Cisco Umbrella有关基于IP的地理阻止的常见问题

目录

简介

本文档介绍从8月1日起向俄罗斯和白俄罗斯的Cisco Umbrella和OpenDNS客户显示的行为更改。这些行为更改还适用于Cisco Umbrella实施基于IP的地理阻止的其他地区。本文档最近更新于2022年7月28日。

DNS客户：

- 如果查询的IP地址被识别为来自俄罗斯、白俄罗斯、克里米亚、卢甘斯克、顿涅茨克、叙利亚、古巴、伊朗、朝鲜和其他受到地理限制的地区，DNS服务将不能应用安全或内容过滤策略。DNS查询仍然会收到有效的响应，并且会得到与世界其他地区的流量相同的服务级别。
- 当用于DNS时，Umbrella漫游安全模块和AnyConnect Umbrella漫游模块继续解析DNS流量。
- 漫游客户端同步和内部域列表可以继续与控制面板同步并提供预期行为（将内部域发送到内部DNS服务器）。 这种情况在未来可能会改变。

SIG客户：

- Umbrella安全Web网关服务器不接受源自IP来自俄罗斯、白俄罗斯、克里米亚、卢甘斯克、顿涅茨克、叙利亚、古巴、伊朗、朝鲜和其他受到地理限制地区的流量。实施方式会导致来自这些区域的连接将Cisco Umbrella服务器视为脱机或不可用。流量不会被接受或处理。
- 默认AnyConnect Umbrella模块配置使其在Umbrella不可用时直接连接到互联网。某些特定的客户配置可能会在“失效关闭”模式下运行，这会导致用户无法访问Internet。
- 目前，外部域列表继续同步，以从Umbrella获取更新。这种情况在未来可能会改变。
- 当Umbrella不可用时，默认Umbrella PAC文件使其直接连接到互联网。某些特定的客户配置（例如，没有默认路由的客户配置）可能会“关闭失败”，导致用户无法访问Internet。
- 通过IP阻止或撤销IKE凭证来断开IPsec隧道。行为和用户体验取决于特定的客户配置。某些配置可以恢复为直接互联网连接，其他配置可以恢复为MPLS，其他配置则可能导致用户失去互联网访问。

所有客户:

- 一旦国家/地区完全实施了基于IP的地理屏蔽，Umbrella控制面板和API访问也会被屏蔽。

如果受影响区域的用户连接到受影响区域之外的公司VPN，而后者又连接到Umbrella，该怎么办？

我们的地理位置阻止基于IP，基于Umbrella服务看到的源IP地址。

思科为什么要这样做？

请访问乌克兰战争：支持我们的客户、合作伙伴和社区以了解更多信息。

如果我的用户被阻止但不在受影响区域之一怎么办？

请联系支持部门，以调查已发布的邮件。

您的地理位置阻止数据的准确性如何？

我们使用行业领先的地理定位服务来确定特定IP地址的国家/地区。

如果与我的IP地址关联的位置有误，该怎么办？

我们建议向以下服务提交更正请求：

- https://www.maxmind.com/en/geoip-location-correction（用于Umbrella的主要服务）
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/contact/
- http://www.ipligence.com/contact/

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）。