安全访问流量引导行为和例外列表配置

目录

问题

使用使用ZTA保护所有互联网目标设置（默认例外配置）时，用户需要明确思科安全访问流量引导行为。以下方面会出现一些具体问题：

- 流量引导决策是否基于DNS解析后的目标IP地址。
- 在引导过程中处理DNS流量的方式。
- 是否需要在Exception列表中的默认.local域条目之外配置其他本地域条目。

相关配置位于：Connect > End User Connectivity > Zero Trust Access >(Zero Trust Access Profiles)> Secure Internet Access > Traffic Steering > Use ZTA to secure all internet destinations

默认例外列表包括私有IP地址范围（A类、B类和C类）和.local域，用户需要了解这些设置的操作行为。

环境

- 思科安全访问
- 零信任访问(ZTA)配置
- 已启用流量控制功能
- 包含专用IP范围和.local域的默认例外列表

分辨率

思科安全访问流量引导行为如下：

流量引导决策流程

根据DNS解析后的目的IP地址做出流量引导决策。系统评估通过DNS名称解析得到的实际目标IP，以确定是否必须通过零信任访问安全堆栈引导流量。

DNS流量处理

DNS查询本身不受流量控制。当终端通过指向内部DNS服务器（通常使用私有IP地址）的DHCP接收DNS服务器分配时，这些DNS通信将绕过流量引导机制并在本地进行处理。

例外列表配置

默认例外列表包括：

- 私有IP地址范围(A类：10.0.0.0/8,B类：172.16.0.0/12,C类：192.168.0.0/16）
- .local域

对于使用自定义本地域（内部域名）的组织，必须将其他域条目添加到例外列表，以确保内部流量不会不必要地引导通过安全堆栈。默认.local条目包含标准的本地网络发现协议，但可能不包括所有组织内部域。

配置验证

要检验配置是否正确，请执行以下操作：

导航到Connect > End User Connectivity > Zero Trust Access > Secure Internet Access > Traffic Steering。

查看例外列表，确保该列表包含特定于贵组织内部基础设施的所有必需私有IP范围和本地域名。

原因

这是有关思科安全访问流量引导功能的操作行为的信息请求。需要澄清的原因在于流量引导逻辑的复杂性以及DNS解析、基于IP的路由决策和异常处理机制之间的交互。

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）。