Créer une liste effective à ne pas déchiffrer pour les services Microsoft 365 dans Secure Access

Table des matières

Introduction

Ce document décrit la manière efficace de créer une liste de ne pas déchiffrer pour contourner le déchiffrement IPS des domaines Microsoft 365 dans Secure Access.

Problème

Le trafic Microsoft 365 est connu pour causer des problèmes lors de son passage par des moteurs d'inspection SSL, proxy ou IPS.
Microsoft suggère de contourner les domaines et les adresses IP classés comme Allow et Optimize, d'après l'article de la base de connaissances :

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

La fonctionnalité de compatibilité actuelle de Microsoft 365 dans Secure Access s'applique uniquement au trafic en passant par le proxy.
Par conséquent, lorsque cette fonctionnalité est activée, aucun décryptage ou inspection n'est appliqué à ce trafic au niveau du proxy, cependant les paramètres de décryptage IPS globaux s'appliquent toujours.

Lorsque le déchiffrement IPS et la fonctionnalité de compatibilité Microsoft 365 sont activés, le trafic destiné à Internet est toujours déchiffré dans les scénarios suivants :

- RAVPN à tunnel complet
- Accès Internet sécurisé via tunnel VPN

Symptômes typiques des problèmes causés par le déchiffrement du trafic Microsoft 365 :

- livraison lente des e-mails via Outlook
- problèmes de performances avec Sharepoint
- mauvaise expérience utilisateur lors de l'utilisation de Teams

Solution de contournement provisoire

Les clients doivent contourner le trafic destiné aux domaines classés comme Autoriser et Optimiser à partir du décryptage IPS :

La création manuelle d'une telle liste est plutôt une tâche fastidieuse, par conséquent le script Python peut être utilisé pour extraire la liste dynamiquement de l'API Microsoft : https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

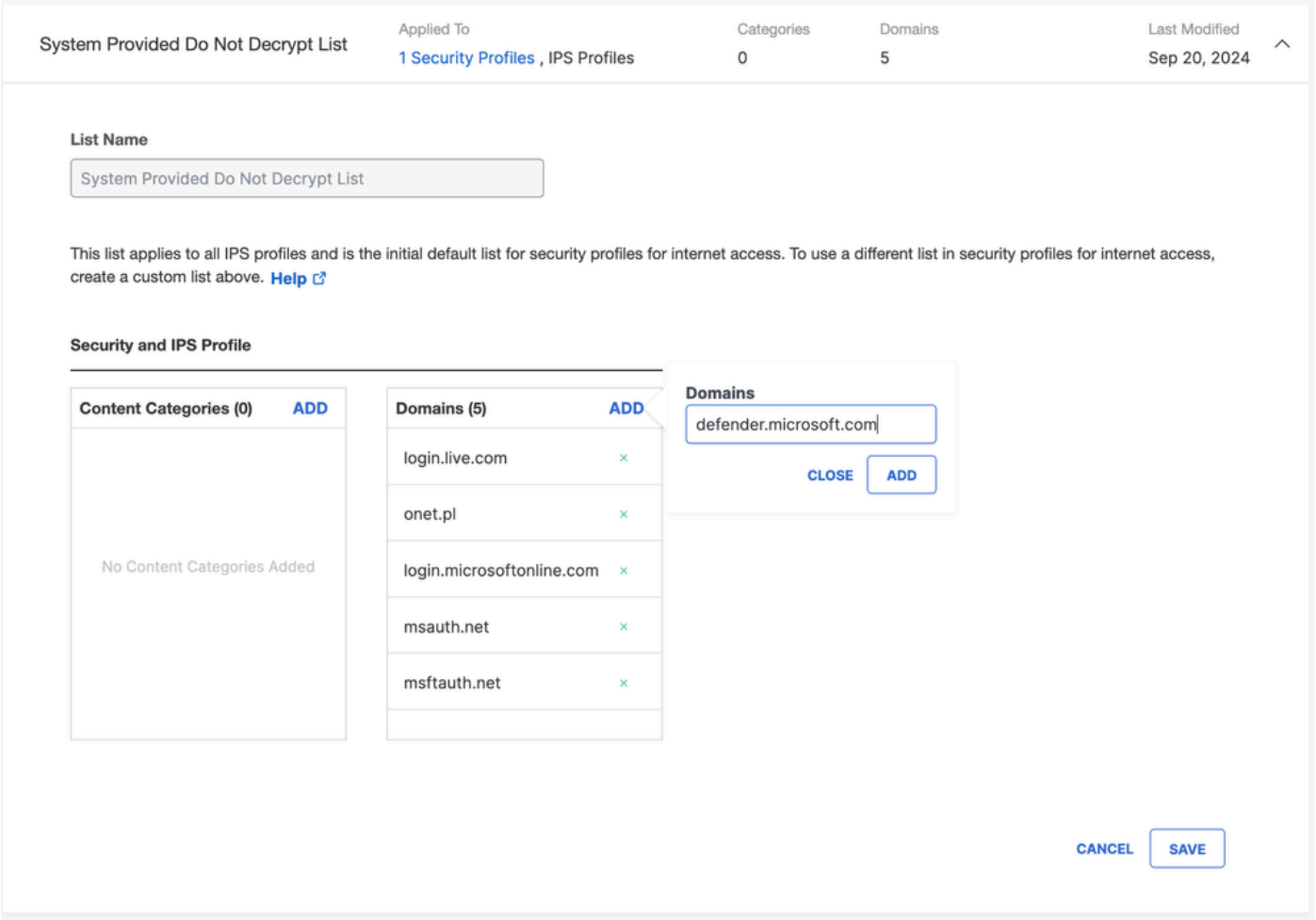
```
import requests

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)
```

Exemple de résultat de ce script au 31 octobre 2024 :

```
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
```

Les domaines de la liste peuvent désormais être ajoutés à la liste Ne pas déchiffrer fournie par le système :



Vous devez ajouter les noms de domaine complets dans Liste de non-déchiffrement fournie par le système, afin de contourner le déchiffrement pour IPS.
La liste Ne pas déchiffrer personnalisée peut uniquement être appliquée aux profils de sécurité.

Solution

L'équipe d'ingénierie Cisco travaille à l'amélioration de la fonctionnalité de compatibilité de Microsoft 365, qui extrairait cette liste automatiquement et permet à l'administrateur d'activer la fonctionnalité de contournement à partir du tableau de bord d'accès sécurisé.

Informations connexes

- Guide de l'utilisateur Secure Access
- Assistance technique et téléchargements — Cisco Systems
- Dépannage du workflow du système de décodage et de prévention des intrusions (IPS) à accès sécurisé

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.