End-of-Life-Funktion für die Durchsetzung der IP-Schicht des Umbrella Roaming Client

Inhalt

Einleitung

Dieses Dokument beschreibt die Cisco Umbrella-Ankündigung, dass die Durchsetzung der IP-Layer-Richtlinien am 31. Juli 2022 eingestellt wird.

Überblick

Die Durchsetzung der IP-Schicht ist eine optionale Funktion für Roaming-Clients, die Umbrella Intelligent Proxy für ausgewählte Cisco Umbrella-Pakete zur Verfügung stellt.

Die Durchsetzung von IP-Schichten ist nicht mehr Bestandteil der Cisco Umbrella-Pakete, die Kunden ab dem 31. August 2021 bestellen. Für Kunden, die zuvor ein Paket mit der IP Layer Enforcement-Option bestellt hatten, funktioniert die Funktion bis zum 31. Juli 2022. Die Cloud-Services, die für den Betrieb der IP-Layer-Durchsetzung erforderlich sind, wurden am 31. Juli 2022 eingestellt.

Die Umbrella DNS Essentials- und DNS Advantage-Pakete von Cisco bieten eine einfach bereitzustellende und zu verwaltende leistungsstarke DNS-Sicherheitslösung. Diese DNS-Pakete schützen weiterhin DNS-Abonnenten vor bösartigen Servern für alle Verbindungen - auch zu unbekannten, nicht kategorisierten Domänen, die sich zu einer bösartigen IP-Adresse auflösen -, die mit einer Umbrella DNS-Anfrage (durch DNS-Layer-Durchsetzung) beginnen.

Die Cisco Umbrella Secure Internet Gateway (SIG)-Pakete bieten eine noch umfassendere Sicherheitsabdeckung für den gesamten Datenverkehr (DNS, IP, Web usw.). SIG umfasst ein Secure Web Gateway ("SWG") zur Analyse des gesamten Datenverkehrs an Webports (IP- oder Domänenziele) sowie eine Cloud Delivered Firewall ("CDFW"), die zusätzlich zur SWG eine Cloud-basierte Firewall nutzt. Damit erweitert Cisco sein Portfolio an Cloud-Sicherheitsfunktionen weit über DNS mit IP-Layer-Durchsetzung hinaus und geht über die Anforderungen von Endgerätesoftware hinaus, um mehr als nur DNS-Schutz zu bieten. Wir empfehlen allen, die mehr als nur eine DNS-Abdeckung benötigen, das Umbrella SIG-Paket in Betracht zu ziehen.

Schützen Sie Ihren Netzwerk-Stack mit Cisco Umbrella, und wenden Sie sich an Ihren Cisco Umbrella Account Manager, um mehr über die Cisco Secure Internet Gateway-Lösung zu erfahren.

Zusätzliche Informationen

AnyConnect-Versionsunterstützung

Die IP-Layer-Durchsetzung wird von AnyConnect Version 4.x bis zum End-of-Life-Datum der IP-Layer-Durchsetzung unterstützt. Version 5.x unterstützt die Durchsetzung auf IP-Ebene nicht. Der Client mit der Marke Cisco Secure Client bietet keine Unterstützung für die Durchsetzung auf IP-Ebene. Bestehende AnyConnect-Benutzer müssen den AnyConnect 4.x-Client weiterhin verwenden, um bis zum End-of-Life-Datum der IP-Layer-Durchsetzung von der IP-Layer-Durchsetzung zu profitieren.

Cisco Alternativen

Cisco Secure Endpoint (ehemals AMP) bietet geräteseitigen Schutz vor direkten IP-Bedrohungen. Dazu gehört auch die Funktion "DFC", die neue Verbindungen für neue Prozesse evaluiert. Diese Funktion soll erweitert werden, um die Umbrella IPLE-Funktion weiter zu ersetzen. Wenden Sie sich an Ihren Account Manager, um das Hinzufügen von Cisco Secure Endpoint zu Ihrer ELA zu besprechen.

SIG deckt den gesamten Webdatenverkehr der SWG und den gesamten öffentlichen Internetdatenverkehr über die Cloud-Firewall ab. Mehr als 95 % der IPLE-Blöcke sind Web-Datenverkehr, der von der SWG abgedeckt wird! (Webdatenverkehr über TCP 443 und 80). Diese Funktion wird von der SWG bereitgestellt und nicht von IPLE unterstützt.

IPLE-Mehrwert für Ihr Unternehmen anzeigen

So berechnen Sie die aktuellen Durchsetzungsblöcke für die IP-Schicht pro Million Protokollzeilen:

1. Melden Sie sich beim Umbrella Dashboard an, und öffnen Sie den Bericht zur Aktivitätssuche.
2. Navigieren Sie zum Protokolltyp "IP Layer Enforcement" (Erzwingung der IP-Schicht) (statt "Alle").
3. Exportieren Sie einen CSV mit 1.000.000 Zeilen, und laden Sie den exportierten Bericht herunter.
4. Filtern Sie alle Zeilen aus, die keine Kategorie "Malware" oder "Botnet" enthalten.
    - Ausschließen von "Nicht autorisierter IP-Tunnelverkehr". Bei dieser Kategorie handelt es sich um Datenverkehr, der den IPSec-Tunnel erreicht und keine Durchsetzungsliste darstellt. Es wird automatisch aus unseren Services entfernt.
    - Notieren Sie sich den Datenverkehrsport. Die Ports 443 und 80 wären durch unser SIG Essentials-Paket vollständig abgedeckt.
5. Die Gesamtzahl der Blöcke entspricht der Blockanzahl für Ihre Organisation. Vergleichen Sie dies mit der Gesamtzahl der DNS-Anfragen in Ihrem Bericht "Total Requests" (Gesamtanforderungen), um den Wirkungsgrad zu berechnen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.