

如何在思科网络安全设备(WSA)上免除Office 365流量的身份验证和解密

目录

[简介](#)

[配置步骤](#)

[1.使用Office365外部源创建自定义URL类别](#)

[2.为Office 365流量创建标识配置文件](#)

[3.将Office 365流量从解密策略中豁免](#)

[参考](#)

简介

本文介绍在网络安全设备(WSA)上免除Office 365流量身份验证和解密的过程。 Office 365和代理存在几个已知的兼容性问题，免除Office 365流量身份验证和解密有助于解决其中一些问题。

注意：这不是Web代理的完全绕行，而且免除解密流量会阻止WSA检查由Office 365客户端生成的加密HTTPS流量。

配置步骤

概述:

1. 使用Office365**外部源**创建自定义URL类别
2. 为Office **365流量**创建标识配置文件
3. 使Office 365流量免于解密**策略**

注意：此过程需要使用动态更新的Office 365外部JSON源，该源包含与Office 365关联的所有URL/IP地址。

注意：AsyncOS版本10.5.3及11.5及以后版本支持此源。

1.使用Office365外部源创建自定义URL类别

- 导航至**Web安全管理器** —> **自定义和外部URL类别**
- 单击“**添加类别**”
- 为类别指定名称，选择类别类型“**外部实时源类别**”，然后选择“**Office 365 Web服务**”选项。
- 如果要**测试WSA**下载Office 365 JavaScript对象表示法(JSON)源的能力，请单击“**开始测试**”。
- 在底部，将“**Auto Update the Feed**”选项设置为“**Hourly**”，间隔为**00:05 (每5分钟)**
- 单击“**Submit**”按钮。

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name:

List Order:

Category Type:

Routing Table: Management

Feed File Location: Cisco Feed Format Office 365 Feed Format Office 365 Web Service

Web Service URL:

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:

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Match specific URLs by regular expressions.

Auto Update the Feed: Do not auto update Hourly

2.为Office 365流量创建标识配置文件

- 导航至Web安全管理器 —>标识配置文件
- 单击“添加标识配置文件”
- 指定名称，将“Identification and Authentication”设置为“Exempt from authentication/identification”。
- 单击“Advanced(高级)”按钮，然后单击“URL Categories (URL类别)”旁边的链接
- 查找您在上一步中创建的类别，选择该类别，然后滚动到页面底部并单击“完成”按钮。

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"/>

现在，标识配置文件应如下所示：

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) <input type="button" value="v"/>

User Identification Method	
Identification and Authentication: ?	<input type="button" value="Exempt from authentication / Identification"/> <input type="button" value="v"/> <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
<input type="button" value="v"/> 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 URL Categories: Office365 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>

- 单击屏幕底部的Submit按钮。

3. 将Office 365流量从解密策略中豁免

- 导航至Web安全管理器 —>解密策略
- 单击“添加策略”
- 指定名称，然后在“Identification Profiles and Users”字段中，选择“Select One or More Identification Profiles”选项，然后从上一步中选择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.

- 单击“Submit”(提交)按钮。
- 单击“URL Filtering”(URL过滤)下的链接，其中显示：“1”
- 将Office 365类别设置为“直通”，然后单击“提交”按钮。

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	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Office365	External Feed	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

- 最后，单击GUI右上角的黄色“Commit Changes”按钮提交更改。

参考

有关如何在WSA中启用Office 365外部源和如何使Office 365免于解密策略的更多正式思科文档：

[如何在AsyncOS中启用Office 365外部源以实现思科网络安全](#)