حل حالات فشل DMARK عن طريق تصحيح مخاذاة SPF و DKIM

المحتويات

مسألة

يتم حظر رسائل البريد الإلكتروني من مجالات معينة بواسطة عبارة البريد الإلكتروني الآمنة (CES/ESA) من Cisco بسبب فشل التحقق من صحة DMARK. يشير تحليل تعقب الرسائل إلى أن رسائل البريد الإلكتروني هذه يتم الاحتفاظ بها في قائمة انتظار العمل ووضعها في العزل أو رفضها، مما يمنعها من الوصول إلى المستلمين المقصودين.

البيئة

- أجهزة عبارة البريد الإلكتروني الآمنة (CES/ESA) من Cisco
- يتم تكوين سياسات SPF و DKIM و DMARK وإنفاذها

قرار

جدول ملخص مخاذاة SPF/DKIM (أمثلة)

آلية	حالة المخاذاة	نطاق المظروف/التوقيع	من مجال الرأس	منطق
SPF	في المخاذاة	sender@example.com	sender@example.com	تطابق مباشر

SPF	في المحاذاة	sender@child.example.com	sender@example.com	تطابق المجال الأصل
SPF	ليس في محاذاة	sender@test.com	sender@example.com	المجال غير متطابق
البريد المُوثّق بمفاتيح النطاق (DKIM)	في المحاذاة	example.com	sender@example.com	تطابق مباشر
البريد المُوثّق بمفاتيح النطاق (DKIM)	في المحاذاة	example.com	sender@child.example.com	تطابق في وضع الاستخاء
البريد المُوثّق بمفاتيح النطاق (DKIM)	ليس في محاذاة	example.com	sender@test.com	المجال غير متطابق

التنسيق مع المرسل (مستحسن)

- تعاون مع مسؤولي مجال المرسل لتصحيح حالات فشل DMARK من خلال ضمان محاذاة SPF و DKIM بشكل مناسب على مستوى الرأس.
- يجب على المرسل:
  - تأكد من أن المجال المستخدم في SPF الذي تم التحقق من صحة البريد من أو البريد الإلكتروني. محاذاة هويّة HELO/EHLO مع المجال في رأس من البريد
  - تنفيذ توقيع DKIM حيث يتم محاذاة المجال المحدد في علامة DKIM Signature D= مع مجال رأس من.
  - تحقق من تكوين نهج DMARK بشكل صحيح لفرض وضع المحاذاة المطلوب (المقيد أو الذي تم ترخيصه) وخيارات إعداد التقارير.
- يعالج هذا النهج السبب الأساسي لفشل DMARK من خلال التركيز على محاذاة المجالات المصدق عليها مع مجال "المرئي من الرأس"، والذي يعد أمرا بالغ الأهمية لإتاحة إمكانية تسليم البريد الإلكتروني على المدى البعيد.

إنشاء إستثناء DMARK (بديل)

- إذا لم يكن الإصلاح بواسطة المرسل ممكنا، قم بإنشاء إستثناء على جهاز ESA لعنوان المرسل المحدد لتجاوز عمليات التحقق من DMARK.
- هذا حل بديل مؤقت ويجب أن يكون مصحوبا بمراقبة.

المراقبة والتحقق

- بعد تنفيذ التغييرات، قم بمراقبة تسليم رسائل البريد الإلكتروني الخاصة بالتنبيه إلى المستلمين المقصودين.
- راجع سجلات تعقب الرسائل للتأكد من أنه تم حل حالات فشل DMARK.
- متابعة تحليل بيانات تعقب الرسائل المحدثة في حالة إستمرار مشاكل التسليم.

السبب

السبب الرئيسي للحجر الصحي للبريد الإلكتروني أو رفضه هو فشل التحقق من DMARK بسبب مشاكل محاذاة SPF و DKIM. تشير حالات الفشل هذه إلى أنه على الرغم من إمكانية نشر سجلات SPF و DKIM بشكل صحيح، إلا أن المجالات التي تمت مصادقتها أثناء تبادل البريد الإلكتروني لا تتوافق مع مجال عنوان من، مما يؤدي إلى عزل رسائل البريد الإلكتروني.

فهم محاذاة DMARK و SPF و DKIM:

- يقوم SPF بمصادقة المجال في أوامر SMTP الخاصة ب MAIL من وأ HELO/EHLO ويتطلب محاذاة هذا المجال مع المجال في رأس من أجل التوافق مع DMARK.
- تستخدم DKIM توقيعات تشفير مع مجال توقيع محدد في D= علامة، والتي يجب أن تتوافق مع مجال رأس من.
- يبني DMARK على SPF و DKIM من خلال طلب أن يتوافق مجال واحد على الأقل من هذه المجالات التي تمت مصادقتها مع مجال من الرأس، إما بالضبط (الوضع المقيد) أو كمجال فرعي (وضع مريح).

يؤدي فشل محاذاة هذا المجال إلى حدوث حالات فشل في DMARK وما يليها من رفض البريد

حيح الإلكتروني أو الحجر الصحي، حتى إذا تم نشر سجلات SPF و DKIM نفسها بشكل صحيح وصالحة.

يضمن التركيز على المحاذاة تطابق الهوية المصدق عليها مع هوية المرسل المرئية، مما يمنع الانتحال ويحسن الثقة بالبريد الإلكتروني.

المحتوى ذي الصلة

- معلومات محاذاة SPF
- معلومات محاذاة DKIM
- أفضل الممارسات لمصادقة البريد الإلكتروني - أفضل الطرق لنشر SPF و DKIM و DMARK - Cisco
- تكوين عامل التصفية الوارد استنادا إلى التحقق من DKIM في ESA - 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).