セキュアアクセスにおけるMicrosoft 365サービスの有効な非暗号化機能リストの作成

内容

はじめに

このドキュメントでは、セキュアアクセスのIPS復号化からMicrosoft 365ドメインをバイパスするDo Not Decryptリストを作成する効果的な方法について説明します。

問題

Microsoft 365トラフィックは、SSLインスペクションエンジン、プロキシ、またはIPSを通過するときに問題を引き起こすことが知られています。
Microsoftでは、KBの記事に基づいて、許可と最適化に分類されたドメインとIPをバイパスすることを推奨しています。

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

Secure Accessの現在のMicrosoft 365互換性機能は、トラフィックにのみ適用されます プロキシを通過します。
その結果、この機能が有効な場合、このトラフィックに対してプロキシレベルで復号化や検査は適用されませんが、グローバルIPS復号化設定は適用されます。

IPS復号化とMicrosoft 365互換性機能が有効になっている場合、インターネット宛てのトラフィックは引き続き次のシナリオで復号化されます。

- フルトンネルRAVPN
- VPNトンネル経由のセキュアなインターネットアクセス

Microsoft 365トラフィックの復号化によって発生する問題の典型的な症状は次のとおりです。

- outlook経由の電子メール配信が遅い
- sharepointのパフォーマンスの問題
- teams使用時のユーザーの操作性が悪い

暫定回避策

お客様は、IPS復号化から、AllowおよびOptimizeに分類されたドメイン宛てのトラフィックをバイパスする必要があります。

このようなリストを手動で作成するのは面倒な作業なので、Pythonスクリプトを使用してMicrosoft APIからリストを動的に取得できます。
https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

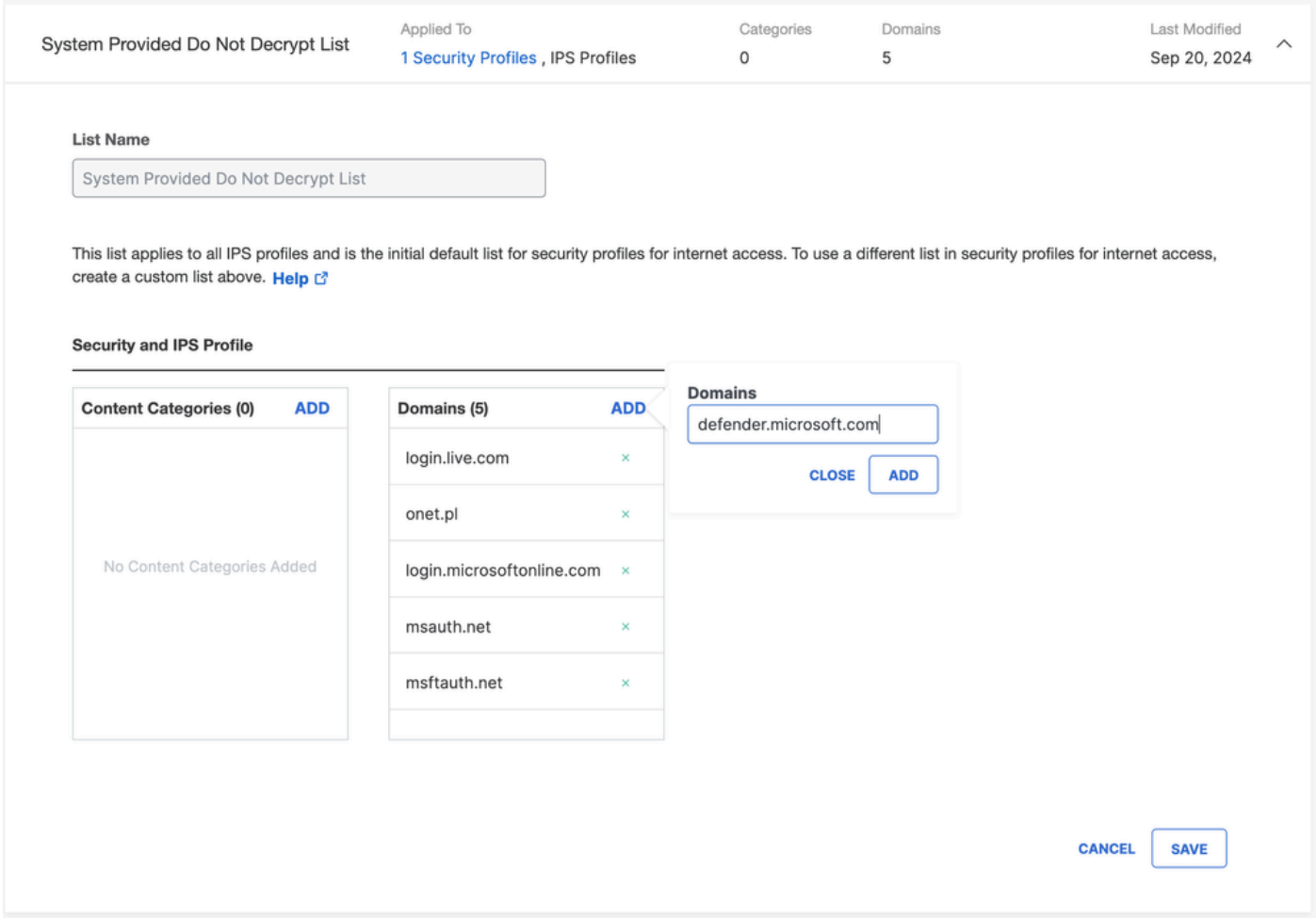
```
import requests

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)
```

2024年10月31日現在のこのスクリプトの出力例：

```
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
```

リストのリストからドメインを「System Provided Do Not Decrypt List:



FQDNを追加する必要があります IPSの復号化をバイパスするために、System Provided Do Not Decrypt Listを使用します。
カスタムDo Not Decryptリストは、セキュリティプロファイルにのみ適用できます。

解決方法

シスコエンジニアリングチームでは、Microsoft 365互換性機能の拡張に取り組んでいます。この機能により、このリストが自動的に取得され、管理者はSecure Access Dashboardからバイパス機能を有効にできます。

関連情報

- セキュアアクセスユーザガイド
- テクニカルサポートとダウンロード - Cisco Systems
- Secure Access Decryption and Intrusion Prevention System(IPS)ワークフローのトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。