

فرع عمل اذاحم - DMARK Architecture

المحتويات

- [المقدمة](#)
- [مصطلحات](#)
- [DMARK - محاذاة المعرف](#)
- [معرفة](#)
- [محاذاة المعرف](#)
- [محاذاة DKIM](#)
- [محاذاة SPF](#)
- [علامات تميز وضع المحاذاة](#)
- [المرجع](#)

المقدمة

يصف هذا المستند مفاهيم بنية "مصادقة الرسائل وإعداد التقارير والمطابقة" (DMARK) المستندة إلى المجال العام، بالإضافة إلى متطلبات محاذاة "إطار عمل نهج المرسل" (SPF) و DomainKeys المحددة للبريد (DKIM) فيما يتعلق ب DMARK.

مصطلحات

يصف هذا القسم ويورد تعريفا لبعض المصطلحات الأساسية المستخدمة ضمن هذا المستند.

- **EHLO/HELO** - الأوامر التي توفر هوية عميل SMTP أثناء تهيئة جلسة SMTP كما هو محدد في RFC 5321.
- **من الرأس** - يحدد الحقل من: مؤلف (مؤلفات) الرسالة. وعادة ما تتضمن اسم العرض (ما يتم عرضه للمستخدم النهائي بواسطة عميل البريد)، بالإضافة إلى عنوان بريد إلكتروني يحتوي على جزء محلي واسم المجال (على سبيل المثال، "John Doe" <johndoe@example.com>) كما هو محدد في RFC 5322.
- **Mail FROM** - يتم اشتقاق هذا الأمر من أمر "البريد" في بداية جلسة SMTP ويوفر تعريف المرسل كما هو محدد في RFC5321. كما يعرف على نطاق واسع باسم مرسل المغلف أو مسار الإرجاع أو عنوان الارتداد.

DMARK - محاذاة المعرف

يربط DMARK ما يصادق عليه DKIM و SPF بما هو مدرج في From header. ويتم ذلك من خلال المحاذاة. تتطلب المحاذاة مطابقة هوية المجال المصادق عليها من قبل SPF و DKIM للمجال في عنوان البريد الإلكتروني المرئي للمستخدم النهائي.

لنبدأ بما هو معرف هذا الطراز ولماذا هو مهم في إشارة إلى DMARK.

معرفة

تحدد المعرفات اسم مجال ليتم مصادقته.

المعرفات في إشارة إلى DMARK:

• فرانسسكو:

يصادق SPF المجال الذي يظهر إما في جزء MAIL من أو EHLO/HELO من محادثة SMTP، أو كليهما. قد تكون هذه مجالات مختلفة، وعادة ما لا تكون مرئية للمستخدم النهائي.

• داكيم:

يصادق DKIM مجال التوقيع الذي تم ربطه بتوقيع ضمن علامة d .

تتم مصادقة معرفات (SPF و DKIM) هذه مقابل معرف المجال المشتق في الرأس من. يتم استخدام مجال من الرأس لأنه أكثر حقول وكيل مستخدم البريد (MUA) شيوعاً لمنشئ الرسالة وهو الحقل الذي يستخدمه المستخدمون النهائيون لتحديد مصدر الرسالة (المرسل)، مما يجعل أيضاً من الرأس From هدفاً أولياً لسوء الاستخدام.

تحذير: يستطيع DMARK حماية إساءة الاستخدام فقط ضد رأس صالح من.

يتعذر على DMARK العمل على:

- رؤوس RFC 5322 التي تم تكوينها بشكل غير صحيح أو غائبة أو متكررة
- الرؤوس غير المتوافقة حيث أنها لن يتم التحقق منها
- عندما يكون هناك أكثر من معرف مجال في الرأس (*)

لذلك، يجب أن تكون هناك عملية بالإضافة إلى DMARK لتحديد الرسائل التي تحتوي على رؤوس غير متوافقة والتي تم تكوينها بشكل غير صحيح وتنفيذ طريقة لوضع علامة عليها وجعلها مرئية كرؤوس غير مؤهلة ل DMARK.

(*) يحتاج DMARK إلى استخراج هوية مجال واحدة من الرأس. إذا كان هناك أكثر من عنوان بريد إلكتروني واحد في الرأس من هذا العنوان سيتم تخطيه في معظم تطبيقات DMARK. يتم ذكر عناوين المعالجة التي تحتوي على أكثر من معرف مجال واحد على أنها خارج النطاق في مواصفات DMARK.

عندما يكون Cisco ESA قادراً على اكتشاف أكثر من معرف مجال واحد، فإنه يترك رسالة مناسبة في سجلات البريد:

```
Machine esa.lab.local) (SERVICE)> grep -i "verification skipped" mail_logs)
```

```
Tue Oct 16 14:13:52 2018 Info: MID 2003 DMARC: Verification skipped (Sending domain could not be (determined
```

محاذاة المعرف

تحدد محاذاة المعرف علاقة بين المجال الذي تمت مصادقته بواسطة SPF و/أو DKIM وFrom header. المحاذاة هي عملية مطابقة يلزم الوفاء بها أيضا بعد التحقق الناجح من SPF و/أو DKIM. تتطلب عملية مصادقة DMARK وجود معرف واحد على الأقل (هوية المجال) مستخدم من قبل SPF أو DKIM ليتم محاذاته مع جزء المجال من عنوان من الرأس.

يقدم DMARK وضعي محاذاة:

- يتطلب الوضع المقيد مطابقة (محاذاة) دقيقة بين أسماء المجالات
 - يسمح الوضع المسترخي بالمجال الفرعي لنفس المجال
- محاذاة المعرف مطلوبة لأن الرسالة يمكن أن تحمل توقيعًا صالحًا من أي مجال، بما في ذلك المجالات المستخدمة بواسطة قائمة مراسلة أو حتى ممثل سيء. ولذلك، فإن مجرد حمل توقيع صحيح لا يكفي لاستنتاج صحة مجال المؤلف.

محاذاة DKIM

يتم الحصول على معرف مجال DKIM من خلال مراجعة علامة $d=$ في توقيع DKIM، ويتم مقارنته مع مجال من الرأس للتحقق من توقيع DKIM بنجاح.

على سبيل المثال، يمكن توقيع الرسالة بالنيابة عن المجال $d=blog.cisco.com$ ، الذي يحدد المجال $blog.cisco.com$ كموقع. يستخدم DMARK هذا المجال ويقارنه بجزء المجال من رأس من (على سبيل المثال، $noreply@cisco.com$). ستفشل المحاذاة بين هذه المعرفات في الوضع المقيد لكنها تمرر باستخدام وضع الاسترخاء.

ملاحظة: يمكن أن يحتوي بريد إلكتروني واحد على توقعات DKIM متعددة، ويعتبر "مرور" DMARK إذا تم محاذاة أي توقيع DKIM والتحقق منه.

محاذاة SPF

تقوم آلية (SPFV1) SPF بمصادقة معرفات المجالات التي تم تسليمها من:

- البريد من الهوية (البريد من الأمر)
- HELO/EHLO (أمر HELO/EHLO)

يحاول البريد من هوية المجال المصادقة بشكل افتراضي. تتم مصادقة هوية مجال HELO بواسطة DMARK فقط للرسائل التي تحتوي على بريد فارغ من الهوية، مثل رسائل الارتداد.

أحد الأمثلة الشائعة على ذلك هو حيث يتم إرسال رسالة بعنوان "بريد من" مختلف (noreply@blog.cisco.com) مقارنة بما هو موجود في الرأس "من" (noreply@cisco.com). سيتم محاذاة جزء MAIL من هوية المجال من noreply@blog.cisco.com مع مجال From Header ل noreply@cisco.com في الوضع المريح ولكن ليس في الوضع المقيد.

علامات تمييز وضع المحاذاة

يمكن تحديد أوضاع محاذاة DMARK في سجل نهج DMARK باستخدام علامات وضع المحاذاة ADKIM وASPF. تشير علامات التمييز تلك إلى الوضع المطلوب لمحاذاة معرف DKIM أو SPF.

الأوضاع يمكن ضبطها إلى مسترخي أو مقيد، مع كون الاسترخاء هو الإعداد الافتراضي إذا لم يكن هناك علامة تمييز. يمكن ضبط ذلك تحت قيمة علامة تمييز ك:

- ر: وضع الإسترخاء
- س: الوضع المقيد

المرجع

- [المعيار RFC5321 - بروتوكول نقل البريد البسيط](#)
- [المعيار RFC5322 - تنسيق رسائل الإنترنت](#)
- [المعيار RFC6376 - توقيعات البريد المعرف بواسطة \(DKIM DomainKeys\)](#)
- [المعيار RFC7208 - إطار عمل سياسة المرسل \(SPF\) للتحويل باستخدام المجالات في البريد الإلكتروني](#)
- [المعيار RFC7489 - مصادقة الرسائل والإبلاغ عنها والمطابقة القائمة على المجال \(DMARK\)](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن تسمل ا