配置SWG以避免与SSL VPN流量冲突

目录

简介

先决条件

- 要求
- 使用的组件

问题

解决方案

简介

本文档介绍如何使用截取的端口解决安全Web网关(SWG)和SSL VPN之间的不兼容问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

适用于AnyConnect的Umbrella SWG可能会遇到某些SSL VPN不兼容的问题，这些SSL VPN使用被SWG代理拦截的端口，例如TCP 443。AnyConnect SWG可能无法可靠地激活和应用覆盖范围。当SWG处于活动状态且VPN流量通过SWG时，网络可靠性可能会降低或变得不可用。在这种情况下，会丢弃非Web流量。此问题影响使用端口80和443的所有SSL VPN。

解决方案

要防止SWG拦截VPN流量，请为VPN域和IP地址配置旁路：

1.在Umbrella控制面板中，导航到Access Deployments > Domain Management > External Domains。

2.将VPN头端服务器的域和IP地址添加到External Domains列表。IP条目可确保VPN流量不会因大

量连接而被SWG代理拦截。

3.等待一小时以传播新设置。

要将SSL VPN用于SWG，请执行以下操作：

1.将VPN域添加到External Domains列表。

2.如果VPN头端域是DNS搜索后缀，客户端将在连接期间自动添加此域。

3.将VPN头端IP地址或IP范围添加到External Domains列表。

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）。