如何防止Web安全工具是一个开放代理

Contents

Introduction

本文描述如何防止Web安全工具(WSA)是一个开放代理。

环境

Cisco WSA， AsyncOS的所有版本

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数据流的客户端。

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请求被发送到它。这假设，请求在WSA监听的端口(默认值是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使用一个公共IP地址并且从互联网是可访问的。

有两种方式这可以被补救：

1. 使用一防火墙上行对WSA为了阻拦从HTTP访问的未授权的源。
2. 创建策略组只允许您的期望子网的客户端。此策略的简单的演示是：
   策略Group1 ：适用分支子网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：阻拦所有协议- HTTP， HTTPS，在HTTP的FTP

更加详细的策略可以在策略组1.上被创建，只要其他规则只适用于适当的客户端子网，其他数据流将捉住“拒绝所有”规则在底部。

使用HTTP连接请求通过以隧道传输非HTTP数据流的客户端

HTTP连接请求用于通过HTTP代理建立隧道非HTTP数据。Connect请求的HTTP的最普通的使用方法是建立隧道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Connect请求的HTTP到WSA。

示例Connect请求是象这样：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只允许连接请求对这些端口：

20， 21， 443， 563， 8443， 8080

如果它是需要的添加另外请连接隧道端口，由于安全原因，它建议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添加他们。允许的连接端口可以在每个策略组找到，在应用程序>协议控制下。

通过一个开放代理被发送的SMTP请求的示例显示得这里：

```
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
```