الكشف عن رسائل البريد الإلكتروني المنتحلة عل ESA وإنشاء إستثناءات

المحتويات

المقدمة

يوضح هذا المستند كيفية التحكم في انتحال البريد الإلكتروني عل Cisco ESA وكيفية إنشاء إستثناءات للمستخدمين المسموح لهم بإرسال رسائل البريد الإلكتروني المنتحلة.

المتطلبات الأساسية

المتطلبات

يجب أن يقوم جهاز أمان البريد الإلكتروني (ESA) بمعالجة كل من رسائل البريد الواردة والصادرة، واستخدام تكوين قياسي من Relaylist لوضع علامة عل الرسائل باعتبارها صادرة.

المكونات المستخدمة

المكونات المحددة المستخدمة تتضمن:

- القاموس: يستخدم لتخزين كافة مجالاتك الداخلية.
- عامل تصفية الرسائل: يستخدم للتعامل مع المنطق لاكتشاف البريد الإلكتروني

المنتحلة وإدخال رأس يمكن لعوامل تصفية المحتوى العمل عليه.
- عزل النهج: يستخدم لتخزين تكرارات رسائل البريد الإلكتروني المنتحلة مؤقتا. ضع في الاعتبار إضافة عنوان IP للرسائل التي تم إصدارها إلى MY_TRUSTED_SPOOF_HOSTS لمنع الرسائل المستقبلية من هذا المرسل من إدخال عزل النهج.
- MY_TRUSTED_SPOOF_HOSTS: قائمة للإشارة إلى عناوين IP للإرسال الموثوق بها. تؤدي إضافة عنوان IP للمرسل إلى هذه القائمة إلى تخطي العزل والسماح للمرسل بالمخالفة. يمكنك وضع المرسلين الموثوق بهم في مجموعة المرسلين MY_TRUSTED_SPOOF_HOSTS حتى لا يتم عزل الرسائل المنتحلة من هؤلاء المرسلين.
- Relaylist: قائمة لمصادقة عناوين IP المسموح بها للترحيل، أو إرسال بريد إلكتروني صادر. في حالة تسليم البريد الإلكتروني عبر مجموعة المرسلين هذه، يفترض أن الرسالة ليست رسالة منتحلة.

ملاحظة: إذا تم إستدعاء أي من مجموعتي المرسلين بشيء مختلف عن RELAYLIST، وأ MY_TRUSTED_SPOOF_HOSTS، فيجب عليك تعديل عامل التصفية باسم مجموعة المرسلين المرادف. أيضا، إذا كان لديك عدة مستمعين، فسيكون لديك أكثر من مستمع واحد من MY_TRUSTED_SPOOF_HOSTS.

تستند المعلومات الواردة في هذا المستند إلى ESA مع أي إصدار من AsyncOS.

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.

معلومات أساسية

يتم تمكين الانتحال بشكل افتراضي على Cisco ESA. هناك العديد من الأسباب الصالحة للسماح للمجالات الأخرى بالإرسال نيابة عنك. وكمثال شائع على ذلك، يريد مسؤول ESA التحكم في رسائل البريد الإلكتروني المنتحلة من خلال وضع الرسائل المنتحلة في الحجر الصحي قبل تسليمها.

لاتخاذ إجراء معين مثل إجراء عزل على البريد الإلكتروني المنتحلة، يجب أولا الكشف عن البريد الإلكتروني المنتحلة.

ما هو انتحال البريد الإلكتروني

انتحال البريد الإلكتروني هو تزييف رأس البريد الإلكتروني بحيث يبدو أن الرسالة نشأت من شخص ما أو مكان ما غير المصدر الحقيقي. انتحال رسائل البريد الإلكتروني هو تكتيك يستخدم في حملات التصيد الاحتيالي والرسائل غير المرغوب فيها لأن الناس يكونون أكثر ميلا لفتح رسالة بريد إلكتروني عندما يعتقدون أنها مرسلة من مصدر شرعي.

كيفية اكتشاف البريد الإلكتروني المنتحل

ترى تصفية أية رسائل تحتوي على مرسل مظروف (من) وسهل من (من) رأس يحتوي

على أحد المجالات الواردة الخاصة بك في عنوان البريد الإلكتروني.

كيفية السماح بالانتحال لمرسلين محددين

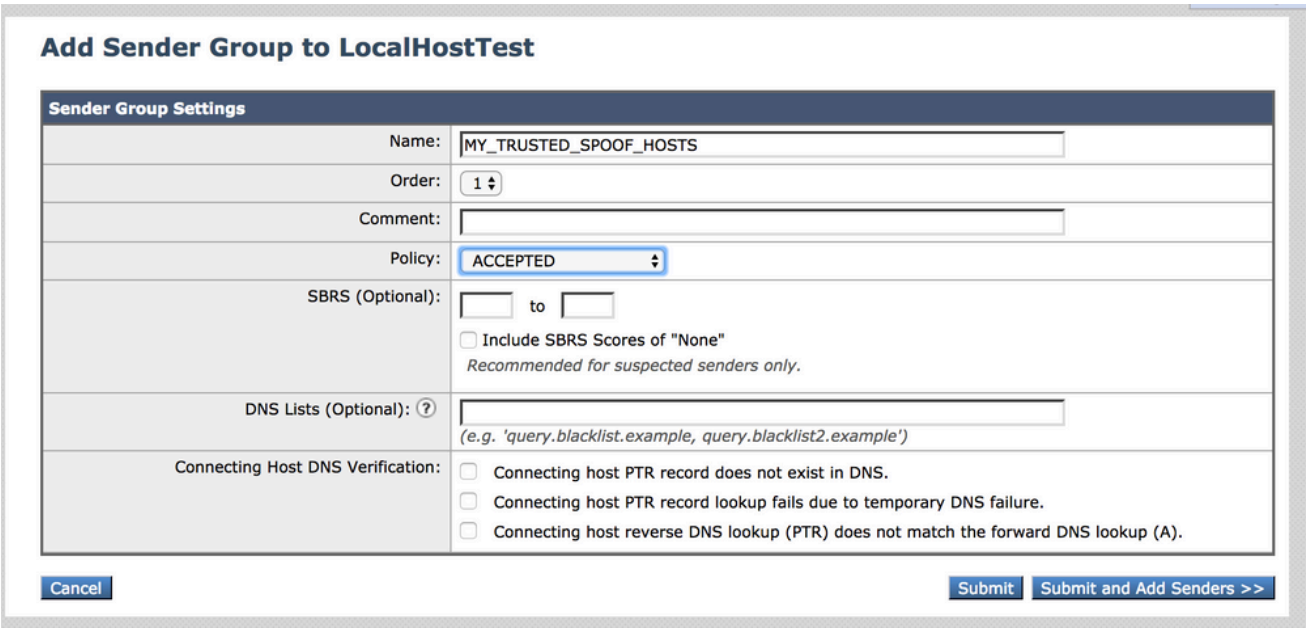
عند تنفيذ عامل تصفية الرسائل المتوفر ضمن هذه المقالة، يتم وضع علامة على الرسائل المنتحلة باستخدام رأس، ويستخدم عامل تصفية المحتوى التالي إجراء على الرأس . الإضافة إستثناء، ما عليك سوى إضافة عنوان IP الخاص بالمرسل إلى MY_TRUSTED_SPOOF_HOSTS.

التكوين

إنشاء SendGroup

1. من واجهة المستخدم الرسومية ESA، انتقل إلى سياسات البريد > نظرة عامة
2. انقر إضافة.
3. في حقل "الاسم"، حدد MY_TRUSTED_SPOOF_HOSTS.
4. في حقل الأمر، حدد 1.
5. لحقل النهج، حدد مقبول.
6. انقر فوق إرسال لحفظ التغييرات.
7. أخيرا، انقر فوق تنفيذ التغييرات لحفظ التكوين

مثال:



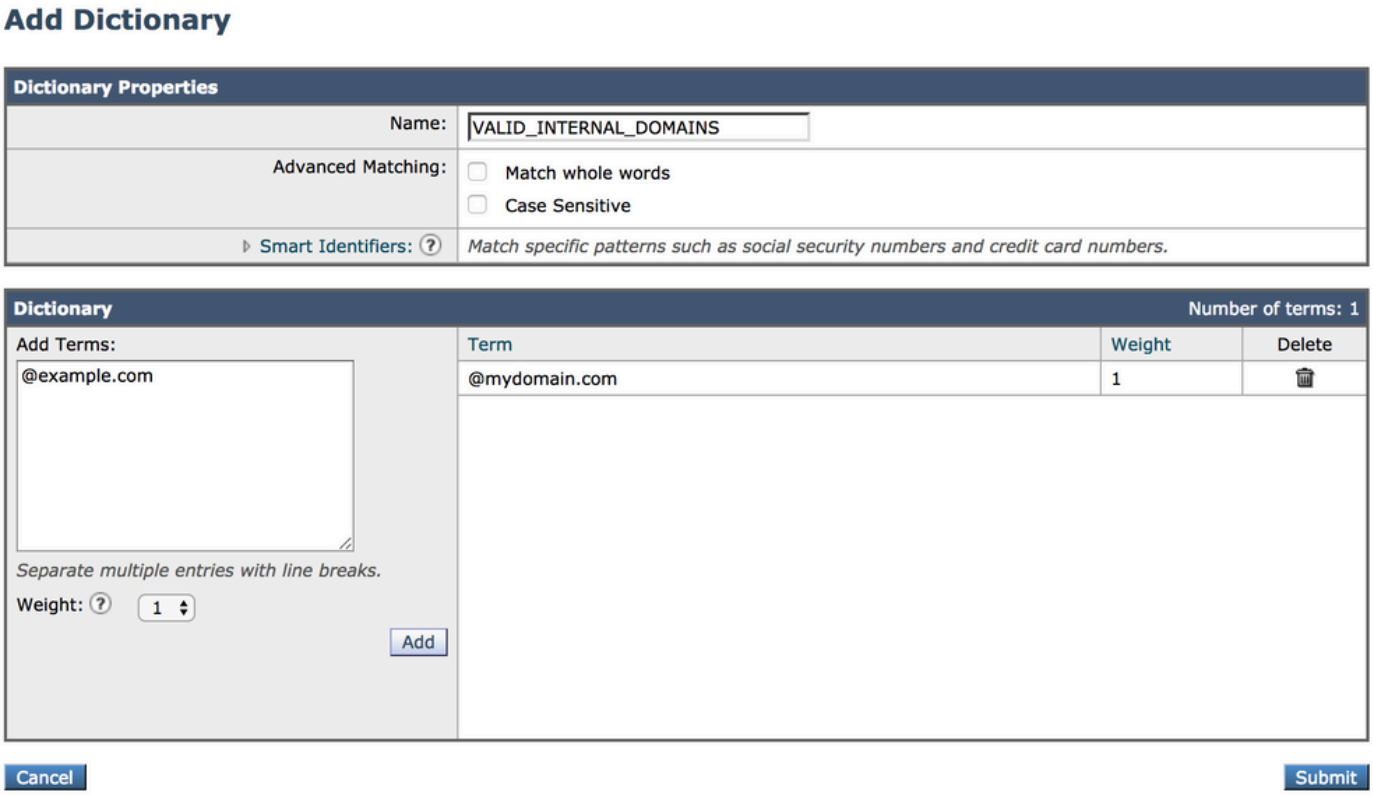
إنشاء قاموس

قم بإنشاء قاموس لكل المجالات التي تريد تعطيل الانتحال لها على ESA:

1. من واجهة المستخدم الرسومية (GUI) ل ESA، انتقل إلى سياسات البريد > القواميس.
2. انقر إضافة قاموس.
3. في حقل "الاسم"، حدد "VALID_INTERNAL_DOMAINS"، لإجراء النسخ واللصق لعامل تصفية الرسائل خاليا من الأخطاء.
4. تحت إضافة شروط، قم بإضافة كل المجالات التي تريد اكتشاف الانتحال. أدخل المجال مع علامة @ قبل انتظار المجال وانقر فوق إضافة.

5. تأكد من إلغاء تحديد خانة إختيار مطابقة الكلمات بأكملها.
6. انقر فوق إرسال لحفظ تغييرات القاموس.
7. أخيرا، انقر فوق تنفيذ التغييرات لحفظ التكوين.

مثال:



إنشاء عامل تصفية رسالة

بعد ذلك، تحتاج إلى إنشاء عامل تصفية رسائل للاستفادة من القاموس الذي تم إنشاؤه للتو، "VALID_INTERNAL_DOMAINS":

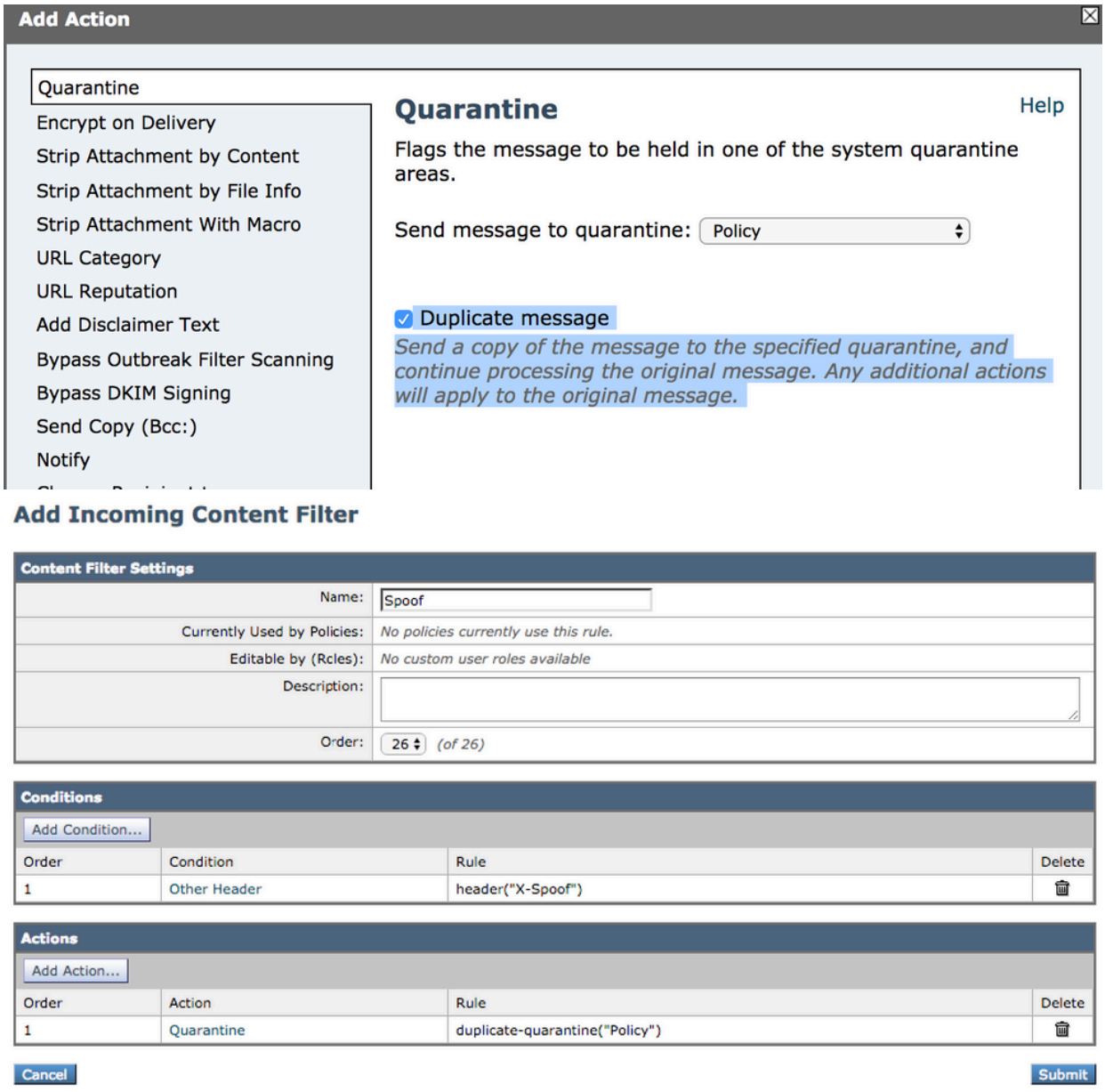
1. ربطت إلى الأمر خط قارن (CLI) من ال ESA.
2. قم بتشغيل عوامل تصفية الأوامر.
3. قم بتشغيل الأمر جديد لإنشاء عامل تصفية رسالة جديد.
4. نسخ مثال عامل التصفية هذا ولصقه، مع إجراء تحريرات لأسماء مجموعة المرسلين الفعلية إذا لزم الأمر:

```
mark_spoofed_messages:
if(
     (mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
 OR  (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
 AND ((sendergroup != "RELAYLIST")
 AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
  )
{
insert-header("X-Spoof", "");
}
```

5. ارجع إلى موجه أوامر واجهة سطر الأوامر (CLI) الرئيسية وشغل الالتزام لحفظ التكوين.
6. انتقل إلى واجهة المستخدم الرسومية (GUI) > سياسات البريد > عوامل تصفية المحتوى الواردة
7. إنشاء عامل تصفية محتوى وارد يتخذ إجراء على عنوان X-Spoof:

    1. إضافة رأس آخر
    2. اسم الرأس: X-Spoof
    3. زر انتقاء عنوان موجود
    4. إضافة إجراء: نسخ إحتياطي (نهج).

> **ملاحظة:** تحتفظ ميزة تكرار الرسالة الموضحة هنا بنسخة من الرسالة، وتستمر في إرسال الرسالة الأصلية إلى المستلم.



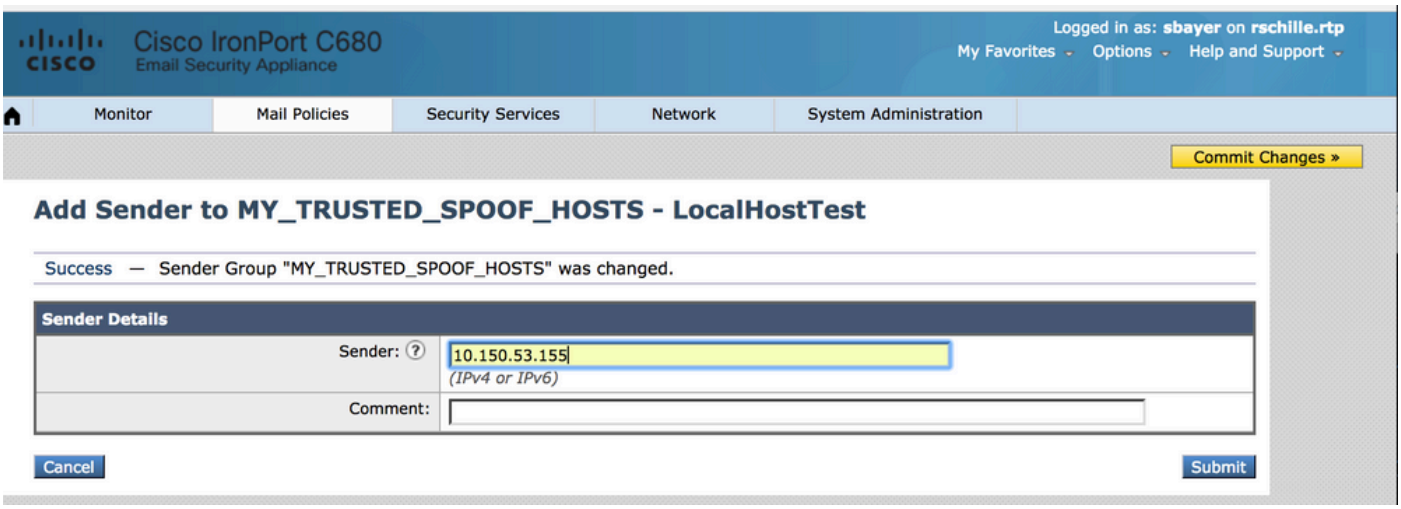
8. ربط عامل تصفية المحتوى بسياسات البريد الوارد في واجهة المستخدم الرسومية (GUI) > سياسات البريد> سياسات البريد الوارد.
9. إرسال التغييرات وتنفيذها.

إضافة إستثناءات لمنصتي_TRUSTED_SPOOF_HOSTS

أخيرا، تحتاج إلى إضافة خاصية الاستثناءات (عناوين IP أو أسماء المضيف) إلى مجموعة معرف MY_TRUSTED_SPOOF_HOST.

1. التنقل عبر واجهة المستخدم الرسومية (GUI) عبر الويب: سياسات البريد > نظرة عامة على HAT
2. انقر فوق مجموعة المرسلين MY_TRUSTED_SPOOF_HOSTS وقم بفتحها.
3. انقر فوق إضافة مرسل... لإضافة عنوان IP أو النطاق أو اسم المضيف أو اسم المضيف الجزئي.
4. انقر فوق إرسال لحفظ تغييرات المرسل.
5. أخيرا، انقر فوق تنفيذ التغييرات لحفظ التكوين.

مثال:



التحقق من الصحة

التحقق من عزل الرسائل المنتحلة

إرسال رسالة إختبار تحدد أحد مجالاتك كمرسل المظروف. تحقق من صحة عمل عامل التصفية كما هو متوقع من خلال تنفيذ تعقب رسالة على تلك الرسالة. النتيجة المتوقعة هي عزل الرسالة لأنك لم تقم بإنشاء أي إستثناءات بعد لوكلاء المرسلين المسموح لهم بالانتحال.

<#root>

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <xxxx_xxxx@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT in the i
```

```
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
```

Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message filter:quarantine_spoofed_messag

```
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

التحقق من تسليم رسائل إستثناء اسم المستخدم

يعد مرسلو الاستثناء الانتحال عناوين IP في مجموعة (مجموعات) المرسل المشار إليها في عامل التصفية أعلاه.

تتم الإشارة إلى Relaylist لأنه يتم إستخدامه من قبل ESA لإرسال بريد صادر. عادة ما تكون الرسائل التي يتم إرسالها بواسطة Relaylist بريد صادر، والذي تضمين هذه إلى إنشاء إيجابيات خاطئة أو رسائل صادرة يتم وضعها في الحجر الصحي بواسطة عامل التصفية أعلاه.

مثال تعقب الرسائل لعنوان IP الخاص بخاصية الاستثناء الذي تمت إضافته إلى MY_TRUSTED_SPOOF_HOSTS. يتم تسليم الإجراء المتوقع وليس إجراء عزل. (يسمح لهذا IP بالانتحال).

<#root>

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <user_xxxx@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT in the i
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598
```

Message accepted for delivery'

```
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

معلومات ذات صلة

- تصفية بريد ESA المنتحلة
- حماية المعلقة باستخدام التحقق من المرسل

المعلومات الداخلية من Cisco

هناك طلب ميزة حول تعريض RAT لمرشحات الرسائل/عوامل تصفية المحتوى لتبسيط هذه العملية:

معرف تصحيح الأخطاء من Cisco CSCus49018 - ENH: عرض جدول وصول المستلم (RAT) لتصفية الشروط

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).