

ديربل اة عم س ني وكت ل اثم : CSC 6.x ينورت ك ل ا ل ا

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [تعذر تلقي رسائل البريد الإلكتروني من بعض المجالات](#)
- [معلومات ذات صلة](#)

المقدمة

يقدم هذا المستند نموذجاً 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 عنواناً مدرجاً 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 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 "معياري 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، تم إزالته من قاعدة البيانات هذه.

التكوين

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

ملاحظة: استخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

1. أخطر 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. أخطر متقدم لمستوى الخدمة.
4. من حقل عناوين IP المعتمدة، حدد نطاق عناوين IP التي تريد إعفاؤها من المسح الضوئي.

TREND MICRO™ InterScan™ for Cisco CSC SSM

SMTP Anti-spam (Email Reputation)

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

Target **Action**

SMTP Anti-spam (Email Reputation): **Disabled**

Email Reputation Services allows you to view global spam information and reports, as well as create or manage Approved and Blocked Sender IP address lists, perform administrative tasks, and configure the service.

[Email Reputation Services Portal](#)

Set Service Level

Standard: Uses the Standard Reputation database to block messages from known spam sources. [Click for more information.](#)

Advanced: Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. [Click for more information.](#)

Approved IP Address(es)

Add approved IP address:

Approved IP address(es):

10.0.0.0/8

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

TREND MICRO™ InterScan™ for Cisco CSC SSM

SMTP Anti-spam (Email Reputation)

Email Reputation is a Smart Protection Network component that verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases, along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets when they first emerge.

Target **Action**

Standard Reputation Database Action

Intelligent action - Permanent denial of connection for Standard Reputation Database matches
SMTP error code: 550 (range 400 - 599; default=550)

Close connection with no error message

Bypass (not recommended)

Dynamic Reputation Database Action

Intelligent action - Temporary denial of connection for Dynamic Reputation Database matches
SMTP error code: 450 (range 400 - 599; default=450)

Close connection with no error message

Bypass (not recommended)

[التحقق من الصحة](#)

لا يوجد حالياً 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 \(CSC\) Security Services Module Cisco ASA Content Security and Control](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

