绕过安全Web设备中的Microsoft更新流量

目录

简介

先决条件

- 要求
- 使用的组件

Microsoft更新

绕过Microsoft更新

- 绕过SWA中的流量

传递Microsoft更新的步骤

相关内容

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补丁、安全更新和功能增强功能。这些更新对维护计算机和网络设备的安全、稳定性和性能至关重要。它们可确保系统免受漏洞攻击，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型文件或大量较小的文件，这可能会占用大量带宽并在代理上处理资源。这可能导致拥塞、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流量是管理这些挑战的一种安全有效的方式。由于Microsoft更新源自受信任的Microsoft服务器，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。这可确保有效交付基本更新，同时为其他安全和内容过滤任务保留代理资源。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

如果您正在考虑避免代理Microsoft Updates流量，主要有两种方法：

1. 旁路：这涉及配置网络以重定向流量，使其永远无法到达SWA。
2. 直通：这涉及将SWA配置为既不解密也不扫描Microsoft更新流量，允许它通过代理而不进行检查。

绕过SWA中的流量

要在配备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	旁路流量
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	要阻止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，允许它通过代理而不进行检查来实现。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

配置Microsoft Update流量的直通分为四个主要阶段:

阶段	步骤
1.为Microsoft更新URL创建自定义URL类别	步骤1.在GUI中，选择Web Security Manager，然后单击Custom and External URL Categories。 步骤2.单击Add Category以添加自定义URL类别。 步骤3.分配唯一的类别名称。 第4步：（可选）添加说明。 第5步：从列表顺序中选择要放在首位的第一个类别。 第6步：从Category Type下拉列表中，选择Local Custom Category。 步骤7.在“站点”部分添加Microsoft更新URL。 提示：您可以从以下位置检查Microsoft更新列表：第2步 — 配置WSUS | Microsoft学习 警告：不要复制/粘贴Microsoft文档中的URL;将它们正确格式化为SWA格式。有关详细信息，请访问：在安全Web设备中配置自定义URL类别 — 思科

	步骤8.提交。
2.创建标识配置文件，以免除Microsoft更新流量进行身份验证	第9步：从GUI中，选择Web Security Manager，然后单击Identification Profiles。 步骤10.单击Add Profile以添加配置文件。 步骤11.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。 步骤12.分配唯一的配置文件名称。 第13步（可选）添加说明。 步骤14.从Insert Above下拉列表中，选择此配置文件在表中的显示位置。 步骤15.在User Identification Method部分，选择Exempt from authentication/identication。 步骤16.在按子网定义成员中，如果要为某些特定用户传递通过Microsoft流量，请输入适用的IP地址或子网，否则将此字段留空以包括所有IP地址。 第17步：从Advanced部分，选择Custom URL Categories。 步骤18.添加为Microsoft更新创建的自定义URL类别。 步骤19.点击完成。 步骤20.提交。
3.创建解密策略以传递Microsoft更新流量	步骤21.从GUI中，选择Web Security Manager，然后单击Decryption Policy。 第22步：点击Add Policy以添加解密策略。 步骤23.使用Enable Policy复选框启用此策略。 步骤24.分配唯一的策略名称。 第25步（可选）添加说明。 第26步：从Insert Above Policy下拉列表中，选择第一个策略。 步骤27.从标识配置文件和用户中，选择您在前面的步骤中创建的标识配置文件。 步骤28.提交。 第29步：在Decryption Policies页面的URL Filtering下，点击与此新解密策略关联的链接。 步骤30.选择Passthrough作为Microsoft Updates URL类别的操作。

	步骤31.提交。
4.创建允许Microsoft更新流量的访问策略	步骤32.从GUI中，选择Web Security Manager，然后单击Access Policy。 第33步：单击Add Policy以添加访问策略。 步骤34.使用Enable Policy复选框启用此策略。 步骤35.分配唯一的策略名称。 第36步（可选）添加说明。 第37步：从Insert Above Policy下拉列表中，选择第一个策略。 步骤38.从标识配置文件和用户中，选择您在前面的步骤中创建的标识配置文件。 步骤39.提交。 步骤40.在Access Policies页面的URL Filtering下，单击与此新访问策略关联的链接 第41步：选择Allow作为为Microsoft更新创建的自定义URL类别的操作。 步骤42.提交。 步骤43.提交更改。

相关内容

- 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Web设备中配置自定义URL类别 — 思科
- 如何免除Office 365流量在思科网络安全设备(WSA)上的身份验证和解密 — 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）。