Erstellung einer effektiven Liste nicht entschlüsselnder Dienste für Microsoft 365-Dienste in sicherem Zugriff

Inhalt

Einleitung

Problem

Zwischenlösung

Lösung

Zugehörige Informationen

Einleitung

In diesem Dokument wird die effektive Methode zum Erstellen einer Liste "Nicht entschlüsseln" beschrieben, um Microsoft 365-Domänen von der IPS-Entschlüsselung in Secure Access zu umgehen.

Problem

Der Datenverkehr von Microsoft 365 verursacht bekanntermaßen Probleme, wenn er über SSL Inspection Engines, Proxy oder IPS geleitet wird.
Microsoft schlägt vor, Domänen und IPs zu umgehen, die als Zulassen und Optimieren kategorisiert sind. Dies wird im folgenden KB-Artikel beschrieben:

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

Die aktuelle Microsoft 365-Kompatibilitätsfunktion in Secure Access gilt nur für Datenverkehr. den Proxy passieren.
Wenn diese Funktion aktiviert ist, wird daher keine Entschlüsselung oder Überprüfung auf diesen Datenverkehr auf Proxyebene angewendet. Die globalen IPS-Entschlüsselungseinstellungen gelten jedoch weiterhin.

Wenn die IPS-Entschlüsselung und die Kompatibilitätsfunktion von Microsoft 365 aktiviert sind, wird der an das Internet gerichtete Datenverkehr in folgenden Szenarien immer noch entschlüsselt:

- Vollständiger Tunnel-RAVPN

- Sicherer Internetzugriff über VPN-Tunnel

Typische Symptome von Problemen, die durch die Entschlüsselung von Microsoft 365-Datenverkehr verursacht werden:

- Langsame E-Mail-Übermittlung über Outlook
- Performance-Probleme mit Sharepoint
- schlechtes Anwendererlebnis bei der Nutzung von Teams

Zwischenlösung

Kunden müssen Datenverkehr umgehen, der an Domänen gerichtet ist, die als Zulassen und Optimieren von IPS-Entschlüsselung kategorisiert sind:

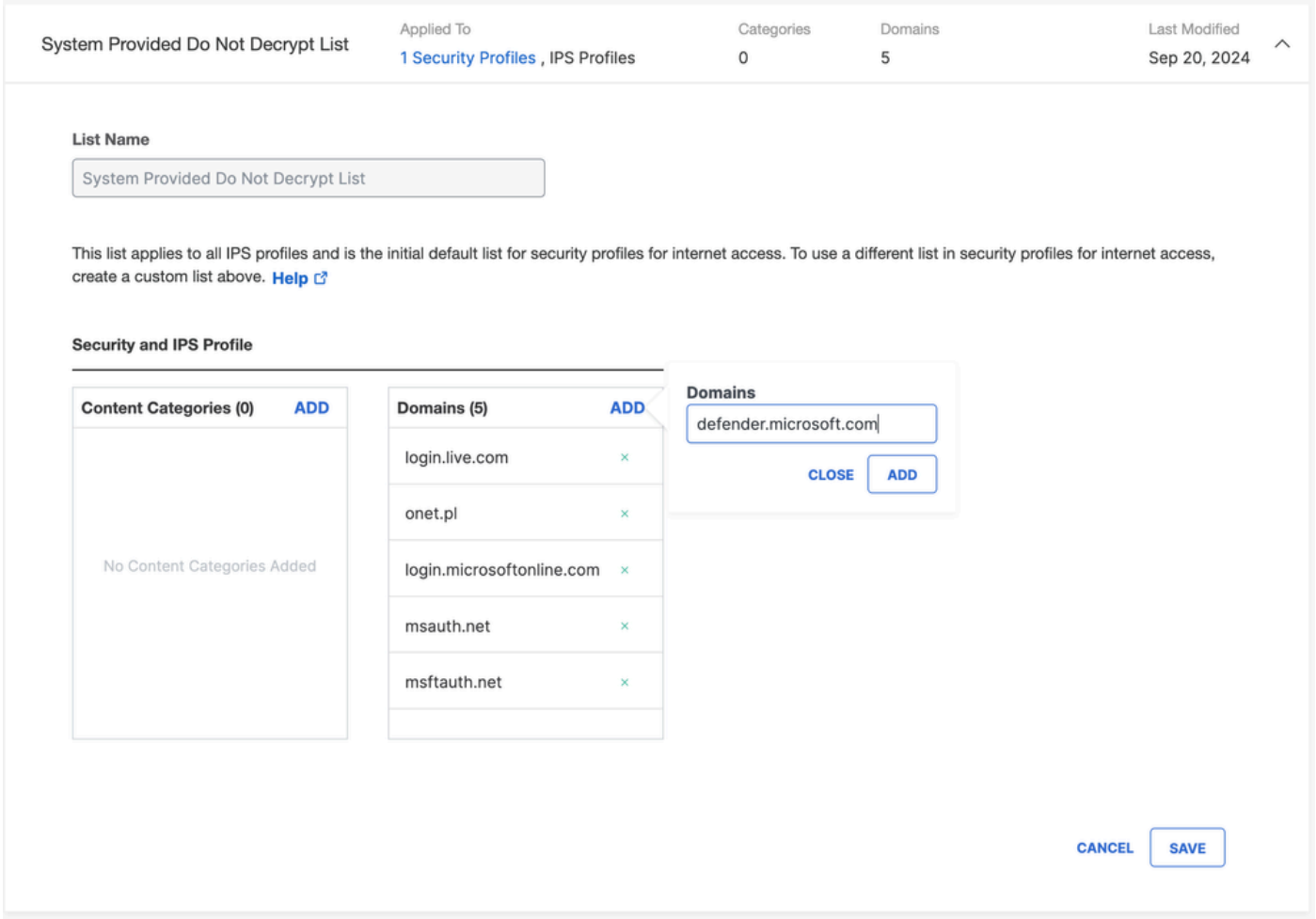
Das manuelle Erstellen einer solchen Liste ist eher umständlich, daher kann das Python-Skript verwendet werden, um die Liste dynamisch von der Microsoft-API abzurufen: https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

```
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)
```

Beispielausgabe dieses Skripts zum 31. Oktober 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
```

Domänen aus der Liste können jetzt zur vom System bereitgestellten Liste nicht entschlüsseln hinzugefügt werden:



Sie müssen die FQDNs hinzufügen in Vom System bereitgestellte Liste "Nicht entschlüsseln", um die Entschlüsselung für IPS zu umgehen.
Die benutzerdefinierte Liste Nicht entschlüsseln kann nur auf Sicherheitsprofile angewendet werden.

Lösung

Das Cisco Technikerteam arbeitet derzeit an der Verbesserung der Kompatibilitätsfunktion für Microsoft 365, mit der diese Liste automatisch abgerufen wird und Administratoren die Umgehungsfunktion über das Secure Access Dashboard aktivieren können.

Zugehörige Informationen

- Benutzerhandbuch zu Secure Access
- Technischer Support und Downloads – Cisco Systems

- Fehlerbehebung beim sicheren IPS-Workflow (Secure Access Decryption and Intrusion Prevention System)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.