

导入安全访问证书后的MacOS互联网访问问题

目录

问题

从门户导入互联网证书后，MacOS用户无法通过Cisco安全访问访问互联网资源。

受影响的服务包括：

- Microsoft Outlook (发送和接收功能)
- Google.com
- AI网站
- 其他Web目标

具有相同配置的Windows用户不会受到影响，并继续正常运行。此问题特别影响MacOS客户端在证书导入后对电子邮件的访问和常规互联网浏览功能。

环境

- 采用统一策略配置的思科安全访问
- 具有从思科安全访问门户导入的互联网证书的MacOS客户端
- 具有相同配置的Windows客户端 (不受影响)
- 正在使用的互联网策略、私有策略、DLP策略、RBI和安全配置文件
- MacOS和Windows之间行为不同的混合操作系统环境

分辨率

解决方法包括将特定Microsoft Outlook终端和应用添加到Do Not Decrypt(DND)列表，以绕过这些服务的SSL检查。

步骤 1：将Outlook终端添加到DND列表

将以下各节中描述的终端或应用程序添加到不解密(DND)配置中，以解决Outlook访问问题。

```
outlook.cloud.microsoft  
outlook.office.com  
outlook.office365.com  
smtp.office365.com
```

步骤 2：验证解决措施

将与Outlook相关的终端添加到DND列表后，请验证受影响的MacOS客户端现在是否可以访问：

- Microsoft Outlook发送和接收功能
- 以前受影响的其它互联网资源

用户确认，在实施这些DND条目后，Outlook应用程序在MacOS设备上继续正常运行。

原因

此问题是由于SSL/TLS加密检查干扰MacOS客户端建立与互联网资源（尤其是Microsoft Outlook服务）的安全连接的能力引起的。加密检查过程阻止在MacOS平台上专门进行正确的证书验证或连接建立，而Windows客户端不受同一检查策略的影响。将受影响的终端添加到Do Not Decrypt列表会绕过对这些特定服务的检查，从而恢复正常连接。

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）。