思科安全访问分段ICMP数据包处理

目录

问题

在禁用DF（不分段）位的情况下发送大于MTU的ICMP回应请求时，不会接收应答。此行为发生在两个特定场景中：

- 当发送超过VPN接口MTU大小且清除DF位的ICMP数据包时，通过VPN接口从RAVPN终端发送
- 在站点路由器和思科安全访问(CSA)之间通过IPsec隧道从本地终端发送超过IPsec隧道接口MTU大小且清除DF位的ICMP数据包

在这两种情况下，均未收到ICMP响应，从而导致有关CSA是否丢弃禁用DF位的分段数据包的问题。

环境

- 思科安全访问(CSA)
- RAVPN（远程接入VPN）终端
- 站点路由器和CSA之间的IPsec隧道
- 超过接口MTU大小的ICMP流量
- 已清除DF位的分段数据包方案

分辨率

思科安全访问在底层和重叠情况下会丢弃分段的数据包。此行为记录在思科安全访问帮助文档中，其中明确指出："底层或重叠中的分段数据包将被丢弃。"

预期行为

思科安全访问旨在丢弃分段的数据包，无论这些数据包是在底层网络还是重叠网络中发生。这适用于：

- 从RAVPN终端发送的ICMP数据包超过VPN接口MTU，且已清除DF位
- 从内部终端通过IPsec隧道发送的ICMP数据包超过隧道接口MTU，且清除了DF位

此行为在涉及思科安全访问基础设施内分段数据包的所有场景中均保持一致。

已为此创建功能请求CSE-I-5739。

原因

Cisco Secure Access的架构旨在丢弃分段的数据包，作为一项安全和性能设计决策。实施此行为是为了防止底层网络方案和重叠网络方案中与数据包重组相关的潜在安全漏洞和处理开销。

相关内容

- 思科安全访问帮助文档 — 分段数据包处理
- 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）。