瞭解用於安全Web網關的防火牆中允許的IP和域

目錄

簡介

本檔案將說明在客戶防火牆中可為安全Web閘道(SWG)允許哪些IP和網域。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據使用PAC檔案的SWG部署或使用SWG模組的AnyConnect使用者端。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

如果您要部署Umbrella的安全Web網關(SWG),Umbrella建議允許SWG的IP空間，以確保允許流量穿過其外圍防火牆。這也適用於客戶可以擁有的任何網路過濾裝置。

IP地址

Cisco Umbrella是一項彈性雲服務，其IP空間是動態的，並且不斷變化。如果您正在部署Umbrella SWG產品，Umbrella建議在其外圍防火牆上允許這些CIDR，以確保它們可以連線到Umbrella SWG服務：

```
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
```

流量量變曲線：

- 協定= TCP
- 埠=出站80和443

域

Umbrella還建議在來源處繞過這些網域，以確保允許所有流量：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。