مثال تكوين تشفير البريد الإلكتروني ESA

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد تشفير البريد الإلكتروني على جهاز أمان البريد الإلكتروني (ESA).

المتطلبات الأساسية

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الطراز: جميع الفئة C والفئة X
- ميزة تشفير المغلفات (PostX) المثبتة

التكوين

تمكين تشفير البريد الإلكتروني على ESA

أتمت هذا steps من ال gui:

1. تحت خدمات الأمان، أختر **Cisco IronPort Email Encryption (تشفير البريد الإلكتروني) > تمكين تشفير البريد الإلكتروني**، وانقر فوق **إعدادات التحرير**.
2. انقر على **إضافة توصيف تشفير** لإنشاء توصيف تشفير جديد.
3. أختر **خدمة Cisco Registered Envelope** أو **جهاز تشفير Cisco IronPort** (في حالة شراء جهاز التشفير) لنوع خدمة المفاتيح.

4. انقر فوق **إرسال التغييرات وتنفيذها**.

5. بعد إنشاء ملف تعريف التشفير، يتم منحك الخيار لتزويده بخادم خدمة المغلفات المسجلة (CRES) من Cisco. يجب عرض زر التزويد بجوار ملف التعريف الجديد. طقطقة **إحتياط**.

إنشاء عامل تصفية محتوى صادر

أتمت هذا steps من ال gui in order to خلقت خارج محتوى مرشح أن يطبق التشفير توصيف. في المثال التالي، سيقوم عامل التصفية بتشغيل التشفير لأي رسالة صادرة بالسلسلة "آمن:" في رأس الموضوع:

1. تحت نهج البريد، أختر عوامل تصفية المحتوى الصادرة، وانقر فوق **إضافة عامل تصفية**.

2. قم بإضافة عامل تصفية جديد مع شرط Subject Header كموضوع == "Secure:" وإجراء التشفير والتسليم الآن (الإجراء النهائي). انقر على **إرسال**.

3. ضمن "نهج البريد"، أختر "نهج البريد الصادر" وقم بتمكين عامل التصفية الجديد هذا في نهج البريد الافتراضي أو نهج البريد المناسبة.

4. تنفيذ التغييرات.

التحقق من الصحة

يوضح هذا القسم كيفية التحقق من عمل التشفير.

1. للتحقق، قم بإنشاء بريد جديد مع **Secure:** في الموضوع وأرسل البريد الإلكتروني إلى حساب ويب (Hotmail، Yahoo، Gmail) لتحديد ما إذا كان مشفرا.

2. تحقق من سجلات البريد كما هو موضح في القسم التالي لضمان تشفير الرسالة عبر "عامل تصفية المحتوى الصادر".

التحقق من صحة معالجة عامل تصفية التشفير في MAIL_LOG

تظهر إدخالات mail_log هذه أن الرسائل تطابق عامل تصفية التشفير المسمى encrypt_message.

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt
                                                        'filter 'Encrypt_Message
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt
                                                        'filter 'Encrypt_Message
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt
                                                        filter ''Encrypt_Message
```

ارجع إلى تحديد المصير النهائي لرسالة ESA للحصول على تعليمات حول كيفية إستخدام أوامر **GREP** أو **FINDEVENT** لتجميع المعلومات من السجلات كما هو موضح في هذا القسم.

استكشاف الأخطاء وإصلاحها

إذا لم يتم تشغيل عامل تصفية التشفير، تحقق من سجلات البريد لنهج البريد الذي تستخدمه رسالة الاختبار. تأكد من تمكين عامل التصفية في نهج البريد هذا، وكذلك عدم تمكين عامل تصفية سابق في هذا النهج باستخدام إجراء **تخطي**

عوامل تصفية المحتوى المتبقية.

تأكد من أن الرسالة (الرسائل) في تعقب الرسائل تستخدم السلسلة الصحيحة أو وضع علامات الموضوع المعين من أجل تشغيل التشفير من خلال عامل تصفية المحتوى.

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).