

Criar lista Não Descriptografar efetiva para Serviços do Microsoft 365 no Acesso Seguro

Contents

[Introdução](#)

[Problema](#)

[Solução temporária](#)

[Solução](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a maneira eficaz de criar uma lista Não descriptografar para ignorar os domínios Microsoft 365 da descriptografia IPS no Secure Access.

Problema

Sabe-se que o tráfego do Microsoft 365 causa problemas quando passa por mecanismos de inspeção SSL, proxy ou IPS.

A Microsoft sugere ignorar domínios e IPs categorizados como Permitir e Otimizar, com base no artigo do KB:

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

O recurso de compatibilidade do Microsoft 365 atual no Secure Access é aplicável apenas ao tráfego passando pelo proxy.

Como resultado, quando este recurso está habilitado, nenhuma descriptografia ou inspeção é aplicada a este tráfego no nível de proxy, no entanto, as configurações globais de descriptografia de IPS ainda se aplicam.

Quando a descriptografia de IPS e o recurso de compatibilidade do Microsoft 365 estão habilitados, o tráfego destinado à Internet ainda é descriptografado nos seguintes cenários:

- RAVPN de túnel completo
- Acesso seguro à Internet via túnel VPN

Sintomas típicos de problemas causados pela descriptografia do tráfego do Microsoft 365:

- entrega de e-mail lenta via Outlook
- problemas de desempenho com o Sharepoint
- experiência de usuário ruim ao usar Equipes

Solução temporária

Os clientes devem ignorar o tráfego destinado a domínios categorizados como Permitir e Otimizar da descritografia de IPS:

Criar tal lista manualmente é uma tarefa complicada, por isso o script Python pode ser usado para puxar a lista dinamicamente da API da 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-b919946339a7"

# Get FQDNs and print them
fqdns = get_fqdns(url)
for fqdn in fqdns:
    print(fqdn)
```

Exemplo de saída deste script a partir de 31 de outubro 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

Os domínios da lista agora podem ser adicionados à lista Não descriptografar fornecida pelo sistema:

System Provided Do Not Decrypt List

Applied To: 1 Security Profiles, IPS Profiles

Categories: 0

Domains: 5

Last Modified: Sep 20, 2024

List Name: System Provided Do Not Decrypt List

This list applies to all IPS profiles and is the initial default list for security profiles for internet access. To use a different list in security profiles for internet access, create a custom list above. [Help](#)

Security and IPS Profile

Content Categories (0) [ADD](#)

No Content Categories Added

Domains (5) [ADD](#)

- login.live.com
- onet.pl
- login.microsoftonline.com
- msauth.net
- msftauth.net

Domains

defender.microsoft.com

[CLOSE](#) [ADD](#)

[CANCEL](#) [SAVE](#)

Você deve adicionar os FQDNs em Lista Não Descriptografar Fornecida pelo Sistema, para ignorar a descriptografia para IPS.

A lista Não descriptografar personalizada só pode ser aplicada a perfis de segurança.

Solução

A Equipe de Engenharia da Cisco está trabalhando no aprimoramento do recurso de compatibilidade do Microsoft 365, que extrairia essa lista automaticamente e permite que o administrador habilite a funcionalidade de desvio do Painel de Acesso Seguro.

Informações Relacionadas

- [Guia do usuário do Secure Access](#)
- [Suporte técnico e downloads – Cisco Systems](#)
- [Solucionar problemas do fluxo de trabalho do Secure Access Decryption and Intrusion Prevention System \(IPS\)](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.