CSC 6.x: مثال تكوين سمعة البريد الإلكتروني

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين سمعة البريد الإلكتروني على الوحدة النمطية لخدمات أمان المحتوى والتحكم (CSC) من Cisco.

المتطلبات الأساسية

المتطلبات

تحتاج إلى ترخيص Security Plus لاستخدام هذه الميزة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco Content Security and Control SSM باستخدام إصدار البرنامج 6.3.

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

سمعة البريد الإلكتروني هي تقنية تقلل من رسائل البريد العشوائي. من خلال تمكين هذه الميزة، يتحقق CSC SSM مما إذا كان منشئ البريد عنوانا مدرجا في القائمة السوداء أم لا. تحتفظ بقائمة قواعد البيانات التي تحتوي على جميع عناوين IP التي تصدر رسائل البريد العشوائي. في حالة العثور على منشئ بريد من هذه القائمة، يعتبر هذا البريد البريد البريد غير هام ويتم إسقاطه.

مستويات الخدمة التي تقدمها تقنية سمعة البريد الإلكتروني (ERS) هي نوعان بشكل أساسي. تستند هذه الخدمات بشكل رئيسي إلى مستوى أصالة عناوين IP للمصدر.

- ERS Standard - يحتوي على المصادر المعروفة للبريد العشوائي
- ERS Advanced - يحتوي على المصادر المعروفة والمصادر المشتبه بها

عند إضافة عنوان IP إلى قاعدة بيانات ERS القياسية، يطلق عليه مصدر بريد عشوائي ومن النادر أن تلاحظ عنوان IP الذي تمت إزالته من هذه القائمة. يحتوي "معيار ERS" على قائمة عناوين IP التي تقوم بإنشاء البريد العشوائي بشكل ثابت.

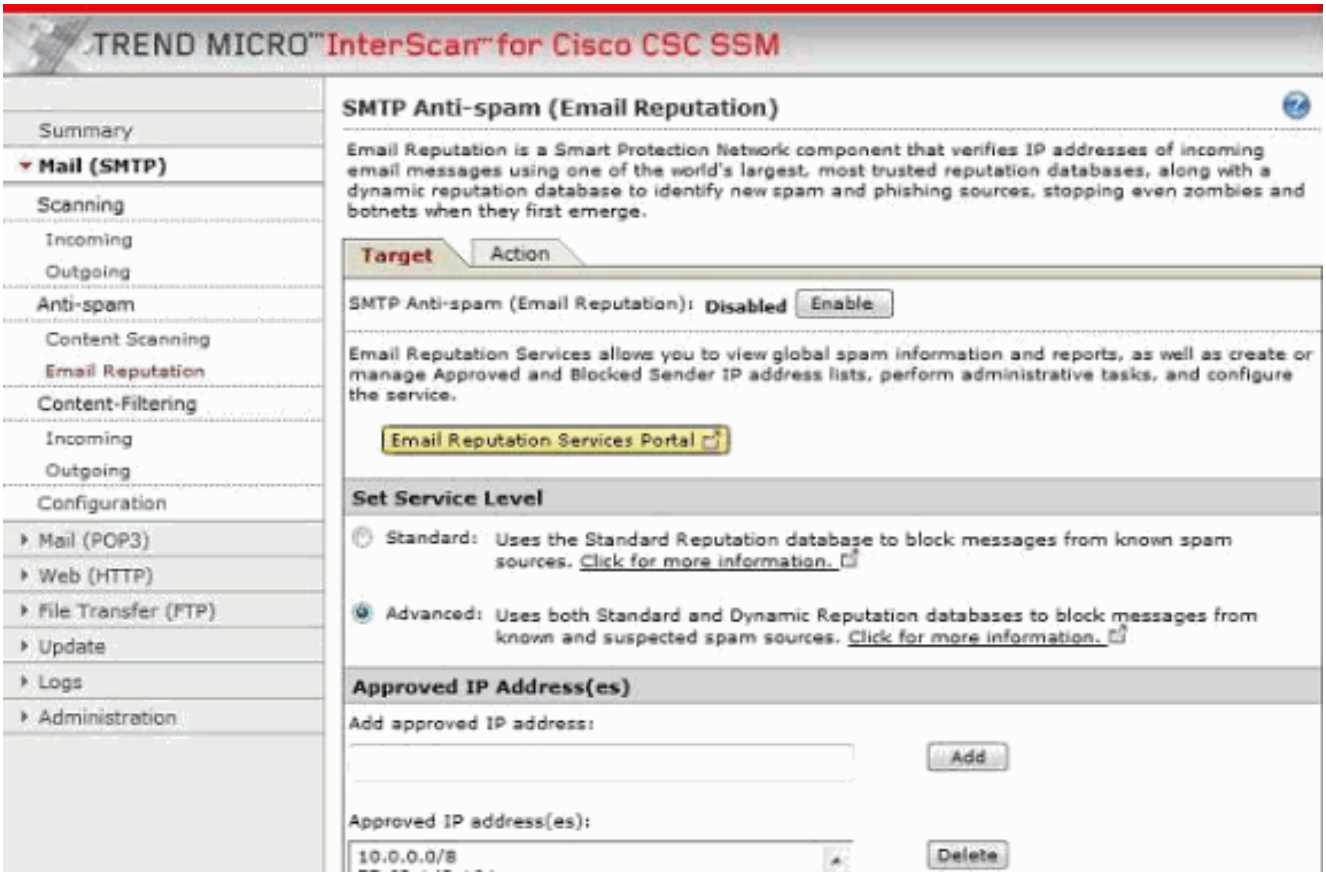
تحتوي ERS Advanced على قائمة بعناوين IP التي من المفترض إزالتها إذا تبين أنها لا تنتج البريد العشوائي بعد ذلك. على سبيل المثال، يمكن إدراج خادم بريد تم إختراقه في قاعدة البيانات هذه في الوقت الذي تم فيه إختراقه. عند استعادته إلى الوضع الطبيعي، تتم إزالته من قاعدة البيانات هذه.

التكوين

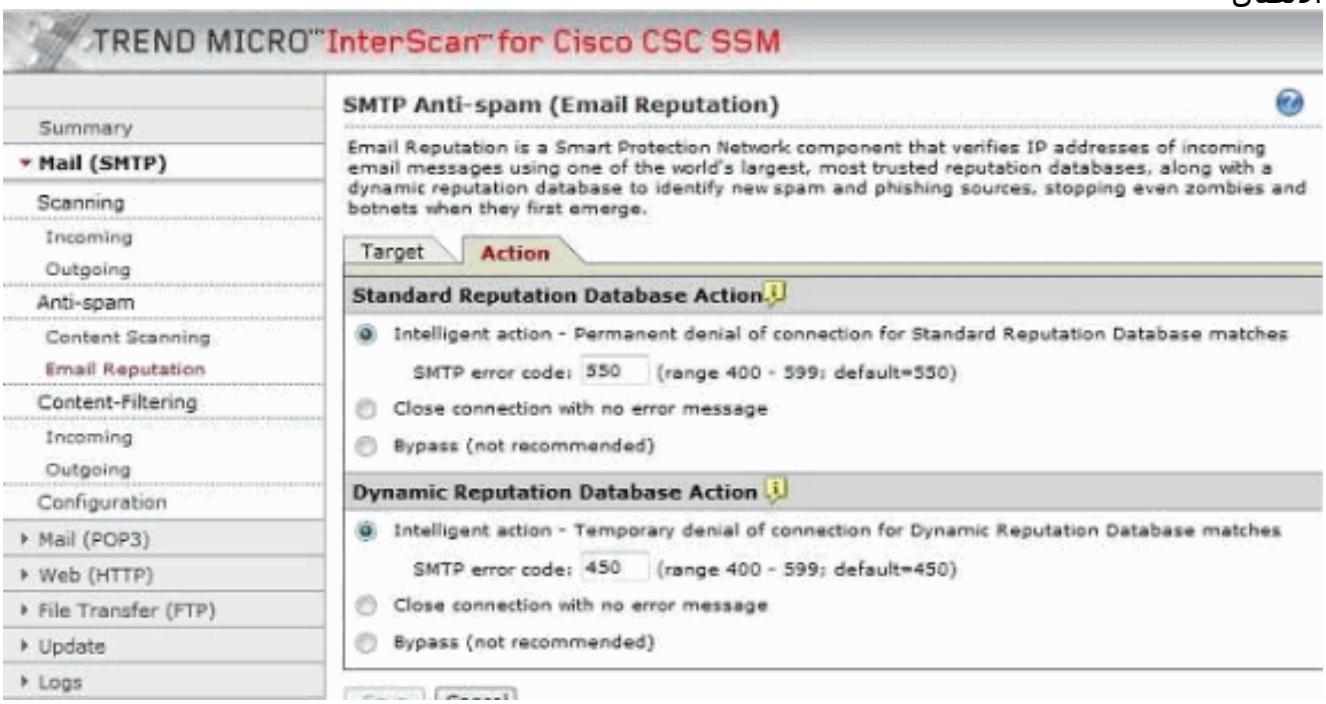
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

1. أختر **بريد (SMTP) > مكافحة البريد العشوائي > سمعة البريد الإلكتروني**. تفتح نافذة جديدة.
2. من علامة التبويب الهدف، انقر فوق **تمكين** لتمكين ميزة سمعة البريد الإلكتروني هذه.
3. أختر **متقدم** لمستوى الخدمة.
4. من حقل عناوين IP المعتمدة، حدد نطاق عناوين IP التي تريد إعفاؤها من المسح الضوئي.



5. من علامة التبويب "إجراء"، حدد نوع الإجراء المستند إلى نهج أمان المؤسسة. تتوفر هذه الإجراءات الثلاثة:إغلاق الاتصال برسالة خطأإغلاق الاتصال بدون رسالة خطأتجاوز الاتصال



التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تعذر تلقي رسائل البريد الإلكتروني من بعض المجالات

المشكلة:

المشكلة هي عدم القدرة على تلقي رسائل البريد الإلكتروني من مجالات معينة. يبدو أن وحدة CSC تمنع رسائل البريد الإلكتروني. عند تجاوز الوحدة، فإن كل شيء يعمل بشكل جيد. يتم تلقي رسالة الخطأ هذه: 06/02/2012 GMT+00:00 NRS 174.37.94.181 RBL-Fail QIL-NA RejectWithErrorCode-550 NA 0 NA 0 NA 14:33:00

الحل:

شكلت in order to حللت هذا إصدار، البريد الإلكتروني سمعة سمة بشكل صحيح.

معلومات ذات صلة

- دعم الوحدة النمطية Cisco ASA Content Security and Control (CSC) Security Services Module
- 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).