Crea elenco elementi non decrittografati valido per i servizi Microsoft 365 in accesso sicuro

Sommario

Introduzione

In questo documento viene descritto come creare in modo efficace un elenco da non decrittografare per ignorare i domini Microsoft 365 dalla decrittografia IPS in Secure Access.

Problema

È noto che il traffico Microsoft 365 causa problemi quando viene passato attraverso motori di ispezione SSL, proxy o IPS.
Microsoft consiglia di ignorare i domini e gli IP classificati come Consenti e Ottimizza, in base all'articolo della Knowledge Base:

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

L'attuale funzionalità di compatibilità con Microsoft 365 in Secure Access è applicabile solo al traffico passaggio attraverso il proxy.
Di conseguenza, quando questa funzione è abilitata, non viene applicata alcuna decrittografia o ispezione al traffico a livello di proxy, ma vengono comunque applicate le impostazioni globali di decrittografia IPS.

Quando la decrittografia IPS e la funzionalità di compatibilità Microsoft 365 sono abilitate, il traffico destinato a Internet viene ancora decrittografato negli scenari seguenti:

- RAVPN tunnel completo
- Accesso sicuro a Internet tramite tunnel VPN

Sintomi tipici dei problemi causati dalla decrittografia del traffico Microsoft 365:

- recapito e-mail lento tramite Outlook
- problemi di prestazioni con Sharepoint
- esperienza utente non valida durante l'utilizzo dei team

Soluzione provvisoria

I clienti devono ignorare il traffico destinato ai domini classificati come Consenti e Ottimizza dalla decrittografia IPS:

La creazione manuale di un elenco di questo tipo è un'operazione piuttosto complessa, pertanto lo script Python può essere utilizzato per estrarre l'elenco in modo dinamico dall'API Microsoft: https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

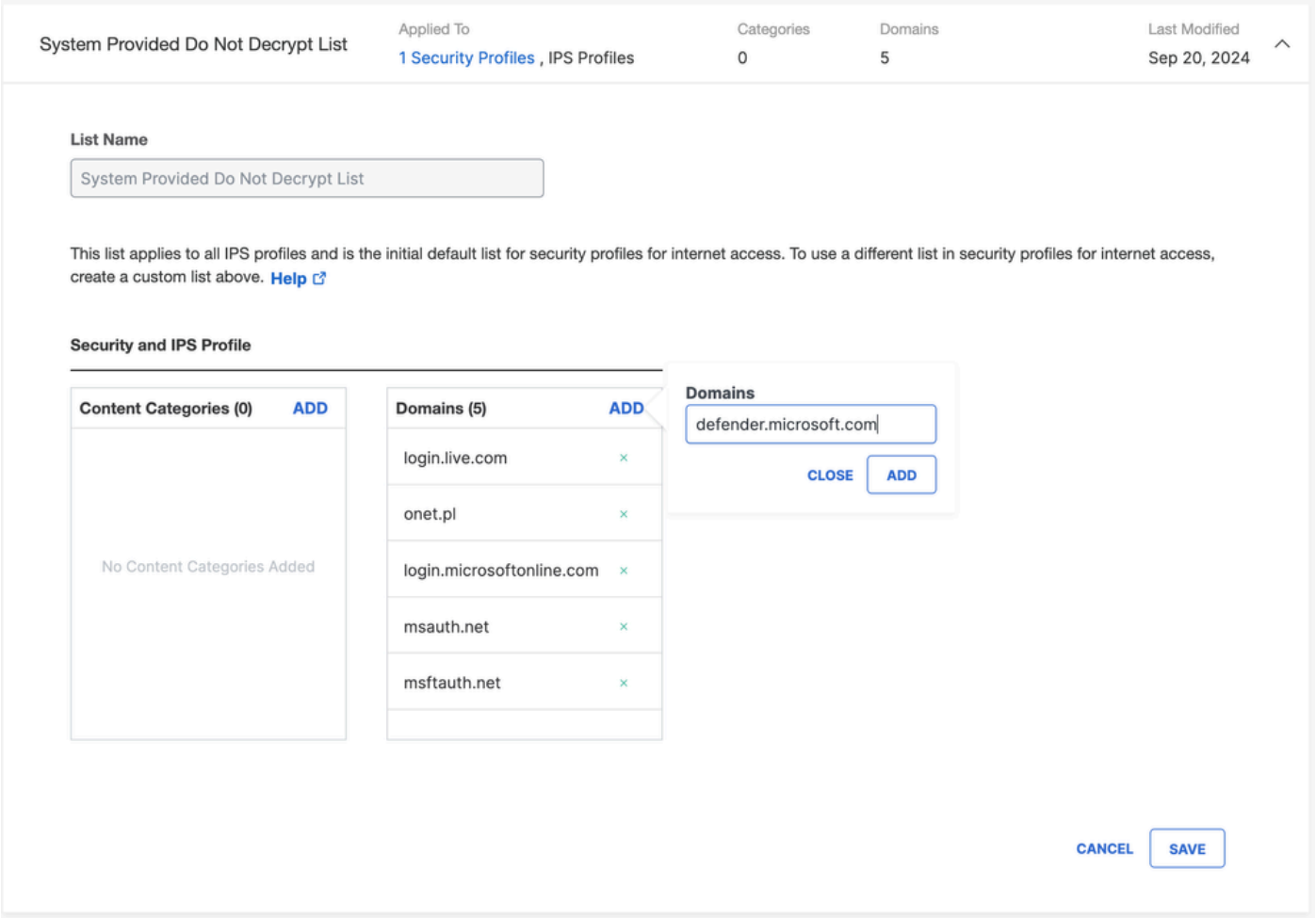
```
import requests

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)
```

Output di esempio di questo script al 31 ottobre 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
```

I domini inclusi nell'elenco possono essere aggiunti all'elenco degli elementi da non decrittografare fornito dal sistema:



È necessario aggiungere gli FQDN in Elenco di non decrittografare fornito dal sistema, per ignorare la decrittografia per IPS.
L'elenco Da non decrittografare personalizzato può essere applicato solo ai profili di sicurezza.

Soluzione

Il team di progettazione Cisco sta lavorando al miglioramento della funzionalità di compatibilità con Microsoft 365, che estrae automaticamente questo elenco e consente all'amministratore di abilitare la funzionalità di bypass da Secure Access Dashboard.

Informazioni correlate

- Guida per l'utente di Secure Access
- Supporto tecnico e download - Cisco Systems

- Risoluzione dei problemi relativi al flusso di lavoro IPS (Secure Access Decryption and Intrusion Prevention System)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).