了解防火墙中允许的安全网络网关的IP

目录

简介

先决条件

- 要求
- 使用的组件

背景

IP 地址

域

简介

本文档介绍安全网络网关(SWG)的防火墙中允许哪些IP和域。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于带有PAC文件的SWG部署或带有SWG模块的AnyConnect客户端。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

如果您要部署Umbrella的安全Web网关(SWG),Umbrella建议允许SWG的IP空间，以确保允许流量通过边界防火墙。这也适用于您拥有的任何网络过滤设备。

有关其他详细信息，请参阅Cisco Umbrella SIG用户指南。

IP 地址

Cisco Umbrella是一种弹性云服务，其IP空间是动态且不断变化的。如果您正在部署Umbrella SWG，Umbrella建议在其周边防火墙上允许这些CIDR，以确保它们可以连接到Umbrella SWG服务：

```
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
```

流量配置文件:

- 协议= TCP
- 端口=出站80和443

域

Umbrella还建议在源位置绕过这些域，以确保允许所有流量：

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

有关安全访问的其他详细信息，请访问：

- 思科安全访问帮助 — DNS要求
- 思科安全访问帮助 — 安全Web网关服务要求

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。