Vue d'ensemble du pare-feu nouvelle génération

L'évolution du comportement des applications et des modèles d'utilisation ont peu à peu érodé la protection qu'offraient les pare-feu traditionnels. Les utilisateurs ont accès à n'importe quelle application, depuis n'importe quel endroit, et de nombreuses fois pour effectuer leur travail. De nombreuses applications utilisent des ports non standard, sautent des ports ou utilisent un chiffrement pour simplifier et rationaliser l'accès des utilisateurs et contourner le pare-feu. Les cybercriminels profitent pleinement de cette utilisation sans entrave des applications pour répandre une nouvelle classe de logiciels malveillants modernes et très ciblés. Il en résulte que le pare-feu traditionnel, avec son filtrage sur le port et le protocole, ne peut plus identifier et contrôler les applications et les menaces modernes franchissant le réseau.

Les tentatives pour permettre le contrôle de l'utilisation des applications et pour protéger les actifs numériques pour tous les utilisateurs ont générés des doublons de politiques de sécurité locale et distante. Cette approche introduit des incohérences de stratégie et ne résout pas les problèmes de visibilité et de contrôle en raison d'une classification inexacte ou incomplète du trafic, d'une gestion complexe et de multiples processus d'analyse générant des temps d'attente. La restauration de la visibilité et du contrôle requiert une toute nouvelle approche, de la base jusqu'à l'activation d'applications sécurisées qui peut uniquement être fournie par un pare-feu nouvelle génération.

Principales fonctions du pare-feu nouvelle génération :

- Identifier des applications, et non des ports. Identification de l'application et de ses fonctionnalités, indépendamment du protocole, du chiffrement ou de la technique d'évasion et utilisation de l'identité en tant que base pour toutes les politiques de sécurité.
- Identifier des utilisateurs, et non des adresses IP. Utilisation des informations de groupes ou d'utilisateurs stockées dans les annuaires d'entreprise pour la visibilité, la création de stratégies, la génération de rapports et l'investigation détaillée — quel que soit l'endroit où se trouve l'utilisateur.
- Bloquer des menaces en temps réel. Protection contre le cycle de vie complet d'une attaque, notamment les applications dangereuses, les vulnérabilités, les logiciels malveillants, les URL à haut risque et un large éventail de contenus et de fichiers malveillants.
- Simplifier la gestion des stratégies. Utilisation sûre et sécurisée des applications à l'aide d'outils graphiques et d'un éditeur de stratégies unifié.
- Activer un périmètre logique. Sécurisation de tous les utilisateurs, y compris des utilisateurs en déplacement ou en télétravail, avec un niveau de sécurité cohérent qui s'étend du périmètre physique au périmètre logique.
- Fournir un débit multi-gigabits. Combinaison de logiciels et de matériel créée dans le but d'offrir des performances à faible latence et à haut débit avec tous les services activés.

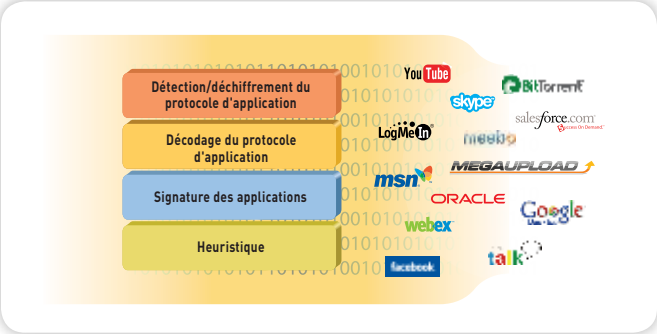
Les pare-feu nouvelle génération de Palo Alto Networks offrent une visibilité et un contrôle sans précédent sur les applications, les utilisateurs et le contenu, à l'aide de trois technologies d'identification uniques : App-ID™, User-ID et Content-ID. Ces technologies d'identification, qui équipent chaque pare-feu Palo Alto Networks, permettent aux entreprises d'activer une utilisation des applications de manière sûre et sécurisée, tout en réduisant considérablement leur coût total de possession via un regroupement des périphériques.

paloalto NETWORKS
the network security company™

App-ID : Reconnaissance de toutes les applications, de tous les ports, tout le temps

La reconnaissance précise du trafic est au cœur de tout pare-feu, le résultat constituant la base de la stratégie de sécurité. Les pare-feu traditionnels classent le trafic par port et protocole, ce qui fut un temps un mécanisme satisfaisant de protection du réseau. Aujourd'hui, les applications abusent facilement des pare-feu fondés sur les ports à l'aide des techniques suivantes : saut de ports, utilisation de SSL et de SSH, attaque furtive sur le port 80 ou utilisation de ports non standard. App-ID résout le problème de visibilité réduite qui affecte la classification du trafic et handicape les pare-feu traditionnels. Grâce à l'application de plusieurs mécanismes de reconnaissance du trafic, le pare-feu détermine l'identité exacte des applications qui transitent par le réseau.

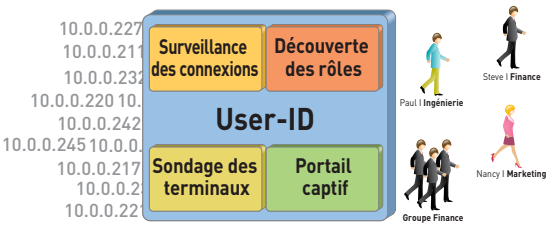
Contrairement aux solutions complémentaires qui reposent uniquement sur des signatures de type IPS, implémentées après une classification fondée sur les ports, chaque App-ID utilise automatiquement jusqu'à quatre mécanismes de classification de trafic différents pour identifier l'application. App-ID surveille continuellement l'état de l'application, en re-classifiant le trafic et en identifiant les différentes fonctions qui sont utilisées.
La stratégie de sécurité détermine comment traiter l'application : bloquer, autoriser ou activer de manière sécurisée (rechercher et bloquer les menaces incorporées, surveiller les transferts de fichiers et les mots-clés non autorisés, ou le contrôle du débit du trafic par le biais de la Qualité de Service).



User–ID : Utilisation des applications selon les utilisateurs et les groupes

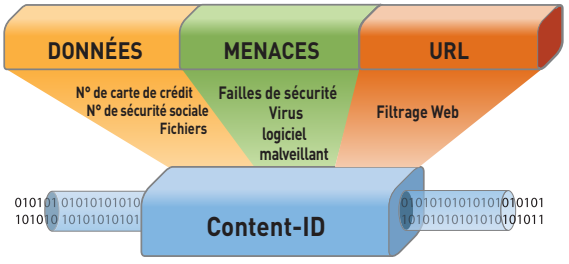
Jusqu'ici, les stratégies de sécurité étaient appliquées sur la base d'adresses IP, mais la nature de plus en plus dynamique des utilisateurs et de l'informatique signifie que les adresses IP seules ne constituent plus un mécanisme suffisant de surveillance et de contrôle de l'activité des utilisateurs. User-ID permet aux entreprises d'étendre les stratégies d'activation des applications sur la base des utilisateurs ou groupes parmi les utilisateurs Microsoft Windows, Apple Mac OS X, Apple iOS et Linux.

Les informations utilisateur peuvent être obtenues à partir des répertoires d'entreprise (Microsoft Active Directory, eDirectory et Open LDAP) et des offres de services de terminal (Citrix et Microsoft Terminal Services) tandis qu'une intégration avec Microsoft Exchange, un portail captif et une API XML permet aux entreprises d'étendre la stratégie aux utilisateurs non Microsoft comme Apple Mac OS X, Apple iOS et UNIX.



Content-ID : Protection du trafic autorisé

De nombreuses applications récentes proposent de nouvelles fonctionnalités importantes mais elles sont également utilisées comme un outil de transmission de logiciels malveillants et de menaces modernes. Conjointement à App-ID, Content-ID offre aux administrateurs une solution à deux têtes pour protéger leur réseau. Suite à l'utilisation d'App-ID pour identifier et bloquer les applications indésirables, les administrateurs peuvent activer en toute sécurité les applications permises en bloquant la propagation des failles de vulnérabilité, des logiciels malveillants modernes, des virus, des botnets et autres logiciels malveillants. Cette protection se fait à travers du réseau indépendamment du port, du protocole ou de la méthode d'évasion. Aux éléments de contrôle qu'offre Content-ID, vient s'ajouter une base de données exhaustive d'URL pour contrôler la navigation sur le Web et des fonctions de filtrage des données.



Utilisation sécurisée des applications

L'intégration transparente d'App-ID, User-ID et Content-ID permet aux entreprises d'établir des stratégies cohérentes d'utilisation des applications, des fonctions de l'application dans de nombreux cas, qui va au-delà d'une autorisation ou d'un refus élémentaire. Grâce à Global Protect, les stratégies qui protègent les utilisateurs dans le réseau de l'entreprise sont étendues à tous les utilisateurs, où qu'ils soient, établissant de fait un périmètre logique pour les utilisateurs nomades.

Les stratégies d'utilisation sécurisée commencent par l'identification de l'application, déterminée par App-ID, qui est ensuite associée à l'utilisateur par User-ID. Le contenu du trafic est alors analysé pour y détecter de possibles menaces, fichiers, mots clés et activités Web par Content-ID. Ces résultats sont présentés dans ACC (Application Command Center) où l'administrateur peut voir, en temps réel, l'activité du réseau. Ensuite, les informations visualisées dans ACC sur les applications, les utilisateurs et le contenu peuvent être converties en stratégies de sécurité appropriées. Il est alors possible de bloquer les applications indésirables tout en autorisant et en activant les autres de manière sécurisée. Enfin, toute analyse détaillée, création de rapport ou investigation peut être réalisée en se basant sur les applications, les utilisateurs et le contenu.

ACC (Application Command Center) : Savoir, c'est pouvoir

Le centre de commandement des applications ACC (Application Command Center) récapitule de manière graphique la base de données du journal pour mettre en évidence les applications franchissant le réseau, leurs utilisateurs et leur impact potentiel sur la sécurité. ACC est dynamiquement mis à jour, en utilisant la reconnaissance continue du trafic assurée par App-ID ; en cas de changement de port ou de comportement par une application, App-ID continue à suivre le trafic, en affichant les résultats dans ACC. D'un simple clic, vous pouvez facilement obtenir une description des applications nouvelles ou inconnues qui apparaissent dans ACC, ainsi que leurs principales fonctionnalités, leurs caractéristiques comportementales, et savoir qui les utilise. Une visibilité supplémentaire des catégories d'URL, des menaces et des données offre une analyse complète et globale de l'activité du réseau. Avec ACC, un administrateur peut très facilement comprendre le trafic qui traverse le réseau et se servir ensuite de ces informations pour créer des stratégies de sécurité mieux fondées.

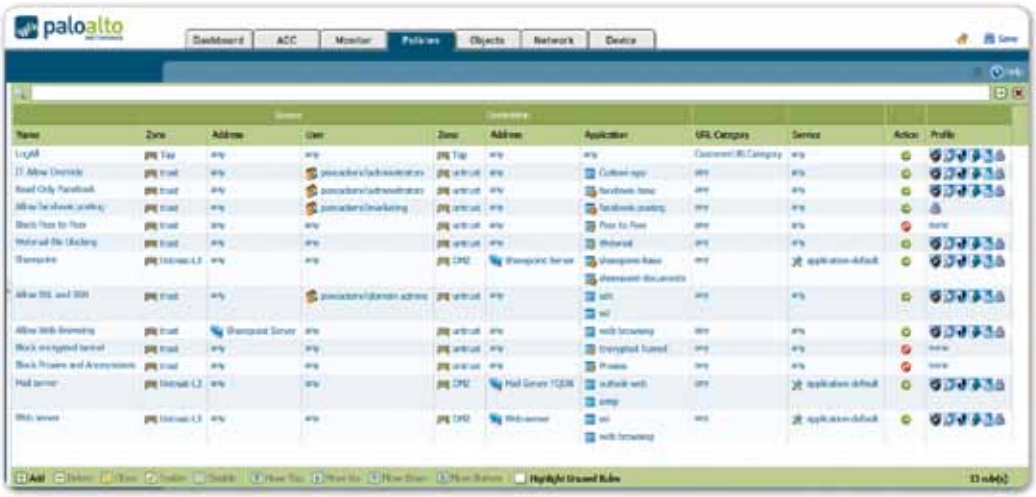
Éditeur de stratégies : Conversion d'informations en stratégies d'utilisation sécurisée

Le fait de savoir quelles applications traversent le réseau, qui en fait usage et les risques potentiels pour la sécurité, permet aux administrateurs de déployer des stratégies d'activation fondées sur les applications, leurs fonctions et les ports, de manière systématique et contrôlée. Les réponses stratégiques peuvent aller d'ouvert (autoriser) à fermé (refuser) en passant par modéré (autoriser certaines applications ou fonctions, puis analyser, ou mettre en forme, planifier, etc.). Quelques exemples :

- Protéger une base de données Oracle en limitant l'accès aux utilisateurs du groupe Finance, en forçant le trafic à transiter par les ports standard et en inspectant le trafic pour y rechercher des failles dans les applications.
- Autoriser uniquement le département Informatique à utiliser un groupe donné d'applications de gestion à distance (par exemple, SSH, RDP, Telnet) via leurs ports standard.
- Définir et appliquer une stratégie d'entreprise qui permet l'utilisation et l'inspection de messageries Web et instantanées mais bloquer leurs fonctions respectives de transfert de fichiers.
- Limiter l'utilisation de l'administration Microsoft SharePoint à la seule équipe d'administration, et autoriser l'accès à des documents Microsoft SharePoint à tous les autres utilisateurs.
- Déployer des stratégies de filtrage web qui autorisent et analysent le trafic vers des sites Web associés aux activités de l'entreprise. Ces stratégies bloquent l'accès aux sites n'ayant aucun lien manifeste avec l'activité professionnelle de d'entreprise. Les pages de blocage personnalisés peuvent guider l'accès aux autres sites.

Visibilité des applications

Affichez la cartographie des applications dans un format clair er lisible. Ajoutez et supprimez des filtres pour en savoir plus sur l'application, ses fonctions et leurs utilisateurs.



Éditeur de stratégies unifié
Une interface simple permet de créer et déployer rapidement des stratégies qui contrôlent les applications, les utilisateurs et le contenu.

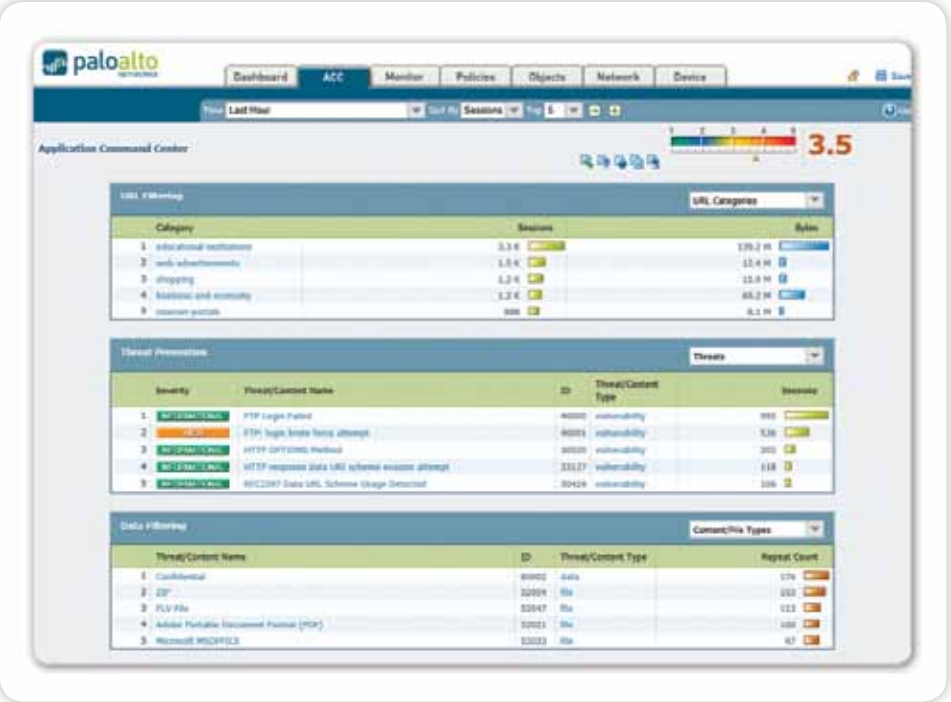
- Mettre en œuvre des stratégies de Qualité de Service autorisant l'utilisation des sites Web et applications multimédia nécessitant un haut débit tout en limitant l'impact sur les applications VoIP (voix sur IP).
- Déchiffrer le trafic SSL vers les sites de messagerie et de réseaux sociaux et rechercher les logiciels malveillants.
- Autoriser les téléchargements de fichiers exécutables à partir de sites Web inconnus uniquement après reconnaissance de l'utilisateur pour éviter les téléchargements automatiques déclenchés par l'activation de failles 0-Day.
- Refuser tout trafic en provenance de pays spécifiques ou bloquer des applications indésirables telles que le partage de fichier P2P ou les services de type proxy et circumventor.

L'intégration étroite du contrôle d'application, basé sur les utilisateurs et les groupes, ainsi que la capacité d'analyser le trafic autorisé à rechercher des menaces de tous types, permet aux entreprises de réduire considérablement le nombre de stratégies qu'ils déploient en plus des ajouts, déplacements et changements d'employés susceptibles de se produire quotidiennement.

Editeur de stratégies : Protection des applications utilisées

L'utilisation sécurisée des applications implique d'autoriser l'accès à ces applications et d'y appliquer des stratégies de prévention de menaces spécifiques et de blocage de fichiers, de données ou d'URL. Chacun des éléments inclus dans Content-ID peut être configuré selon l'application.

- **Système de prévention des intrusions :** La protection contre les vulnérabilités implique un riche ensemble de fonctionnalités de prévention des intrusions (IPS) capables d'empêcher les failles de sécurité au niveau du réseau et de l'application, les vulnérabilités de la couche applicative, les dépassements de mémoire tampon, les attaques par refus de service et les attaques par analyse des ports.
- **Antivirus réseau : La protection par antivirus sur flux bloque des millions de logiciels malveillants, y compris les virus PDF et les programmes malveillants dissimulés dans les fichiers compressés ou dans le trafic Web (HTTP/HTTPS compressé). Le déchiffrement SSL basé sur une stratégie permet aux entreprises de se protéger contre les logiciels malveillants qui circulent via les applications chiffrées en SSL.**
- **Filtrage des URL :** Une base de données de filtrage des URL, totalement intégrée et personnalisable, permet aux administrateurs d'appliquer des stratégies de navigation Web extrêmement précises, en complément des stratégies de contrôle et de visibilité des applications et de la protection de l'entreprise contre un spectre étendu de risques en termes de loi, de réglementation et de productivité.
- **Filtrage de fichiers et de données :** Des fonctionnalités de filtrage de données permettent aux administrateurs de mettre en œuvre des stratégies permettant de réduire les risques liés à un transfert de fichiers et de données. Les transferts et les téléchargements peuvent être contrôlés en fonction du contenu des fichiers (par opposition au seul examen de l'extension de fichier), afin de déterminer leur autorisation ou non. Les fichiers exécutables, qui se trouvent habituellement dans les téléchargements automatiques, peuvent être bloqués, protégeant par conséquent le réseau contre la propagation de logiciels malveillants non détectés. Enfin, les fonctions de filtrage des données peuvent détecter et contrôler le flux de modèles de données confidentiels (numéros de carte de crédit ou dictionnaire de mots-clés).



Visibilité du contenu et des menaces
Affichez l'activité de transfert de données/fichiers, de menaces et d'URL dans un format clair et facile à lire. Ajoutez et supprimez des filtres pour en savoir plus sur des éléments individuels.

Détection des logiciels malveillants modernes et leur prévention

Les logiciels malveillants ont évolué pour devenir une application réseau extensible qui fournit aux attaquants un accès et un contrôle sans précédent à l'intérieur du réseau ciblé. À mesure que la puissance des logiciels malveillants modernes augmente, il est essentiel que les entreprises soient en mesure de détecter ces menaces immédiatement, avant même que la menace ait défini une signature. Les pare-feu de nouvelle génération de Palo Alto Networks fournissent aux entreprises une approche multi-facettes basée sur l'analyse directe des fichiers exécutables et du trafic réseau afin de protéger leurs réseaux, même avant que les signatures soient disponibles.

- **WildFire™ :** En utilisant une approche de type cloud, WildFire expose des fichiers exécutables malveillants inédits en observant directement leur comportement dans un environnement virtualisé sécurisé. WildFire recherche des actions malveillantes au sein de fichiers exécutables Microsoft Windows tels que la modification de valeurs de registre ou de fichiers du système d'exploitation, la désactivation de mécanismes de sécurité ou l'injection de code dans des processus en cours. Cette analyse directe identifie rapidement et avec précision les logiciels malveillants, même lorsqu'aucun mécanisme de protection n'est disponible. Les résultats sont immédiatement envoyés à l'administrateur pour une réponse appropriée et une signature est automatiquement développée et livrée à tous les clients dans la version successive.

- **Détection comportementale de réseau de zombies :** App-ID classifie l'ensemble du trafic au niveau de l'application, exposant ainsi tout trafic inconnu sur le réseau, ce qui est souvent une indication de l'activité de logiciels malveillants ou autres menaces. Le rapport comportemental de réseau de zombies analyse le comportement du réseau qui est indicatif d'une infection de botnet telle que la visite répétée de sites malveillants, en utilisant l'adressage DNS dynamique, les discussions IRC et autres comportements potentiellement suspects. Les résultats sont affichés sous la forme d'une liste d'hôtes potentiellement infectés qui peuvent être étudiés en tant que membres possibles d'un réseau de zombies.

Surveillance du trafic : Analyse, création de rapports et investigation

Les pratiques recommandées en matière de sécurité stipulent que les administrateurs doivent trouver un point d'équilibre entre la proactivité, apprendre et s'adapter en permanence en vue de la protection des actifs de l'entreprise, et la réactivité, enquêter, analyser et rapporter les incidents concernant la sécurité. ACC et l'éditeur de stratégies peuvent permettre d'appliquer de manière proactive des stratégies d'utilisation des applications, tandis qu'un jeu complet d'outils de surveillance et de reporting fournit aux entreprises les moyens nécessaires pour analyser et créer des rapports sur l'application, les utilisateurs et le contenu transitant par le pare-feu nouvelle génération de Palo Alto Networks.

- **App-Scope :** Complément de l'affichage en temps réel des applications et du contenu fourni par ACC, App-scope procure une vue dynamique et personnalisable de l'activité des applications, du trafic et des menaces au fil du temps.

- **Création de rapports :** Des rapports prédéfinis peuvent être utilisés tels quels, personnalisés ou regroupés dans un seul rapport afin de s'adapter aux exigences particulières. Tous les rapports peuvent être exportés au format CSV ou PDF et exécutés et envoyés par courrier électronique selon une planification.

- **Journalisation :** Un filtrage des journaux en temps réel facilite l'examen rigoureux et rapide de chaque session franchissant le réseau. Les résultats du filtrage des journaux peuvent être exportés vers un fichier CSV ou envoyés à un serveur syslog pour archivage hors connexion ou analyse plus approfondie.

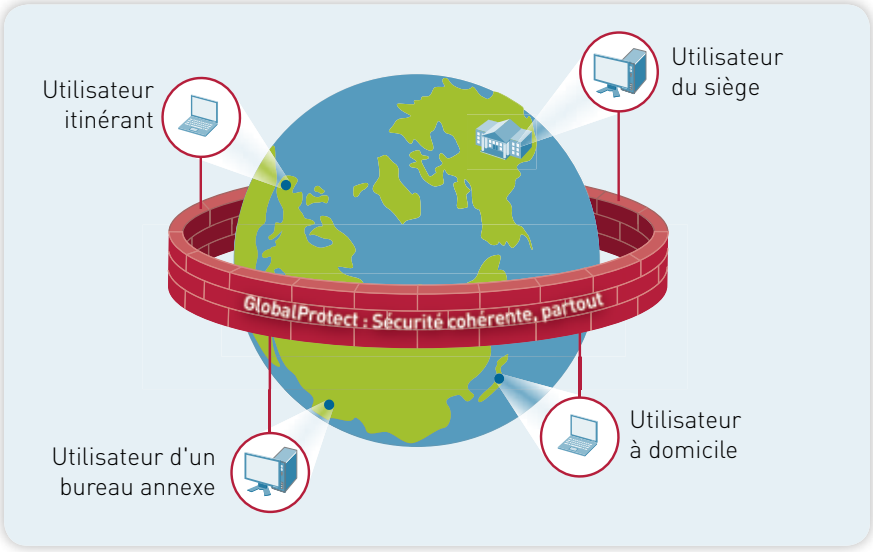
- **Outil de corrélation de trace :** Accélérez les investigations suite aux incidents grâce à une vue centralisée et corrélée de tous les journaux pour le trafic, les menaces, les URL et les applications liés à une session individuelle.

GlobalProtect : Sécurité cohérente, partout

Les applications ne sont pas les seules forces du changement dans l'entreprise. De plus en plus, les utilisateurs finaux s'attendent tout simplement à se connecter et à travailler à partir de n'importe quel endroit avec n'importe quel périphérique de leur choix. En conséquence, les équipes informatiques ont du mal à étendre la sécurité à ces périphériques et lieux qui peuvent être bien au-delà du périmètre traditionnel de l'entreprise. GlobalProtect relève ce défi en étendant des politiques de sécurité cohérentes à tous les utilisateurs indépendamment de leur emplacement et leur périphérique.

Tout d'abord, GlobalProtect assure une connectivité sécurisée pour tous les utilisateurs avec un réseau VPN transparent qui prend en charge un éventail de périphériques, notamment Microsoft Windows, Apple Mac OS X et Apple iOS. Une fois connecté, tout le trafic est classé par le pare-feu, des stratégies d'utilisation sont appliquées, le trafic est analysé, une recherche des menaces est lancée afin de protéger le réseau et l'utilisateur.

En outre, GlobalProtect peut appliquer des contrôles supplémentaires basés sur l'état du périphérique de l'utilisateur final. Par exemple, un utilisateur peut se voir refuser l'accès à certaines applications ou zones sensibles du réseau si le périphérique dispose d'un antivirus périmé ou n'a pas de chiffrement de disque activé. Cela permet au personnel informatique d'activer l'utilisation des applications en toute sécurité à travers une gamme de types de périphériques d'utilisateur final, tout en conservant une approche cohérente de sécurité de nouvelle génération.



GlobalProtect
Mettez en œuvre des stratégies cohérentes d'utilisation sécurisée des applications pour tous les utilisateurs, où qu'ils soient

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054
Téléphone principal : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087
www.paloaltonetworks.com