Effectieve Do Not Decrypt List maken voor Microsoft 365 Services in Secure Access

Inhoud

Inleiding

Dit document beschrijft de effectieve manier om een Do Not Decrypt-lijst te maken om Microsoft 365-domeinen te omzeilen van IPS-decryptie in Secure Access.

Probleem

Het is bekend dat Microsoft 365-verkeer problemen veroorzaakt wanneer het wordt doorgegeven via SSL-inspectiemotoren, proxy of IPS.
Microsoft stelt voor om domeinen en IP's te omzeilen die gecategoriseerd zijn als Toestaan en Optimaliseren, gebaseerd op KB-artikel:

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

De huidige Microsoft 365-compatibiliteitsfunctie in Secure Access is alleen van toepassing voor verkeer het passeren door de proxy.
Dientengevolge, wanneer deze eigenschap wordt toegelaten, wordt geen decryptie of inspectie toegepast op dit verkeer op het volmachtsniveau, nochtans zijn de globale IPS decryptie instellingen nog van toepassing.

Wanneer IPS-decryptie en Microsoft 365 Compatibiliteitsfunctie zijn ingeschakeld, wordt internetverkeer nog steeds gedecrypteerd in scenario's:

- Full Tunnel RAVPN
- Beveiligde internettoegang via VPN-tunnel

Typische symptomen van problemen veroorzaakt door decryptie van Microsoft 365 verkeer:

- langzame e-maillevering via Outlook
- prestatieproblemen met Sharepoint
- slechte gebruikerservaring bij gebruik van Teams

Tussenfase-tijdelijke oplossing

Klanten moeten verkeer omzeilen dat is bestemd voor domeinen die zijn gecategoriseerd als Toestaan en optimaliseren tegen IPS-decryptie:

Het handmatig maken van een dergelijke lijst is eerder een lastige taak, vandaar dat het Python script kan worden gebruikt om de lijst dynamisch uit Microsoft API te halen: https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

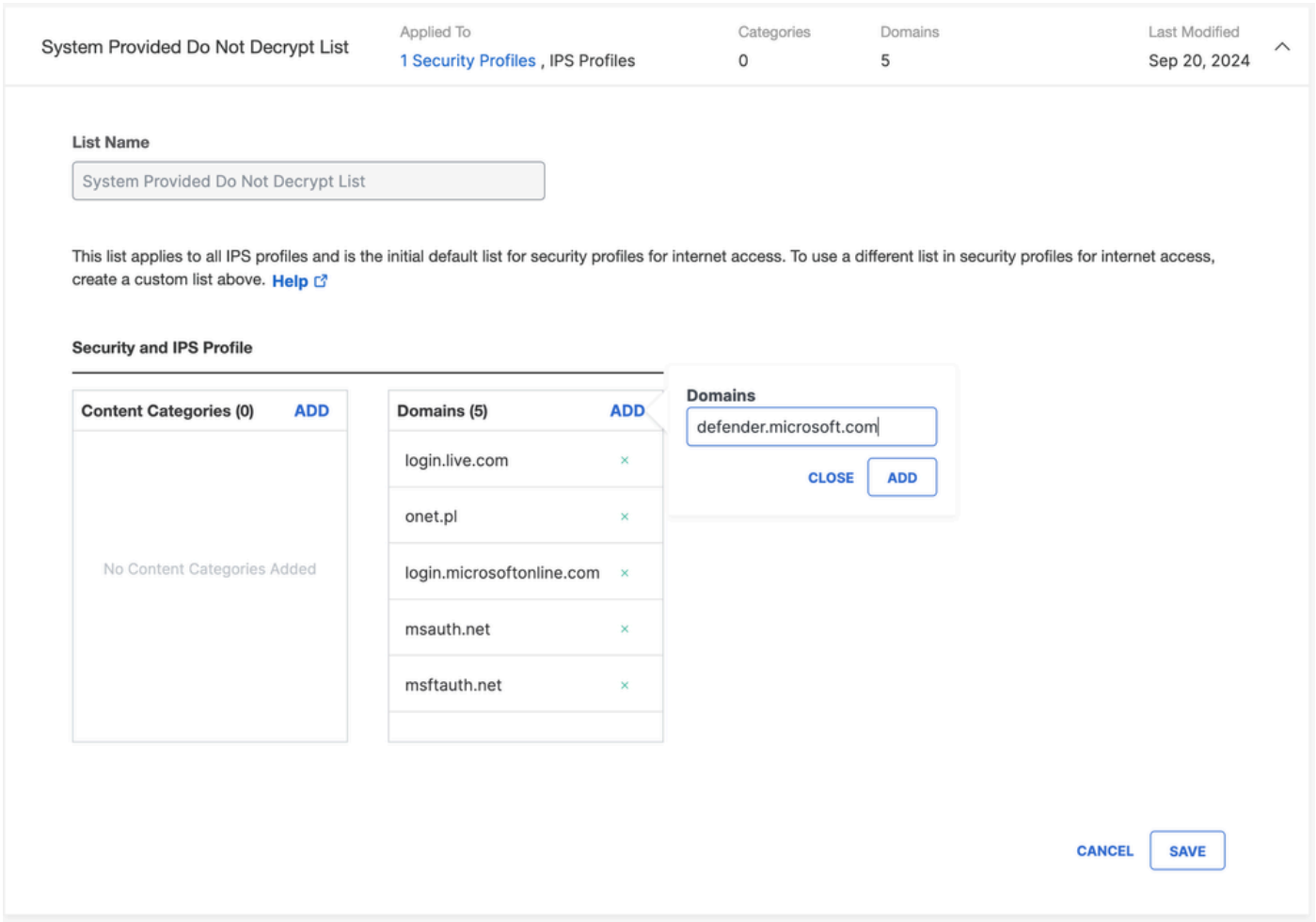
```
import requests

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)
```

Voorbeeld van dit script vanaf 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
```

Er kunnen nu domeinen uit de lijst worden toegevoegd aan het verstrekte Systeem Niet ontcijferen Lijst:



U moet FQDN's toevoegen in Verstrekt systeem decrypteert geen lijst, om decryptie voor IPS te mijden.
Aangepaste Do Not Decrypt lijst kan alleen worden toegepast op Beveiligingsprofielen.

Oplossing

Cisco Enginering Team werkt aan het verbeteren van de Microsoft 365 compatibiliteitsfunctie, die deze lijst automatisch zou halen en admin toestaat om de bypass functionaliteit van Secure Access Dashboard.

Gerelateerde informatie

- Gebruikershandleiding voor Secure Access
- Technische ondersteuning en downloads – Cisco Systems

- Probleemoplossing voor Secure Access Decryptie en Inbraakpreventiesysteem (IPS)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.