如何防止 Web 安全设备成为开放代理

文档编号：117933
作者：Josh Wolfer 和 Siddharth Rajpathak，Cisco TAC 工程师。
2014 年 7 月 15 日

目录 问题：

环境：思科网络安全设备 (WSA)，所有 AsyncOS 版本。在以下两种情况下，

可考虑使用 WSA 作为开放代理：

1. 非网络中驻留的 HTTP 客户端可以通过代理访问网络
2. 客户端使用 HTTP CONNECT 请求通过隧道传输非 HTTP 流量

这两种情况会造成完全不同的影响，下面将进行详细探讨。

非网络中驻留的 HTTP 客户端可以通过代理访问网络

默认情况下，WSA 会代理发送给它的任何 HTTP 请求，并假设该请求位于 WSA 正在侦听的端口（默认为 80 和 3128）。 这可能存在问题，因为您可能不希望任何网络的任何客户端都能使用 WSA。如果 WSA 使用的是公共 IP 地址并且可从互联网进行访问，这可能会成为一个重大问题。

可通过以下 2 种方式修复该问题：

1. 在 WSA 的上游利用防火墙来阻止未经授权的源进行 HTTP 访问。

2. 创建策略组，以仅允许所需子网上的客户端进行访问。 下面是此策略的简要说明：

策略组 1：应用到子网 10.0.0.0/8（假设这是客户端网络）。 添加所需的操作。 默认策略：阻止所有协议 - HTTP、HTTPS、FTP over HTTP

可以在策略组 1 的基础上创建更详细的策略。 只要其他规则仅应用到相应的客户端子网，所有其他流量均将捕获最后一条规则“deny all”。

客户端使用 HTTP CONNECT 请求通过隧道传输非 HTTP 流量

HTTP CONNECT 请求用于通过 HTTP 代理隧道传输非 HTTP 数据。 HTTP CONNECT 请求的最常见用途是用于通过隧道传输 HTTPS 流量。

为将客户端明确配置为可以访问 HTTPS 站点，必须首先将 HTTP CONNECT 请求发送至 WSA。

CONNECT 请求的示例如下所示：CONNECT http://www.website.com:443/ HTTP/1.1

此请求告知 WSA，客户端需要通过 WSA 建立到端口 443 上的 http://www.website.com/ 的隧道。

HTTP CONNECT 请求可用于通过隧道连接任何端口。 由于潜在的安全问题，默认情况下，WSA 仅允许对下列端口的 CONNECT 请求：

20、21、443、563、8443、8080

如果需要添加额外的 CONNECT 隧道端口，出于安全考虑，建议您在将这些端口添加到其他策略组，并将该策略组仅应用到需要此额外访问权限的客户端 IP 子网。
您可以在“应用”(Applications) –>“协议控制”(Protocol Controls) 下，找到每个策略组中允许的 CONNECT 端口。

通过开放代理发送 SMTP 请求的示例如下：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

更新日期：2014 年 7 月 15 日 文档编号：117933