如何在安全Web设备上阻止未知应用

目录

简介

本文档介绍几种阻止思科安全网络设备上未知应用的方法。

阻止未知应用的方法

您可以单独或组合使用其中任何一种方法。

> **注意**：此知识库文章引用不是由思科维护或支持的软件。提供该信息只是为了方便您使用。如需进一步协助，请联系软件供应商。

基于用户代理字符串阻止应用

第一种防御是使用用户代理字符串阻止未知应用。

- 在下添加用户代理 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** 列。
- 在下面添加用户代理字符串 **Block Custom User Agents** （每行一个）。

注意：可以使用“参考”下提供的链接搜索用户代理。

基于应用可视性控制阻止应用

如果启用了应用可视性控制(AVC)(在 **GUI > Security Services > Web Reputation and Anti-Malware**)，然后您可以根据应用类型（如代理、文件共享、Internet实用程序等）阻止访问。您可以在 **Web Security Manager > Access Policies > Applications** 列。

基于MIME类型阻止应用

如果用户代理不存在，您可以尝试添加多用途互联网邮件扩展(MIME)类型：

- 在下添加MIME类型 **Web Security Manager** > **Web Access Policies** > **Objects** 列。
- 在中添加对象/MIME类型 **Block Custom MIME Types** 部分（每行一个）。 例如，要阻止BitTorrent应用，请输入 application/x-bittorrent。

注意：可以使用“参考”下提供的链接搜索MIME类型。

阻止访问策略中的URL类别

确保在访问策略中阻止过滤器规避、非法活动、非法下载等类别。如果某些应用使用已知URL或IP地址进行连接，则可以阻止其关联的预定义URL类别，或使用其IP地址、完全限定域名(FQDN)或匹配域的正则表达式将其配置到阻止的自定义URL类别中。您可以在 **Web Security Manager > Access Policies > URL Categories** 列.

在访问策略中限制HTTP CONNECT端口配置

某些应用可以使用HTTP CONNECT方法连接到不同的端口。仅允许在HTTP CONNECT端口配置域中的已知端口或环境中所需的特定端口：

- HTTP CONNECT可在 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** 列。
- 添加允许的端口 **HTTP CONNECT Ports**。

阻止特定IP地址的访问

对于您只知道要访问的目标IP地址的应用，可以使用L4流量监控功能阻止对这些特定IP地址的访问。您可以在 **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**。

如何查找应用使用的用户代理或MIME类型

如果您不知道某些应用程序正在使用哪种用户代理或MIME类型，则可以执行以下任一步骤来查找此信息：

- 在客户端的计算机上使用WireShark(Ethereal)运行数据包捕获，并过滤“http”协议。
- 在安全Web设备上运行捕获(在 **Support and Help** > **Packet Capture**)，按客户端的IP地址过滤。

参考

注意：此处列出的外部网站仅供参考。链接和内容不受思科控制，可能会发生变化。

用户代理列表

用户代理String.Com（在useragentstring.com）

MIME类型列表

- 常见MIME类型（在mozilla.org）
- MIME类型：MIME类型的完整列表（在w3cub.com）
- MIME类型的完整列表（在sitepoint.com）