恢复主对等IP时安全访问网络隧道组内部服务器错误

目录

问题

当尝试在Cisco安全访问的网络隧道组(NTG)中修改远程对等体IP时，用户尝试将主隧道IP恢复为先前配置的值时，可能会在UI中遇到“Internal Server Error”（内部服务器错误）。具体场景包括：

- NTG最初配置了主隧道IP和辅助IP，两个隧道都成功建立。
- 为了测试目的，主隧道IP更改为不同的IP地址，可以毫无问题地接受该地址。
- 当尝试将主隧道IP恢复为原始值时，系统无法保存配置并在UI中返回“Internal Server Error”（内部服务器错误）。
- 此行为始终可重复，在尝试重复使用先前配置的IP地址时出现。
- 原始IP以前工作正常，与辅助隧道IP没有冲突。

环境

- 思科安全访问（以前称为Cisco Umbrella for SSE）
- 专用接入的网络隧道组配置
- 使用主要和辅助对等IP的双隧道配置
- 基于Web的管理界面

分辨率

此问题由后端验证/状态问题引起，其中原始对等IP在配置更改后会保留或卡在后端系统中。必须遵循下一节中介绍的故障排除和解决步骤：

步骤 1：收集诊断信息

收集以下信息以进行后端验证：

- 安全访问组织ID
- 网络隧道组名称
- 受影响的主隧道的隧道ID
- 为NTG选择的地区/数据中心
- 保存尝试失败的确切时间戳，包括时区
- 确认原始IP是否出现在任何其他NTG中（当前或之前）
- 失败的保存尝试的浏览器HAR捕获

步骤 2：捕获浏览器HAR文件

收集失败保存尝试的诊断数据：

- 打开浏览器开发人员工具
- 转至Network选项卡
- 启用保留日志
- 重现保存失败
- 导出HAR文件并将其附加到支持案例


注意：在上传HAR文件之前清理/删除所有会话令牌或cookie。

步骤 3：后端验证和清理

此问题需要后端干预，无法仅从UI解决。以下操作必须由思科技术支持执行：

- 吸引安全访问后端/SSE平台团队
- 验证过时的peer-IP保留
- 检查孤立的隧道对象
- 识别与特定NTG配置关联的重复后端密钥
- 清除原始IP的陈旧隧道对等体引用
- 如有必要，强制后端重新同步NTG对象
- 释放绑定到NTG UUID的对等IP分配

步骤 4：备选分辨率方法

如果后端清理无法立即执行，请尝试以下过程：

- 删除网络隧道组主配置
- 等待5分钟
- 使用所需的IP地址重新添加NTG

⚠警告：有可能。此处提到的详细信息似乎包含执行后可能会产生重大影响的过程或命令。请确保SME或业务部门在执行或推荐之前已评估上述程序或命令。

步骤 5：临时解决方法

如果NTG处于生产状态且无法删除：

- 继续使用辅助隧道进行连接

- 从您的供应商/合作伙伴处获取备用公有IP
- 更新NTG主设备以使用备选IP
- 确认减少冗余，直到后端问题得到解决

原因

此问题是由思科安全访问后端系统中的软件漏洞引起的。当主对等体IP更改并恢复为原始值时，后端验证系统错误地将原始IP视为仍处于分配或保留状态，即使它应该可以重复使用。这会导致后端验证失败，该失败被用户界面屏蔽为通用“内部服务器错误”。 后端系统在配置更改过程中无法正确清除或释放IP保留，从而造成永久状态问题，阻止IP在同一NTG中重复使用。

相关内容

- 排除故障并收集思科安全访问的基本信息
- 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）。