Web Security Appliance가 오픈 프록시가 되는 것을 방지하는 방법은 무엇입니까?

문서 ID: 117933

기고자: Josh Wolfer 및 Siddharth Rajpathak, Cisco TAC 엔지니어
2014년 7월 15일

목차 질문:

환경: Cisco WSA(Web Security Appliance), 모든 버전의 AsyncOS WSA가 오픈

프록시(Open Proxy)로 간주될 수 있는 두 가지 경우는 다음과 같습니다.

1. 네트워크에 상주하지 않는 HTTP 클라이언트가 프록시를 통과할 수 있는 경우
2. 클라이언트가 HTTP CONNECT 요청을 사용하여 non-HTTP 트래픽 통과를 터널링하는 경우

이 두 가지 시나리오의 결과는 완전히 다르며 아래에서 좀 더 자세히 알아보겠습니다.

네트워크에 상주하지 않는 HTTP 클라이언트가 프록시를 통과할 수 있는 경우

기본적으로 WSA는 모든 HTTP 요청이 전송되는 프록시이며, 이러한 요청은 WSA가 수신하는 포트에 있는 것으로 간주됩니다(기본값은 80과 3128). 네트워크의 어떠한 클라이언트도 WSA를 사용 할 수 없도록 하려는 경우 이는 문제가 될 수 있습니다. 또한 WSA가 공용 IP 주소를 사용하고 인터넷에서 이 주소에 액세스할 수 있는 경우에는 큰 문제가 될 수 있습니다.

이 문제를 해결할 수 있는 2가지 방법은 다음과 같습니다.

1. HTTP 액세스에서 무단 소스를 차단하려면 WSA로 가는 방화벽 업스트림을 활용합니다.

2. 원하는 서브넷에 있는 클라이언트만을 허용하도록 정책 그룹을 생성합니다. 이 정책의 간단한 데모는 다음과 같습니다.

정책 그룹 1: 서브넷 10.0.0.0/8에 적용됩니다(이 서브넷이 클라이언트 네트워크인 것으로 가정). 원하는 작업을 추가합니다. 기본 정책: 모든 프로토콜 차단 – HTTP, HTTPS, FTP over HTTP

좀 더 자세한 정책은 Policy Group 1(정책 그룹 1) 위에 생성할 수 있습니다. 다른 규칙이 해당 클라이언트 서브넷에만 적용되는 한, 다른 모든 트래픽에서는 하단의 "모두 거부" 규칙을 탐지합니다.

클라이언트가 HTTP CONNECT 요청을 사용하여 non-HTTP 트래픽 통과를 터널링하는 경우

HTTP CONNECT 요청은 HTTP 프록시를 통해 non-HTTP 데이터를 터널링하는 데 사용됩니다. HTTP CONNECT 요청이 가장 일반적으로 사용되는 경우는 HTTPS 트래픽을 터널링하는 것입니다.

명시적으로 구성된 클라이언트가 HTTPS 사이트에 액세스하려면 우선 HTTP CONNECT 요청을 WSA에 보내야 합니다.

CONNECT 요청의 예: CONNECT http://www.website.com:443/ HTTP/1.1

이 요청의 내용은 클라이언트가 포트 443에서 WSA를 통해 http://www.website.com/으로 터널링하고자 한다는 것입니다.

HTTP CONNECT 요청은 포트를 터널링하는 데 사용할 수 있습니다. 잠재적인 보안 문제로 인해, 기본적으로 WSA는 다음과 같은 포트에만 CONNECT 요청을 허용합니다.

20, 21, 443, 563, 8443, 8080

CONNECT 터널 포트를 보안상의 이유로 추가해야 하는 경우 이러한 추가 액세스가 필요한 클라이언트 IP 서브넷에만 적용되는 추가적인 정책 그룹에 추가하는 것이 좋습니다. "Applications"(애플리케이션) –> "Protocol Controls"(프로토콜 제어) 아래의 각 정책 그룹에서 허용된 CONNECT 포트를 찾을 수 있습니다.

오픈 프록시를 통해 SMTP 요청을 전송하는 예는 다음과 같습니다. 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

업데이트 날짜: 2014년 7월 15일 문서 ID: 117933