

عميق ينعت اذام: ESA لوح ةل وادتم ةلئسأ كنكمي فيكو، "none" ب ةصاخلا SBRS ؟تامالعل هذه فاشتكأ

المحتويات

[المقدمة](#)

[ماذا تعني قيمة SBRS ل "none"، وكيف يمكنك الكشف عن هذه العلامات؟](#)

المقدمة

يوضح هذا المستند كيفية فهم نقاط سمعة (SBRS) SenderBase واكتشافها.

ماذا تعني قيمة SBRS ل "none"، وكيف يمكنك الكشف عن هذه العلامات؟

يتم تعيين SBRS إلى عنوان IP بناء على أكثر من 50 عاملا مختلفا، مثل حجم البريد الإلكتروني وشكاوى المستخدم وضربات spamtrap. يمكن أن تتراوح SBRS من -10 إلى +10، وتعكس احتمال أن يكون البريد من عنوان IP المرسل بريد عشوائي. تشير النتائج السلبية للغاية إلى المرسلين الذين من المرجح جدا أن يرسلوا بريد عشوائي، وتشير النتائج الإيجابية للغاية إلى المرسلين الذين من غير المحتمل أن يرسلوا بريد عشوائي.

ومع ذلك، تحتوي بعض عناوين IP على علامة SenderBase "بلا". إذا لم يتمكن ESA من الاتصال بخوادم SBRS، فإن عنوان IP المتصل يستلم علامة "none". بيانات SBRS في الوقت المناسب تماما ولا يقوم الجهاز بتخزين علامات SBRS في ذاكرة مؤقتة لأكثر من 30 دقيقة تقريبا. في حالة وجود مشكلة اتصال منقطعة بخوادم SBRS، من المحتمل أن يظهر عنوان IP "الذي تم تسجيله" سابقا كعلامة "لا شيء".

وإلا، فإن نتيجة SenderBase تستند إلى بيانات موضوعية يجمعها SenderBase حول عنوان IP. من المحتمل عدم وجود محفوظات ومعلومات كافية لعنوان IP معين لتخصيص سمعة دقيقة له. هذا يعني أن حجم البريد الوارد من عنوان IP على مدار الـ 30 يوما الماضية منخفض جدا، أو لم يتم رؤية أي بريد في تلك الفترة الزمنية. قام SenderBase بتحديد أن عنوان IP هذا يحتوي على حجم صوت منخفض، يتم حسابه باستخدام عينة من إجمالي حركة مرور البريد الإلكتروني على مستوى العالم. في حالة وجود حجم صوت منخفض لخدم/مجال معين، قد لا يظهر في النماذج التي تم تجميعها بواسطة SenderBase. قد لا يكون مستوى الحجم مرتفعا بما يكفي ليكون ذا دلالة إحصائية. لا توجد عتبة دقيقة للوقت الذي تكون فيه حركة المرور مرتفعة بما يكفي لبدء تجميع نقطة، ولكن يقدر أن تكون حركة مرور البريد الإلكتروني الحالية حوالي عشرة مليارات رسالة في اليوم. قد تقوم أفضل الأجهزة المضيفة المرسله في يوم معين بإرسال ما يقرب من عشرة ملايين رسالة كل يوم. في ظل هذه الخلفية، من غير المحتمل أن يتم تسجيل خادم يرسل بضع مئات من رسائل البريد الإلكتروني يوميا. لا توجد شكاوى حول عنوان IP هذا، ولا يظهر هذا العنوان على أي من القوائم السوداء المستندة إلى DNS.

ملاحظة: لا تساوي نتيجة "لا شيء" درجة "0". وتعني درجة 0.0 أن SenderBase قد جمعت كميات متساوية من المعلومات الإيجابية والسلبية عن هذا المرسل، وخصت له سمعة محايدة

من السهل إضافة مرسلي السمعة "none" إلى مجموعة SENDERGROUP عبر واجهة المستخدم الرسومية (GUI) عبر الويب:

انتقل إلى سياسات البريد < نظرة عامة على HAT واختر SendGroup. توصي Cisco بالانتقال إلى "SuspectedList" < تحرير الإعدادات وتحديد خانة الاختيار لإضافة المرسلين "none" الذين تم تسجيلهم إلى المجموعة.

ملاحظة: لا توصي Cisco برفض الاتصالات من المرسلين "بلا" ل SBRS أو إسقاطها. إذا كانت هناك مشكلة تمنع الاتصال بمزرعة SBRS الزائدة عن الحاجة، فإن جهاز أمان البريد الإلكتروني من (Cisco (ESA الخاص بك سيسقط كل البريد الوارد الخاص بك. في معظم الحالات، يجب عليك استخدام نهج قبول أو كبح تدفق البريد بدلاً من ذلك

يمكن تغيير مجموعات المرسلين هذه على أساس كل مرسل إذا قمت بإضافة عنوان IP الخاص بالمرسل إلى مجموعة مرسل في "جدول الوصول إلى المضيف" (HAT). إذا كنت تريد مطابقة "بلا" في عامل تصفية الرسائل في SenderBase Reputation، لا يمكنك إدخال:

```
"if (reputation == "(?i)none"
```

وذلك لأن السمعة هي قيمة رقمية، ولا يمكن مقارنتها بسلسلة. على أي حال، مرشح سلبي بسيط سيطابق علامات "بلا":

```
:sbrs_none  
(if not (reputation <= 10  
}  
;('insert-header('X-SBRS-none', '$reputation  
{
```

ملاحظة: يكون سلوك مقارنات نقاط SBRS هو نفسه إذا تم تعطيل نقاط SBRS على مستمع أو إذا كانت مفقودة بالفعل: في كلتا الحالتين، تكون البيانات مفقودة.

