

Erlaubte IPs und Domänen in Firewalls für ein sicheres Web-Gateway verstehen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[IP-Adressen](#)

[Domänen](#)

Einleitung

In diesem Dokument wird beschrieben, welche IPs und Domänen in den Firewalls des Kunden für Secure Web Gateway (SWG) zugelassen werden können.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf SWG-Bereitstellungen mit einer PAC-Datei oder einem AnyConnect-Client mit SWG-Modul.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Wenn Sie Umbrella's Secure Web Gateway (SWG) bereitstellen, empfiehlt Umbrella, den IP-Bereich der SWG zuzulassen, um sicherzustellen, dass der Datenverkehr durch die Perimeter-Firewalls fließt. Dies gilt auch für alle Webfilter-Appliances, die Kunden zur Verfügung stehen.

IP-Adressen

Cisco Umbrella ist ein elastischer Cloud-Service, dessen IP-Adressraum dynamisch ist und sich ständig verändert. Wenn Sie das Umbrella SWG-Produkt bereitstellen, empfiehlt Umbrella, die folgenden CIDRs auf den Perimeter-Firewalls zuzulassen, um sicherzustellen, dass sie eine Verbindung zum Umbrella SWG-Service herstellen können:

67.215.64.0/19
146.112.0.0/16
151.186.0.0/16
155.190.0.0/16
185.60.84.0/22
204.194.232.0/21
208.67.216.0/21
208.69.32.0/21

Datenverkehrsprofil:

- Protokoll = TCP
- Ports = ausgehend 80 und 443

Domänen

Umbrella empfiehlt außerdem, diese Domänen an der Quelle zu umgehen, um sicherzustellen, dass der gesamte Datenverkehr zugelassen wird:

isrg.trustid.ocsp.identrust.com
*.cisco.com
*.opendns.com
*.umbrella.com
*.okta.com
*.oktacdn.com
*.pingidentity.com
secure.aadcdn.microsoftonline-p.com

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.