تكوين الماسح الضوئي للتهديدات لكل سياسة المسح ل SEG

المحتويات

المقدمة

يصف هذا المستند خدمة وتكوين ماسح التهديدات الضوئي (TS) لكل دمج سياسة لعبارة البريد الإلكتروني الآمنة (SEG) من Cisco.

المتطلبات الأساسية

معرفة إعدادات SEG العامة والتكوين مرغوب.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 والإصدارات الأحدث.
- خدمة Graymail.
- خدمة مكافحة البريد العشوائي.
- نهج البريد الوارد.

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

نظرة عامة

تم دمج Threat Scan (TS) المكون الفرعي الذي تم تنشيطه حديثا لخدمة Graymail مع AntiSpam Case مما يوفر مزيدا من الفعالية في الكشف عن AntiSpam.

بمجرد تنشيط خدمة Graymail، تصبح خيارات تمكين ماسح التهديدات نشطة داخل كل إعداد

AntiSpam لنهج البريد الوارد. ام إن يمكن TS يحسن الكشف الشامل عن مكافحة البريد العشوائي مع التركيز على كشف تهريب HTML:

- تحليل HTML واكتشاف البرامج النصية الضارة
- كشف تحليل URL وإعادة التوجيه

يتحكم محرك حالة مكافحة البريد العشوائي في الخدمتين، حيث يقوم بإدارة التحديثات وإدانة البريد العشوائي.

يحتوي TS على إعدادات تمكين/تعطيل مرئية داخل كل إعداد لمكافحة البريد العشوائي لنهج البريد الوارد.

يؤثر قرار الحظر على البريد الإلكتروني على الأحكام، مما يزيد من وزن الحكم النهائي في قضية مكافحة البريد العشوائي.

التكوين

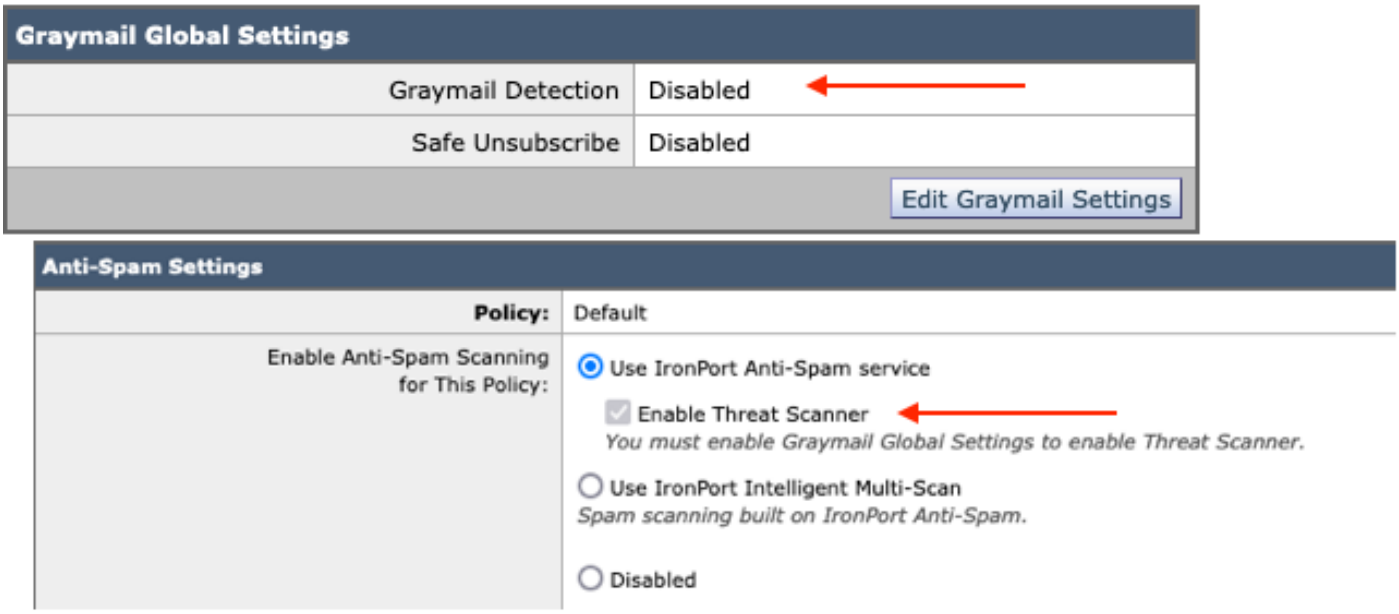
يتألف التكوين من إجراءين، تمكين اكتشاف Graymail وتمكين TS ضمن خيارات البريد الوارد.

- يجب تمكين خدمة Graymail العمومية لتنشيط TS.
- يصبح خيار "مكافحة البريد العشوائي" لنهج البريد الوارد في "تمكين ماسح التهديدات الضوئي" متوفرا بمجرد تمكين Graymail بشكل عام.

إعداد واجهة الويب

لتمكين Graymail داخل WebUI:

- انتقل إلى خدمات الأمان
  - IMS و Graymail
    - إعدادات Graymail العمومية
      - تحرير إعدادات Graymail.
        - حدد الخيار لتمكين كشف Graymail.
- إرسال التغييرات وإلتزامها لإنهاء الإجراء.

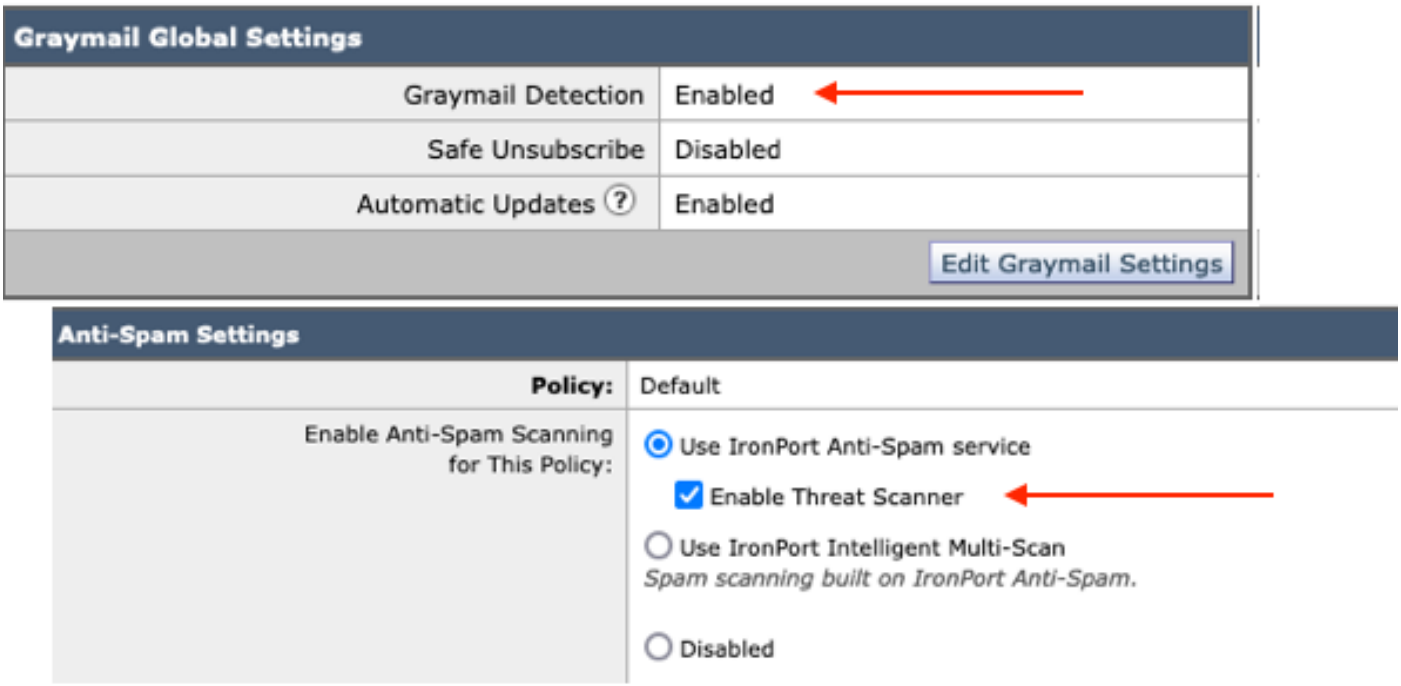


طريقة العرض قبل الإعداد

بمجرد تمكين Graymail، يصبح مربع تحديد ماسح التهديدات متوفرا لكل نهج بريد وارد.

لتمكين "الماسح الضوئي للتهديدات" ضمن WebUI:

- انتقل إلى نهج البريد
  - نهج البريد الوارد
    - حدد نهج البريد المطلوب
      - حدد مكافحة البريد العشوائي.
        - تمثل أعلى صفحة التكوين خيار خانة الاختيار لتمكين الماسح الضوئي الذي يمثل تهديدا.
- إرسال التغييرات وتنفيذها لإنهاء التكوين



خيار الماسح الضوئي للتهديدات ضمن مكافحة البريد العشوائي

إعداد واجهة سطر الأوامر

قم بتمكين خدمة Graymail باستخدام أوامر CLI.

- IMSANDGRAYMAILCONFIG
  - غرايميل
    - إعداد
      - هل ترغب في إستخدام "الكشف عن رسائل الجريب ميل"؟ [Y] >
        - هل ترغب في تمكين التحديثات التلقائية لمحرك Graymail؟ [Y]>
  - أكمل المطالبات المتبقية للعودة إلى مطالبة الجهاز الرئيسي.

- قم بإلتزام + إضافة التعليقات المطلوبة > إكمال الإجراء بالضغط على المفتاح "إرجاع".

تمكين "مامسح التهديدات الضوئي" أو تعطيله ضمن "سياسة" من CLI.

- CLI> policyConfig

هل ترغب في تكوين أولوية نهج البريد الوارد أو نهج البريد الصادر أو تطابق الرؤوس؟

1. نهج البريد الوارد
2. نهج البريد الصادر
3. تطابق أولوية الرؤوس

[1]> 1

تكوين نهج البريد الوارد

1 - الشامل(1)
2. Blocked_list
3. allowed_list
4. Allow_spoof
5. افتراضي

أدخل اسم أو رقم الإدخال الذي ترغب في تحريره:
[]> 1

أختر العملية التي تريد تنفيذها:
- الاسم - تغيير اسم النهج
- جديد - إضافة صف وضع نهج جديد
- حذف - إزالة صف وضع النهج
- طباعة - طباعة صفوف أعضاء السياسة
- مكافحة البريد العشوائي - تعديل نهج مكافحة البريد العشوائي
- برنامج AntiVirus - تعديل نهج مكافحة الفيروسات
- التفشي - تعديل سياسة عوامل تصفية التفشي
- البرامج الضارة المتقدمة - تعديل نهج الحماية المتقدمة من البرامج الضارة
- Graymail - تعديل نهج Graymail
- ThreatDefenseSupervisor - تعديل موصل الدفاع عن التهديد

- عوامل التصفية - تعديل عوامل التصفية
[]> مكافحة البريد العشوائي

أختر العملية التي تريد تنفيذها:
- تعطيل - تعطيل نهج مكافحة البريد العشوائي (تعطيل جميع الإجراءات المتعلقة بالسياسة)
- تمكين - تمكين نهج مكافحة البريد العشوائي
[]> تمكين

بدء تكوين مكافحة البريد العشوائي

هل ترغب في إستخدام Intelligent Multi-Scan على هذا النهج؟ [N]>

هل ترغب في إستخدام IronPort Anti-Spam على هذا النهج؟ [Y]>

تم تعريف بعض الرسائل بشكل إيجابي على أنها بريد عشوائي. بعض الرسائل هي تم تعريفه على أنه بريد عشوائي مشتبه فيه. يمكنك تعيين البريد العشوائي المشتبه به في مكافحة البريد العشوائي ل IronPort
الحد الأدنى.
تنطبق خيارات التكوين على الرسائل التي تم تعريفها بشكل إيجابي على أنها سبام:
هل ترغب في تمكين معالمة خاصة لحكم "مسح التهديدات"؟ [N]> y

استمر في تحديد القائمة لإكمال خيارات نهج البريد، واضغط على "مفتاح الإرجاع" لقبول الإجراء الافتراضي لكل خيار.

أكمل الحفظ باستخدام الأوامر.

- قم بإلتزام + إضافة التعليقات المطلوبة > إكمال الإجراء بالضغط على المفتاح "إرجاع".

التحقق من الصحة

كيفية قراءة السجلات وتفسيرها.

يمثل التسجيل عبر البريد الخاص بمسح التهديدات حكم موقت فقط، بينما تمثل القضية الحكم النهائي.

سجلات البريد تظهر حكمين مختلفين لمسح التهديدات النظيف مقابل المدانين

- إذا كان الحكم الموقت الصادر من المسح الضوئي بالتهديد نظيفا، فإن السجل يتم تقديمه بشكل مشابه إلى هذه العينات.
  - معلومات: الحكم الموقت على بريد الجراد - شرعي (0) <رسالة نظيفة>
  - معلومات: الحكم الموقت على رسائل البريد - MCE (11) <حملة بريد إلكتروني متنوعة>
- إذا كان الحكم الادانه الصادر من المسح الضوئي بالتهديد، فإن السجل يعرض بشكل مماثل على هذه العينات.

- المعلومات: الحكم المؤقت على أداة الكشف عن التهديدات - التصيد الاحتيالي (101)
- المعلومات: الحكم المؤقت على برنامج ThreatScan - فيروس (2)

عينة سجلات البريد: القرار النظيف لماسح التهديدات يستخدم مختلف العبارات: الحكم في الكتابة على البريد.

<#root>

```
Wed Jan 31 08:19:32 2024 Info: MID 3189755
```

interim graymail verdict - LEGIT (0) <Clean message>

```
Wed Jan 31 08:19:33 2024 Info: MID 3189755 interim verdict using engine: CASE negative
Wed Jan 31 08:19:33 2024 Info: MID 3189755 using engine: CASE spam negative
```

تعقب الرسائل ال يظهر إدخال سجل ماسح التهديدات، الحالة فقط: الحكم النهائي.

إن هذه العينات من ماسح التهديدات (TS) تقدم 4 سيناريوهات للحكم.

ملاحظة: فئات "التصيد الاحتيالي" و"الفيروسات" هما الفئتان الوحيدتان اللتان تزيدان من وزن حكم القضية

عينة سجلات البريد: إدانة Phishing TS وإدانة AntiSpam كلاهما حاضران

<#root>

```
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

interim

ThreatScanner verdict - PHISHING (101)

```
 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:23 2024 Info: MID 3057397 interim verdict using engine: CASE spam positive
Thu Jan 25 09:05:23 2024 Info: MID 3057397
```

using engine: CASE spam positive

```
Thu Jan 25 09:05:23 2024 Info: Message aborted MID 3057397 Dropped by CASE
```

عينة التعقب: ال يوجد إدانة Phishing TS وإدانة الحالة موجودة.

25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 07:05:23 (GMT -08:00)	Message 3057397 scanned by Anti-Spam engine: CASE. Final verdict: Positive

عينة سجلات البريد: إدانة Phishing TS والسلاب السلبي لمكافحة البريد العشوائي كالهام موجود.

```
<#root>

Thu Jan 25 09:05:47 2024 Info: MID 3057413

interim ThreatScanner verdict - PHISHING (101)

 <Message detected as phishing either by heuristic analysis or by detecting the link as fraudulent>
Thu Jan 25 09:05:47 2024 Info: MID 3057413 interim verdict using engine: CASE spam negative
Thu Jan 25 09:05:47 2024 Info: MID 3057413

using engine: CASE spam negative
```

نموذج التعقب: تمت إدانة Phishing TS والسلبيات الخاصة بمكافحة البريد العشوائي موجودة.

25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
25 Jan 2024 07:05:47 (GMT -08:00)	Message 3057413 scanned by Anti-Spam engine: CASE. Final verdict: Negative

نموذج سجلات البريد: الإدانة في Virus TS وعينة الإدانة في AntiSpam لسجلات البريد.

```
<#root>

Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim

ThreatScanner verdict - VIRUS (2)

 <Virus detected by ThreatScanner engine>
Thu Jan 25 13:37:16 2024 Info: MID 3066060 interim verdict using engine: CASE spam positive
Thu Jan 25 13:37:16 2024 Info: MID 3066060

using engine: CASE spam positive


Thu Jan 25 13:37:16 2024 Info: Message aborted MID 3066060 Dropped by CASE
```

نموذج التعقب: لا يوجد إدانة ضد Virus TS وتوجد إدانة ضد AntiSpam.

25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 matched per-recipient policy DEFAULT for inbound mail policies.
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Interim verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 scanned by Anti-Spam engine: CASE. Final verdict: Positive
25 Jan 2024 11:37:16 (GMT -08:00)	Message 3066060 aborted: Dropped by CASE

عينة سجلات البريد: توجد إدانة Virus TS و AntiSpam السلبية.

<#root>

```
Jan 23 21:38:57 2024 Info: MID 3013692
```

interim ThreatScanner verdict - VIRUS (2)

```
 <Virus detected by ThreatScanner engine>
Jan 23 21:38:58 2024 Info: MID 3013692 interim verdict using engine: CASE spam negative
Jan 23 21:38:58 2024 Info: MID 3013692
```

using engine: CASE spam negative

نموذج التعقب: عدم وجود إدانة ل Virus TS ووجود AntiSpam السلبي.

23 Jan 2024 19:38:57 (GMT -08:00)	Message 3013692 matched per-recipient policy DEFAULT for inbound mail policies.
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
23 Jan 2024 19:38:58 (GMT -08:00)	Message 3013692 scanned by Anti-Spam engine: CASE. Final verdict: Negative

تحتوي سجلات Graymail على قرار "ماسح التهديدات" والمحتوى الداعم لتحليل TALOS إذا تم إجراء اعتراض إيجابي خاطئ.

أدى وجود النتائج الأولية لماسح التهديدات إلى تمرير تسجيل غرامي بسرعة أكبر. لمعالجة هذا السلوك، تم إجراء تعديلات SEG على سجلات Graymail.

- يعمل AsyncOS 15.5 على تعيين اشتراك السجل الافتراضي لملفات سجل Graymail إلى 20 زيادة الاحتفاظ بالسجل.
  - لا تتغير إعدادات ملف السجل إذا تم تعيين الإعداد أعلى من 20 عند الترقية.
- تعرض الرسائل المؤقتة المدانة بالبريد الجراد الوارد نتائج المسح الأولي الكاملة، على مستوى المعلومات.
- يتم عرض نتائج الفحص من خلال Graymail لكافة الرسائل الأخرى على مستوى تصحيح الأخطاء.

معلومات ذات صلة

- دليل إعداد أمان البريد الإلكتروني
- صفحة بدء تشغيل عبارة البريد الإلكتروني الآمن من Cisco لدعم الأدلة

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).