目录

问题：

环境：思科Web安全工具(WSA)， AsyncOS所有版本

有WSA可以认为一个开放代理的两个区域：

1. 在您的网络不驻留的HTTP客户端通过能对代理
2. 客户端使用HTTP连接请求通过建立隧道非HTTP数据流

这些方案中的每一个有完全不同的暗示，并且如下较详细地讨论。

在您的网络不驻留的HTTP客户端通过能对代理

WSA，默认情况下，代理所有HTTP请求发送对它，假设请求打开在WSA侦听的端口(默认是80和3128)。因为您不可以从任何网络的任何客户端能使用WSA，这可能摆在是您的一问题。这是可以是一个巨大的问题，如果WSA使用公网IP地址并且从互联网是可访问。

有2种方式这可以被补救：

1. 使用一防火墙上行对WSA为了阻塞从HTTP访问的未授权的源。

2. 创建策略组只允许您的希望的子网的客户端。此策略的一简单演示如下：

策略组1 ：应用分支子网10.0.0.0/8 (假设此是您的客户端网络)。添加您的所需的动作。
默认策略：阻塞所有协议- HTTP， HTTPS，在HTTP的FTP

更多详细的策略可能在策略组1.上创建，只要其他规则只适用对适当的客户端子网，其他流量将捉住“在底部拒绝所有”规则。

客户端使用HTTP连接请求通过建立隧道非HTTP数据流

HTTP连接请求用于通过HTTP代理建立隧道非HTTP数据。HTTP连接请求的最普通的使用情况是为建立隧道HTTPS流量。为了一个明确地配置的客户端能访问HTTPS站点，它必须首先发送HTTP连接请求WSA。

连接请求的示例是象这样：连接http://www.website.com:443/ HTTP/1.1

这告诉WSA客户端希望通过WSA建立隧道到在端口443的http://www.website.com/。

HTTP连接请求可以用于建立隧道所有端口。默认情况下由于潜在的安全问题， WSA只允许连接请求到以下端口：

20， 21， 443， 563， 8443， 8080

如果它是需要的添加另外的连接通道端口，由于安全原因，推荐您在仅适用于客户端IP子网需要此另外的访问的一个另外的策略组中添加他们。允许连接端口可以在每个策略组找到，在“应用程序下” - > “协议控制”。

发送一SMTP请求示例通过一个开放代理如下：
myhost$ telnet proxy.mydomain.com 80
尝试xxx.xxx.xxx.xxx…
连接对proxy.mydomain.com。
转义字符是‘^]’。
连接smtp.foreigndomain.com:25 HTTP/1.1
主机：smtp.foreigndomain.com

HTTP/1.0 200已建立连接

220 smtp.foreigndomain.com ESMTP
直升机测验
250个smtp.foreigndomain.com