Crear una lista efectiva de no descifrado para los servicios de Microsoft 365 en Secure Access

Contenido

Introducción

Este documento describe la manera efectiva de crear una lista de No descifrar para saltarse los dominios de Microsoft 365 del descifrado IPS en Secure Access.

Problema

Se sabe que el tráfico de Microsoft 365 causa problemas cuando se transmite a través de motores de inspección SSL, proxy o IPS.
Microsoft sugiere omitir dominios e IP categorizados como Permitir y Optimizar, según el artículo de KB:

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

La función de compatibilidad actual de Microsoft 365 en Secure Access sólo se aplica al tráfico pasando a través del proxy.
Como resultado, cuando se habilita esta función, no se aplica descifrado ni inspección a este tráfico en el nivel de proxy, sin embargo, la configuración de descifrado IPS global sigue aplicándose.

Cuando se habilitan el descifrado IPS y la característica de compatibilidad de Microsoft 365, el tráfico con destino a Internet se descifra en los siguientes escenarios:

- RAVPN de túnel completo
- Acceso seguro a Internet a través del túnel VPN

Síntomas típicos de problemas causados por el descifrado del tráfico de Microsoft 365:

- entrega lenta de correo electrónico mediante Outlook
- problemas de rendimiento con Sharepoint
- mala experiencia del usuario al utilizar equipos

Solución alternativa provisional

Los clientes deben omitir el tráfico destinado a dominios categorizados como Permitir y Optimizar del descifrado IPS:

Crear dicha lista manualmente es más bien una tarea engorrosa, por lo tanto, el script Python se puede utilizar para extraer la lista dinámicamente desde la API de Microsoft: https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

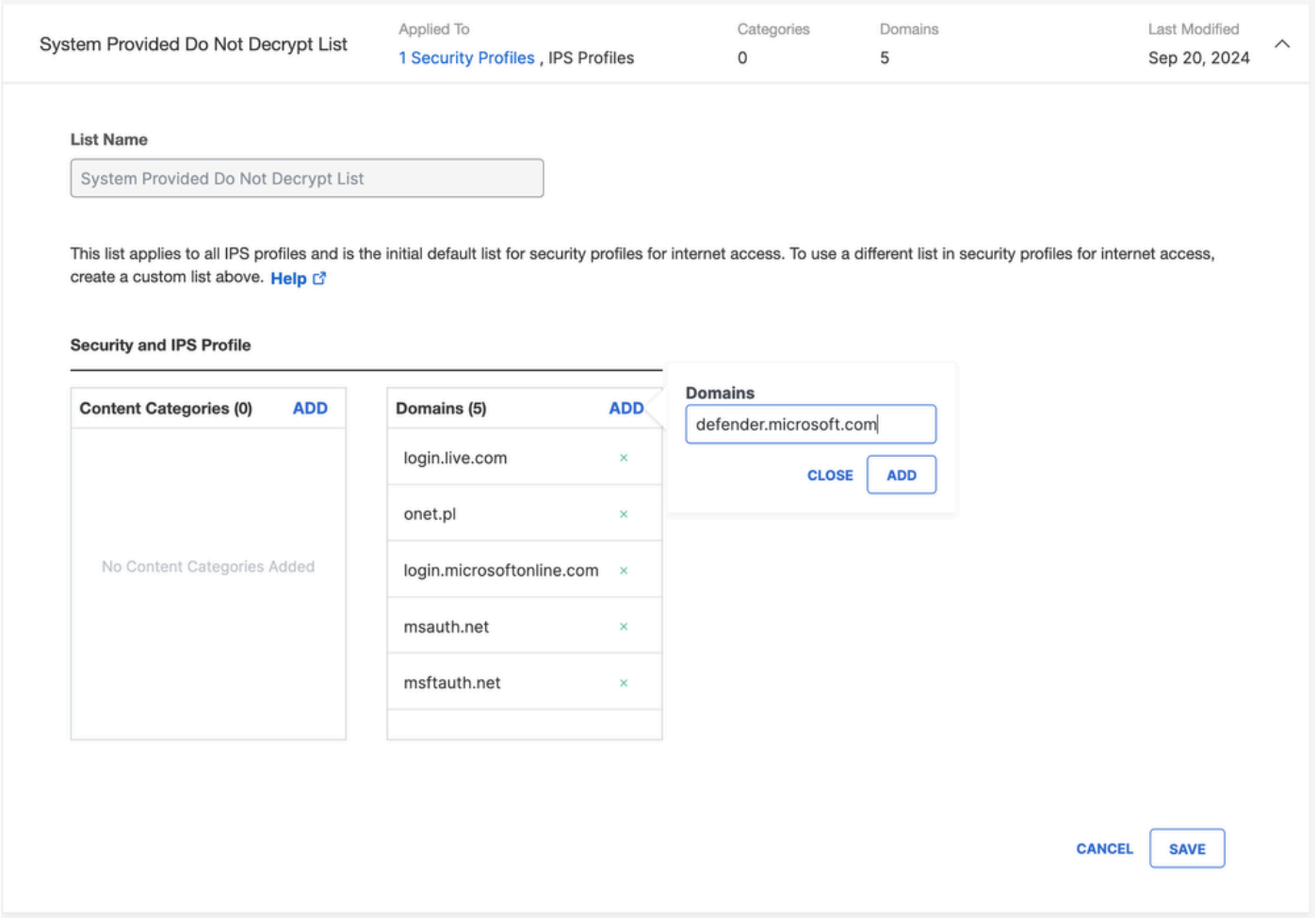
```
import requests

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)
```

Ejemplo de salida de este script a 31 de octubre de 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
```

Los dominios de la lista se pueden agregar ahora a la lista No descifrar proporcionada por el sistema:



Debe agregar los FQDN en La lista No descifrar proporcionada por el sistema, para omitir el descifrado para IPS.
La lista No descifrar personalizada solo se puede aplicar a los perfiles de seguridad.

Solución

El equipo de ingeniería de Cisco está trabajando para mejorar la función de compatibilidad de Microsoft 365, que extraería esta lista automáticamente y permitiría al administrador habilitar la funcionalidad de omisión desde el panel de acceso seguro.

Información Relacionada

- Guía del usuario de Secure Access
- Soporte técnico y descargas: Cisco Systems

- Solución de problemas de flujo de trabajo de Secure Access Decryption and Intrusion Prevention System (IPS)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).