如何阻塞在思科Web安全工具的未知应用程序？

目录

问题

如何阻塞在思科Web安全工具的未知应用程序？

注意：此知识库文章参考没有维护也思科不支持的软件。信息被提供作为礼貌为您的便利。对于进一步协助，请联系软件供应商。

1. 第一防御是使用“用户代理”字符串阻塞这样应用程序。因为我们不认识这些的所有用户代理应用程序，您在下面链路将需要搜索他们。
   我们能添加“用户代理”在***Web安全经理>Access策略>协议和用户代理的***列下<for需要的访问policy>。-->Add在***‘块自定义用户代理下的***用户代理字符串***：’***(一每条线路)。

2. 如果应用程序可见性控制(AVC)启用*(在GUI > Security Services> Web名誉和反恶意软件下)*，则我们能阻止根据应用类型的访问类似代理，文件共享，互联网工具。我们能根据***Web安全经理>Access策略***执行此***> ‘应用程序的****列<for需要的访问policy>*。
3. 如果用户代理不存在，您能尝试添加MIME类型(示例：位洪流应用程序)。
   我们能添加“MIME”类型*在****Web安全经理> Web访问策略>对象****列<for下需要的访问policy>*。---在对象/笑剧的>Add输入‘**块自定义MIME类型的**部分类似application/x-bittorrent (一每条线路)。

4. 保证类别类似过滤器避免，非法活动在访问策略阻塞。如果一些应用程序使用已知URL或IP地址他们的连接，则我们在一个阻止自定义URL类别能阻塞他们的assocaited预定义的URL类别或配置他们使用他们的IP地址、FQDN或者REGEX匹配域的。我们能*根据****Web安全经理>Access策略***执行此***> “URL类别”***列。
5. 一些应用程序能使用HTTP连接方法连接到不同的端口。只请准许知道端口或在您的在HTTP的环境需要的特定端口连接端口配置域。
   HTTP连接可以配置*在****Web安全经理>Access策略>协议和用户代理的****列下<for需要的访问policy>*。-->Add允许端口在‘**HTTP连接端口下：’**

6. 对于您只知道关于访问的目的地IP地址的应用程序，您能使用L4流量监控功能阻止担心的IP地址的访问。我们能添加目的地IP*在****Web安全经理> L4流量监控>其他怀疑的恶意软件地址下。***

如果对哪些是没有察觉的‘某些应用程序使用用户代理’或‘笑剧类型’，则您能执行之一以下找到此信息：

- 运行数据包捕获以Wireshark (Ethereal)在客户端机器并且为‘http’协议过滤。
- 运行在WSA的捕获(在“支持和帮助” > “数据包捕获下”)，过滤在客户端IP地址。

用户代理列表：
==========

http://www.user-agents.org/

MIME类型列表：
==========
http://www.webmaster-toolkit.com/mime-types.shtml

http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx