Comprendre les adresses IP autorisées dans les pare-feu pour la passerelle Web sécurisée

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Fond](#)

[Adresses IP](#)

[Domaines](#)

Introduction

Ce document décrit les adresses IP et les domaines autorisés dans les pare-feu pour la passerelle Web sécurisée (SWG).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les déploiements SWG avec un fichier PAC ou un client AnyConnect avec un module SWG.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fond

Si vous déployez la passerelle Web sécurisée (SWG) d'Umbrella, Umbrella recommande d'autoriser l'espace IP des SWG pour garantir que le trafic est autorisé à travers leurs pare-feu de périmètre. Cela s'applique également à tous les appareils de filtrage Web dont vous disposez.

Pour plus d'informations, reportez-vous au Guide de l'utilisateur de Cisco Umbrella SIG.

Adresses IP

Cisco Umbrella est un service cloud élastique, dont l'espace IP est dynamique et en constante évolution. Si vous déployez Umbrella SWG, Umbrella recommande d'autoriser ces routeurs CIDR sur leurs pare-feu de périmètre afin de s'assurer qu'ils peuvent se connecter au service Umbrella SWG :

```
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
```

Profil de trafic :

- Protocole = TCP
- Ports = Sortants 80 et 443

Domaines

Umbrella recommande également de contourner ces domaines à la source pour s'assurer que tout le trafic est autorisé :

```
isrg.trustid.ocsp.identrust.com
*.cisco.com
*.opendns.com
```

```
*.umbrella.com
*.okta.com
*.oktacdn.com
*.pingidentity.com
secure.aadcdn.microsoftonline-p.com
```

Pour plus d'informations sur l'accès sécurisé, consultez :

- Aide de Cisco Secure Access - Exigences DNS
- Aide de Cisco Secure Access - Conditions requises pour le service Secure Web Gateway

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.