# دليل أفضل الممارسات لعمليات تصفية مكافحة البريد غير الهام ومكافحة الفيروسات ورسائل البريد الإلكتروني الجذاب وتفشي الأمراض

## المحتويات



## نظرة عامة

الغالبية العظمى من التهديدات، الهجمات، والإزعاج الذي يواجه المنظمة عبر البريد الإلكتروني يأتي في شكل البريد العشوائي، البرامج الخبيثة، والهجمات المخلوطة. يتضمن جهاز أمان البريد الإلكتروني (ESA) من Cisco العديد من التقنيات والميزات المختلفة لقطع هذه التهديدات على البوابة قبل دخولها إلى المؤسسة. يصف هذا المستند نهج أفضل الممارسات لتكوين عوامل تصفية مكافحة البريد العشوائي ومكافحة الفيروسات والبريد الجداري والتفشي، على كل من تدفق البريد الإلكتروني الوارد والصادر.

## مكافحة البريد العشوائي

تتناول الحماية من البريد العشوائي مجموعة كاملة من التهديدات المعروفة بما في ذلك البريد العشوائي والتصيد الاحتيالي والهجمات على أجهزة الكمبيوتر المحمولة، بالإضافة إلى تهديدات البريد الإلكتروني القصيرة المدى التي يصعب اكتشافها مثل عمليات الاحتيال "419". بالإضافة إلى ذلك، تحدد الحماية من البريد العشوائي التهديدات المخلوطة الجديدة والمتطورة مثل هجمات البريد العشوائي التي توزع محتوى ضار من خلال عنوان URL للتنزيل أو منفذ.

يقدم أمان البريد الإلكتروني من Cisco حلول مكافحة البريد العشوائي التالية:

- تصفية مكافحة البريد العشوائي من IronPort (IPAS)
- التصفية الذكية للمسح الضوئي المتعدد (IMS) من Cisco

يمكنك ترخيص كلا الحلين وتمكينهما على ESA لديك ولكن يمكنك إستخدام واحد فقط في نهج بريد معين. ولأغراض هذه الوثيقة المتعلقة بأفضل الممارسات، سنستخدم ميزة IMS.

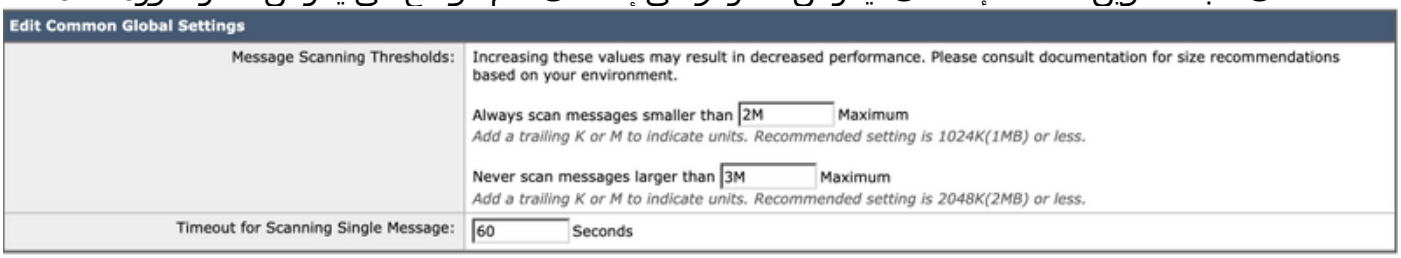
## التحقق من مفتاح الميزة

- على ESA، انتقل إلى **إدارة النظام > مفاتيح الميزات**
- ابحث عن ترخيص Intelligent Multi-Scan وتأكد من أنه نشط.

## تمكين المسح الضوئي المتعدد الذكي (IMS) بشكل عام

- تشغيل يعرض الأمر إسا، تبحر إلى **الأمان الخدمات> IMS و Graymail**
- انقر يعرض الأمر **تمكين**زر على **إعدادات IMS العمومية**:

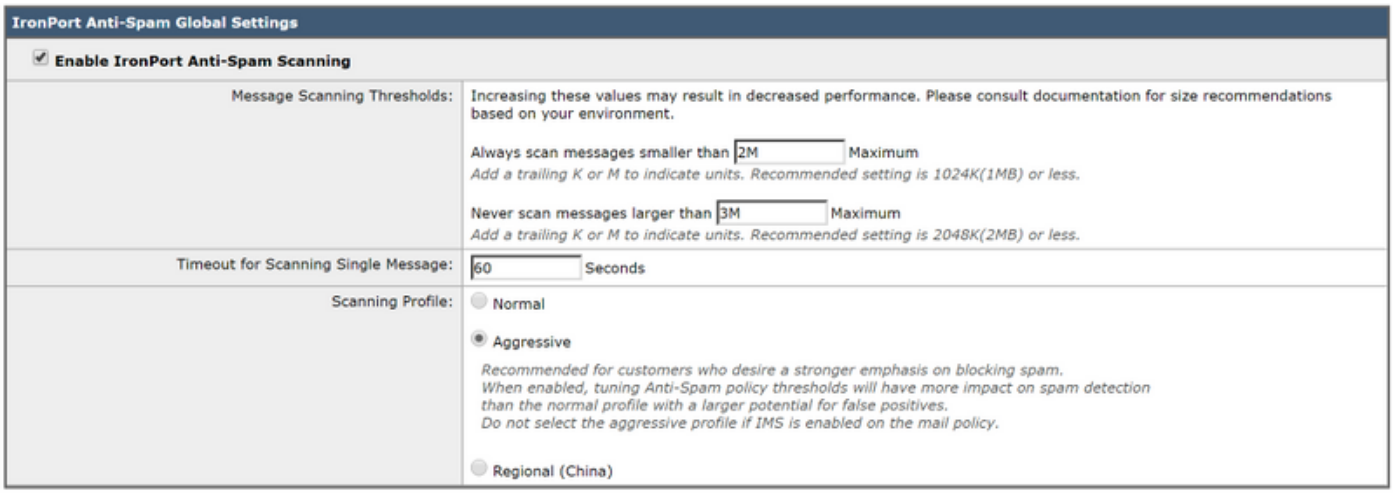

- البحث عن **الإعدادات العمومية** و انقر على **تحرير الإعدادات العامة**
- هنا أنت علبة التكوين متعدد الإعدادات. يعرض الأمر أوصى إعدادات هم موضح في يعرض الأمر صورة أدناه:




- انقر على **إرسالو التزم التغييرات.**

إذا لم يكن لديك اشتراك ترخيص IMS:

- انتقل إلى **خدمات الأمان > IronPort Anti-Spam**
- انقر يعرض الأمر **تمكين**زر **نظرة عامة على IronPort Anti-Spam**
- انقر على **تحرير الإعدادات العامة**
- هنا أنت علبة التكوين متعدد الإعدادات. يعرض الأمر أوصى إعدادات هم موضح في يعرض الأمر صورة أدناه:




- توصي Cisco باختيار ملف تعريف **رائع** للمسح الضوئي لعميل يرغب في التركيز بشدة على حظر البريد العشوائي.
- انقر على **إرسالو التزم تغييرات**

## تمكين الفحص المركزي للبريد العشوائي

بما أن خيار Anti-Spam هو أن يتم إرساله إلى العزل، فمن المهم التأكد من إعداد عزل البريد العشوائي:

- انتقل إلى **خدمات الأمان > عزل البريد العشوائي**
- انقرتينغ يعرض الأمر **التكوين**زر إرادة نتعاطى أنت إلى يعرض الأمر جريبمستحق صفحة.
- هنا أنت علبة تمكين يعرض الأمر حجر من قبل تدقيق يعرض الأمر **تمكين**صندوق و نقطةه حجر إلى نتنازل متمركز تشغيل أمنالإدارة Aمكبر (SMA) من قبلملء في SMA**الاسمو IP العنوان.** يعرض الأمر أوصى إعدادات هم موضح أدناه:

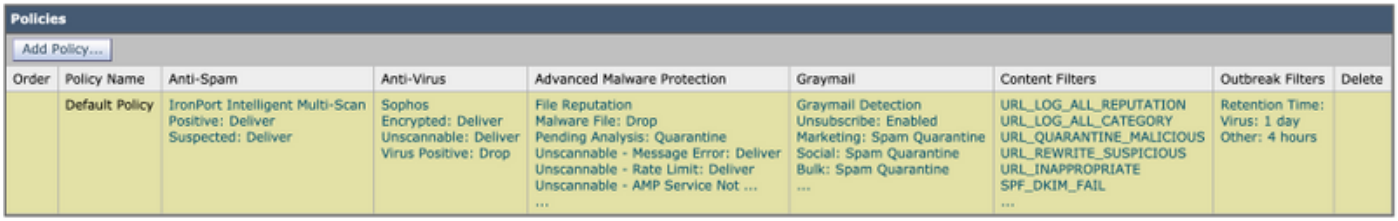

- انقر على **إرسالو التزم تغييرات**

لمزيد من المعلومات حول إعداد الحجر الصحي المركزي، يرجى الرجوع إلى مستند أفضل الممارسات:
[أفضل الممارسات لإعداد الحجر الصحي المركزي الخاص بالسياسات والفيروسات والتفشيات، والهجرة من وكالة الفضاء الأوروبية إلى وكالة الخدمات الصحية الصغيرة والمتوسطة]

## تكوين مكافحة البريد العشوائي في السياسات

مرة واحدة ذكي متعدد - مسح لديه تم مكون عالميا ، أنت علبة الآن تطبيق ذكي متعدد - مسح إلى بريد السياسات:

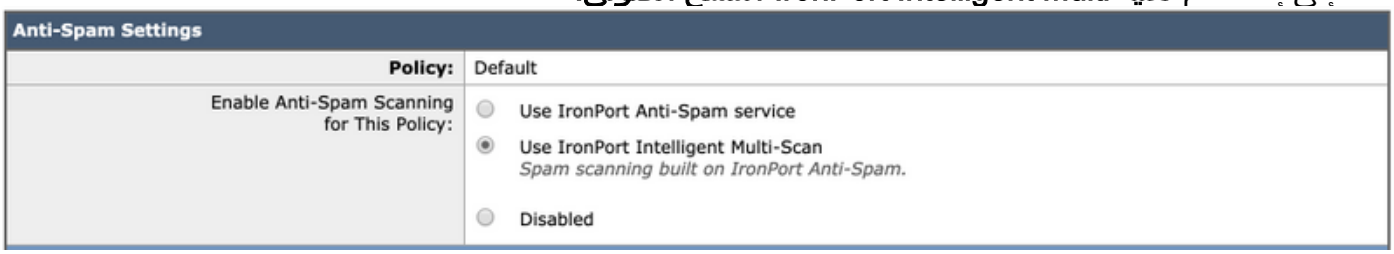
- انتقل إلى **نهج البريد > نهج البريد الوارد**
- تستخدم نهج البريد الوارد إعدادات مكافحة البريد العشوائي ل IronPort بشكل افتراضي.
- سيتيح النقر فوق الارتباط الأزرق تحت **مكافحة البريد العشوائي** لهذا النهج المعين إستخدام إعدادات مكافحة البريد العشوائي المخصصة.
- سيظهر أدناه مثال يوضح النهج الافتراضي باستخدام إعدادات مكافحة البريد العشوائي المخصصة:




قم بتخصيص إعدادات مكافحة البريد العشوائي لنهج البريد الوارد عن طريق النقر فوق الارتباط الأزرق تحت **مكافحة البريد العشوائي** للنهج الذي تريد تخصيصه.

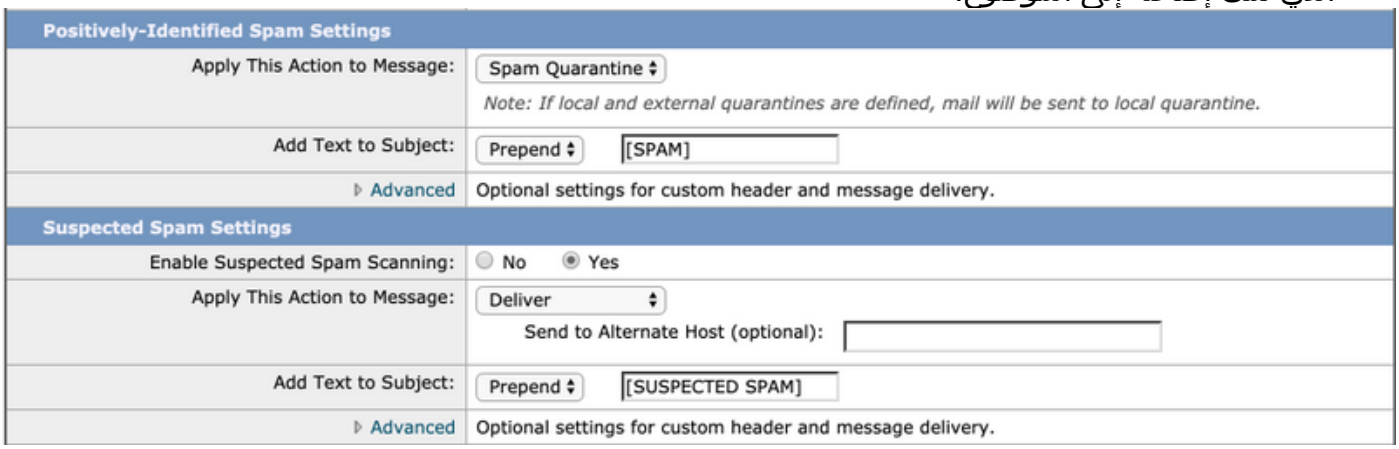
هنا أنت علبة تحديد يعرض الأمر مضاد-Sبام مسح خيار أنت مرتجى إلى تمكين من أجل هذا السياسة.

- من أجل يعرض الأمر غرض من هذا الأفضل شبقجليد وثيقة، طقطقة يعرض الأمر راديو زر التالي إلى إستخدام **تقنية IronPort Intelligent Multi-المسح الضوئي:**

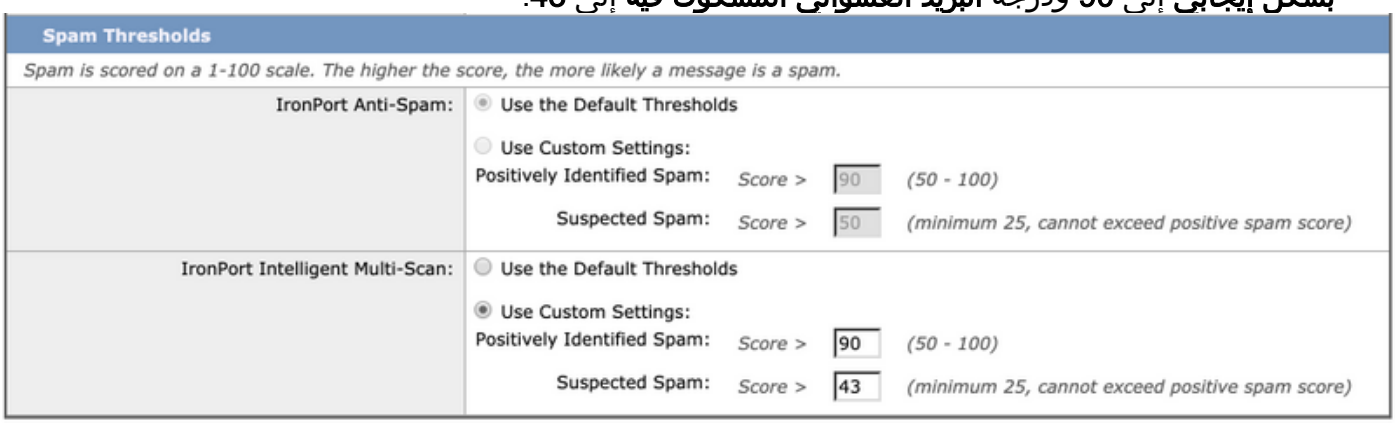



يتضمن القسمان التاليان **إعدادات بريد عشوائي محددة بشكل إيجابي وإعدادات بريد عشوائي مشتبه فيها:**

- أفضل الممارسات الموصى بها هي تكوين إجراء **العزل** على إعداد **البريد العشوائي المحدد بشكل إيجابي** باستخدام النص المضاف مسبقا **[البريد العشوائي]** الذي تمت إضافته إلى الموضوع؛
- تطبيق **التسليم** كإجراء **لإعدادات البريد العشوائي المشتبه فيها** مع النص المقبل **[البريد العشوائي المشتبه فيه]** الذي تمت إضافته إلى الموضوع:




- يمكن تغيير إعداد **حد البريد العشوائي**، والإعدادات الموصى بها هي تخصيص درجة **البريد العشوائي المحدد بشكل إيجابي** إلى **90** ودرجة **البريد العشوائي المشكوك فيه** إلى **43**:



- انقر على **إرسالو التزم تغييرات**

# مكافحة الفيروسات

يتم توفير الحماية ضد الفيروسات من خلال محركين من إنتاج جهات خارجية - Sophos و McAfee. سوف تقوم هذه المحركات بتصفية جميع التهديدات الخبيثة المعروفة، وإسقاطها وتنظيفها أو الحجر الصحي عليها كما تم تكوينها.

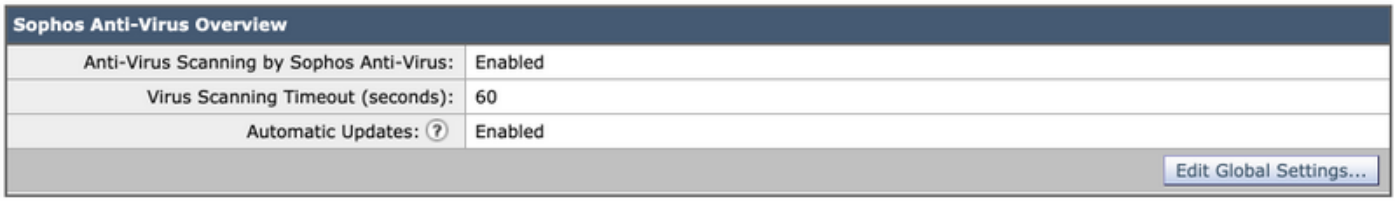
## التحقق من مفاتيح الميزة

للتحقق من تمكين كل من مفتاحي الميزة ونشاطهما:

- انتقل إلى **إدارة النظام > مفاتيح الميزات**
- تأكد من أن تراخيص **Sophos Anti-Virus** و**McAfee** نشطة.

## تمكين فحص مكافحة الفيروسات

- تبحر إلى **الأمان الخدمات> مكافحة الفيروسات - سوفوس**
- انقر يعرض الأمر **تمكين**زر.
- تأكد من **تمكين التحديث التلقائي** ومن أن تحديث ملفات مكافحة الفيروسات ل Sophos يعمل بشكل جيد. إذا لزم الأمر، انقر فوق **Update Now (التحديث الآن)** لبدء تحديث الملف على الفور:





- انقر على **إرسالو التزم التغييرات.**

إذا كان ترخيص McAfee نشطا أيضا، فعليك التنقل إلى **الأمان الخدمات> برنامج Anti-Virus - McAfee**

- انقر يعرض الأمر **تمكين**زر.
- تأكد من **تمكين التحديث التلقائي** ومن أن تحديث ملفات مكافحة الفيروسات في McAfee يعمل بشكل جيد. إذا لزم الأمر، انقر فوق **Update Now (التحديث الآن)** لبدء تحديث الملف على الفور.
- انقر على **إرسالو التزم تغييرات**

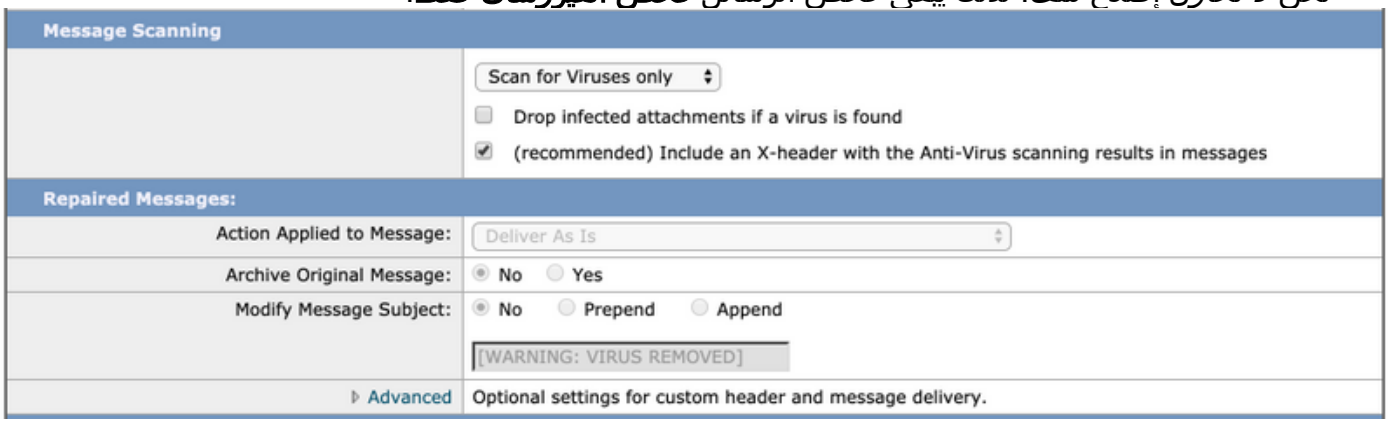
## تكوين مكافحة الفيروسات في نهج البريد

في نهج البريد الوارد، يوصى بما يلي:

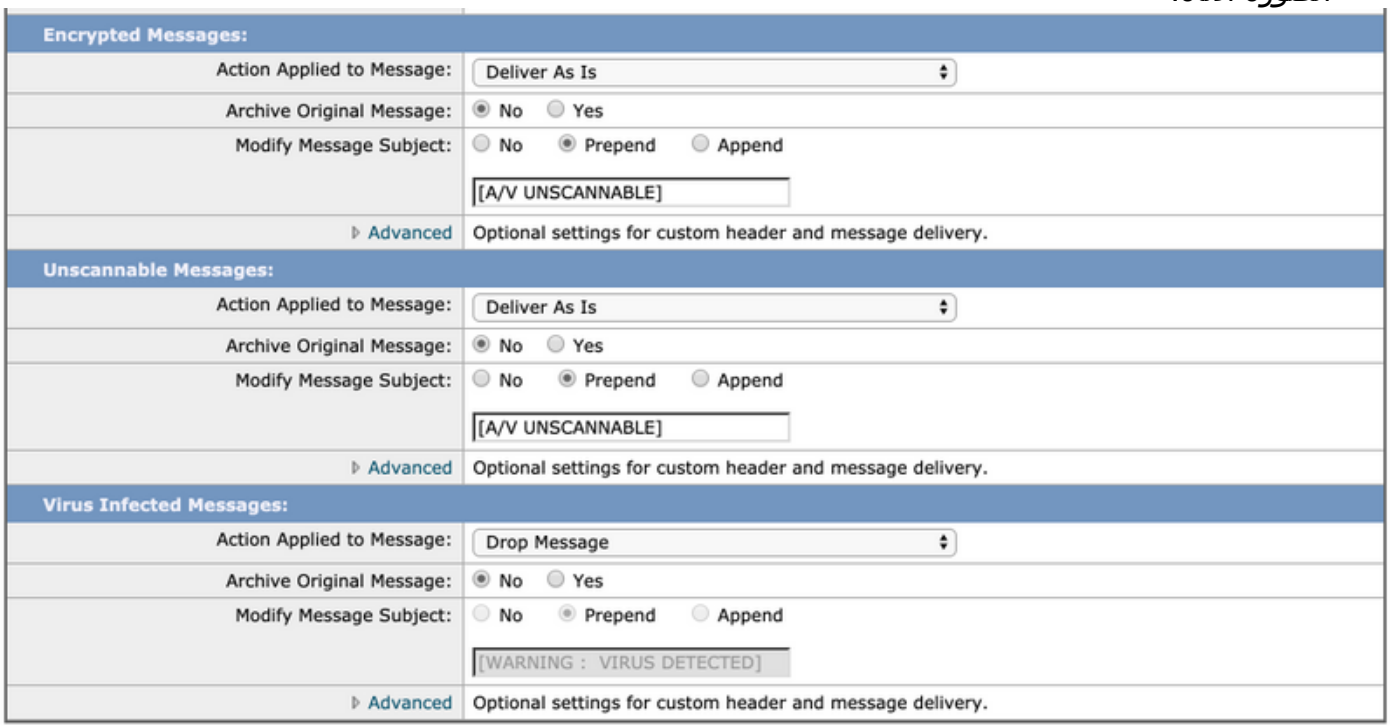
- انتقل إلى **نهج البريد > نهج البريد الوارد**
- قم بتخصيص إعدادات **مكافحة الفيروسات** لنهج البريد الوارد بالنقر فوق الارتباط الأزرق الموجود تحت مكافحة الفيروسات للنهج الذي ترغب في تخصيصه.
- هنا أنت علبة تحديد يعرض الأمر مضاد-فيروس مسح خيار أنت مرتجى إلى تمكين من أجل هذا السياسة.

- من أجل يعرض الأمر غرض من هذا bEST Pفعلجليد مستند، حدد كل من **McAfee** و**Sophos Anti-Virus**:


- نحن لا نحاول إصلاح ملف، لذلك يبقى فحص الرسائل **فحص الفيروسات فقط**:




- الإجراء الموصى به لكل من **الرسائل المشفرة** و**التي لا يمكن مسحها ضوئيا** هو **تسليم الوضع كما هو** باستخدام سطر موضوع معدل لانتباههم.
- السياسة الموصى بها لمكافحة الفيروسات هي **إسقاط** جميع **الرسائل المصابة بالفيروس** كما هو موضح في الصورة أدناه:




- انقر على **إرسالو التزم تغييرات**

يوصى باتباع نهج مماثل لنهج البريد الصادر، ومع ذلك، لا نوصي بتعديل سطر الموضوع على البريد الإلكتروني الصادر.

## غرايميل

يتكون حل إدارة البريد الإلكتروني في جهاز أمان البريد الإلكتروني من مكونين: محرك مسح مدمج للبريد الجيري

وخدمة إلغاء الاشتراك القائمة على السحابة. يتيح حل إدارة بريد الجذب للمؤسسات تحديد البريد الجراي باستخدام محرك بريد الجراد المدمج وتطبيق عناصر التحكم المناسبة في السياسات وتوفير آلية سهلة للمستخدمين النهائيين لإلغاء الاشتراك في الرسائل غير المرغوب فيها باستخدام خدمة إلغاء الاشتراك.

تتضمن فئات Graymail البريد الإلكتروني للتسويق والبريد الإلكتروني للشبكة الاجتماعية والبريد الإلكتروني المجمع. تتضمن الخيارات المتقدمة إضافة رأس مخصص، وإرسال إلى مضيف بديل وأرشفة الرسالة. للحصول على هذه الممارسة الأفضل، سنقوم بتمكين ميزة "إلغاء الاشتراك الآمن ل Graymail" لنهج البريد الافتراضي.

## التحقق من مفتاح الميزة

- على ESA، انتقل إلى **إدارة النظام > مفاتيح الميزات**
- ابحث عن **إلغاء الاشتراك في Graymail Safe** وتأكد من أنه نشط.

## تمكين خدمات Graymail و Safe Unsubscribe

- تشغيل يعرض الأمر إسا، تبحر إلى **الأمان الخدمات> IMS و Graymail**
- انقر يعرض الأمر **تحرير إعدادات Graymail**زر على **إعدادات Graymail العمومية**
- تحديد جميع الخيارات - **تمكين كشف Graymail**، **وتمكين إلغاء الاشتراك الآمن** وتمكين **التحديثات التلقائية**:

| Graymail Global Settings | |
|---|---|
| Graymail Detection | Enabled |
| Safe Unsubscribe | Enabled |
| Automatic Updates ⓘ | Enabled |
| | Edit Graymail Settings |

- انقر على **إرسالو التزم تغييرات**

## تكوين Graymail و Safe Unsubscriin policy

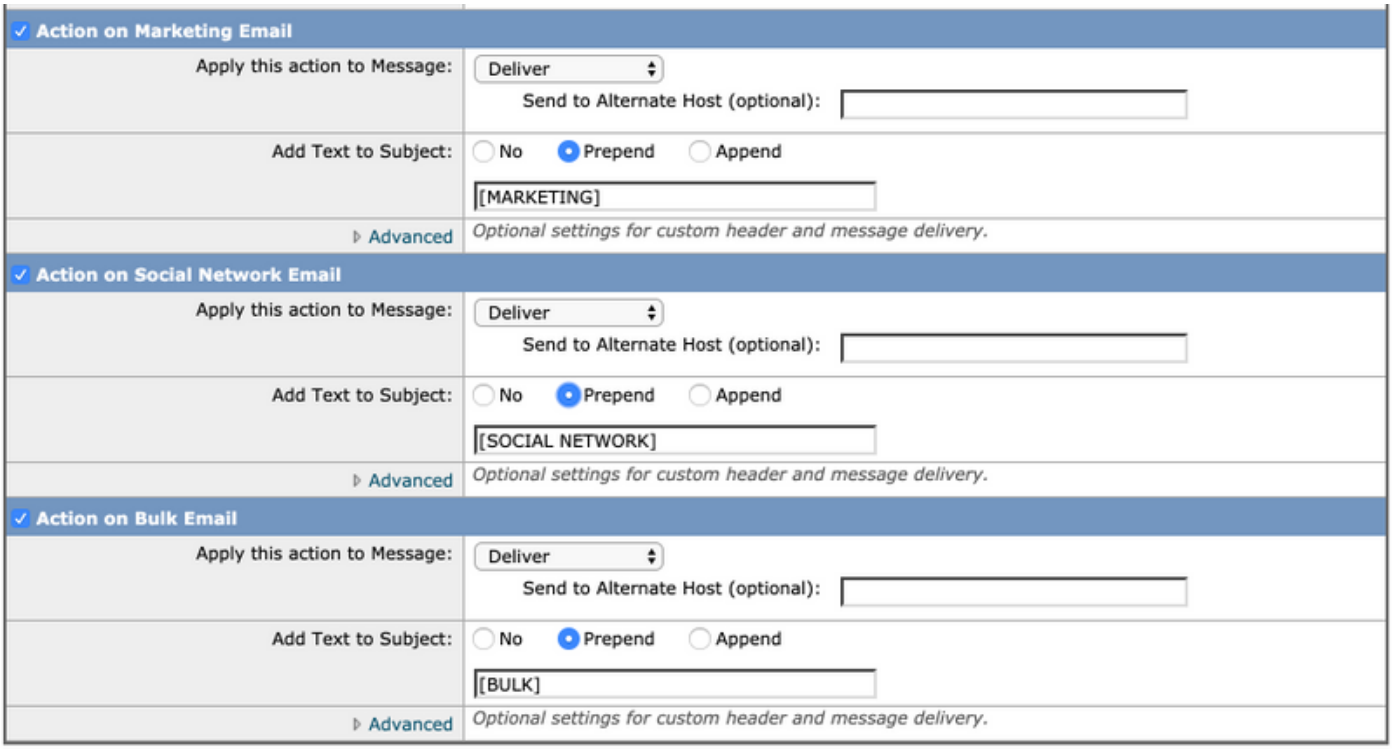
ون غرايميل وإلغاء الاشتراك الآمن لديه تم مكون عالميا ، أنت علبة الآن تطبيق هذه الخدمات إلى بريد السياسات.

- انتقل إلى **نهج البريد > نهج البريد الوارد**
- سيتيح النقر فوق الارتباط الأزرق تحت **Graymail** إستخدام إعدادات Graymail المخصصة لهذا النهج.
- هنا أنت علبة تحديد غرايميلخيارات أنت مرتجى إلى تمكين من أجل هذا السياسة.
- من أجل يعرض الأمر غرض من هذا أفضل درجة pفعلجليد وثيقة، طقطقة يعرض الأمر راديو زر التالي لتمكين **اكتشاف Graymail لهذا النهج وتمكين إلغاء الاشتراك في Graymail لهذا النهج**:

| Graymail Settings | |
|---|---|
| **Policy:** | DEFAULT |
| **Enable Graymail Detection for This Policy:** | Yes No |
| **Enable Graymail Unsubscribing for This Policy:** | Yes No |
| | Perform this action for: All Messages (Recommended) Unsigned Messages |

تتضمن الأقسام الثلاثة التالية **الإجراء الخاص بإعدادات البريد الإلكتروني التسويقية**، **والإجراء الخاص بإعدادات البريد الإلكتروني للشبكة الاجتماعية، والإجراء الخاص بإعدادات البريد الإلكتروني المجمع**.

- وتتمثل أفضل الممارسات الموصى بها في تمكينها جميعا والاستمرار في العمل على النحو **الذي** يتم به التسليم مع إضافة نص سابق الذكر إلى الموضوع فيما يتعلق بالفئات على النحو المبين أدناه:




- انقر على **إرسالو التزم تغييرات**

يجب أن يحتوي نهج البريد الصادر على Graymail يبقى في حالة **معطل**.

## عوامل تصفية التفشي

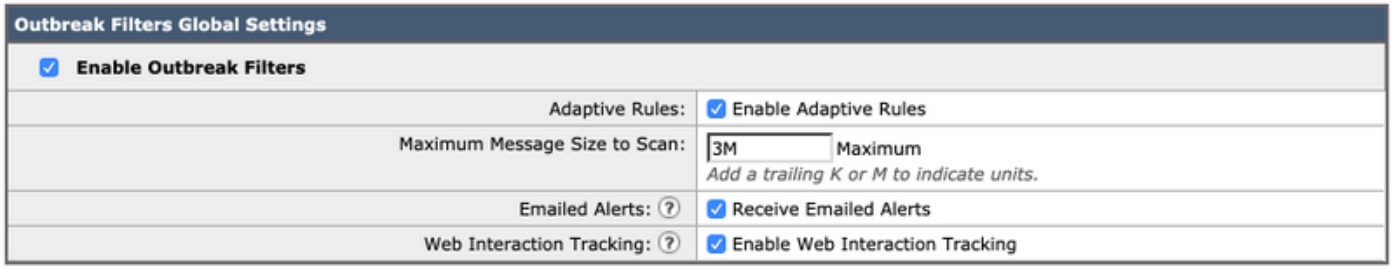
تقوم "عوامل تصفية التفشي" بدمج المشغلات في محرك مكافحة البريد العشوائي وتقنيات مسح URL واكتشافه والمزيد لوضع علامات على العناصر التي تقع خارج فئة البريد العشوائي الحقيقي بشكل صحيح - على سبيل المثال، رسائل البريد الإلكتروني الخادعة ورسائل البريد الإلكتروني المخادعة ومعالجتها بشكل صحيح باستخدام إعلامات المستخدم أو الحجر الصحي.

### التحقق من مفتاح الميزة

- على ESA، انتقل إلى **إدارة النظام > مفاتيح الميزات**
- ابحث عن **عوامل تصفية التفشي** وتأكد من أنها نشطة.

### تمكين خدمة عوامل تصفية التفشي

- تشغيل يعرض الأمر إسا، تبحر إلى **الأمان الخدمات> عوامل تصفية التفشي**
- انقر يعرض الأمر **تمكين**زر على **نظرة عامة على مرشحات التفشي**
- هنا أنت علبة التكوين متعدد الإعدادات. يعرض الأمر أوصى إعدادات هم موضح في يعرض الأمر صورة أدناه:

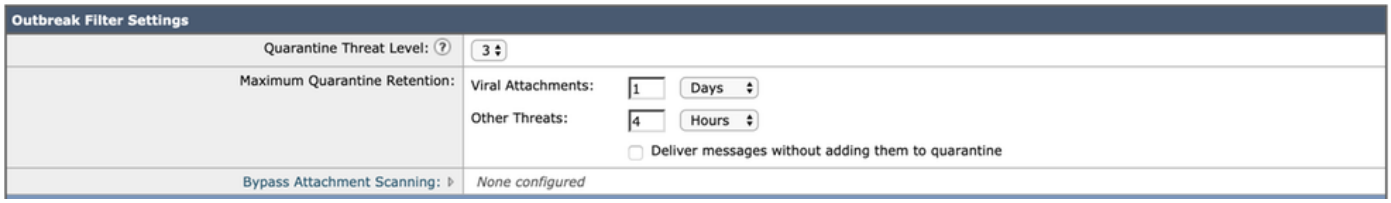



- انقر على **إرسالو التزم التغييرات.**

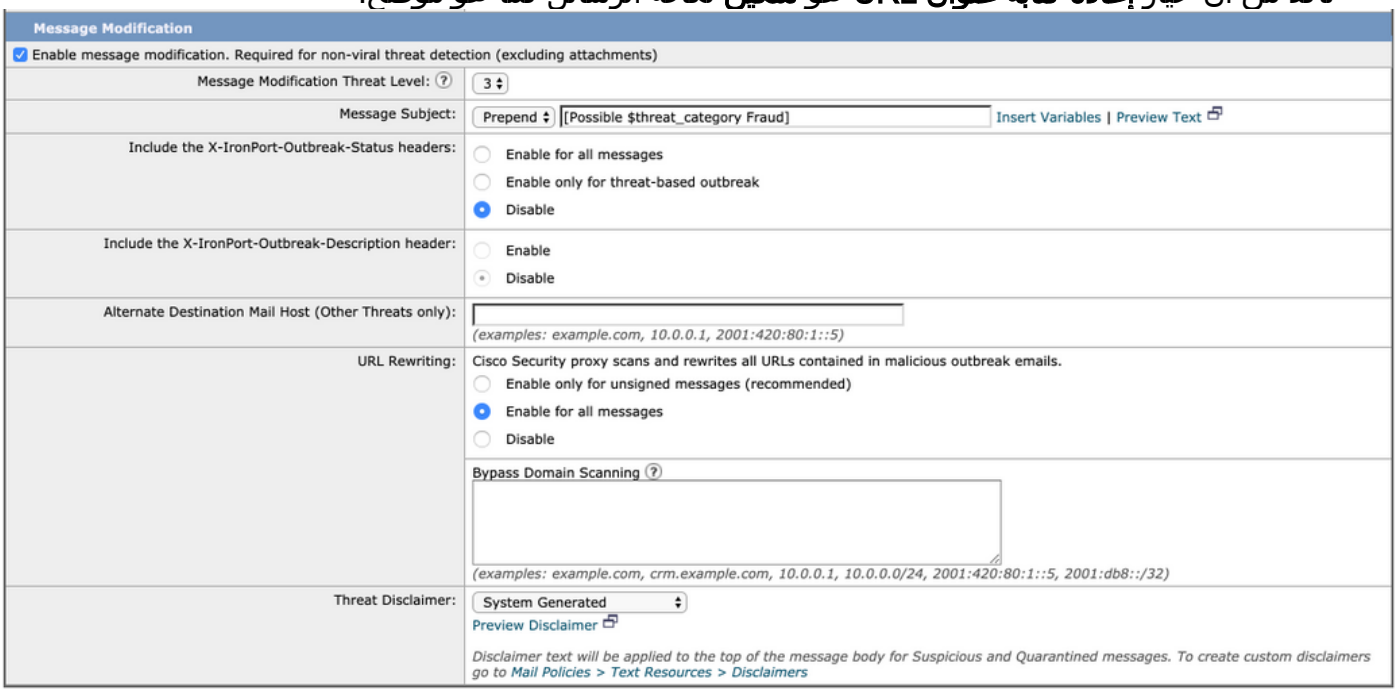
## تكوين عوامل تصفية التفشي في السياسات

عوامل تصفية ما بعد التفشي لديه تم مكون عالميا ، أنت علبة الآن تطبيق هذه الميزة على بريد السياسات.

- انتقل إلى **نهج البريد** > **نهج البريد الوارد**
- سيتيح النقر فوق الارتباط الأزرق ضمن **عوامل تصفية التفشي** لهذا النهج المعين إستخدام إعدادات عوامل تصفية التفشي المخصصة.
- من أجل يعرض الأمر غرض من هذا الأفضل شبقجليد الوثيقة، ونحتفظ بإعدادات مرشح التفشي بالقيم الافتراضية:




- يمكن لعوامل تصفية التفشي إعادة كتابة عناوين URL إذا تم اعتبارها ضارة أو مشتبه فيها أو مزيفة. حدد **تمكين تعديل الرسالة** لاكتشاف التهديدات المستندة إلى URL وإعادة كتابتها.
- تأكد من أن خيار **إعادة كتابة عنوان URL** هو **تمكين** لكافة الرسائل كما هو موضح:




- انقر على **إرسالو التزم تغييرات**

يجب أن يحتوي نهج البريد الصادر على **عوامل تصفية التفشي** تبقى في حالة **معطلة**.

## القرار

يهدف هذا المستند إلى وصف تكوينات الممارسات الافتراضية أو الأفضل لعوامل تصفية مكافحة البريد العشوائي ومكافحة الفيروسات ورسائل الجذب والتفشي في جهاز أمان البريد الإلكتروني (ESA). تتوفر جميع عوامل التصفية هذه على كل من سياسات البريد الإلكتروني الوارد والصادر، ومن المستحسن إجراء التكوين والتصفية على كليهما - بينما يكون معظم الحماية خاصا بالوارد، فإن تصفية التدفق الصادر توفر الحماية ضد رسائل البريد الإلكتروني التي تم إرسالها أو الهجمات الضارة الداخلية.

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).