验证旁路行为功能以实现安全访问Microsoft 365兼容性

目录

问题

在配置启用Microsoft 365兼容性功能的思科安全访问时，不确定是否从安全网络网关(SWG)处理和TLS解密自动绕过特定的Microsoft相关完全限定域名(FQDN)。具体而言，需要说明这些域的旁路行为：

- do.dsp.mp.mi crosoft.com
- dl.delivery.mp.mi crosoft.com
- manage.microsoft.com

主要关注点在于这些域是否需要手动添加到“不解密”列表，或者当启用Microsoft 365兼容性时是否自动排除这些域。此外，SWG级旁路与IPS级解密设置之间的交互存在混淆，尤其是对于manage.microsoft.com，文档显示，建议仍需要手动进行不解密列表配置。

环境

- 思科安全访问
- 已启用Microsoft 365兼容性功能
- 已配置安全网络网关(SWG)检测和TLS解密
- 正在使用的IPS解密策略
- 需要连接的Microsoft管理和更新服务

分辨率

Microsoft 365兼容性功能行为已通过实验室测试验证，结果如下：

Microsoft 365兼容性功能范围

Microsoft 365兼容性功能可免除在Microsoft的终端类别中标记为“优化”和“允许”的Microsoft 365相关域执行SWG检查和策略实施。这样，流向这些域的流量就可以在SWG层原封不动地通过。

实验室检测结果

测试在启用Microsoft 365兼容性的受控实验室环境中进行。针对指定的FQDN观察到此行为：

步骤 1：启用Microsoft 365兼容性功能

Microsoft 365兼容性功能已在Secure Access配置中激活。

步骤 2：测试到目标FQDN的流量

使用标准互联网浏览器生成到三个FQDN中每个的Web流量：

- do.dsp.mp.mi crosoft.com
- dl.delivery.mp.mi crosoft.com
- manage.microsoft.com

步骤 3：验证控制面板中的旁路行为

对安全访问控制面板的分析确认，启用Microsoft 365兼容性功能时，不会对这些特定目标的流量进行Web流量检测和解密。

步骤 4：确认DNS引导行为

流向这些目的地的DNS流量继续通过安全访问引导，这符合已记录的行为，除非配置了特定DNS免除。

关键行为发现

根据测试结果和文档分析：

- SWG旁路：启用Microsoft 365 Compatibility时，会从网络流量检测绕过三个指定的FQDN。
- TLS解密：这些域在SWG层绕过解密。
- DNS引导：除非明确免除，否则将继续通过安全访问处理DNS查询。
- 域覆盖：虽然规范并未完全绕过“*.microsoft.com”作为一个完整域，但实际操作中会绕开测试的特定URL。

IPS层注意事项

Microsoft 365兼容性功能在SWG层运行。对于IPS级解密旁路，仍需要手动配置：

- 如果这些域也需要IPS解密绕行，则可能需要手动添加Do Not Decrypt List。
- “不解密”列表主要影响IPS端解密，而不是SWG处理。
- 这解释了为什么即使启用Microsoft 365兼容性，文档仍可以参考将manage.microsoft.com添加到Do Not Decrypt List。

原因

混淆源于思科安全访问的分层架构，其中Microsoft 365兼容性会影响SWG级处理，而IPS解密则作为具有自身配置要求的单独层运行。Microsoft 365兼容性功能可自动处理符合条件的Microsoft域的SWG旁路，但IPS解密策略可能需要通过Do Not Decrypt List进行单独配置。

相关内容

- Cisco Secure Access Microsoft 365兼容性文档

- 为思科安全访问创建有效的不解密列表
- 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）。