绕过安全Web设备中的Microsoft更新流量

目录

简介

本文档介绍在安全网络设备(SWA)中绕过Microsoft更新流量的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。

思科建议您安装以下工具：

- 物理或虚拟SWA
- 对SWA图形用户界面(GUI)的管理访问

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

Microsoft更新

Microsoft更新是Microsoft为其操作系统和软件应用程序发布的基本修补程序、安全更新和功能增强。这些更新对于维护计算机和网络设备的安全性、稳定性和性能至关重要。它们可以确保系统不受漏洞影响，修复漏洞，并将新功能或改进集成到软件中。

Microsoft更新对代理服务器（例如Cisco SWA）的影响可能很大。这些更新通常涉及下载大文件或大量小文件，这会占用代理上的大量带宽和处理资源。这可能会导致拥塞、网络性能下降和代理基础设施上的负载增加，从而可能影响整体用户体验和其他关键网络操作。

绕过来自代理的Microsoft Update流量是应对这些挑战的一种安全有效的方法。由于Microsoft更新来自受信任的Microsoft服务器，因此允许此流量绕过代理有助于降低代理服务器上的负载，而不会影响网络安全。这可以确保有效提供基本更新，同时保留代理资源以用于其他安全和内容过滤任务。但是，必须谨慎实施此类旁路配置，以维护整体网络安全和遵守组织策略。

绕过Microsoft更新

如果您考虑避免代理Microsoft更新流量，主要有两种方法

1. 旁路：这包括配置网络以重定向流量，使其永远无法到达SWA。
2. 直通：这包括将SWA配置为既不解密也不扫描Microsoft更新流量，从而使其无需检查即可通过代理。

绕过SWA中的流量

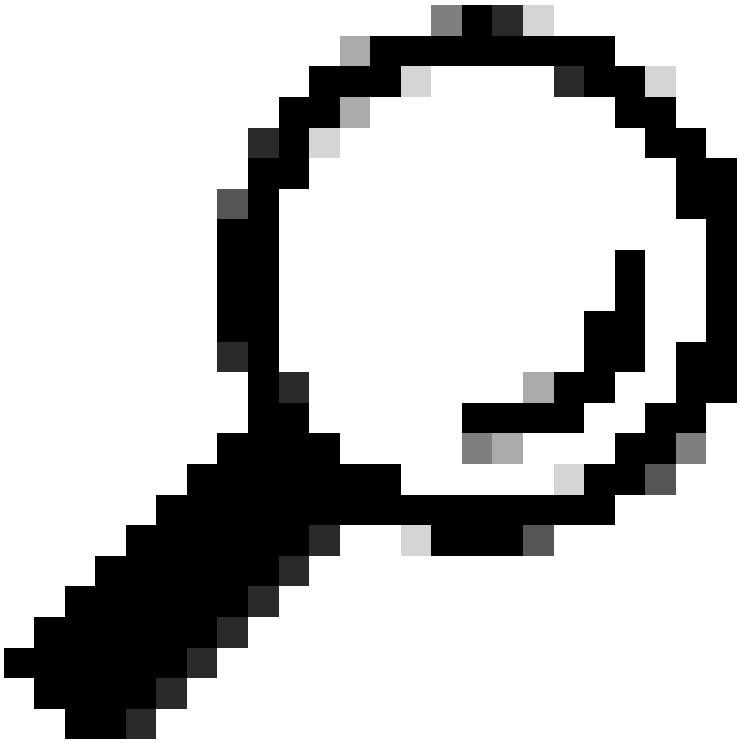
要在配备了SWA的网络中绕过Microsoft Updates流量，方法因代理部署设置而异：

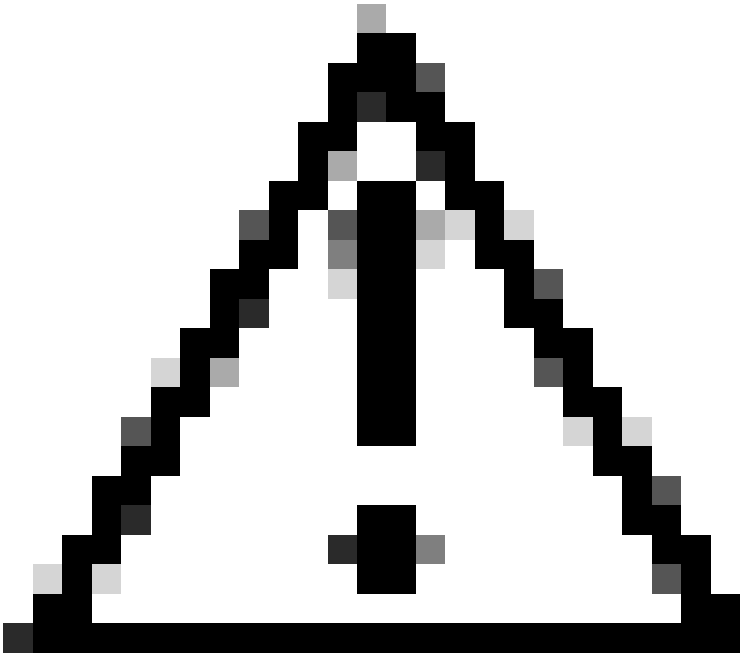
部署类型	绕过流量
透明部署	您可以在负责将流量转发到代理服务器的路由器或第4层交换机上重定向Microsoft Updates流量。
	您可以直接在SWA图形用户界面(GUI)中配置旁路设置。
显式部署	要防止Microsoft Updates流量到达SWA，必须在源配置旁路。这意味着免除客户端计算机上的相关URL，以确保流量不会重定向到SWA。

如果绕过特定流量需要大量网络重新设计且不可行，另一种方法是配置SWA以通过特定类型的流量。这可以通过将SWA设置为既不解密也不扫描指定流量，从而使其无需检查即可通过代理来实现。此方法可确保有效传送基本流量，同时将对网络性能和代理资源的影响降至最低。

传递Microsoft更新的步骤

传递Microsoft Updates流量分为四个主要阶段：

阶段	步骤
1. 为Microsoft更新URL创建自定义URL类别	第1步：从GUI中，选择网络安全管理器，然后点击自定义和外部URL类别。 第2步：点击Add Categories添加自定义URL类别。 第4步：分配唯一的CategoryName。 第5步（可选）添加说明。 第六步：从列表顺序中，选择要放在首位的第一个类别。 步骤 7.从Category 下拉列表中选择Local Custom Category。 步骤 8 在站点部分中添加Microsoft更新URL。  提示：您可以从以下链接查看Microsoft更新列表：第2步-配置WSUS | Microsoft学习

	 注意：请勿按原样复制/粘贴Microsoft文档中的URL；请将它们正确格式化为SWA格式。 有关更多信息，请访问：在安全Web设备中配置自定义URL类别-思科 步骤 9提交。
2. 创建标识配置文件，使Microsoft Updates流量免于进行身份验证	第10步：从GUI中，选择网络安全管理器，然后点击标识配置文件。 第11步：点击Add Profile添加配置文件。 第12步：使用Enable Identification Profile复选框启用此配置文件，或快速禁用此配置文件而不将其删除。 第13步：分配唯一的profileName。 第14步（可选）添加说明。 第15步：从上述插入(Insert)下拉列表中，选择此配置文件在表中的显示位置。 步骤 16 在用户标识方法部分中，选择免除身份验证/标识。 第17步：在Define Members by Subnet中，如果要为某些特定用户传递Microsoft流量，请输入适用的IP地址或子网，或者将此字段留空以包括所有IP地址。 步骤 18.从高级部分中，选择自定义URL类别。 步骤 19.添加为Microsoft更新创建的自定义URL类别。 步骤 20.单击完成。

	步骤 21. 提交。
3. 创建解密策略以传递Microsoft更新流量	第22步：从GUI，选择网络安全管理器，然后点击解密策略。 步骤 23. 单击Add Policy添加解密策略。 第24步：使用Enable Policy复选框启用此策略。 第25步：分配唯一的PolicyName。 第26步（可选）添加说明。 第27步：从Insert Above Policy下拉列表中，选择第一个策略。 第28步：从Identification Profiles and Users中，选择您在前面的步骤中创建的标识配置文件。 步骤 29提交。 第30步：在Decryption Policies页面的URL Filtering下，点击与此新解密策略关联的链接。 第32步：选择Passthroughas作为Microsoft更新URL类别的操作。 步骤 32提交。
4. 创建允许Microsoft更新流量的访问策略	第33步：从GUI，选择网络安全管理器，然后点击访问策略。 步骤 34 单击Add Policy添加访问策略。 第35步：使用Enable Policy复选框启用此策略。 第36步：分配唯一的PolicyName。 第37步（可选）添加说明。 第38步：从Insert Above Policy下拉列表中，选择第一个策略。 第39步：从Identification Profiles and Users中，选择您在前面的步骤中创建的标识配置文件。 步骤 40提交。 步骤 9 在访问策略页上的URL过滤下，点击与此新访问策略相关联的链接 第10步：选择允许(Select)是为Microsoft更新创建的自定义URL类别的操作。 步骤 11提交。

	步骤 12提交更改。

相关信息

- 思科安全Web设备AsyncOS 15.0用户指南- GD（通用部署）-对最终用户进行策略应用分类[思科安全Web设备] -思科
- 在安全网络设备中配置自定义URL类别-思科
- 如何使Office 365流量免于在思科网络安全设备(WSA)上进行身份验证和解密-思科
- 使用安全Web设备最佳实践-思科
- 绕过安全Web设备中的身份验证-思科

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。