تكوين عامل التصفية الوارد استنادا إلى التحقق من DKIM في ESA

المقدمة

يوضح هذا المستند كيفية تكوين جهاز أمان البريد الإلكتروني (ESA) لاتخاذ أي إجراء على التحقق من صحة البريد الإلكتروني المعرف لمفاتيح المجال (DKIM) من خلال تكوين عامل تصفية محتوى وارد أو عامل تصفية رسائل.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إس
- معرفة أساسية بتكوين عامل تصفية المحتوى
- معرفة أساسية بتكوين عوامل تصفية الرسائل
- معلومات حول تكوين الحجر الصحي للسياسات والفيروسات والحالات الخاصة بالفاشية مركزيا

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

التكوين

الخطوة 1. تكوين التحقق من DKIM

تأكد من تمكين التحقق من DKIM. انتقل إلى **نهج البريد > نهج تدفق البريد**.

لتكوين التحقق من DKIM على ESA يشبه التحقق من SPF. في **معلمات النهج الافتراضية** لنهج تدفق البريد، بسطاء قم بتشغيل التحقق من DKIM **إلى**.

الخطوة 2. التحقق من الإجراء النهائي

أولا، تحديد الإجراء الذي يتعين إتخاذه وفقا لعملية التحقق التي تقوم بها إدارة كيم. على سبيل المثال: إسقاط أو إضافة عالمة أو إجراء عزل. إذا كان الإجراء النهائي هو إجراء عزل للبريد، راجع إجراءات الحجر الصحي التي تم تكوينها.

- إذا كنت لا تستخدم الإدارة المركزية:

انتقل إلى **ESA >Monitor> السياسة والحجر الصحي للفيروسات والتفشي**.

- إذا قمت بتكوين الإدارة المركزية (SMA):

انتقل إلى **SMA >البريد الإلكتروني >عزل الرسائل >السياسة والحجر الصحي للفيروسات والتفشي**، كما هو موضح في الصورة:

Policy, Virus and Outbreak Quarantines

Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Las
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	
Policy	Centralized Policy	0	Retain 10 days then Delete	
Unclassified	Unclassified	0	Retain 30 days then Release	
Virus	Antivirus	0	Retain 30 days then Delete	

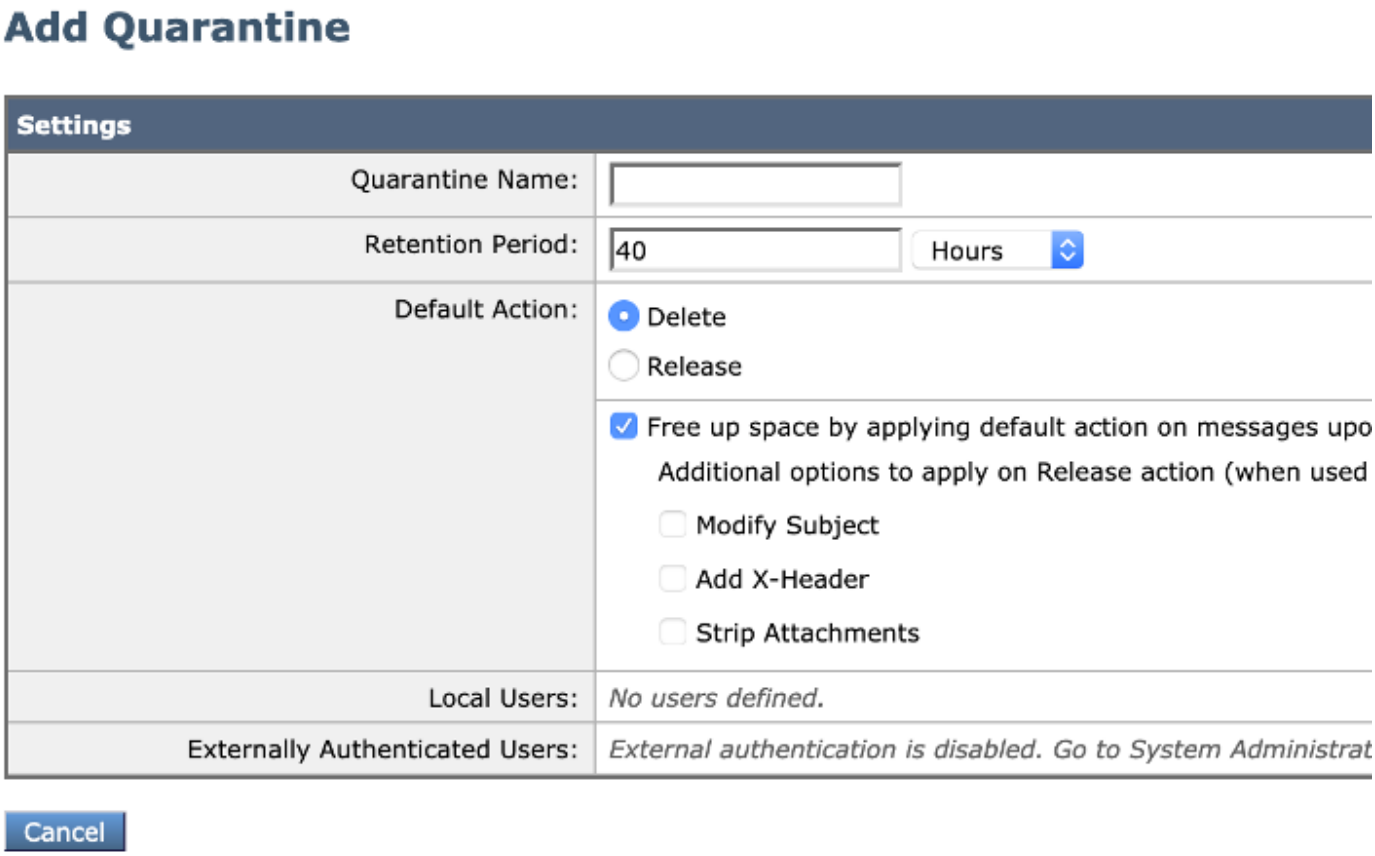
Available space for

في حالة عدم وجود حجر صحي خاص لخدمات مصادقة الرسائل المستندة إلى **DKIM**/المجال وإعداد التقارير والمطابقة (DMARK)/إطار عمل سياسة المرسل (SPF). يوصى بإنشاء واحدة.

أثناء العمل في النهج والحجر الصحي الخاص بالفيروس والتفشي، حدد **إضافة عزل النهج**:

هنا، يمكنك إعداد:

- اسم الحجر الصحي: ل ex، **DkimQuarantine**
- فترة الاستبقاء: يرجع الأمر إليك ويعتمد على إحتياجات مؤسستك والإجراء الافتراضي. بعد فترة الاستبقاء إلى البريد الإلكتروني سيتم حذفها أو إصدارها وتسليمها، ويتم تحديدها من خلال التحديد الخاص بك، كما هو موضح في الصورة:



الخطوة 3. عامل التصفية الوارد ل ESA

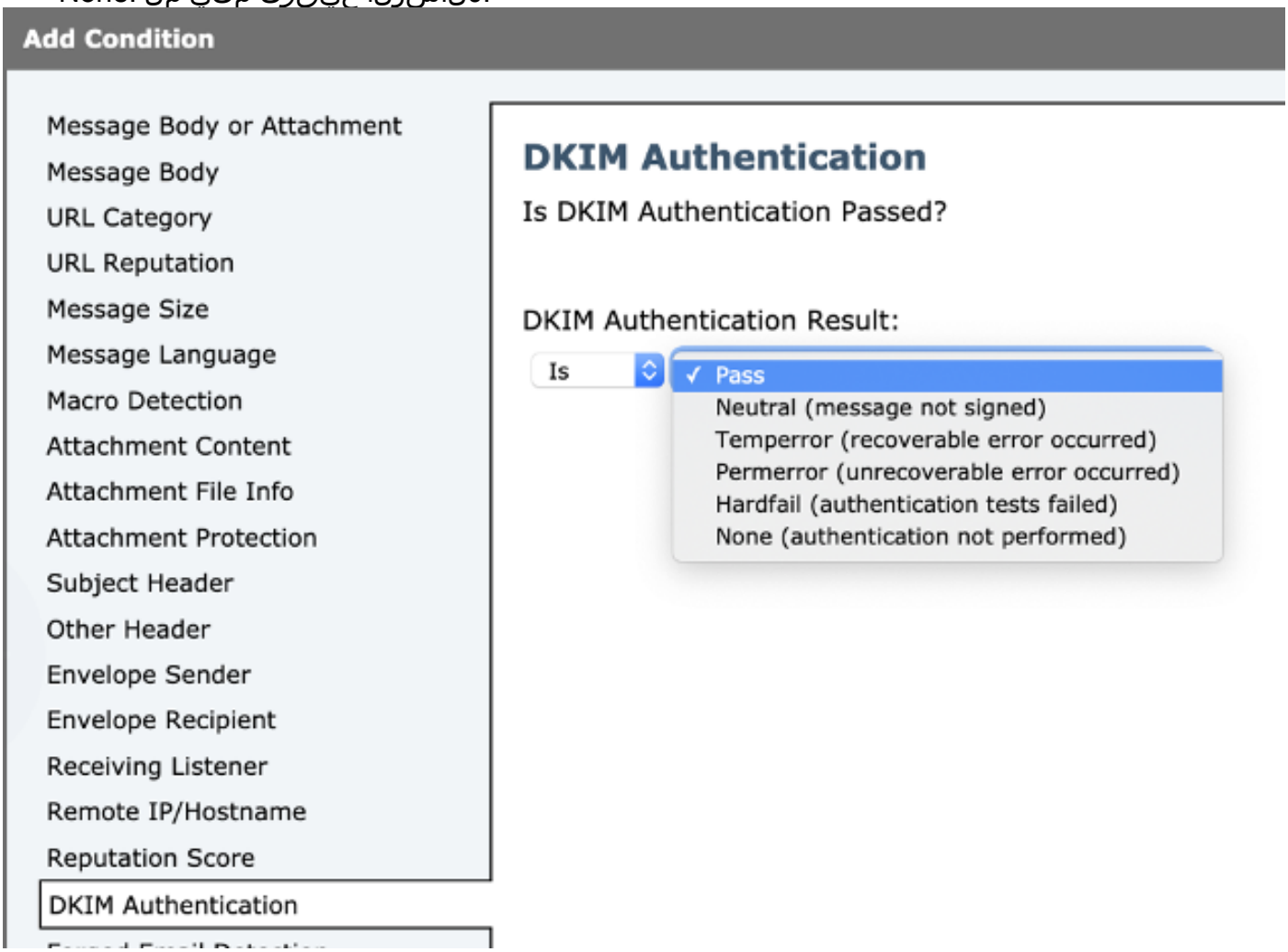
أ. إنشاء عامل تصفية محتوى وارد ل ESA:

انتقل إلى **ESA > سياسات البريد > عوامل تصفية المحتوى الواردة > إضافة عامل تصفية**.

- القسم الأول: يمكنك تكوين **الاسم والوصف والترتيب** للمرشح:

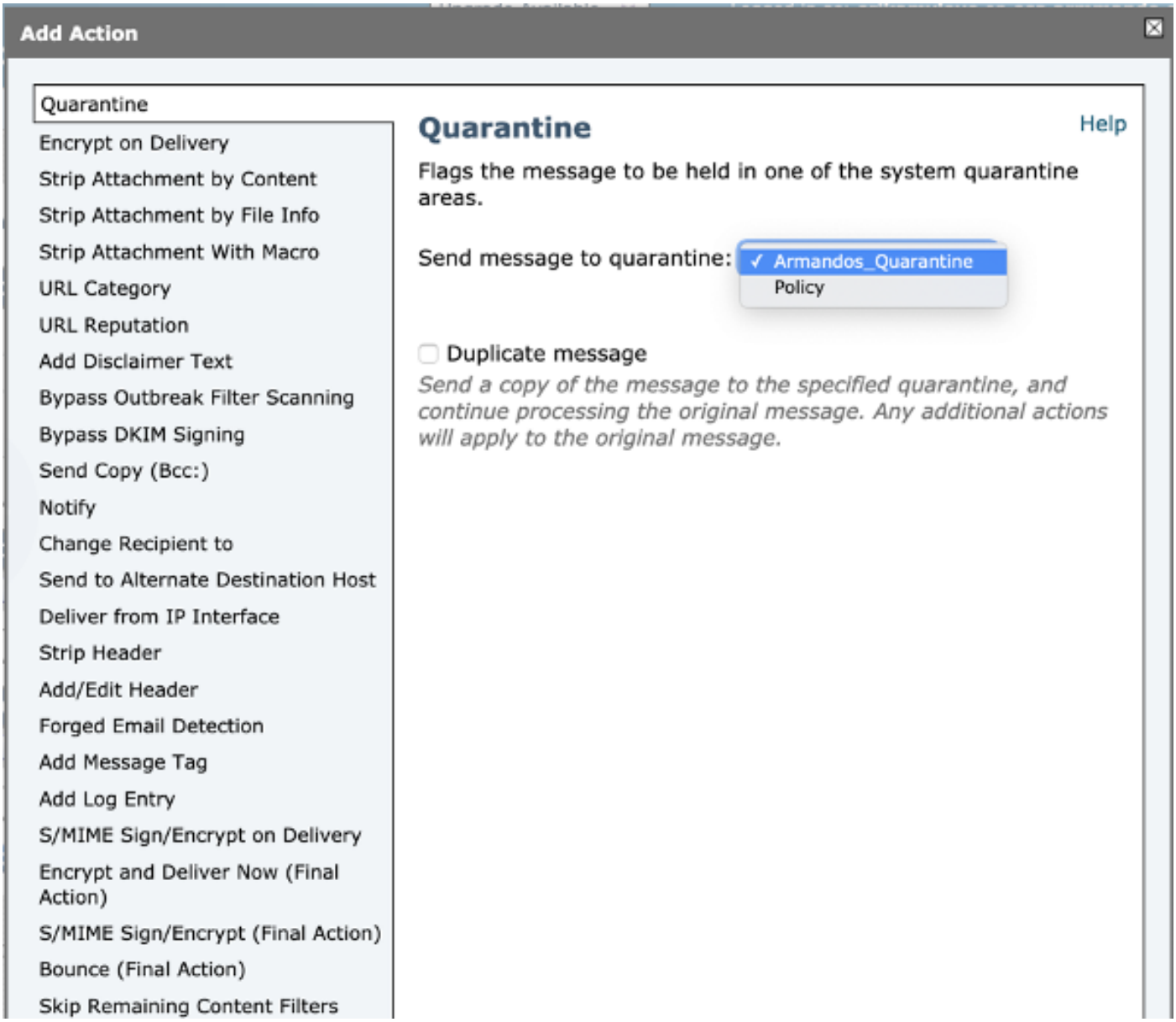
- القسم الثاني: إضافة شرط. أنت يستطيع أضفت، أكثر من واحد شرط وأنت يستطيع شكلت كثير محتوى مرشح in order to اتخذت إجراء على DKIM تدقيق: المصادقة - النتائج الموقعة والمعنى:

- نجحت الرسالة في إختبارات المصادقة.
- محايد: لم يتم إجراء المصادقة.
- درجة الحرارة: حدث خطأ قابل للاسترداد.
- بيرمينرور: حدث خطأ لا يمكن إصلاحه.
- فشل ثابت: فشلت إختبارات المصادقة.
- None. لم يتم توقيع الرسالة.



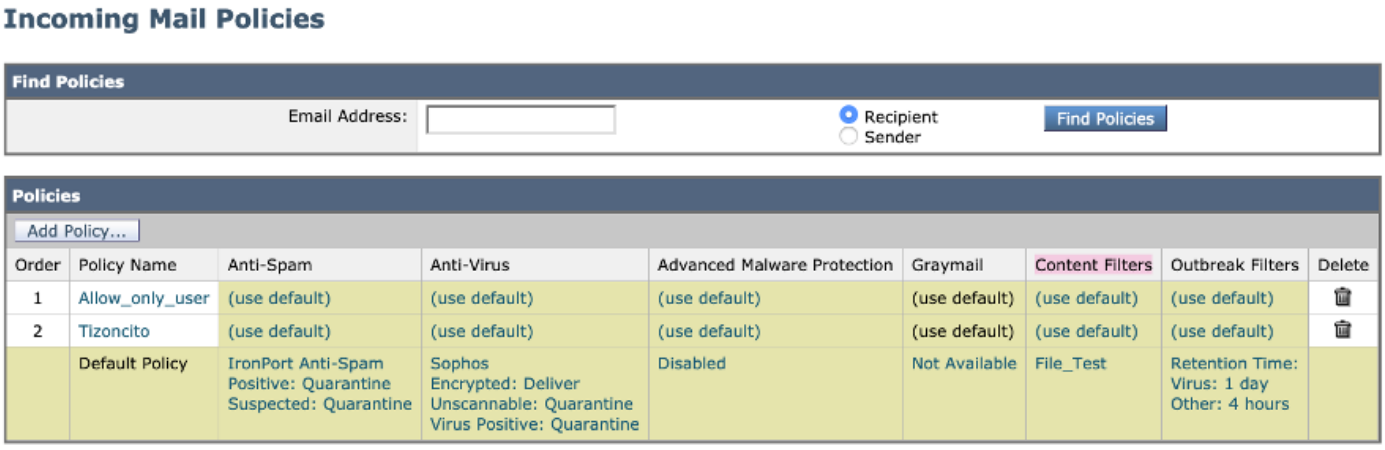
ملاحظة: متطلبات التحقق من DKIM: يجب على المرسل توقيع الرسالة قبل التحقق منها. يجب أن يحتوي مجال الإرسال على مفتاح عام متاح في DNS للتحقق.

- القسم الثالث: حدد إجراء. يمكنك إضافة أكثر من إجراء واحد مثل إضافة إدخال سجل، وإرسال إلى العزل، وإسقاط البريد الإلكتروني، والتنبيه، وما إلى ذلك. في هذه الحالة، حدد العزل المكون مسبقا، كما هو موضح في الصورة:



إضافة عامل تصفية جديد إلى نهج تدفق البريد:

بمجرد إنشاء عامل تصفية. من ESA أضف عامل التصفية على كل نهج تدفق بريد حيث تريد التحقق من DKIM باستخدام الإجراء النهائي. انتقل إلى **ESA>نهج البريد >نهج البريد الوارد**، كما هو موضح في الصورة:



انقر فوق عمود **عوامل تصفية المحتوى** و صف **نهج تدفق البريد**.

ملاحظة: لا يعني الإجراء (إستخدام الافتراضي) أنه تم تكوينه كإعدادات نهج الافتراضية. قم بتكوين كل نهج تدفق بريد مع عوامل التصفية المطلوبة.

ب. إنشاء عامل تصفية رسائل ESA:

شكلت كل رسالة مرشح من ESA CLI. أدخل **عوامل تصفية** الأوامر واتبع التعليمات:

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script.  Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

بمجرد إنشاء عامل التصفية، راجع وسيلة الإيضاح: **تمت إضافة عوامل تصفية واحدة**.

تكون الشروط والإجراءات المطلوب تكوينها هي نفسها تلك المستخدمة من قبل عامل تصفية المحتوى الوارد.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

عامل تصفية المحتوى الوارد:

- من واجهة مستخدم ويب ESA (WebUI)

أ. التحقق من تكوين عامل التصفية:

انتقل إلى **ESA >سياسات البريد >عوامل تصفية المحتوى الواردة.** يجب تكوين عامل التصفية وفقا للترتيب المحدد مسبقا في القائمة المعروضة.

ب. التحقق من تطبيق عامل التصفية:

انتقل إلى **ESA>سياسات البريد >سياسات البريد الوارد**.

يجب إظهار اسم عامل التصفية في عمود عوامل تصفية المحتوى وصف نهج تدفق البريد. إذا كانت القائمة كبيرة والاسم، انقر فوق قائمة المرشحات لتحديد عوامل التصفية المطبقة على النهج.

عامل تصفية الرسائل:

```
From ESA CLI:
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
```

```
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name

  1           Y      Y     DKIM_Filter
```

تظهر القائمة ما إذا تم تكوين عامل التصفية ونشاطه.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

التحقق من التكوين:

يجب التأكد من:

- تم تحديد نهج تدفق البريد: عند التحقق
- هناك إجراء تم تكوينه في عامل تصفية المحتوى أو عامل تصفية الرسائل
- في حالة عامل تصفية المحتوى، تحقق من أن عامل التصفية مرتبط بتدفق البريد

التحقق من تعقب الرسائل:

يسمح لنا تعقب الرسائل بالملاحظة:

- نتيجة التحقق من DKIM، على سبيل المثال:
- إدخال السجل الذي تم تكوينه (إذا تم تكوين واحد)
- عامل التصفية المطبق (الاسم والإجراء المتخذ)

تتبع من ESA:

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
```

```
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

معلومات ذات صلة

- أفضل الممارسات ESA-SPF-DKIM-DMARK
- دليل المستخدم النهائي لجهاز أمان البريد الإلكتروني
- DKIM RFC4871
- DKIM RFC8301
- DKIM RFC8463
- الدعم التقني والمستندات - Cisco Systems

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).