كيفية منع جهاز أمان الويب من أن يكون وكيلا مفتوحا

المحتويات

المقدمة

يوضح هذا المستند كيفية منع جهاز أمان الويب (WSA) من أن يكون وكيلا مفتوحا.

البيئة

Cisco WSA، جميع إصدارات AsyncOS

هناك مجالان يمكن إعتبار WSA وكيل مفتوح لهما:

1. يمكن لعملاء HTTP الذين لا يقيمون على الشبكة الخاصة بك الوكيل من خلال.
2. العملاء الذين يستخدمون طلبات اتصال HTTP لنقل البيانات بخلاف HTTP عبر.

ولكل سيناريو من هذه السيناريوهات آثار مختلفة تماما، وستناقش بمزيد من التفصيل في الأقسام التالية.

يمكن لعملاء HTTP الذين لا يقيمون على الشبكة الخاصة بك الوكيل من خلال

سيقوم WSA، بشكل افتراضي، بوكيل أي طلب HTTP يتم إرساله إليه. هذا يفترض أن الطلب يكون على المنفذ الذي يستمع إليه WSA على (الافتراضيات 80 و 3128). قد يمثل هذا مشكلة، حيث قد لا تريد أن يتمكن أي عميل من أي شبكة من إستخدام WSA. قد تكون هذه مشكلة كبيرة إذا كانت WSA تستخدم عنوان IP عام ويمكن الوصول إليها من الإنترنت.

وهناك طريقتان يمكن بهما علاج هذا الوضع:

1. أستخدم تدفق جدار حماية إلى WSA لحظر المصادر غير المعتمدة من وصول HTTP.
2. قم بإنشاء مجموعات سياسات للسماح بالعملاء على الشبكات الفرعية المطلوبة فقط. والدليل البسيط على هذه السياسة هو:
   مجموعة السياسات 1: تنطبق على الشبكة الفرعية 8/10.0.0.0 (يفترض أنها شبكة العميل الخاصة بك). قم بإضافة الإجراءات التي تريدها.
   النهج الافتراضي: حظر جميع البروتوكولات - HTTP و HTTPS و FTP عبر HTTP

يمكن إنشاء سياسات أكثر تفصيلا فوق مجموعة النهج 1. طالما أن القواعد الأخرى تنطبق فقط على الشبكات الفرعية المناسبة للعملاء، فإن جميع حركات المرور الأخرى ستمسك بالقاعدة "رفض الكل" في الجزء السفلي.

العملاء الذين يستخدمون طلبات اتصال HTTP لنقل البيانات غير HTTP عبر

يتم إستخدام طلبات اتصال HTTP لأنفاق البيانات بخلاف HTTP عبر وكيل HTTP. أكثر الاستخدامات شيوعا لطلب اتصال HTTP هو نفق حركة مرور HTTPS. لكي يتمكن العميل الذي تم تكوينه بشكل صريح من الوصول إلى موقع HTTPS، يجب عليه أولا إرسال طلب HTTP Connect إلى WSA.

مثال على طلب اتصال على هذا النحو: الاتصال HTTP/1.1 http://www.website.com:443/

وهذا يوضح ل WSA أن العميل يرغب في الانتقال عبر WSA إلى http://www.website.com/ على المنفذ 443.

يمكن إستخدام طلبات اتصال HTTP للنفق بين أي منفذ. نظرا لمشاكل الأمان المحتملة، يسمح WSA بطلبات الاتصال بهذه المنافذ فقط بشكل افتراضي:

20 و 21 و 443 و 563 و 8443 و 8080

إذا كانت هناك حاجة لإضافة منافذ نفق "الاتصال" إضافية، لأسباب أمنية، فمن المستحسن إضافتها في مجموعة سياسات إضافية تنطبق فقط على الشبكات الفرعية ل IP العميل التي تحتاج إلى هذا الوصول الإضافي. يمكن العثور على منافذ الاتصال المسموح بها في كل مجموعة من مجموعات النهج، ضمن تطبيقات > عناصر تحكم البروتوكول.

يتم عرض مثال على طلب SMTP المرسل من خلال وكيل مفتوح هنا:

```
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
smtp.foreigndomain.com ESMTP 220
HELO test
smtp.foreigndomain.com 250
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).