阻止安全网络设备中的流量

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[阻止流量](#)

- [按源阻止的原因](#)
- [按目标阻止的原因](#)

[阻止流量的步骤](#)

[在透明代理部署中使用正则表达式阻止站点](#)

[相关内容](#)

简介

本文档介绍在安全网络设备(SWA)中阻止流量的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。

Cisco 建议您：

- 已安装物理或虚拟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。

阻止流量

在SWA中阻止流量是确保网络安全、保持对内部策略的合规性以及防止恶意活动的关键步骤。以下是阻止流量的一些常见原因：

按源阻止的原因

- 单个或多个用户泛洪：当一个或多个用户产生过多流量时，网络就会被淹没，从而导致性能下降和潜在的服务中断。
- 由应用程序（用户代理）进行的不受信任的资源访问：某些应用程序可能会尝试访问不受信任或可能有害的资源。阻止这些用户代理有助于防止安全漏洞和数据泄露。
- 限制特定IP范围的Internet访问：某些IP地址或范围可能需要限制访问Internet，这是出于安全策略或为了防止未经授权的使用。
- 可疑流量行为：必须阻止可能表明恶意活动或安全威胁的异常模式或行为的流量，以保护网络。

按目标阻止的原因

- 符合公司内部政策：企业或机构通常有限制访问某些网站或在线资源的策略，以确保工作效率和遵守法律或法规要求。
- 不受信任的站点：阻止对被认为不可信或可能有害的网站的访问有助于保护用户免受网络钓鱼、恶意软件和其他在线威胁的侵害。
- 恶意行为：必须阻止已知托管恶意内容或从事有害活动的站点，以防止安全事故和数据泄露。

阻止流量的步骤

一般来说，阻止SWA中的流量主要有三个阶段：

- 为用户创建标识配置文件。
- 阻止解密策略中的HTTPS流量。
- 阻止访问策略中的HTTP流量。

阶段	阻止特定用户访问任何网站	阻止特定用户访问某些网站

自定义URL类别	不能应用.	为您计划阻止其访问的站点创建自定义URL类别。 有关更多信息，请访问： 在安全Web设备 — 思科中配置自定义URL类别。
标识配置文件	第1步：从GUI中，选择Web Security Manager，然后选择Identification Profiles。 步骤2.选择Add Profile以添加配置文件。 步骤3.使用Enable Identification Profile复选框启用此配置文件，或快速禁用它而不将其删除。 步骤4.分配唯一的配置文件名称。 第5步：（可选）添加说明。 步骤6.从Insert Above下拉列表中，选择此配置文件在表中的显示位置。 第7步：在User Identification Method部分，选择Exempt from authentication/identication。 第8步：在按子网定义成员中，输入应用此标识配置文件的IP地址或子网。您可以使用IP地址、无类域间路由(CIDR)块和子网。	注意：要阻止所有用户访问某些网站，无需创建单独的ID配置文件。这可以通过全局解密/访问策略进行有效管理。 第1步：从GUI中，选择Web Security Manager，然后选择Identification Profiles。 步骤2.选择Add Profile以添加配置文件。 步骤3.使用Enable Identification Profile复选框启用此配置文件，或快速禁用它而不将其删除。 步骤4.分配唯一的配置文件名称。 第5步：（可选）添加说明。 步骤6.从Insert Above下拉列表中，选择此配置文件在表中的显示位置。 第7步：在User Identification Method部分，选择Exempt from authentication/identication。 第8步：在按子网定义成员中，输入应用此标识配置文件的IP地址或子网。您可以使用IP地址、无类域间路由(CIDR)块和子网。 步骤9.选择Advanced并添加要阻止访问的URL类别。
解密策略	第1步：从GUI中，选择Web Security Manager，然后选择Decryption Policy。 步骤2.选择Add Policy以添加解密策略。	第1步：从GUI中，选择Web Security Manager，然后选择Decryption Policy。 步骤2.选择Add Policy以添加解密策略。

<table>
<tr>
<td></td>
<td>步骤3.使用Enable Policy复选框启用此策略。
步骤4.分配唯一的策略名称。
第5步：（可选）添加说明。
第6步：从Insert Above Policy下拉列表中，选择第一个策略。

第7步：从Identification Profiles and Users，选择您在前面的步骤中创建的标识配置文件。

步骤8.提交。

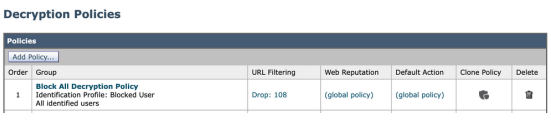
第9步：在Decryption Policies页面的URL Filtering下，点击与此新解密策略关联的链接。

提示：假设您正在阻止所有URL类别，可以通过删除自定义URL类别并仅使用预定义的URL类别来优化策略。这可避免将URL与自定义URL类别进行匹配的额外步骤，从而减少SWA上的处理负载。

步骤10.选择Drop作为每个URL类别的操作。

第11步：在同一页面上，向下滚动到Uncategorized URLs，然后从下拉列表中选择Drop。

步骤12.提交。



图像 — 用于阻止特定用户的所有网站的解密策略</td>
<td>步骤3.使用Enable Policy复选框启用此策略。
步骤4.分配唯一的策略名称。
第5步：（可选）添加说明。
第6步：从Insert Above Policy下拉列表中，选择第一个策略。

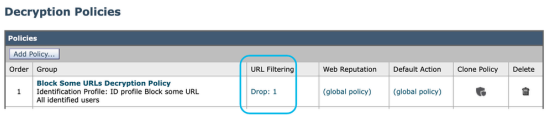
第7步：从Identification Profiles and Users，选择您在前面的步骤中创建的标识配置文件。

步骤8.提交。

第9步：在Decryption Policies页面，在URL Filtering下，点击与此新解密策略关联的链接。

第10步：选择Drop作为为阻止的网站创建的Custom URL类别的操作。

步骤11.单击提交。



图像 — 阻止解密策略中的某些URL</td>
</tr>
<tr>
<td>访问策略</td>
<td>第1步：在GUI中，选择Web Security Manager，然后单击Access Policy。

步骤2.单击Add Policy以添加访问策略。</td>
<td>第1步：在GUI中，选择Web Security Manager，然后单击Access Policy。

步骤2.单击Add Policy以添加访问策略。</td>
</tr>
</table>

步骤3.使用Enable Policy复选框启用此策略。
步骤4.分配唯一的策略名称。
第5步：（可选）添加说明。
第6步：从Insert Above Policy下拉列表中，选择第一个策略。

第7步：从Identification Profiles and Users，选择您在前面的步骤中创建的标识配置文件。

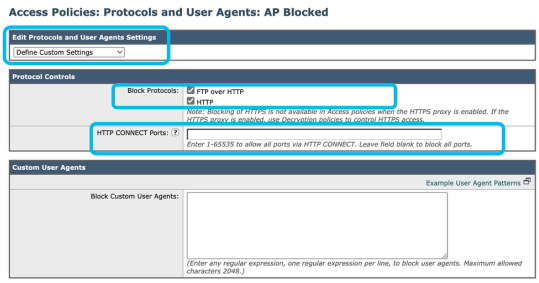
步骤8.提交。

第9步：在Access Policies页面的Protocols and User Agents下，点击与此新访问策略关联的链接。

第10步：在Edit Protocols and User Agents Settings 下拉列表中，选择Define Custom Settings。

第11步：在Block Protocols中，选中FTP over HTTP和HTTP的复选框。

步骤12.在HTTP CONNECT端口中，删除每个端口号以阻塞所有端口。



映像 — 访问策略中的阻止协议和连接端口

步骤13.提交。

第14步。（可选）在Access Policies页的URL Filtering下，点击与此新访问策略关联的链接，并选择Block作为每个URL类别的操作，然后选择Uncategorized URLsSubmit。

提示：假设您正在阻止所有URL类别，可以通过删除自定

步骤3.使用Enable Policy复选框启用此策略。
步骤4.分配唯一的策略名称。
第5步：（可选）添加说明。
第6步：从Insert Above Policy下拉列表中，选择第一个策略。

第7步：从Identification Profiles and Users，选择您在前面的步骤中创建的标识配置文件。

步骤8.提交。

第9步：在Access Policies页上，在URL Filtering下，点击与此新访问策略关联的链接

步骤10.选择Block作为为阻止的网站创建的Custom URL类别的操作操作。

步骤11.点击提交。

步骤12.提交更改。



图像 — 阻止访问策略中的某些URL

	义URL类别并仅使用预定义的URL类别来优化策略。这可避免将URL与自定义URL类别进行匹配的额外步骤，从而减少SWA上的处理负载。	
	步骤15.提交更改。  映像 — 用于阻止所有站点的访问策略	

警告：在透明代理部署中，SWA无法读取HTTPS流量的用户代理或完整URL，除非流量已解密。因此，如果使用用户代理配置标识配置文件或使用正则表达式配置自定义URL类别，此流量将无法与标识配置文件匹配。

在透明代理部署中使用正则表达式阻止站点

在透明代理部署中，如果计划阻止具有正则表达式条件的自定义URL类别（例如，阻止访问某些YouTube通道），可以使用以下步骤：

步骤1.为主站点创建自定义URL类别。(在本例中：YouTube.com）。

第2步：创建解密策略，分配此自定义URL类别并将操作设置为解密。

步骤3.创建访问策略，使用正则表达式分配自定义URL类别（在本例中为YouTube通道分配自定义URL类别），并将操作设置为“阻止”。

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

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）。