为SWA中的Microsoft Update流量配置范围请求

目录

简介

先决条件

- 要求
- 使用的组件

范围请求

代理环境中的范围请求

启用Microsoft更新的范围请求

为Microsoft更新启用范围请求的步骤

- 步骤1.启用范围请求
- 步骤2.为Microsoft更新URL创建自定义URL类别
- 步骤3.（可选）创建标识配置文件以免除Microsoft更新流量进行身份验证
- 步骤4.（可选）创建解密策略以通过Microsoft更新流量
- 步骤5.创建访问策略以允许Microsoft更新流量的范围请求

修改访问日志

确认

相关内容

简介

本文档介绍允许Microsoft更新流量使用安全Web设备(SWA)中的范围请求的步骤。

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。

范围请求

范围请求是HTTP协议的一项功能，它允许客户端（如Web浏览器或下载管理器）仅从服务器请求文件的特定部分，而不是一次下载整个文件。这对于恢复中断的下载、流媒体或高效地访问大型文件非常有用。客户端在HTTP请求的Range报头中指定所需的字节范围，如果服务器支持范围请求，则服务器以206 Partial Content状态代码进行响应，仅传送请求的文件段。

此机制可在多个场景中增强性能和用户体验。例如，在视频流中，范围请求允许播放器仅获取播放所需的数据段，这降低了带宽使用率，提高了响应速度。同样，下载管理器使用范围请求将文件拆分为数据块并并行下载，从而加速了整个过程。范围请求在缓存和代理系统中也起着关键作用，支持部分更新和减少冗余数据传输。

代理环境中的范围请求

在代理环境中，范围请求在优化带宽使用率和提高内容交付效率方面起着关键作用。当启用范围请求时，代理服务器只能从源服务器获取所需的字节段，并在本地缓存这些字节段。这允许客户端请求部分内容（例如视频或大型文件的特定片段），并从代理缓存快速接收该内容（如果可用）。它还支持并行下载和恢复功能，这在带宽有限或延迟较高的环境中很有用。

但是，当范围请求被禁用时，代理必须从源服务器获取整个文件，即使客户端只需要一小部分。这会导致不必要的数据传输、代理服务器和源服务器上的负载增加，以及客户端的响应时间变慢。它还会阻止有效的缓存策略，因为代理无法存储或提供部分内容。在流传输场景中，这会导致缓冲延迟或用户体验下降。出于安全或策略原因，可以禁用范围请求，但这样做通常会牺牲性能和灵活性。

例如，假设有10个用户尝试通过代理服务器从100 MB的文件中分别下载1 MB的流量。

已禁用范围请求：

- 禁用范围请求时，代理无法仅获取每个用户所需的1 MB数据段。相反，它必须从源服务器为每个请求下载完整的100 MB文件。这会导致：
  - 从源到代理的总流量：10 × 100 MB = 1000 MB(1 GB)
  - 客户端只使用10 MB的数据。
  - 剩下的990 MB被浪费，导致带宽使用效率低下，并且增加了代理服务器和源服务器上的负载。

已启用范围请求：

- 启用范围请求后，代理仅为每个用户获取请求的1 MB:
  - 从源到代理的总流量：10 × 1 MB = 10 MB
  - 代理可以缓存这些数据段，并在需要时将其提供给其他用户。
  - 这可以减少90倍的流量，加快响应速度，显着提高资源利用率。

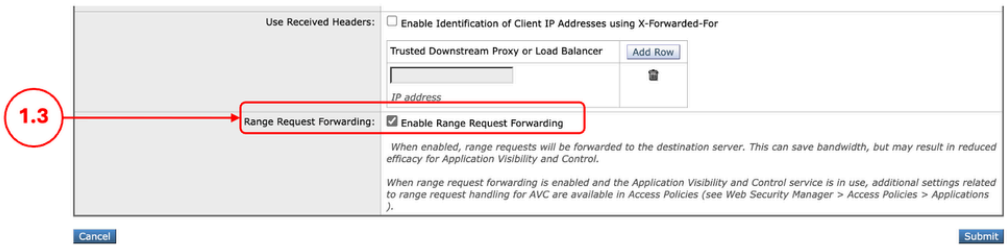
启用Microsoft更新的范围请求

尽管范围请求增强了性能，但它会阻碍SWA环境中的安全扫描和策略实施，因为这些系统无法完全检查部分内容。本文仅将范围请求使用限于Microsoft Update流量。

⚠ 注意：启用范围请求转发可能会干扰基于策略的应用可视性与可控性(AVC)效率，并可能危害安全性。

为Microsoft更新启用范围请求的步骤

步骤1.启用范围请求	第1.1步：在GUI中，点击Security Services并选择Web Proxy。 第1.2步。单击Edit Settings。 第1.3步：选中复选框Enable Range Request Forwarding。 第1.4步。单击提交。

<table>
<tr><td></td><td>

映像 — 启用范围请求转发</td></tr>
<tr><td>步骤2.为Microsoft更新URL创建自定义URL类别</td><td>第2.1步：从GUI中，选择Web Security Manager，然后点击自定义和外部URL类别。
第2.2步：单击Add Category以添加自定义URL类别。
步骤2.3.分配唯一的类别名称。
第2.4步（可选）添加说明。

第2.5步：从列表顺序中选择要放在首位的第一个类别。

第2.6步：从Category Type下拉列表中，选择Local Custom Category。

第2.7步：在“站点”部分添加Microsoft更新URL。

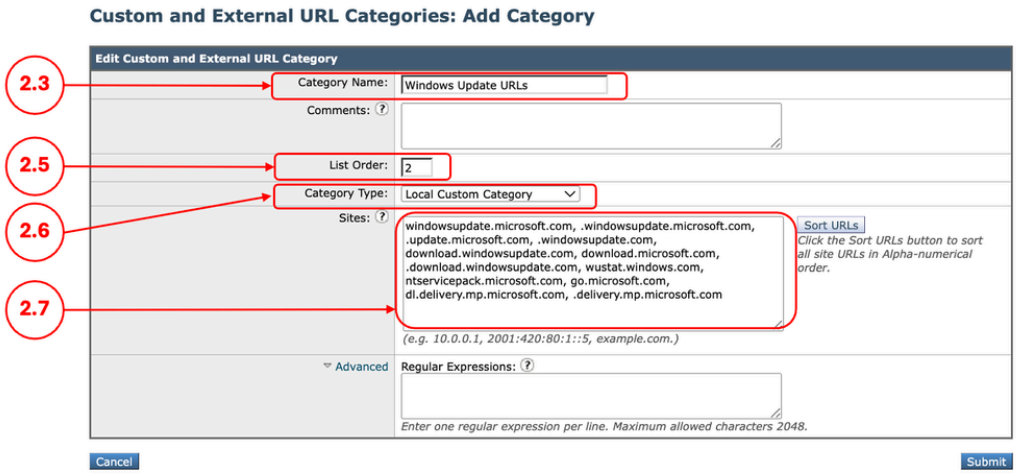
提示：您可以通过此链接检查Microsoft更新列表：第2步 — 配置WSUS | Microsoft学习

警告：请勿复制/粘贴Microsoft文档中所列出的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

以下是一个示例：

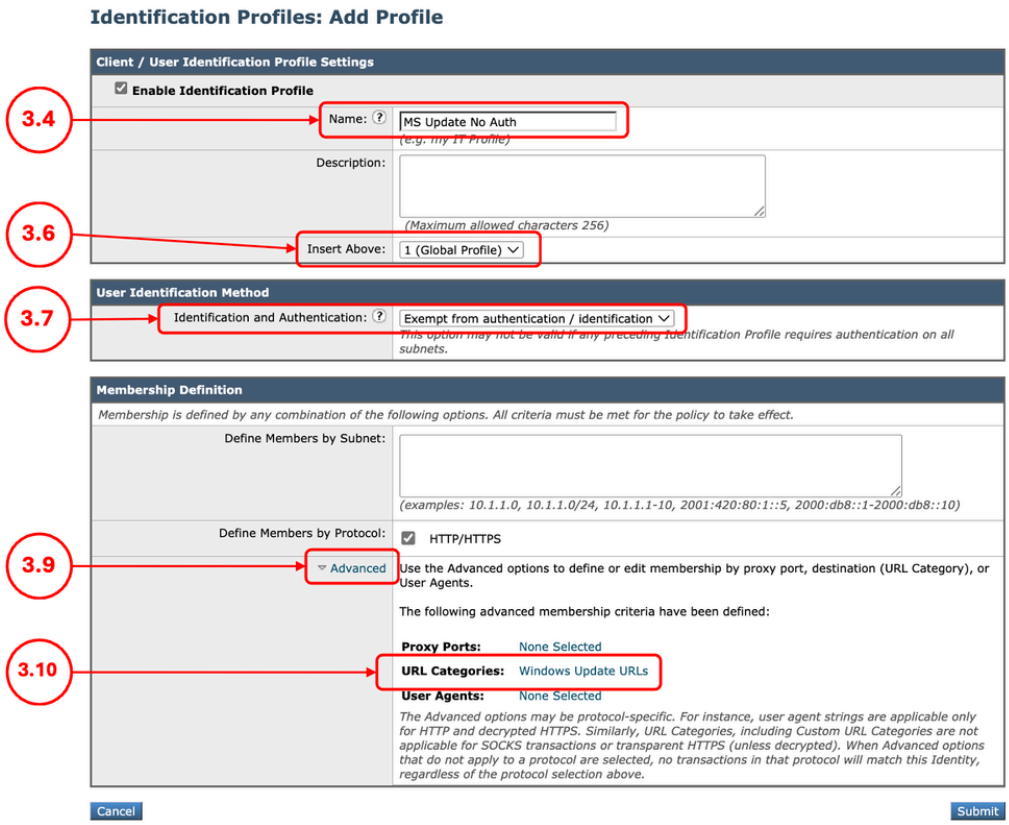
http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com

第2.8步。单击提交。</td></tr>
</table>



图像 — 创建自定义URL类别

步骤3.（可选）创建标识配置文件以免除Microsoft更新流量进行身份验证 注意：此操作是为了减少SWA上用于Microsoft更新的流量的身份验证负载。	第3.1步：从GUI中选择Web Security Manager，然后单击Identification Profiles。 第3.2步：单击Add Profile以添加配置文件。 步骤3.3.确保选中Enable Identification Profile复选框。 步骤3.4.分配唯一的配置文件名称。 第3.5步（可选）添加说明。 第3.6步：从Insert Above下拉列表中，选择此配置文件在表中的显示位置。 第3.7步：在User Identification Method部分，选择Exempt from authentication/identication。 第3.8步在按子网定义成员中，如果要通过特定用户的Microsoft流量，请输入适用的IP地址或子网，或将此字段留空以包括所有IP地址。 第3.9步：从高级部分，选择自定义URL类别。 第3.10步。添加为Microsoft更新创建的自定义URL类别。 第3.11步。单击完成。 步骤3.12.单击提交。



图像 — 创建标识配置文件

步骤4.（可选）创建解密策略以通过Microsoft更新流量

注意：Microsoft更新使用HTTP和HTTPS流量传递更新链接。此操作可降低SWA上的解密负载。

第4.1步：从GUI中选择Web Security Manager，然后单击Decryption Policy。

第4.2步：单击Add Policy以添加解密策略。

步骤4.3.分配唯一的策略名称。
第4.4步（可选）添加说明。
第4.5步：从Insert Above Policy下拉列表中，选择第一个策略。

第4.6步：从Identification Profiles和Users中，选择Select One or more Identification Profiles。

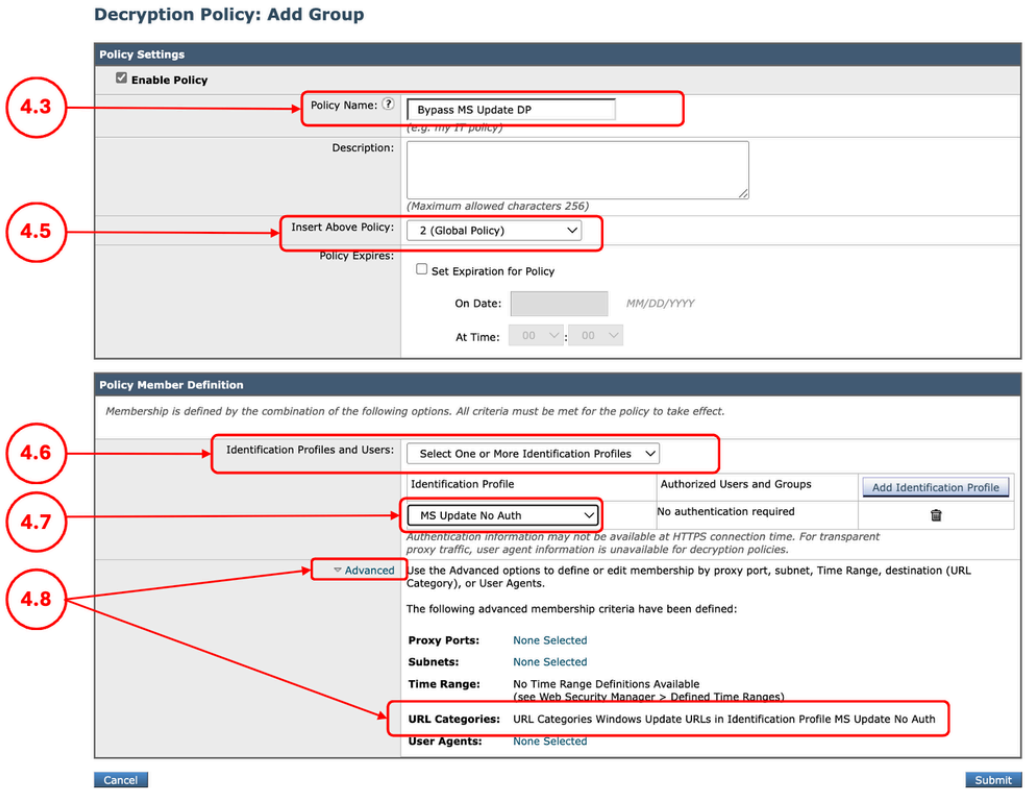
第4.7步。选择您在第3步中创建的标识配置文件，然后跳至第4.11步。

第4.8步：如果没有为Windows更新创建ID配置文件，请从Advanced部分选择Custom URL Categories。

第4.9步添加为第2步中的Microsoft更新创建的自定义URL类别。

第4.10步。单击完成。

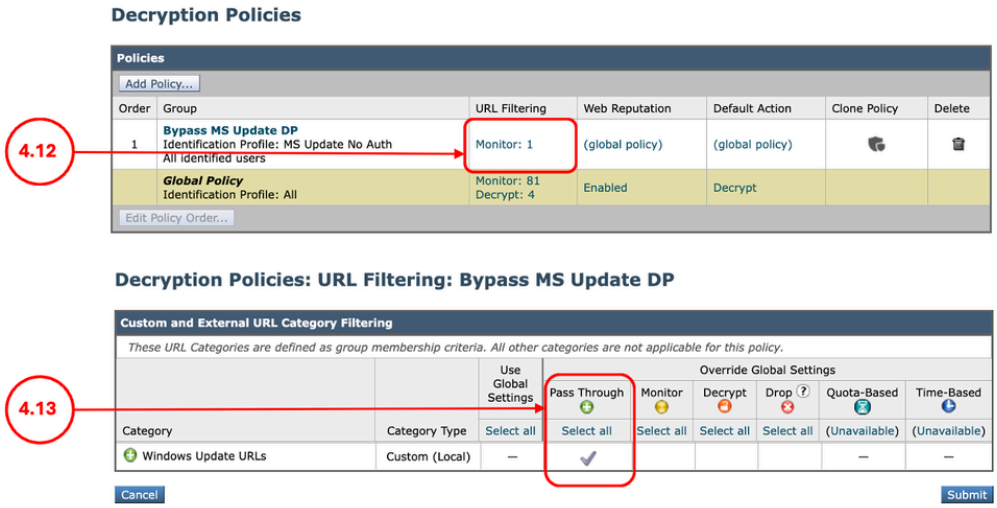
第4.11步。单击提交。



映像 — 创建解密策略

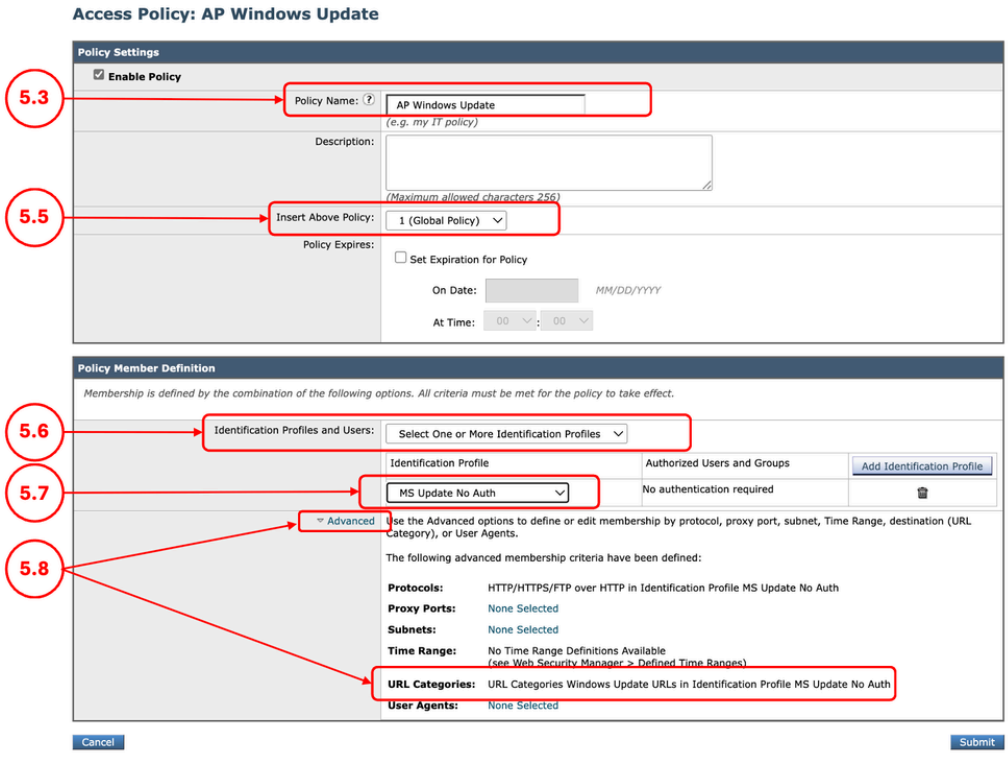
第4.12步：在URL过滤下的解密策略页面中，点击与新解密策略相关的链接。

第4.13步。选择Pass Through作为Microsoft Updates URL类别的操作。

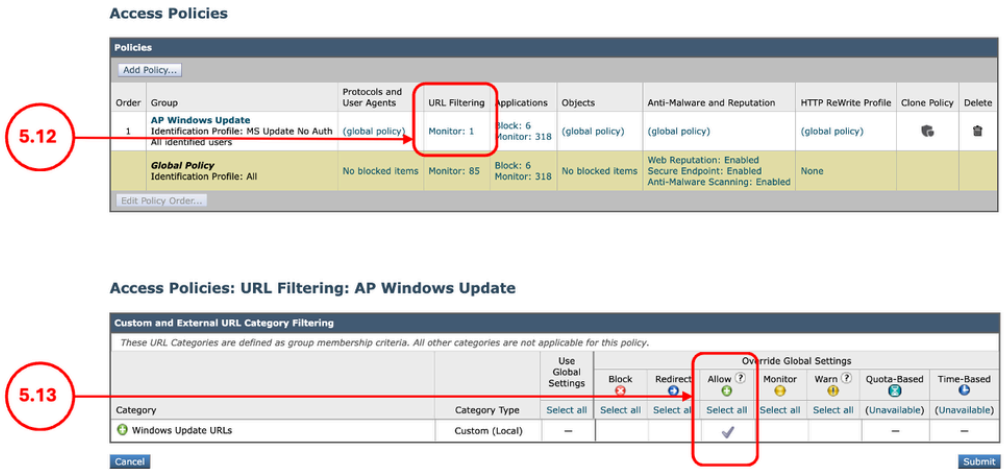


图像 — 为URL类别设置操作传递

第4.14步。单击提交。

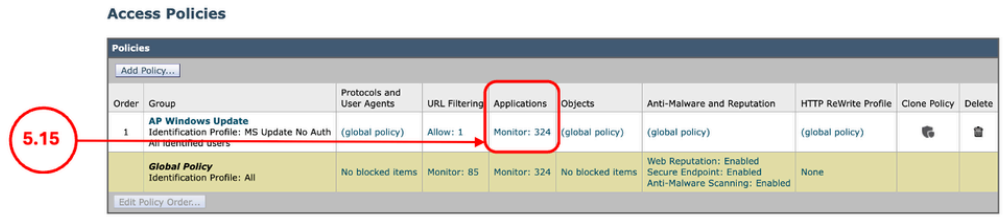
步骤5.创建访问策略以允许Microsoft更新流量的范围请求	第5.1步：在GUI中，点击Web Security Manager并选择Access Policy。 第5.2步：单击Add Policy以添加访问策略。 步骤5.3.分配唯一的策略名称。 第5.4步（可选）添加说明。 第5.5步：从Insert Above Policy下拉列表中，选择第一个策略。 第5.6步：从Identification Profiles和Users中，选择Select One or more Identification Profiles。 步骤5.7.选择您在第3步中创建的标识配置文件，然后跳至步骤5.11。 第5.8步：如果您未从Advanced（高级）部分为Windows Update创建ID配置文件，请选择Custom URL Categories（自定义URL类别）。 第5.9步添加为第2步中的Microsoft更新创建的自定义URL类别。 第5.10步。单击完成。 步骤5.11.提交。  映像 — 创建访问策略 第5.12步：在URL过滤(URL Filtering)下的Access Policies（访问策略）页面，点击与新访问策略相关的链接。 第5.13步：选择允许作为为Microsoft更新创建的自定义URL类别的操作。

第5.14步。单击提交。



图像 — 设置Action Allow for the URL Category

第5.15步：在Applications下的Access Policies页面上，点击与新访问策略相关的链接。

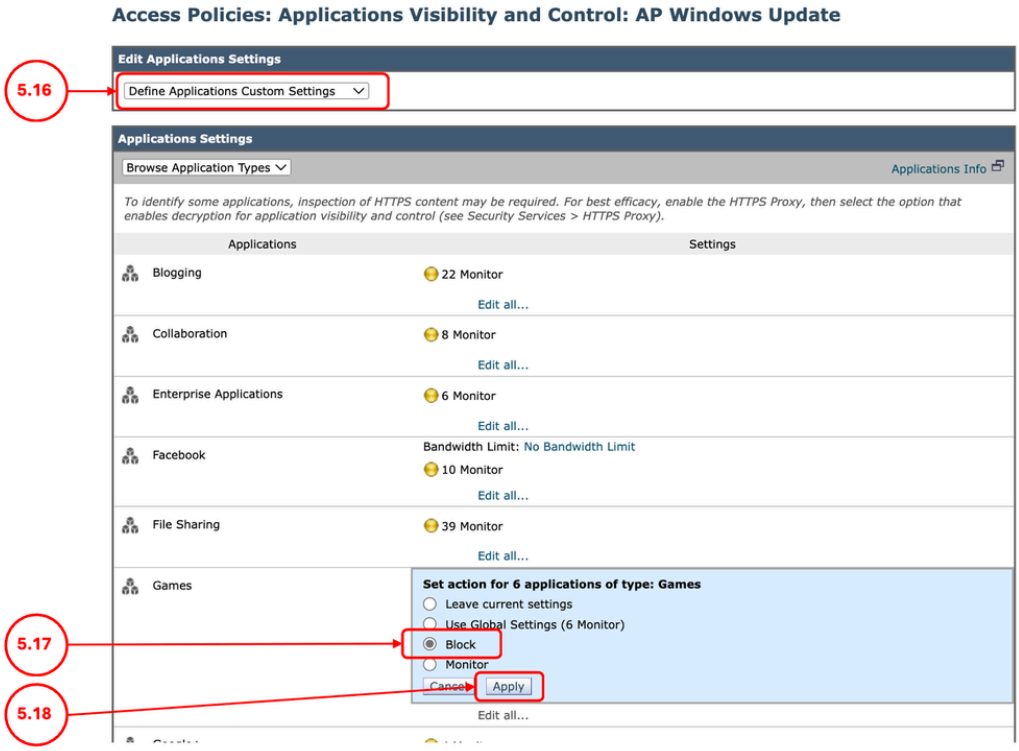


图像 — 编辑应用可视性与可控性

第5.16步：在Edit Applications Settings部分，选择Define Applications Custom Settings。

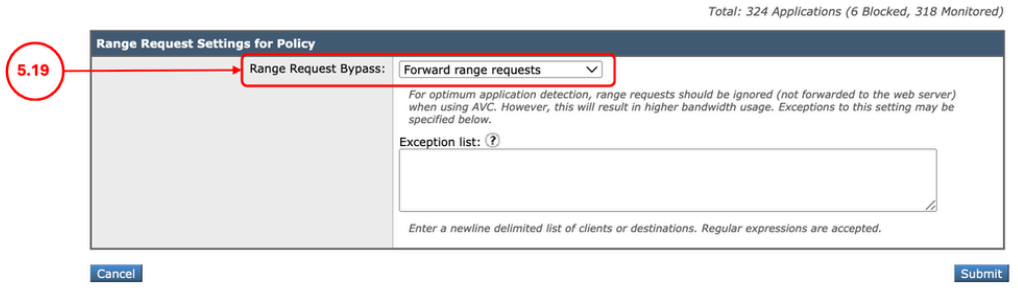
第5.17步：在Applications Settings部分，单击Edit all for Games应用，并将操作设置为Block。

第5.18步。单击应用。



图像 — 将一个应用操作设置为阻止

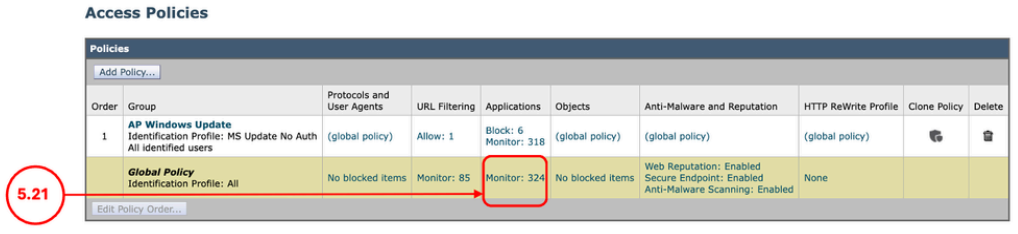
步骤5.19.向下滚动到Range Request Settings for Policy部分，确保已选中Forward range requests。



图像 — 策略的范围请求设置

第5.20步。单击提交。

第5.21步：在Applications下的Access Policies页上，点击与Global Policy关联的链接。



	映像 — 默认访问策略应用设置 步骤5.22.向下滚动到Range Request Settings for Policy部分，确保选中Do Not Forward range requests部分。 步骤5.23.提交更改。

修改访问日志

要进一步了解访问日志中的范围请求，您可以添加以下自定义字段：

[客户端范围= %<范围：]	显示客户端请求的范围（字节）
[content= %>Content-Length:]	显示下载的内容大小（字节）

有关向SWA访问日志添加自定义字段的详细信息，请参阅访问日志中的配置性能参数指南。

确认

运行此CURL命令以向SWA发送范围请求：

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

从CURL的输出中可以看到HTTP响应为HTTP/1.1 206:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

从访问日志中，您可以看到操作为TCP_CLIENT_REFRESH_MISS/206:

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

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
- 如何在思科网络安全设备(WSA)上免除Office 365流量身份验证和解密 — 思科
- 配置访问日志中的性能参数
- 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）。