零信任访问和VPN连接的地理访问限制

目录

问题

需要零信任访问(ZTA)和VPN连接的地理访问限制的组织可以发现，在尝试实施基于国家/地区的访问控制时，需要禁用现有的ZTA和VPN策略。当策略因无法在安全SSE产品界面中定位本地地理限制选项而被禁用时，用户会完全无法访问所需的资源。使用内置产品功能无法配置限制对仅来自特定国家/地区的连接访问的特定要求，导致在试图实施此类限制而停用现有策略时会对用户造成广泛影响。

环境

- 思科安全访问服务边缘(SASE)/安全SSE产品
- 零信任访问(ZTNA)实施
- 需要地理访问控制的VPN服务
- 私有资源访问策略
- 需要国家/地区特定访问限制的组织

分辨率

Cisco Secure SSE产品目前不提供本地功能，以根据用户地理位置或国家/地区限制私有资源访问。可考虑采用以下各节所述的方法解决此限制。

功能请求提交

必须向Cisco提交功能请求，以增加ZTA和VPN访问的地理限制功能。此增强请求由产品团队评估，以考虑是否可能包含在未来的版本中。组织可以与其思科客户经理合作，根据业务需求确定此类功能请求的优先顺序。

手动应急方案

可能的手动解决方法包括将特定国家/地区的公有IP地址范围作为网络对象组添加到访问策略中。

步骤 1：从相应的地区互联网注册机构(RIR)获取国家/地区的公有IP地址范围。

步骤 2：创建包含已标识IP范围的网络对象组。在访问策略配置中配置网络对象组，以包括分配给目标国家/地区的特定IP地址范围。

步骤 3：将网络对象组应用于访问策略。修改现有访问策略以引用创建的网络对象组，从而有效地限制对源自指定IP范围的连接的访问。

重要限制

此手动方法具有很大的局限性，因为它依赖于静态IP范围定义，无法考虑可绕过地理限制的动态IP分配、移动用户或VPN服务。此外，此方法需要持续维护以确保IP范围的准确性。

临时策略管理

在永久解决方案可用之前，组织必须避免同时禁用所有ZTA和VPN策略。相反，请考虑实施阶段性方法，其中关键访问策略保持有效，而地理限制要求通过替代方法得到满足，或者等待产品改进。

原因

Cisco Secure SSE产品架构不包括用于私有资源访问的本地地理访问控制功能。产品访问策略框架围绕用户身份、设备状态和基于网络的控制而设计，但是没有将地理位置作为策略实施参数。这表示产品功能差距，而不是配置问题或软件缺陷。

相关内容

- 思科技术支持和下载

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）。