

管理Pulse Secure和Umbrella漫游客户端之间的冲突

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[概述](#)

[Pulse Secure部署不受支持](#)

[Pulse Windows 10 App样式连接。](#)

[Pulse Secure](#)

[使用具有分离DNS的基于FQDN的分割隧道实现脉冲安全](#)

简介

本文档介绍如何管理Pulse Secure和Umbrella Roaming Client之间的冲突。

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Umbrella漫游客户端。

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。

概述

如果您当前将Pulse Secure用作VPN客户端并希望安装Umbrella Roaming Client，则本文为必读文章。虽然一些用户报告成功使Cisco Umbrella漫游客户端与Pulse Secure VPN配合使用的情况有限，但存在许多不兼容问题，目前不受支持。

如果您遇到Umbrella漫游客户端兼容性问题，则支持的解决方案是迁移到AnyConnect Umbrella漫游安全模块。自2021年4月起，此内容将包含在Umbrella DNS订阅中。主要帐户持有者可以访问此软件，其地址为：software.cisco.com。如果您不确定哪个帐户具有访问权限或存在访问权限问题，请联系您的客户经理或通过umbrella-support@cisco.com联系您的Umbrella支持团队，以便代表

您联系您的客户经理。

Pulse Secure部署不受支持

Pulse Secure已知在以下两种情况下与Umbrella漫游客户端冲突：

Pulse Windows 10 App样式连接。

- 影响:脉冲无法连接

Pulse Secure

- 影响:在断开连接时，由于VPN连接期间的脉冲修改，保存的本地DNS可以保留在VPN值或127.0.0.1而不是WiFi/以太网值上。此修改是非VPN NIC上Umbrella修改和Pulse修改之间的冲突。
 - 断开连接后，用户连接会中断，直到DHCP租用续订。
- 解决方案：
 - 切换到AnyConnect中的Umbrella漫游安全模块。(不需要AnyConnect VPN。用于Umbrella的AnyConnect许可证包含在DNS包中，或者可以提供来解决此已知冲突。)

使用具有分离DNS的基于FQDN的分割隧道实现脉冲安全

- 影响:AC RSM与基于脉冲FQDN的分割隧道VPN配合使用时，不会进入加密/保护模式。VPN拆分DNS配置未按预期运行，其行为与全通道DNS相同。只有禁用AC RSM时，Pulse VPN的拆分DNS才能正常工作。
- 解决方案：
 - 切换到VPN配置的基于IP的分割隧道

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）。