

# ةي فرصت تاي لم عمل تاس رامم لاض فأ ليلد ةح فاك م و ماه ل ا ريغ دي ربل ا ةح فاك م ينورت كل ل ا دي ربل لئ اس رو ت اس وري ف ل ا ض ارم أ ل ا يش ف ت و با ذج ل ا

## المحتويات

[نظرة عامة](#)

[مكافحة البريد العشوائي](#)

[التحقق من مفتاح الميزة](#)

[تمكين المسح الضوئي المتعدد الذكي \(IMS\) بشكل عام](#)

[تمكين الفحص المركزي للبريد العشوائي](#)

[تكوين مكافحة البريد العشوائي في السياسات](#)

[مكافحة الفيروسات](#)

[التحقق من مفاتيح الميزة](#)

[تمكين فحص مكافحة الفيروسات](#)

[تكوين مكافحة الفيروسات في نهج البريد](#)

[غراميل](#)

[التحقق من مفتاح الميزة](#)

[تمكين خدمات Safe Unsubscribe و Graymail](#)

[تكوين Safe Unsubscribe policy و Graymail](#)

[عوامل تصفية التفتيش](#)

[التحقق من مفتاح الميزة](#)

[تمكين خدمة عوامل تصفية التفتيش](#)

[تكوين عوامل تصفية التفتيش في السياسات](#)

[القرار](#)

## 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 والتفتيش، 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 استخدام 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 تمكينزر على إعدادات IMS العمومية:

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
<a href="#">Edit IMS Settings</a>	

- 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:

Edit Common Global Settings	
Message Scanning Thresholds:	Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment. Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i> Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- انقر على إرسالو التزم التغييرات.

إذا لم يكن لديك اشتراك ترخيص IMS:

- انتقل إلى خدمات الأمان < IronPort Anti-Spam
- انقر يعرض الأمر تمكينزر 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:

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> <b>Enable IronPort Anti-Spam Scanning</b>	
Message Scanning Thresholds:	Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment. Always scan messages smaller than <input type="text" value="2M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less. Never scan messages larger than <input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<input type="radio"/> Normal <input checked="" type="radio"/> Aggressive <i>Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</i> <input type="radio"/> Regional (China)

- 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
- انقرتبنغ يعرض الأمر التكوينزر إرادة تتعاطى أنت
- هنا أنت علبة تمكين يعرض الأمر حجر من قبل تدقيق يعرض الأمر تمكينصندوق و نقطة ه حجر إلى تتنازل متمرکز تشغيل أمنالإدارة A مكبر (SMA) من قبلملء في ISMA الاسمو IP العنوان. يعرض الأمر أوصى إعدادات هم موضح أدناه:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> <b>Enable External Spam Quarantine</b>	
Name:	<input type="text" value="centralized_spam"/> (e.g. spam_quarantine)
IP Address:	<input type="text" value="sma_ip_address"/>
Port:	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: <input type="text" value="Quarantine"/>

- 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 استخدام إعدادات مكافحة البريد العشوائي المخصصة.
- سيظهر أدناه مثال يوضح النهج الافتراضي باستخدام إعدادات مكافحة البريد العشوائي المخصصة:

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

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

- من أجل يعرض الأمر غرض من هذا الأفضل شبقجلید وثيقة، طقطقة يعرض الأمر راديوزر التالي إلى استخدام تقنية IronPort Intelligent Multi-المسح الضوئى:

Anti-Spam Settings	
<b>Policy:</b>	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

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:

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <input type="button" value="v"/> <i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>
Add Text to Subject:	Prepend <input type="button" value="v"/> [SPAM]
<input type="button" value="v"/> Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [SUSPECTED SPAM]
<input type="button" value="v"/> Advanced	Optional settings for custom header and message delivery.

- 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:

Spam Thresholds	
<i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

• 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 مفاتيح 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 تمكينزر.
- 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:

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: ?	Enabled
<a href="#">Edit Global Settings...</a>	

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available
No updates in progress.			
<a href="#">Update Now</a>			

• انقر على إرسالو التزم التغييرات.

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

- انقر يعرض الأمر تمكينزر.
- 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 علبه تحديد يعرض الأمر مضاد-فيروس مسح خيار أنت مرتجي إلى تمكين من أجل هذا السياسة.

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

Anti-Virus Settings	
Policy:	DEFAULT
Enable Anti-Virus Scanning for This Policy:	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

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

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: VIRUS REMOVED]
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.

- الإجراء الموصى به لكل من الرسائل المشفرة والتي 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:

Encrypted Messages:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message <input type="button" value="v"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
<input type="button" value="Advanced"/>	Optional settings for custom header and message delivery.

- 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 Unsubscribe 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 استخدام إعدادات Graymail المخصصة لهذا النهج.
- هنا أنت علبة تحديد غرايميلخيارات أنت مرتجي 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:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Perform this action for:	<input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> 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:

✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
▶ Advanced	Optional settings for custom header and message delivery.
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
▶ Advanced	Optional settings for custom header and message delivery.
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
▶ Advanced	Optional settings for custom header and message delivery.

- 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 إعلانات 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 تمكينزر على نظرة عامة على مرشحات التفشي
- هنا أنت علبة التكوين متعدد الإعدادات. يعرض الأمر أوصى إعدادات هم موضح فى يعرض الأمر صورة أدناه:

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> Enable Outbreak Filters	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units.
Emailed Alerts: (?)	<input checked="" type="checkbox"/> Receive Emailed Alerts
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> Enable Web Interaction Tracking

- انقر على إرسالو التزم التغييرات.

## تكوين عوامل تصفية التفشي في السياسات

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

- انتقل إلى نهج البريد < نهج البريد الوارد
- سيتم النقر فوق الارتباط الأزرق ضمن عوامل تصفية التفشي لهذا النهج المعين استخدام إعدادات عوامل تصفية التفشي المخصصة.
- من أجل يعرض الأمر غرض من هذا الأفضل شبكجديد الوثيقة، ونحتفظ بإعدادات مرشح التفشي بالقيم الافتراضية:

Outbreak Filter Settings	
Quarantine Threat Level: ?	3
Maximum Quarantine Retention:	Viral Attachments: 1 Days Other Threats: 4 Hours <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- 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:

Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3
Message Subject:	Prepend [Possible \$threat_category Fraud] Insert Variables   Preview Text
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> (examples: example.com, 10.0.0.1, 2001:420:80:1::5)
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
Bypass Domain Scanning ?	<input type="text"/> (examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)
Threat Disclaimer:	System Generated Preview Disclaimer Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources > Disclaimers

- 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.

