如何防止網路安全裝置成為開放式代理

目錄

簡介

本文說明如何防止網路安全裝置(WSA)成為開放代理。

環境

Cisco WSA，AsyncOS的所有版本

WSA可以被視為開放代理有兩個方面：

1. 不駐留在網路上的HTTP客戶端可以通過進行代理。
2. 使用HTTP CONNECT請求通過隧道傳輸非HTTP流量的客戶端。

每個設想方案都具有完全不同的含義，將在下一節中更詳細地討論。

不駐留在您網路上的HTTP使用者端可以透過進行代理

預設情況下，WSA將代理傳送到它的任何HTTP請求。這會假設要求位於WSA偵聽的連線埠上（預設值為80和3128）。 這可能會造成問題，因為您可能不希望來自任何網路的任何客戶端能夠使用WSA。如果WSA使用公有IP地址並且可從Internet訪問，則這可能是一個大問題。

有兩種方法可以解決此問題：

1. 在WSA的上游使用防火牆，以阻止未經授權的源訪問HTTP。
2. 建立策略組以僅允許所需子網上的客戶端。此策略的簡單演示如下：
   策略組1:適用於子網10.0.0.0/8（假定這是您的客戶端網路）。 新增所需的操作。
   預設策略：阻止所有協定 — HTTP、HTTPS、FTP over HTTP

可以在策略組1上方建立更詳細的策略。只要其他規則僅適用於相應的客戶端子網，所有其他流量將在底部捕獲「全部拒絕」規則。

使用HTTP CONNECT請求通過隧道傳輸非HTTP流量的客戶端

HTTP CONNECT請求用於通過HTTP代理隧道傳輸非HTTP資料。HTTP CONNECT請求的最常見用途是通過HTTPS流量傳輸。為了讓明確配置的客戶端訪問HTTPS站點，必須首先向WSA傳送HTTP CONNECT請求。

CONNECT請求的示例如下：連線http://www.website.com:443/ HTTP/1.1

這通知WSA客戶端希望通過WSA隧道連線到埠443上的http://www.website.com/。

HTTP CONNECT請求可用於隧道連線任何埠。由於潛在的安全問題，預設情況下WSA僅允許對這些埠的CONNECT請求：

20、21、443、563、8443、8080

如果出於安全原因，需要新增其他CONNECT隧道埠，建議將它們新增到僅應用於需要此額外訪問的客戶端IP子網的其他策略組中。每個策略組的Applications > Protocol Controls下都存在允許的CONNECT埠。

下面顯示了通過開放代理傳送的SMTP請求的示例：

```
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
```