare-feu hôtes
- Configuration du chiffrage de disque
- Configuration du produit de sauvegarde des données
- Conditions d'hôte personnalisées (par exemple, entrées de registre, logiciels en cours d'exécution)

Contrôle de l'accès aux applications et données

Les équipes chargées de la sécurité peuvent établir des politiques en fonction des informations relatives aux applications, aux utilisateurs, au contenu et à l'hôte afin de maintenir un contrôle granulaire des accès à une application donnée. Ces politiques peuvent être associées à des utilisateurs ou à des groupes spécifiques définis dans un répertoire pour que les organisations puissent fournir des niveaux d'accès adaptés aux besoins métier. L'équipe de sécurité peut établir d'autres stratégies de sécurité avec authentification multifacteurs afin d'offrir d'autres garanties d'identification avant tout accès aux ressources et aux applications particulièrement sensibles.

BYOD sécurisé et activé

Les effets des politiques de BYOD modifient le nombre de permutations de cas pratiques dont doivent tenir compte les équipes de sécurité. Il est nécessaire de permettre l'accès aux applications à un plus grand nombre d'employés et de sous-traitants sur une large palette d'appareils mobiles.

L'intégration des solutions de gestion des périphériques mobiles, comme AirWatch® et MobileIron®, aident les organisations à déployer GlobalProtect et ajoutent d'autres mesures de sécurité grâce à l'échange d'informations et à la configuration des hôtes. Lorsqu'elles sont utilisées avec GlobalProtect, l'organisation peut assurer la visibilité et l'application des stratégies de sécurité application par application, tout en maintenant la séparation des données personnelles, afin de répondre aux attentes des utilisateurs dans le cadre des scénarios BYOD.

GlobalProtect prend en charge le VPN SSL sans client pour un accès sécurisé aux applications du data center et au cloud pour les appareils non gérés. Cette approche est simple et sure, car elle permet l'accès à certaines applications via une interface Web, sans que l'utilisateur n'ait à installer de client ni à configurer de tunnel.

L'architecture a toute son importance

L'architecture flexible de GlobalProtect offre de nombreuses possibilités qui permettent aux organisations de résoudre un grand nombre de problématiques de sécurité. Au niveau le plus élémentaire, les organisations peuvent utiliser GlobalProtect à la place des passerelles VPN traditionnelles. Elles s'affranchissent ainsi de la complexité liée à la gestion d'une passerelle VPN tierce autonome.

Grâce à des options de sélection de passerelles et de connexion manuelles, les organisations peuvent adapter la configuration aux besoins métier.

Dans un déploiement plus complet visant à sécuriser le trafic, il est possible de déployer GlobalProtect avec une connexion VPN toujours active à l'aide d'un tunnélisation complète. Ainsi, la protection est toujours présente et transparente pour l'utilisateur.

Passerelles basées dans le cloud

Au fur et à mesure que les collaborateurs se déplacent, des changements interviennent au niveau de la charge de trafic. Ce point est tout particulièrement vrai si l'on considère le mode d'évolution des entreprises, que ce soit sur une base temporaire (comme une catastrophe naturelle dans une région) ou permanente (comme la pénétration de nouveaux marchés).

Le service cloud GlobalProtect est une option de cogestion permettant de déployer la couverture dans les lieux où l'organisation en a besoin, à l'aide de vos stratégies de sécurité. Il peut être utilisé avec les pare-feu existants, votre architecture étant ainsi capable de s'adapter à l'évolution des conditions.

Le service cloud GlobalProtect prend en charge la mise à l'échelle automatique, qui affecte de nouveaux pare-feu de façon dynamique en fonction de la charge et de la demande dans chaque région.

Conclusion

Les protections assurées par la plateforme de sécurité nouvelle génération de Palo Alto Networks jouent un rôle majeur dans la prévention des violations. Utilisez GlobalProtect pour étendre la protection de la plateforme aux utilisateurs, quel que soit l'endroit où ils se trouvent. Grâce à GlobalProtect les organisations peuvent appliquer leur politique de sécurité de façon uniforme et ainsi maintenir leur protection contre les cyberattaques même lorsque les utilisateurs quittent le bureau.

Fonctionnalités de GlobalProtect

Catégorie	Caractéristiques techniques
Connexion VPN	IPsec
	SSL
	VPN sans client
	VPN par application sur Android™, iOS, Windows® 10
Sélection de la passerelle	Sélection automatique
	Sélection manuelle
	Sélection de la passerelle externe en fonction de l'emplacement de la source
	Sélection de la passerelle interne en fonction de l'IP de la source
Méthodes de connexion	Ouverture de session utilisateur (toujours activée)
	À la demande
	Pré-ouverture de session (toujours activée)
	Pré-ouverture de session, puis à la demande
Mode de connexion	Mode interne
	Mode externe
Protocoles de couche 3	IPv4
	IPv6
Authentification unique	Authentification unique (fournisseurs d'informations d'identification Windows)
	Authentification unique Kerberos

Catégorie	Caractéristiques techniques
Segmentation de tunnel	Avec routes
	Sans routes
Méthodes d'authentification	SAML 2.0
	LDAP
	Certificats du client
	Kerberos
	RADIUS
	Authentification à deux facteurs
Rapports de profil d'informations sur l'hôte, application de la stratégie et notifications	Gestion des correctifs
	Protection anti-logiciel espion sur l'hôte
	Protection antivirus sur l'hôte
	Pare-feu sur l'hôte
	Cryptage de disque
	Sauvegarde de disque
	Prévention des pertes de données
	Conditions de profil d'informations sur l'hôte personnalisées (par exemple, entrées de registre, logiciels en cours d'exécution)
Authentification multifacteurs	Authentification avancée pour l'accès aux ressources sensibles
Autres fonctionnalités	ID utilisateur
	Basculement VPN IPsec vers SSL
	Application de la connexion GlobalProtect pour l'accès au réseau
	Gestion des certificats utilisateur automatique basée sur SCEP
	Exécution de scripts avant et après les sessions
	Personnalisation dynamique de l'application GlobalProtect
	Configuration de l'application en fonction des utilisateurs, des groupes et/ou des systèmes d'exploitation
	Détection interne/externe automatique
	Mise à niveau manuelle/automatique de l'application GlobalProtect
	Sélection des certificats avec OID
	Blocage de tout accès par des appareils inconnus ou volés
	Prise en charge des cartes à puce pour la connexion/déconnexion
	Distribution transparente des autorités de certification racine de confiance pour le décryptage SSL
	Désactivation de l'accès direct au réseau local
	Pages d'accueil et d'aide personnalisables
	Connexion RDP à un client distant

Catégorie	Caractéristiques techniques
Intégration MDM/EMM	AirWatch
	MobileIron
Outils de gestion et API	Plateforme de sécurité nouvelle génération Palo Alto Networks, y compris sous forme matérielle (PA-7000 Series, PA-3000 Series et PA-200) et virtuelle (VM-Series)
	Microsoft InTune®
	Service cloud GlobalProtect
Plateformes prises en charge par GlobalProtect	Microsoft® Windows et Windows UWP
	Apple® Mac® OS X®
	Apple iOS
	Système d'exploitation Google® Chrome®
	Système d'exploitationAndroid®
	Linux® pris en charge par le biais d'un client StrongSwan et VPNC tiers
Authentification étendue IPsec	Client IPSec Apple iOS
	Client IPSec Android
Traduction de l'application GlobalProtect	Anglais
	Espagnol
	Allemand
	Français
	Japonais
	Chinois

3000 Tannery Way
Santa Clara, CA 95054, États-Unis

Accueil téléphonique : +1 408 753 4000
Service commercial : +1 866 320 4788
Assistance : +1 866 898 9087

www.paloaltonetworks.com

globalprotect-ds-082817