# حماية المعلقة باستخدام التحقق من المرسل

## المحتويات



## المقدمة

بشكل افتراضي، لا يمنع جهاز أمان البريد الإلكتروني (ESA) من التسليم الوارد للرسائل التي يتم مخاطبتها "من" نفس المجال من الانتقال إلى نفس المجال. وهذا يسمح "بخداع" الرسائل من قبل شركات خارجية تمارس أعمال مشروعة مع العميل. تعتمد بعض الشركات على منظمة الطرف الثالث لإرسال البريد الإلكتروني نيابة عن الشركة مثل الرعاية الصحية ووكالات السفر، إلخ.

## حماية المعلقة باستخدام التحقق من المرسل

### تكوين سياسة تدفق البريد (MFP)

1. من واجهة المستخدم الرسومية: **سياسات البريد > سياسات تدفق البريد > إضافة سياسة...**
2. قم بإنشاء MFP جديد باستخدام اسم ذي صلة مثل SPOOF_ALLOW
3. في قسم *التحقق من المرسل*، قم بتغيير تكوين جدول إستثناء *إستخدام التحقق من المرسل* من **إستخدام الإعداد الافتراضي** إلى **إيقاف التشغيل**.
4. في **نهج البريد > نهج تدفق البريد > معلمات النهج الافتراضية**، قم بتعيين تكوين *جدول إستثناء التحقق من المرسل إلى* **قيد التشغيل**.

### تكوين HAT

1. من واجهة المستخدم الرسومية: **سياسات البريد > نظرة عامة على HAT > إضافة مجموعة مرسل...**
2. قم بتعيين الاسم وفقا لذلك إلى MFP الذي تم إنشاؤه مسبقا، أي SPOOF_ALLOW.
3. قم بتعيين الترتيب بحيث يكون أعلى من مجموعتي AllowList و BLOCKLIST Sender.
4. قم بتعيين نهج SPOOF_ALLOW إلى إعدادات "مجموعة المرسلين" هذه.
5. انقر فوق **إرسال وإضافة المرسلين...**
6. قم بإضافة عناوين IP أو المجالات التي تهاجم خارجية ترغب السماح لها باختطاف المجال الداخلي.

### تكوين جدول الاستثناء

1. من واجهة المستخدم الرسومية: **نهج البريد > جدول الاستثناء > إضافة إستثناء التحقق من المرسل...**
2. إضافة المجال المحلي إلى جدول إستثناء التحقق من المرسل
3. تعيين إلى **رفض**

# التحقق من الصحة

عند هذه النقطة، سيتم رفض البريد الوارد من *Your.domain* إلى *your.domain* ام لم يتم إدراج MFP ال بـ اقترانه سيكون حيث ،المرسلين مجموعة الخاص بـ SPOOF_ALLOW في المرسل استثناء التحقق من المرسل يستخدم جدول إستثناء التحقق من المرسل.

وسيظهر مثال على ذلك من خلال إكمال جلسة عمل برنامج telnet يدوي للمستمع:

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

تم تكوين ESA على إستجابة SMTP العام 553 تتيجة مباشرة لجدول الاستثناءات كما تم الخطوات الوارد أعلاه.

من سجلات البريد، يمكن رؤية عنوان IP الخاص بـ 192.168.0.9 غير موجود في عنوان IP الصحيح لمجموعة المرسلين الصحيحة:

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

سيظهر عنوان IP مسموح به مطابق لعينة التكوين من الخطوات أعلاه على النحو التالي:

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
```

```
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

## معلومات ذات صلة

- البحث في السجلات باستخدام Regex مع WSA GREP و SMA و ESA
- تحديد المصير النهائي لرسالة ESA
- 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).