对零信任访问配置文件配置的MS团队问题进行故障排除

目录

问题

注册用于安全互联网访问的零信任访问(ZTA)配置文件的用户遇到了Microsoft Teams呼叫连接问题。将用户添加到ZTA配置文件时，Microsoft Teams呼叫意外断开连接，其他用户无法向受影响的用户发起呼叫。但是，当受影响的用户从其一侧发起呼叫时，呼叫连接成功。

该问题被隔离到已注册到ZTA配置文件的用户，表明ZTA策略或路由配置影响Teams呼叫连接。流量日志显示Microsoft Teams从ms-teams.exe等进程到所需范围的IP地址（例如52.115.245.30:3480，属于52.112.0.0/14）的流量被ZTA客户端拦截，而不是直接进入互联网。

环境

- 具有零信任访问(ZTA)配置文件的思科安全访问
- 使用“使用ZTA保护所有互联网目标”配置的ZTA配置文件
- Microsoft Teams应用程序
- 具有ZTA功能的思科安全客户端
- 用户注册了ZTA配置文件以进行安全互联网访问

分辨率

要解决此问题，请将Microsoft Teams流量异常添加到ZTA配置文件配置中，以允许Teams流量绕过ZTA隧道并直接连接到互联网：

1.定位至控制面板>最终用户连接>零信任访问，然后找到受影响的ZTA配置文件。

2.选择ZTA配置文件，然后选择编辑>安全Internet访问。

3.根据Microsoft的官方文档，将以下IP范围和FQDN添加到例外列表:

IP范围：

```
52.112.0.0/14
52.122.0.0/15
2603:1063::/38
2603:1027::/48
2603:1037::/48
2603:1047::/48
2603:1057::/48
2620:1ec:6::/48
2620:1ec:40::/42
```

FQDN:

```
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
teams.microsoft.com
*.keydelivery.mediaservices.windows.net
*.streaming.mediaservices.windows.net
aka.ms
```

4.添加例外说明，例如：

```
MS Teams exception as per: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-addre
```

5.保存配置更改。等待几分钟以应用更改。

6.确保在受影响的终端上重新同步ZTA客户端策略。这可能需要重新启动零信任访问代理服务或重新启动客户端设备。

7.测试团队呼叫功能以确认：

- 现在成功连接传入到受影响用户的来电
- Teams呼叫不再意外断开
- Teams流量绕过ZTA隧道直接连接到Internet

注意：实施例外后，Teams流量不会出现在安全访问活动日志中，因为它完全绕过ZTA隧道。

原因

此问题是由通过ZTA安全互联网接入隧道而非直接连接到互联网的Microsoft Teams流量导致的。当使用“Secure All Internet Destinations”选项配置ZTA配置文件时，它会拦截Teams媒体流量，包括实时通信所需的UDP流量。这会导致连接问题，尤其是对于传入呼叫和媒体流。

Microsoft建议绕过来自代理服务器的Microsoft Teams流量和SSL检查，以实现最佳性能和呼叫质量。当ZTA配置缺少Teams流量的必要例外时，应用程序媒体流将通过ZTA客户端进行处理，而不是采用实时通信所需的直接路径。

相关内容

- Microsoft 365 URL和IP地址范围 — Microsoft Teams
- Microsoft Teams代理服务器建议
- 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）。