

如何防止Web安全工具是一个开放代理

目录

[简介](#)

[环境](#)

[在您的网络不驻留的HTTP客户端通过能对代理](#)

[使用HTTP连接请求通过以隧道传输非HTTP流量的客户端](#)

简介

本文描述如何防止Web安全工具(WSA)是一个开放代理。

环境

思科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. 使用HTTP连接请求通过以隧道传输非HTTP流量的客户端。

这些方案中的每一个在以下部分有完全不同的暗示，并且较详细地讨论。

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。这假设，请求在WSA侦听的端口(默认是80和3128)。因为您也许不希望从所有网络的任何客户端能使用WSA，这也许摆在是问题。这是可以是一个巨大的问题，如果WSA使用一公网IP地址并且从互联网是可访问。

有两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是：
策略组1：应用分支子网10.0.0.0/8 (假设这是您的客户端网络)。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

更多详细的策略可以在策略组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。

使用HTTP连接请求通过以隧道传输非HTTP流量的客户端

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连接请求到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只允许连接请求到这些端口：

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>协议控制下。

通过一个开放代理发送的SMTP请求的示例显示此处：

```
myhost$ telnet proxy.mydomain.com 80
Trying xxx.xxx.xxx.xxx...
Connected to proxy.mydomain.com.
Escape character is '^]'.
CONNECT smtp.foreigndomain.com:25 HTTP/1.1
Host: smtp.foreigndomain.com HTTP/1.0 200 Connection established
220 smtp.foreigndomain.com ESMTP
HELO test
250 smtp.foreigndomain.com
```