Fin de vie de la fonctionnalité d'application de la couche IP du client d'itinérance Umbrella

Table des matières

[Introduction](#)

[Aperçu](#)

[Informations supplémentaires](#)

Introduction

Ce document décrit l'annonce de Cisco Umbrella selon laquelle la mise en oeuvre de la couche IP prendra fin le 31 juillet 2022.

Aperçu

L'application de couche IP est une fonctionnalité facultative pour les clients itinérants, disponible avec le proxy intelligent Umbrella pour certains packages Cisco Umbrella.

L'application de la couche IP ne sera plus incluse dans les packages Cisco Umbrella commandés par les clients à partir du 31 août 2021. Pour les clients qui ont déjà commandé un package contenant l'option IP Layer Enforcement (Application de la couche IP), la fonctionnalité continue de fonctionner jusqu'au 31 juillet 2022. Les services côté cloud requis pour l'application de la couche IP seront arrêtés le 31 juillet 2022.

Les packages Cisco Umbrella DNS Essentials et DNS Advantage constituent une solution de sécurité DNS puissante, facile à déployer et à gérer. Ces packages DNS continuent à protéger les abonnés DNS contre les serveurs malveillants pour toutes les connexions (même vers des domaines inconnus et non classés qui se résolvent en une adresse IP malveillante) qui commencent par une requête DNS Umbrella (via l'application de couche DNS).

Les packages Cisco Umbrella Secure Internet Gateway (SIG) incluent une couverture de sécurité encore plus avancée pour tout le trafic (DNS, IP, Web, etc.). SIG inclut une passerelle Web sécurisée (« SWG ») pour analyser tout le trafic sur les ports Web (destinations IP ou de domaine), et un pare-feu fourni dans le cloud (« CDFW ») qui couche sur un pare-feu basé dans le cloud en plus de SWG. Cela améliore l'efficacité de la gamme de solutions de sécurité cloud de Cisco bien au-delà du DNS avec application de la couche IP, et au-delà de l'exigence d'un logiciel de point d'extrémité pour fournir une protection plus efficace que celle du DNS. Nous encourageons tous ceux qui ont besoin d'une couverture plus étendue que DNS à considérer le paquet Umbrella SIG.

Protégez votre pile réseau avec Cisco Umbrella et contactez votre responsable de compte Cisco Umbrella dès aujourd'hui pour en savoir plus sur la solution Cisco Secure Internet Gateway.

Informations supplémentaires

Prise en charge des versions AnyConnect

L'application de couche IP est prise en charge sur AnyConnect version 4.x jusqu'à la date de fin de vie de l'application de couche IP. La version 5.x ne prend pas en charge l'application de couche IP. Le client de marque Cisco Secure Client ne prend pas en charge la mise en application de la couche IP. Les utilisateurs AnyConnect existants doivent continuer à utiliser le client AnyConnect 4.x pour utiliser la fonctionnalité d'application de couche IP jusqu'à la date de fin de vie de l'application de couche IP.

Solutions de rechange Cisco

Cisco Secure Endpoint (anciennement AMP) offre une protection sur les périphériques contre les menaces directes sur IP. Cela inclut la fonctionnalité appelée « DFC » qui évalue les nouvelles connexions pour les nouveaux processus. Cette fonctionnalité devrait évoluer pour remplacer la fonctionnalité IPLE d'Umbrella. Contactez votre gestionnaire de compte pour discuter de l'ajout de Cisco Secure Endpoint à votre CLE.

SIG assure la couverture de tout le trafic Web sur SWG et de tout le trafic Internet public avec Cloud Firewall. Plus de 95 % des blocs IPLE sont du trafic Web couvert par SWG ! (trafic Web sur TCP 443 et 80). Cette fonctionnalité est fournie par SWG et n'est pas alimentée par IPLE.

Afficher la valeur ajoutée d'IPLE pour votre entreprise

Pour calculer les blocs d'application de couche IP actuels pour votre organisation par million de lignes de journal, procédez comme suit :

1. Connectez-vous au tableau de bord Umbrella et ouvrez le rapport de recherche d'activité.
2. Accédez au type de journal « Application de la couche IP » (en passant de « Tous »).
3. Exportez un fichier CSV de 1 000 000 lignes et téléchargez le rapport exporté.
4. Filtrez toutes les lignes qui ne contiennent pas de catégorie « Malware » ou « Botnet ».
    - Exclure le « Trafic de tunnel IP non autorisé ». Cette catégorie correspond au trafic qui atteint le tunnel IPSec et qui n'est pas une liste d'application. Il est automatiquement supprimé de nos services.
    - Notez le port de trafic. Les ports 43 et 80 auraient été entièrement couverts par notre package SIG Essentials.
5. Le nombre total de blocs correspond au nombre de blocs de votre organisation. Comparez cela au nombre total de requêtes DNS dans votre rapport « Total Requests » pour calculer un pourcentage d'efficacité.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.