阻止安全Web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

相关信息

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)的管理权限。

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、保持内部策略合规性和防范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：当一个或多个用户生成过多流量时，可能会使网络不堪重负，导致性能下降和潜在的服务中断。
- 不受信任的资源访问（按应用程序[用户代理]）：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漏。
- 限制特定IP范围的Internet访问：由于安全策略或防止未经授权使用，可能需要限制某些IP地址或范围访问Internet。
- 可疑流量行为：必须阻止表现出异常模式或行为可能表明存在恶意活动或安全威胁的流量，以保护网络。

按目标阻止的原因

- 遵守公司内部政策：企业或机构通常制定政策，限制对某些网站或在线资源的访问，以确保工作效率和遵守法律或法规要求。
- 不可信站点：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参与有害活动的网站，以防止安全事故和数据泄露。

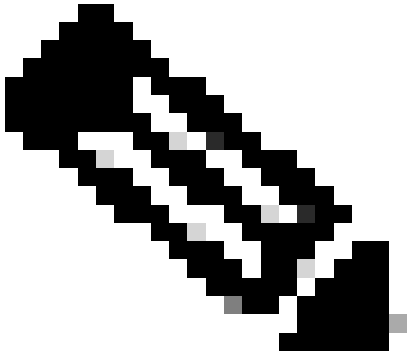
.

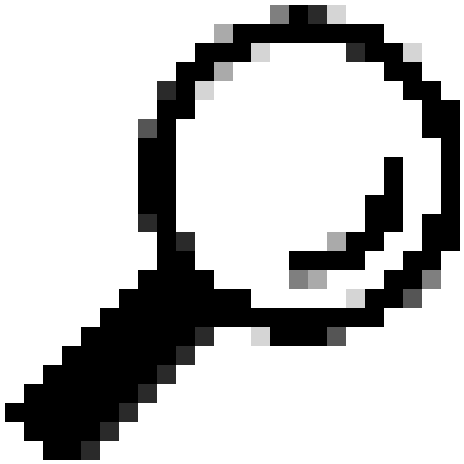
阻止流量的步骤

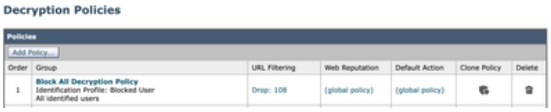
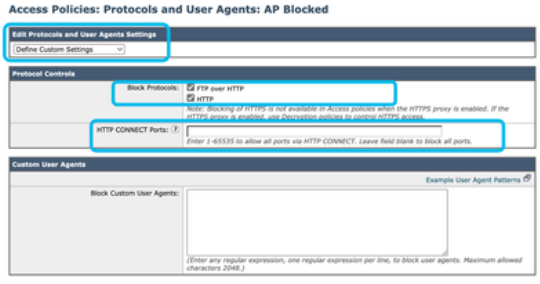
一般来说，阻止SWA中的流量有3个主要阶段：

- 创建用户的标识配置文件。
- 在解密策略中阻止HTTPS流量。
- 在访问策略中阻止HTTP流量。

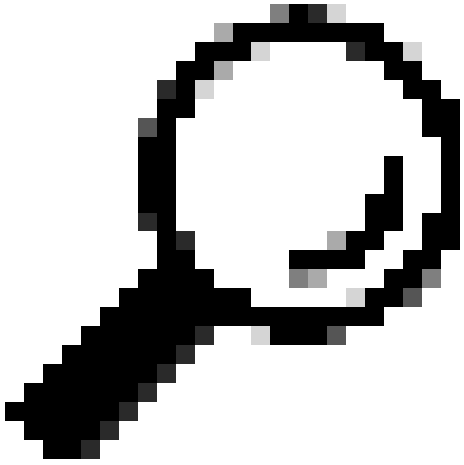
阶段	阻止特定用户访问任何网站	阻止特定用户访问某些网站
自定义URL类别	不能应用.	为计划阻止访问的站点创建自定义URL类别。 有关详细信息，请访问： 在安全网络设备中配置自定义URL类别-思科

标识配置文件	步骤1:在GUI中，选择网络安全管理器，然后单击标识配置文件。 第二步：单击Add Profile添加配置文件。 第三步：使用Enable Identification Profile复选框可启用此配置文件，或快速禁用此配置文件而不将其删除。 第四步：分配唯一的配置文件名称。 第5步（可选）添加说明。 第六步：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 7. 在User Identification Method部分中，选择Exempt from authentication/identication。 步骤 8在Define Members by Subnet中，输入此标识配置文件必须应用的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/访问策略得到有效管理。 步骤1:在GUI中，选择网络安全管理器，然后单击标识配置文件。 第二步：单击Add Profile添加配置文件。 第三步：使用Enable Identification Profile复选框可启用此配置文件，或快速禁用此配置文件而不将其删除。 第四步：分配唯一的配置文件名称。 第5步（可选）添加说明。 第六步：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 7. 在User Identification Method部分中，选择Exempt from authentication/identication。 步骤 8在Define Members by Subnet中，输入此标识配置文件必须应用的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 单击高级，然后添加您要阻止访问的URL类别。
解密策略	步骤1:在GUI中，选择网络安全管理器，然后单击解密策略。 第二步： 单击Add Policy以添加解密策略。	步骤1:在GUI中，选择网络安全管理器，然后单击解密策略。 第二步： 单击Add Policy以添加解密策略。

	第三步：使用Enable Policy复选框启用此策略。 第四步：分配唯一的策略名称。 第5步（可选）添加说明。 第六步：从Insert Above Policy下拉列表中，选择第一个策略。 步骤 7.从Identification Profiles and Users中，选择您在上一步中创建的标识配置文件。 步骤 8提交。 步骤 9在解密策略页的URL过滤下，点击与此新解密策略相关联的链接。	第三步：使用Enable Policy复选框启用此策略。 第四步：分配唯一的策略名称。 第5步（可选）添加说明。 第六步：从Insert Above Policy下拉列表中，选择第一个策略。 步骤 7.从Identification Profiles and Users中，选择您在上一步中创建的标识配置文件。 步骤 8提交。 步骤 9 在解密策略页上的URL过滤下，点击与此新解密策略相关联的链接。 步骤 10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“Submit”。  图像-阻止解密策略中的某些URL
	 提示：假设您正在阻止所有URL类别，您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。这通过避免将URL与自定义URL类别进行匹配的额外步骤，减少了SWA上的处理负载。	
	步骤 10选择Drop作为每个URL类别的操作。 步骤 11 在同一页中，向下滚动到Uncategorized URLs，并从下拉列表中选择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	
访问策略	步骤1:在GUI中，选择网络安全管理器，然后单击访问策略。 第二步： 单击Add Policy添加访问策略。 第三步：使用Enable Policy复选框启用此策略。 第四步：分配唯一的策略名称。 第5步（可选）添加说明。 第六步：从Insert Above Policy下拉列表中，选择第一个策略。 步骤 7.从Identification Profiles and Users中，选择您在上一步中创建的标识配置文件。 步骤 8提交。 步骤 9在访问策略页上的协议和用户代理下，点击与此新访问策略相关联的链接。 步骤 10 在编辑协议和用户代理设置下拉列表中，选择定义自定义设置。 步骤 11在 Block Protocols选择 复选框 FTP over HTTP和HTTP。 步骤 12在 HTTP CONNECT Ports，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。	步骤1:在GUI中，选择网络安全管理器，然后单击访问策略。 第二步： 单击Add Policy添加访问策略。 第三步：使用Enable Policy复选框启用此策略。 第四步：分配唯一的策略名称。 第5步（可选）添加说明。 第六步：从Insert Above Policy下拉列表中，选择第一个策略。 步骤 7.从Identification Profiles and Users中，选择您在上一步中创建的标识配置文件。 步骤 8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：选择阻止(Block)作为为阻止的网站创建的自定义URL类别的操作。 步骤 11提交。 步骤 12提交更改。  图像-阻止访问策略中的某些URL

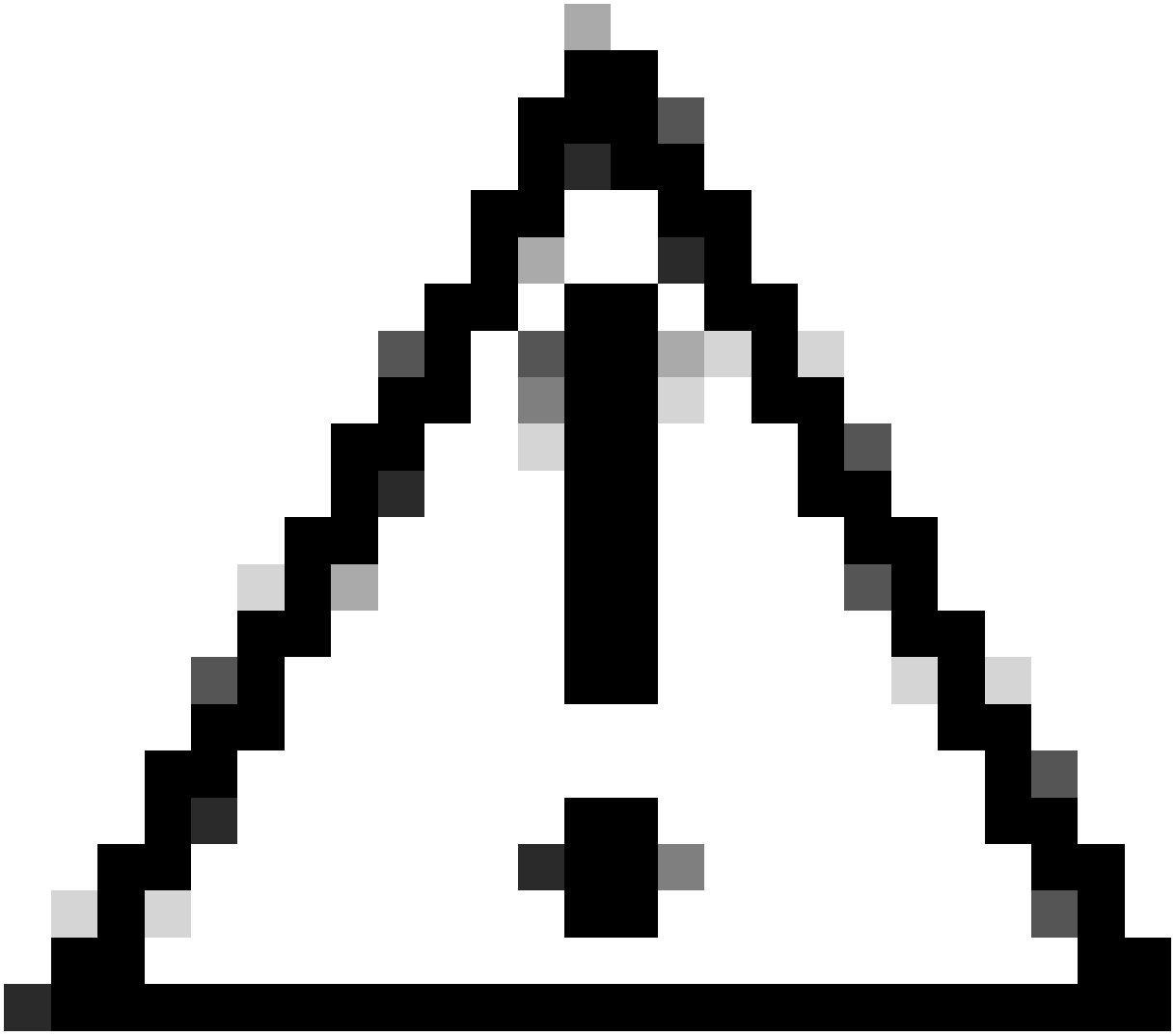
第14步（可选）在访问策略页的URL过滤下，点击与此新访问策略相关联的链接，并 选择Block作为每个URL类别的操作，并且 未分类的URL，然后Submit。



提示：假设您正在阻止所有URL类别，您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。这通过避免将URL与自定义URL类别进行匹配的额外步骤，减少了SWA上的处理负载。

步骤 16提交更改。

图像-阻止所有站点的访问策略



注意：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，如果您使用用户代理或带正则表达式的自定义URL类别来配置标识配置文件，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频道），可以使用以下步骤：

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

第二步：创建解密策略，分配此自定义URL类别，并将Action设置为Decrypt。

第三步：创建访问策略，将自定义URL类别分配给正则表达式（在本示例中，为YouTube频道指定自定义URL类别），并将“操作”设置为“阻止”。

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

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）。