在安全访问中排除专用应用的APP_UNREACHABLE故障

目录

问题

当尝试通过Cisco Secure Access访问零信任网络访问(ZTNA)应用时，用户会遇到“Application Unreachable”错误消息。

- Connector在控制面板中显示正常/活动，并且应用由其所有者确认正在运行。
- 故障可能会影响一个应用程序的所有用户，而由同一连接器服务的其他应用程序则正常工作。
- 在连接器池部署中，故障可能间歇性出现 — 会话成功或失败，具体取决于池中的哪个连接器被选中。

环境

- 采用ZTNA的思科安全专用接入部署
- 为ZTNA访问配置的专用资源
- 用于专用资源访问的资源连接器部署

分辨率

步骤1.测试连接器网段的直接连通性

- 资源连接器是锁定的装置，不提供外壳访问来直接运行curl或nc等命令。相反，从与连接器位于同一子网/VLAN中的测试主机（或临时VM）执行可达性测试，以便它遵循与应用相同的网络路径、路由和防火墙规则:

```
curl -v http://APP_IP:PORT/health
nc -zv APP_IP PORT
```

- 如果失败，则问题在网络路径或应用服务器上得到确认 — 请先解决此问题，然后再查看任何安全访问配置。

注意：来自不同子网的测试无法确定 — 防火墙规则和路由是按源进行评估的，因为测试源必须尽可能密切地镜像连接器的IP位置。

步骤2.检验专用资源配置

- 在Secure Access控制面板中，导航到Resources > Private Resources，打开受影响的专用资源，并将配置的IP、FQDN和端口字符与运行应用的实际绑定地址和端口进行比较。
- 任何不匹配情况（服务器迁移后过时的IP、错误的端口、HTTP与HTTPS）都会产生APP_UNREACHABLE，即使网络路径非常健康。

步骤3.验证连接器的DNS解析

- 如果私有资源由FQDN定义，请验证分配给连接器的DNS服务器是否可以解析它。从Resource Connector CLI（VM部署提供具有支持的标准Linux故障排除命令的诊断CLI），运行：

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- 确认返回了正确的私有IP。确保连接器的网络配置点位于可解析专用应用FQDN的内部DNS服务器；使用公共解析程序配置的连接器无法解析内部区域。

步骤4.检查防火墙路径

- 确认防火墙规则（网络防火墙和应用服务器上的主机防火墙）允许从连接器IP地址到所需端口上的应用服务器IP的流量。

步骤5.在资源连接器上使用tcpdump捕获流量

- 在Resource Connector上运行数据包捕获，观察通往应用的最后一英里连接尝试。tcpdump实用程序在Resource Connector上可用 — 请参阅在Resource Connectors上运行tcpdump指南。

提示：要使捕获在连接器组部署中成为确定性的，请暂时在组中仅启用一个Resource Connector，以便资源的所有会话都经过该捕获，然后运行在应用程序服务器和端口上过滤的捕获。

- 例如：

```
tcpdump 'host x.x.x.x and tcp port 443'
```

（其中x.x.x.x是应用服务器IP，443是应用的端口）

- 解释结果：没有SYN-ACK的出站SYN表示防火墙丢弃或应用未侦听；即时RST表示主机可访问，但没有任何内容绑定到该端口；没有发往应用的数据包表示会话未到达此连接器或DNS解析为意外地址。
- 捕获完成后，重新启用组中的其余连接器。

原因

- 防火墙阻止连接器到应用流量:基于网络或主机的防火墙会阻止连接器主机IP和应用服务器IP之间的所需端口。

- 安全访问中的私有资源配置不匹配:在专用资源定义(Resources > Private Resources)中配置的IP、FQDN或端口与应用实际侦听的内容不匹配（例如，应用已移至新IP，或在配置443时在8443上侦听）。
- 连接器的DNS解析故障:专用资源由FQDN定义，但连接器DNS服务器不解析专用应用FQDN。
- 应用服务器关闭或未侦听:通过其他衡量标准，服务器看起来运行正常，但并未绑定到预期端口，或者在主机保持正常工作状态时服务崩溃。
- 连接器池中的部分可达性:池中的一个或多个连接器位于无法到达应用的网段内，因此只有分配给这些连接器的会话会失败。

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）。