ZTNA无客户端源IP地址限制

目录

问题

当尝试对通过ZTNA无客户端发布的基于浏览器的应用实施访问控制时，管理员会发现根据特定允许的公有IP地址限制访问不能作为配置选项。要求是仅允许从指定的源IP地址进行访问，同时阻止通过具有自定义域的ZTNA无客户端访问的应用程序的所有其他源IP。

环境

- 思科安全访问 — 零信任网络访问(ZTNA)
- ZTNA无客户端（基于浏览器的访问）
- 使用自定义域发布的应用程序
- 所有受影响的软件版本

分辨率

思科安全访问平台不支持ZTNA无客户端URL的源IP地址访问限制。此限制适用于通过ZTNA Clientless发布的所有应用，无论它们使用的是自定义域还是标准ZTNA URL。

ZTNA无客户端架构不提供在应用级别实施基于IP的访问控制列表或允许列表功能的功能。访问控制通过零信任框架内的其他身份验证和授权机制进行管理，例如：

- 用户身份验证
- 设备状况评估
- 多重身份验证

- 特定于应用的策略

需要基于IP的源访问控制的组织可能需要考虑替代方法，或等待将来可以包含此功能的产品增强功能。
请与思科客户团队联系，提出功能增强请求。

原因

ZTNA无客户端服务架构在其当前功能集中不包含源IP地址过滤功能。这是产品限制，而不是配置问题。

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）。