Web Security Appliance가 개방형 프록시가 되는 것을 방지하는 방법

목차

[소개](#)
[환경](#)
[네트워크에 상주하지 않는 HTTP 클라이언트는](#)
[HTTP CONNECT 요청을 사용하여 비 HTTP 트래픽을 터널링하는 클라이언트](#)

소개

이 문서에서는 WSA(Web Security Appliance)가 열린 프록시가 되는 것을 방지하는 방법에 대해 설명합니다.

환경

Cisco WSA, 모든 버전의 AsyncOS

WSA를 오픈 프록시로 간주할 수 있는 영역은 두 가지입니다.

1. 네트워크에 상주하지 않는 HTTP 클라이언트는 프록시를 통해 프록시를 수행할 수 있습니다.
2. 비 HTTP 트래픽을 터널링하기 위해 HTTP CONNECT 요청을 사용하는 클라이언트.

이러한 각 시나리오는 완전히 다른 영향을 미치며 다음 섹션에서 더 자세히 설명합니다.

네트워크에 상주하지 않는 HTTP 클라이언트는

WSA는 기본적으로 HTTP 요청을 프록시합니다.이는 WSA가 수신하는 포트에 요청이 있다고 가정합니다(기본값은 80 및 3128). 네트워크의 어떤 클라이언트도 WSA를 사용할 수 없게 하려는 경우 이 문제가 발생할 수 있습니다.WSA가 공용 IP 주소를 사용하며 인터넷에서 액세스할 수 있는 경우 이는 큰 문제가 될 수 있습니다.

이 문제를 해결할 수 있는 두 가지 방법이 있습니다.

1. HTTP 액세스에서 무단 소스를 차단하려면 WSA에 대한 방화벽 업스트림을 활용합니다.
2. 원하는 서브넷의 클라이언트만 허용하도록 정책 그룹을 생성합니다.이 정책의 간단한 데모는 다음과 같습니다.
   정책 그룹 1:서브넷 10.0.0.0/8에 적용됩니다(클라이언트 네트워크인 것으로 가정). 원하는 작업을 추가합니다.
   기본 정책:모든 프로토콜 차단 - HTTP, HTTPS, FTP over HTTP

정책 그룹 1 위에 더 자세한 정책을 만들 수 있습니다. 다른 규칙이 해당 클라이언트 서브넷에만 적용되는 한, 다른 모든 트래픽은 맨 아래에 있는 "모두 거부" 규칙을 catch합니다.

HTTP CONNECT 요청을 사용하여 비 HTTP 트래픽을 터널링하

는 클라이언트

HTTP CONNECT 요청은 HTTP 프록시를 통해 비 HTTP 데이터를 터널링하는 데 사용됩니다 .HTTP CONNECT 요청의 가장 일반적인 사용법은 HTTPS 트래픽을 터널링하는 것입니다.명시적으로 구성된 클라이언트가 HTTPS 사이트에 액세스하려면 먼저 HTTP CONNECT 요청을 WSA에 보내야 합니다.

CONNECT 요청의 예는 다음과 같습니다.연결 http://www.website.com:443/ HTTP/1.1

이는 클라이언트가 WSA를 통해 포트 443에서 http://www.website.com/으로 터널링하려는 것을 WSA에 알려줍니다.

HTTP CONNECT 요청은 모든 포트를 터널링하는 데 사용할 수 있습니다.잠재적인 보안 문제로 인해 WSA에서는 기본적으로 다음 포트에 대한 CONNECT 요청만 허용합니다.

20,21,443, 563, 8443, 8080

보안상의 이유로 추가 CONNECT 터널 포트를 추가해야 하는 경우 이 추가 액세스가 필요한 클라이언트 IP 서브넷에만 적용되는 추가 정책 그룹에 추가하는 것이 좋습니다.허용되는 CONNECT 포트는 각 정책 그룹의 Applications(애플리케이션) > Protocol Controls(프로토콜 제어)에서 찾을 수 있습니다.

열린 프록시를 통해 전송되는 SMTP 요청의 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
```