

如何免除Office 365流量在思科網路安全裝置(WSA)上的身份驗證和解密

目錄

[簡介](#)

[配置步驟](#)

[1.使用Office365外部源建立自定義URL類別](#)

[2.為Office 365流量建立標識配置檔案](#)

[3.免除Office 365流量使用解密策略](#)

[參考](#)

簡介

本文描述免除Office 365流量在網路安全裝置(WSA)上進行身份驗證和解密的相關過程。 Office 365和代理存在幾個已知的相容性問題，免除Office 365流量身份驗證和解密可以解決其中的一些問題。

附註：這不是Web代理的完全繞行，而免除流量解密會阻止WSA檢查Office 365客戶端生成的加密HTTPS流量。

配置步驟

概觀:

1. 使用Office365外部源建立自定義URL類別
2. 為Office 365流量建立標識配置檔案
3. 將Office 365流量從解密策略中免除

附註：此過程需要使用動態更新的Office 365外部JSON源，該源包含與Office 365關聯的所有URL/IP地址。

附註：AsyncOS版本10.5.3及更高版本支援此饋送。

1.使用Office365外部源建立自定義URL類別

- 導航到Web Security Manager->自定義和外部URL類別
- 按一下「Add Category」
- 為類別分配名稱，將類別型別選擇為「外部即時源類別」，然後選擇Office 365 Web服務"。
- 如果要測試WSA下載Office 365 JavaScript Object Notation(JSON)源的能力，請按一下「Start Test」。
- 在底部，將「Auto Update the Feed」選項設定為「Hourly」，間隔為00:05 (每5分鐘)
- 按一下「Submit」按鈕。

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:	Office365
List Order:	1
Category Type:	External Live Feed Category
Routing Table:	Management
Feed File Location: ?	<input type="radio"/> Cisco Feed Format ? <input type="radio"/> Office 365 Feed Format ? <input checked="" type="radio"/> Office 365 Web Service ?
	Web Service URL: <input type="text" value="https://endpoints.office.com/enc"/>
	<input type="button" value="Start Test"/>
	Checking DNS resolution of feed server... Success: Resolved 'endpoints.office.com' address: 138.91.80.132 Retrieving feed content from server... Success: Downloaded and Parsed the feed file. Test completed successfully.
Excluded Sites: ?	<input type="text"/> <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small>
	<input type="button" value="Sort URLs"/> <small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small>
> Advanced	Match specific URLs by regular expressions.
Auto Update the Feed:	<input type="radio"/> Do not auto update <input checked="" type="radio"/> Hourly <input type="button" value="Every 00:05 (HH:MM)"/>

2. 為Office 365流量建立標識配置檔案

- 導航到Web安全管理器 —>標識配置檔案
- 按一下「添加標識配置檔案」
- 分配名稱，將「Identification and Authentication」設定為「Exempt from authentication/identification」。
- 按一下「Advanced」按鈕，然後按一下「URL Categories」旁邊的連結
- 查詢在上一步中建立的類別，選擇該類別，然後滾動到頁面底部並按一下「完成」按鈕。

Identity Profiles: Policy "Office365.ID": Membership by URL Categories

Advanced Membership Definition: URL Category

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

Custom and External URL Categories		
Category	Category Type	
Office365	External Feed	<input checked="" type="checkbox"/>

標識配置檔案現在應如下所示：

Identification Profiles: Office365.ID

Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> Enable Identification Profile	
Name: ?	<input type="text" value="Office365.ID"/> <small>(e.g. my IT Profile)</small>
Description:	<input type="text"/>
Insert Above:	1 (Global Profile) ▾

User Identification Method	
Identification and Authentication: ?	<input type="text" value="Exempt from authentication / Identification"/> ▾ <small>This option may not be valid if any preceding Identification Profile requires authentication on all subnets.</small>

Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	<input type="text"/> <small>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP
Advanced	<p>Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p>Proxy Ports: None Selected</p> <p>URL Categories: Office365</p> <p>User Agents: None Selected</p> <p><small>The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.</small></p>

Cancel Submit

- 按一下螢幕底部的「Submit」按鈕。

3.免除Office 365流量使用解密策略

- 導航到網路安全管理器 — >解密策略
- 按一下「Add Policy」
- 分配名稱，然後在「Identification Profiles and Users」欄位中，選擇「Select One or More Identification Profiles」選項，並從上一步中選擇您的Office 365身份。

Decryption Policy: Add Group

Policy Settings

Enable Policy

Policy Name: (e.g. my 11 policy)

Description:

Insert Above Policy:

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile	Authorized Users and Groups	<input type="button" value="Add Identification Profile"/>
<input type="button" value="Office365.ID"/> <input type="button" value="v"/>	No authentication required	<input type="button" value="x"/>

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user-agent information is unavailable for decryption policies.

Define additional group membership criteria.

- 按一下「Submit」按鈕。
- 按一下「URL Filtering」下的連結，該連結顯示「Monitor:1」
- 將Office 365類別設定為「Passthrough」，然後按一下「Submit」按鈕。

Decryption Policies: URL Filtering: Office365.DP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through <input type="button" value="v"/>	Monitor <input type="button" value="v"/>	Decrypt <input type="button" value="v"/>	Drop <input type="button" value="v"/>	Quota-Based <input type="button" value="v"/>	Time-Based <input type="button" value="v"/>
<input type="button" value="Office365"/> <input type="button" value="v"/>	External Feed	—	<input checked="" type="button" value="Select all"/>	<input type="button" value="Select all"/>	<input type="button" value="Select all"/>	<input type="button" value="Select all"/>	(Unavailable)	(Unavailable)

- 最後，按一下GUI右上角的黃色「Commit Changes」按鈕提交更改。

參考

有關如何啟用Office 365外部源和如何免除Office 365在WSA中的解密策略的更多Cisco正式文檔：

[如何在AsyncOS中啟用思科網路安全的Office 365外部源](#)