تمكين ميزة DHP ل ESA

المحتويات

المقدمة

يوضح هذا المستند كيفية تمكين ميزة "منع هجوم حصاد الدليل" (DHAP) على جهاز أمان البريد الإلكتروني (ESA) من Cisco لمنع هجمات حصاد الدليل (DHAs).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco ESA
- AsyncOS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جميع إصدارات AsyncOS.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

DHA هي تقنية يتم إستخدامها من قبل مرسلي البريد العشوائي لتحديد موقع عناوين البريد الإلكتروني الصحيحة. هناك أسلوبان أساسيان يستخدمان من أجل توليد العناوين التي يستهدفها DHA:

- يقوم مرسل البريد العشوائي بإنشاء قائمة بكل المجموعات الممكنة من الأحرف والأرقام، ثم يقوم بتذييل اسم المجال.
- يستخدم مرسل البريد العشوائي هجوم قاموس قياسي عند إنشاء قائمة تجمع بين الأسماء الأولى الشائعة وأسماء الألقاب والأحرف الأولى.

DHP هي ميزة مدعومة على أجهزة أمان المحتوى من Cisco التي يمكن تمكينها عند إستخدام التحقق من قبول بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP). تقوم ميزة DHP بتتبع عدد عناوين المستلمين غير الصالحة من

مرسل معين.

بمجرد تجاوز المرسل للحد المعرف من قبل المسؤول، يتم إعتبار المرسل غير موثوق به، ويتم حظر البريد من ذلك المرسل بدون إنشاء "متطلبات تصميم الشبكة" (NDR) أو إنشاء رمز الخطأ. يمكنك تكوين العتبة استنادا إلى سمعة المرسل. على سبيل المثال، يمكن أن يكون للمرسلين غير الموثوق بهم أو المشبوهين حد DHAP منخفض، ويمكن للمرسلين الموثوق بهم أو الموثوق بهم أن يكون لديهم حد DHP مرتفع.

تمكين DHAP

لتمكين ميزة DHP، انتقل إلى **سياسات البريد > جدول الوصول إلى المضيف (HAT)** من واجهة المستخدم الرسومية (GUI) الخاصة بجهاز أمان المحتوى وحدد **سياسات تدفق البريد**. أختر النهج الذي ترغب في تحريره من عمود **اسم النهج**.

تحتوي HAT على أربع قواعد وصول أساسية يتم إستخدامها للعمل عند الاتصالات من الأجهزة المضيفة البعيدة:

- **قبول**: يتم قبول الاتصال، ويتم تقييد قبول البريد الإلكتروني أكثر من قبل إعدادات المصغي. ويتضمن هذا الجدول جدول وصول المستلم (للمستمعين العامين).
- **رفض**: يتم قبول الاتصال في البداية، ولكن العميل الذي يحاول الاتصال يتلقى تحية 4XX أو 5XX. لم يتم قبول أي بريد إلكتروني.
- **TCPREFUSE**: تم رفض الاتصال على مستوى TCP.
- **الترحيل**: تم قبول الاتصال. يسمح باستلام أي مستلم ولا يخضع لقيود جدول وصول المستلم. يتوفر توقيع "مفاتيح المجال" فقط على نهج تدفق البريد للترحيل.

في قسم **حدود تدفق البريد** في النهج المحدد، ابحث عن تكوين **منع هجوم حصاد الدليل (DHAP)** وتعيينه عن طريق تعيين الحد الأقصى. عدد المستلمين غير صحيح في الساعة. يمكنك أيضا إختيار تخصيص الحد الأقصى. مستلمون غير صحيحين لكل ساعة والرمز الأقصى. عدد المستلمين غير صحيح لكل ساعة إذا كنت ترغب في ذلك.

أنت ينبغي كررت هذا قسم in order to شكلت DHP لنهج إضافية.

تأكد من إرسال كافة التغييرات في واجهة المستخدم الرسومية (GUI) وتنفيذها.

ملاحظة: توصي Cisco باستخدام الحد الأقصى للعدد بين خمسة وعشرة **للحد الأقصى لعدد المستلمين غير الشرعيين في الساعة من** إعداد **مضيف بعيد**.

ملاحظة: للحصول على معلومات إضافية، ارجع إلى **دليل مستخدم AsyncOS** على بوابة دعم Cisco.

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).