启用安全访问网络安全的Azure VPN客户端连接失败

目录

问题

从Umbrella迁移到SSE并使用新分配的SIA许可证启用网络安全后，启用网络安全时，无法为用户建立Azure VPN客户端连接。Azure VPN客户端连接问题会影响所有客户端，阻止它们连接到VPN。从客户端计算机卸载Cisco Secure Access Client时，VPN连接会恢复，表明安全访问客户端阻止与Azure VPN服务的连接。

禁用Web安全或卸载Cisco Secure Access Client会还原VPN连接，但在需要网络安全保护时，这会影响用户对Azure VPN上资源的访问。

环境

- 启用网络安全的Cisco Secure Access（以前称为SIA）
- Azure VPN客户端
- 从Umbrella到SSE的迁移已完成
- 新分配的SIA许可证

分辨率

解决方法涉及将Azure VPN网关公共IP地址添加到SSE/SWG例外列表，以防止阻止VPN连接的流量拦截。

步骤 1：确定Azure VPN网关IP地址

确定Azure VPN网关的公共IP地址。

步骤 2：将基于IP的例外添加到SSE/SWG

1. — 将Azure虚拟网关公有IP地址添加到思科安全访问环境中的SSE/SWG例外列表。

2. — 登录到Cisco Secure Access Dashboard — 点击Connect — 最终用户连接 — Internet Security — 添加例外。这可以防止安全Web网关拦截和检查发往Azure VPN网关的流量。

步骤 3：测试 VPN 连接性

应用基于IP的异常后，测试Azure VPN连接，以验证客户端是否能够在启用网络安全的情况下成功建立VPN连接。

步骤 4：扩展测试

将基于IP的异常的测试扩展到整个环境中的其他用户，以确保功能一致，然后再考虑是否解决所有问题。

原因

发生此问题的原因是安全Web网关(SWG)异常机制需要域的DNS查找来创建域到IP缓存条目。当Azure VPN客户端直接连接到IP地址而不对VPN URL执行DNS查询时，SWG模块无法将域映射到IP地址。因此，SWG继续检查并拦截发往IP地址的流量，从而阻止VPN连接的建立。

数据包捕获分析显示Azure网关IP没有针对VPN URL的DNS查询以及不可见的SWG侦听流量，确认SWG由于缓存中没有正确的域到IP映射而阻止连接。

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）。