在安全访问中为Microsoft 365服务创建有效的不解密列表

目录

简介

本文档介绍创建不解密列表以绕过Microsoft 365域从安全访问中的IPS解密的有效方法。

问题

已知Microsoft 365流量在通过SSL检查引擎、代理或IPS时会导致问题。
Microsoft根据知识库文章建议绕过分类为“允许和优化”的域和IP:

https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

安全访问中的当前Microsoft 365兼容性功能仅适用于流量 通过代理。
因此，启用此功能后，不会在代理级别对此流量应用解密或检查，但是全局IPS解密设置仍然适用。

启用IPS解密和Microsoft 365兼容性功能后，在下列情况下仍会解密发往互联网的流量：

- 全通道RAVPN
- 通过VPN隧道安全访问互联网

Microsoft 365流量解密所导致的问题的典型症状：

- 通过Outlook传送电子邮件的速度缓慢
- sharepoint的性能问题
- 使用Teams时用户体验不佳

临时解决方法

客户必须绕过发往Allow和Optimize from IPS解密的域的流量：

手动创建此类列表相当麻烦，因此Python脚本可用于从Microsoft API动态提取列表：
https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

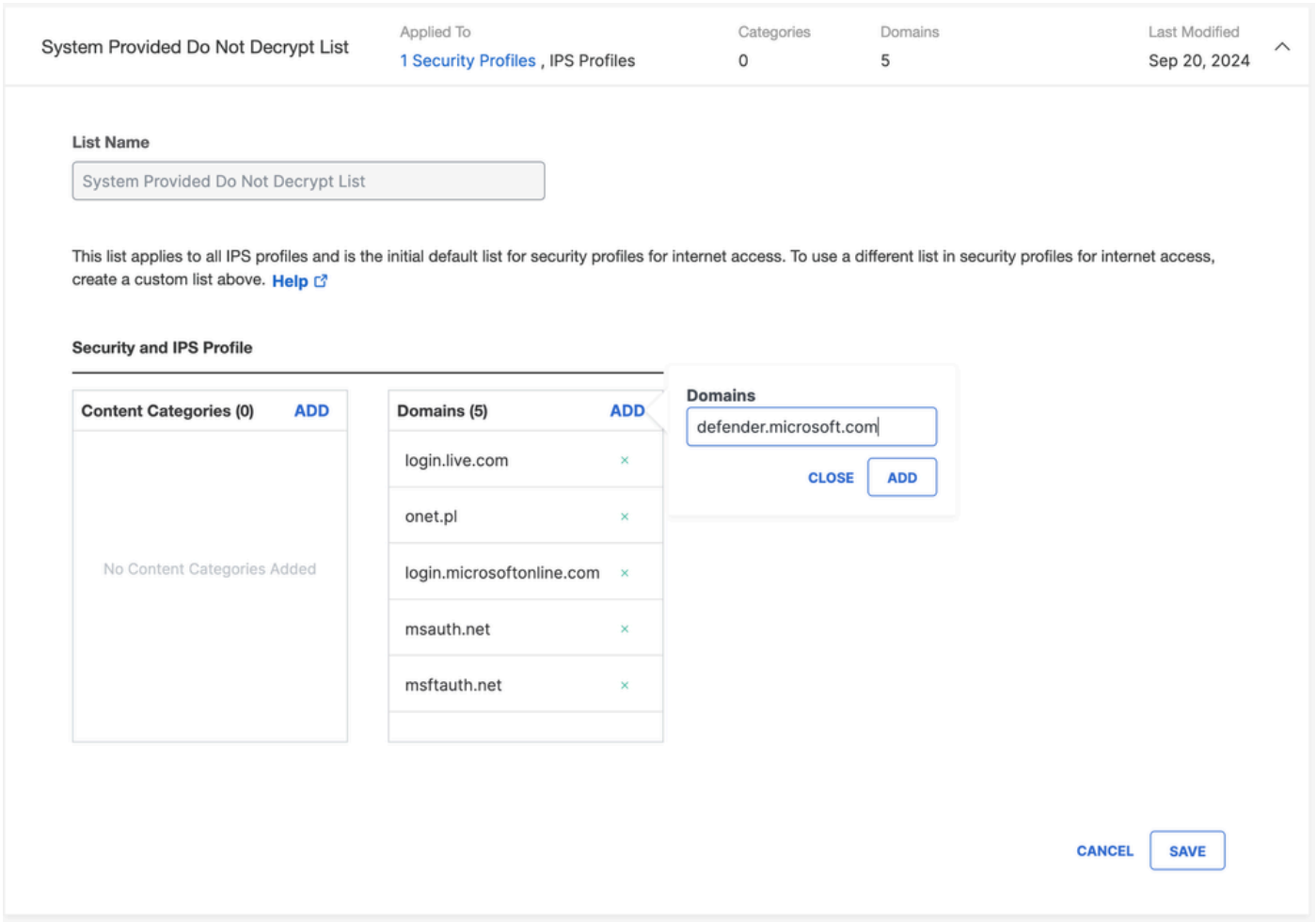
```
import requests

def get_fqdns(url):
    try:
        response = requests.get(url)
        response.raise_for_status()
        data = response.json()

        fqdns = []
        for item in data:
            if item.get('category') in ['Allow', 'Optimize']:
                for fqdn in item.get('urls', []):
                    fqdns.append(fqdn)

        return fqdns

    except requests.exceptions.RequestException as e:
        print(f"Error fetching data: {e}")
        return []

# URL to fetch the endpoint data
url = "https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946

# Get FQDNs and print them
fqdns = get_fqdns(url)
for fqdn in fqdns:
    print(fqdn)
```

此脚本截至2024年10月31日的输出示例：

```
outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
outlook.office365.com
smtp.office365.com
*.protection.outlook.com
*.mail.protection.outlook.com
*.mx.microsoft
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
```

```
teams.microsoft.com
*.sharepoint.com
*.officeapps.live.com
*.online.office.com
office.live.com
*.auth.microsoft.com
*.msftidentity.com
*.msidentity.com
account.activedirectory.windowsazure.com
accounts.accesscontrol.windows.net
adminwebservice.microsoftonline.com
api.passwordreset.microsoftonline.com
autologon.microsoftazuread-sso.com
becws.microsoftonline.com
ccs.login.microsoftonline.com
clientconfig.microsoftonline-p.net
companymanager.microsoftonline.com
device.login.microsoftonline.com
graph.microsoft.com
graph.windows.net
login.microsoft.com
login.microsoftonline.com
login.microsoftonline-p.com
login.windows.net
logincert.microsoftonline.com
loginex.microsoftonline.com
login-us.microsoftonline.com
nexus.microsoftonline-p.com
passwordreset.microsoftonline.com
provisioningapi.microsoftonline.com
*.protection.office.com
*.security.microsoft.com
compliance.microsoft.com
defender.microsoft.com
protection.office.com
purview.microsoft.com
security.microsoft.com
```

现在可以将列表列表中的域添加到System Provided Do Not Decrypt List:



您必须添加FQDN 系统提供的不解密列表，以绕过IPS的解密。
自定义不解密列表只能通过应用到安全配置文件。

解决方案

思科工程团队正在致力于增强Microsoft 365兼容性功能，该功能将自动提取此列表，并允许管理员从安全访问控制面板启用旁路功能。

相关信息

- 安全访问用户指南
- 技术支持和下载 - 思科系统公司
- 安全访问解密和入侵防御系统(IPS)工作流程故障排除

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）。