تكوين دفتر يومية آمن لعبارة البريد الإلكتروني لكل نهج لتأمين الدفاع عن تهديد البريد الإلكتروني

المحتويات

المقدمة

يصف هذا المستند خطوات تكوين عبارة البريد الإلكتروني الآمنة (SEG) لإجراء عمل اليومية لكل سياسة للدفاع الآمن عن تهديد البريد الإلكتروني (SETd).

المتطلبات الأساسية

من المفيد معرفة الإعدادات العامة والتكوين لعبارة البريد الإلكتروني الآمن (SEG) من Cisco مسبقا.

المكونات المستخدمة

يتطلب هذا الإعداد كليهما؛

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 والإصدارات الأحدث
- مثيل الدفاع ضد تهديد البريد الإلكتروني (SETD) من Cisco.
- موصل الدفاع عن التهديد (TDC). "الصلة المحددة بين التقنيتين."

"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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

يمكن دمج Cisco SEG مع SETd لتوفير حماية إضافية.

- يقوم إجراء دفتر يومية SEG بتحويل البريد الإلكتروني الكامل لكافة الرسائل

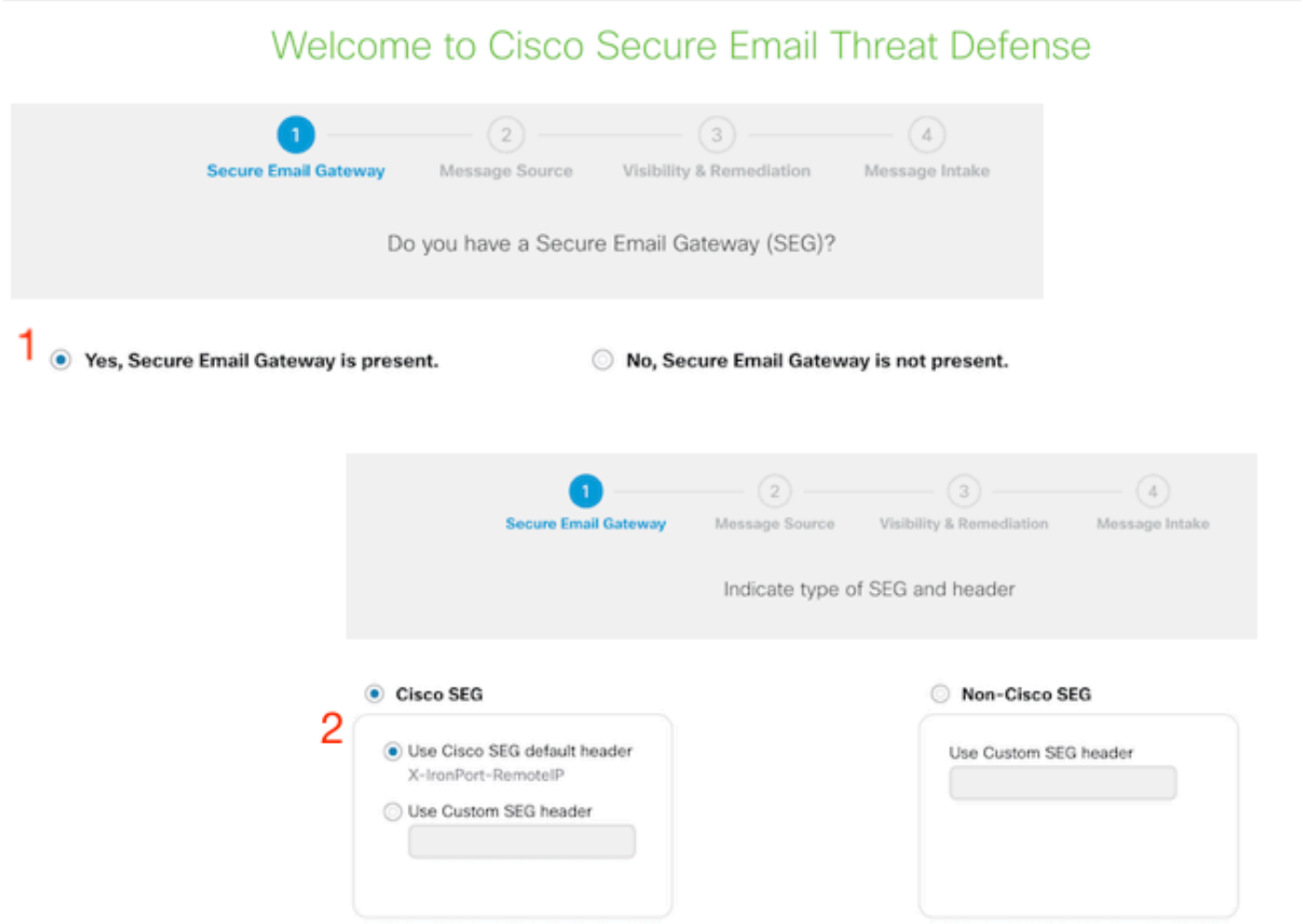
النظيفة.

- توفر "مجموعة الخدمات الخاصة" خيار الاختيار الانتقائي لتدفقات البريد الوارد استنادا إلى تطابق "نهج كل بريد".
- يسمح خيار SEG لكل نهج بثلاثة خيارات، بدون فحص، عنوان إدخال رسالة افتراضي، أو عنوان إدخال رسالة مخصص.
  - يمثل "عنوان الإدخال الافتراضي" حساب SET الأساسي الذي يقبل البريد لمثيل حساب معين.
  - يمثل "عنوان إدخال الرسالة المخصص" حساب SET آخر يقبل البريد للمجالات المختلفة المحددة. ينطبق هذا السيناريو على بيئات SETD الأكثر تعقيدا.
- تحتوي الرسائل المنشورة على معرف رسالة SEG (متوسط) ومعرف اتصال الوجهة DCID
- تحتوي قائمة انتظار التسليم على قيمة مماثلة للمجال، "the.tdc.queue"، لالتقاط عدادات نقل SETd.
  - يمكن عرض العدادات النشطة "the.tdc.queue" هنا: cli>tophosts أو SEG Reporting > حالة التسليم (غير CES).
  - يمثل "the.tdc.queue" موصل الدفاع عن التهديد (TDC) المكافئ لاسم مجال الوجهة.

التكوين

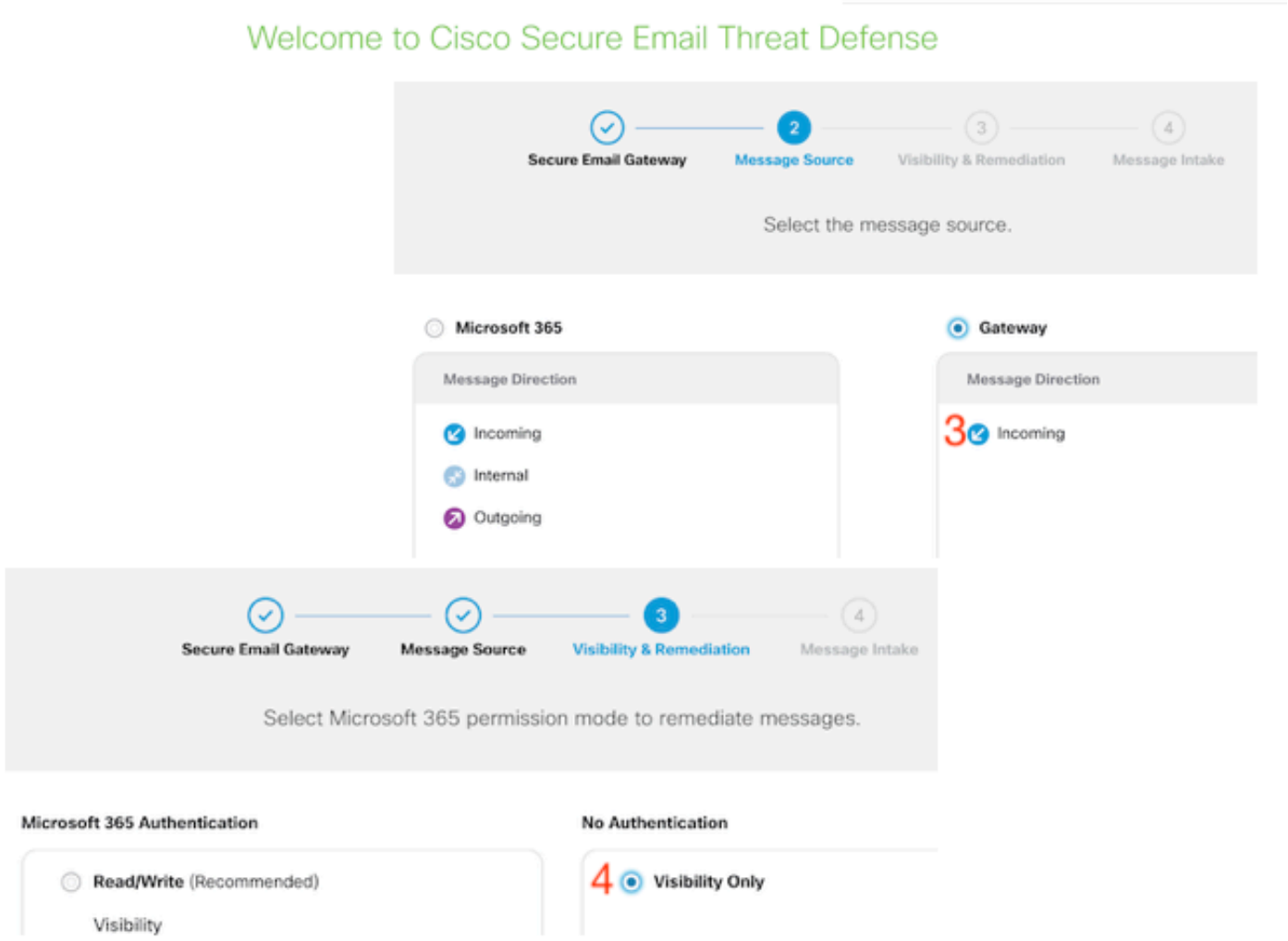
قم بتعيين خطوات الإعداد الأولي لإنشاء "عنوان إدخال الرسالة".

1. نعم، عبارة البريد الإلكتروني الآمنة موجودة.
2. Cisco SEG

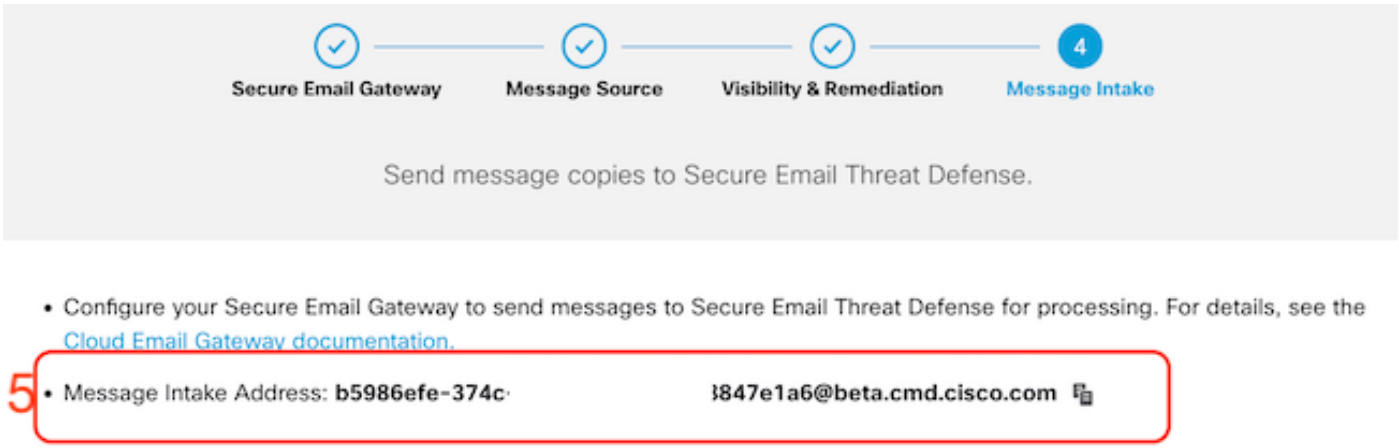


3. إتجاه الرسالة = الوارد.

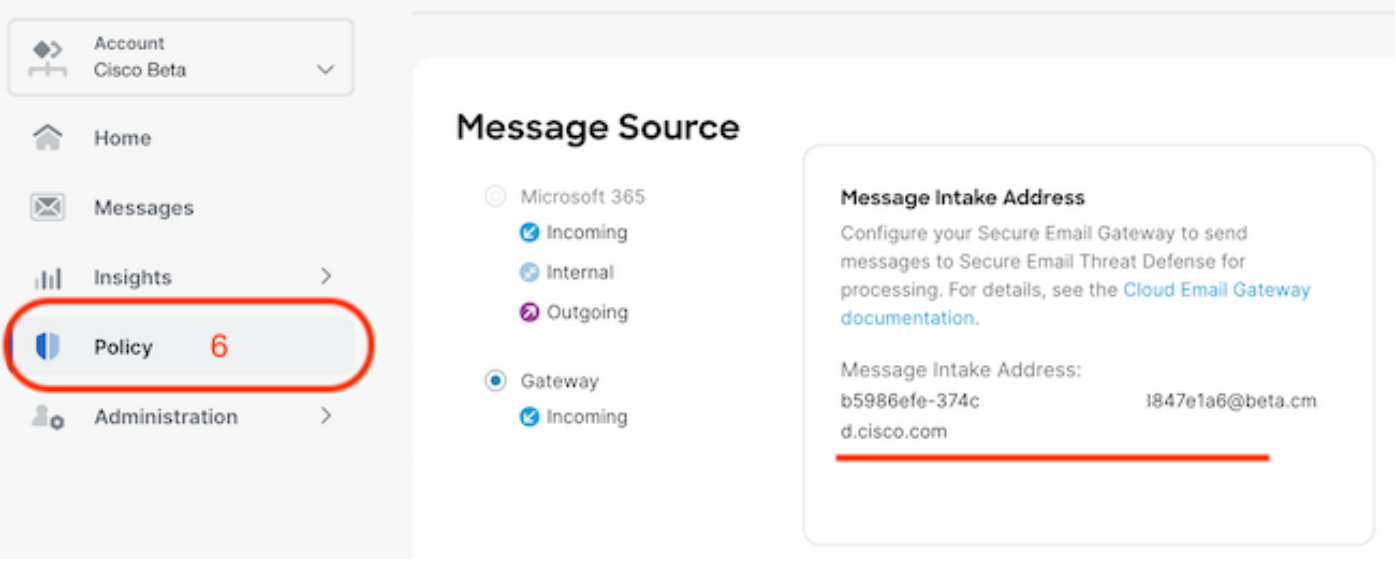
4. لا توجد مصادقة = إمكانية الرؤية فقط.



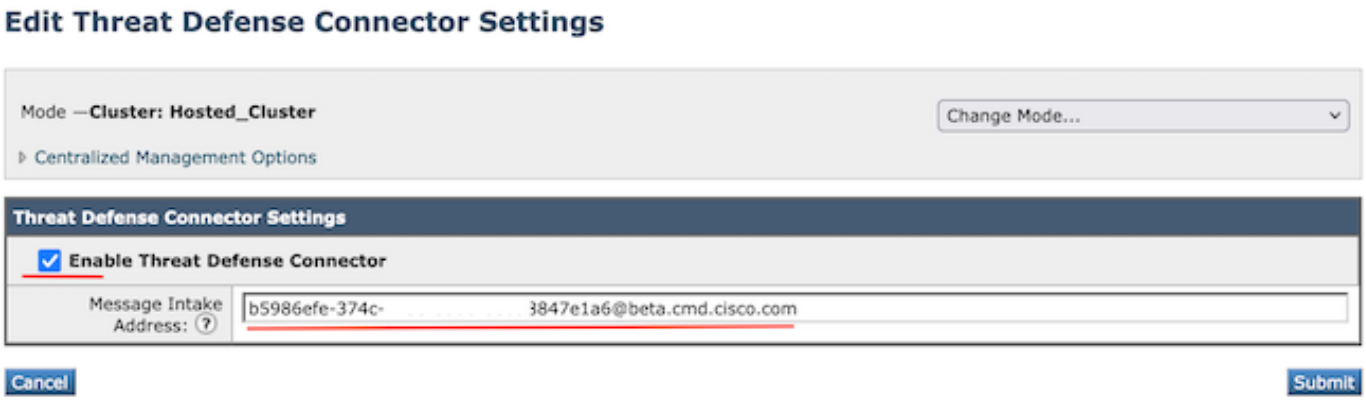
5. يتم تقديم عنوان إدخال الرسالة بعد قبول الخطوة 4.



6. إذا كنت بحاجة إلى إستدراد إعداد مادة نشر عنوان إدخال الرسالة، انتقل إلى قائمة "النهج".

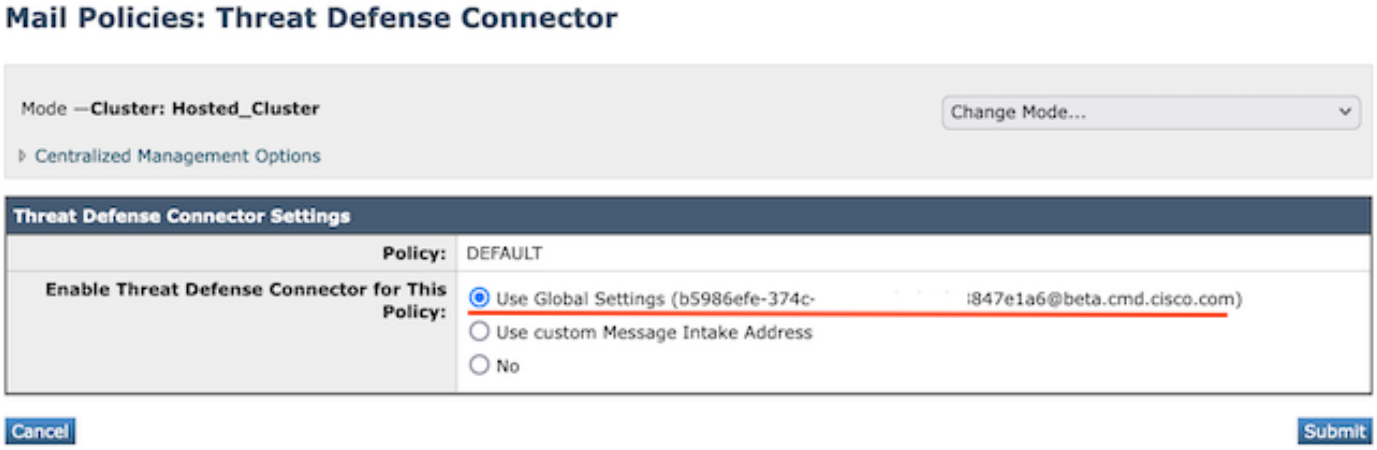


الانتقال إلى SEG WebUI، انتقل إلى خدمات الأمان > إعدادات موصل الحماية ضد التهديد.



انتقل إلى نهج البريد:

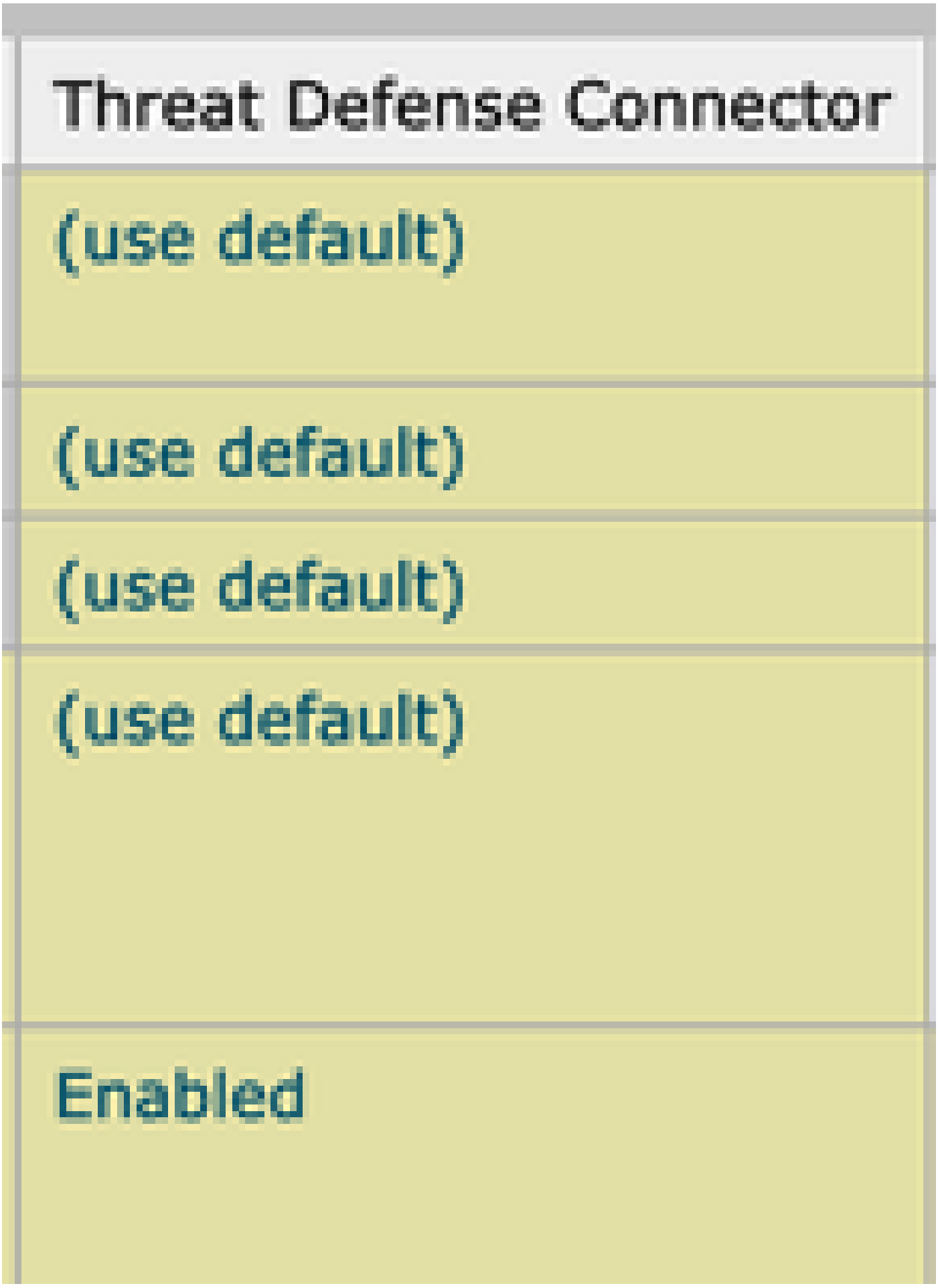
- نهج البريد الوارد
  - الخدمة الأخيرة إلى اليمين هي "Threat Defense Connector".
- يظهر إرتباط الإعدادات، "معطل"، لأول مرة في تكوين.



سيتم ملء عنوان إدخال الرسالة المخصص باستخدام مثيل SETD ثانوي.

ملاحظة: من المهم عند إستخدام عنوان الإدخال المخصص تكوين معايير مطابقة نهج البريد للالتقاط حركة مرور المجال الصحيحة.

تعرض طريقة العرض الأخيرة للإعداد قيمة "ممكن" للخدمة التي تم تكوينها.


Threat Defense Connector
(use default)
(use default)
(use default)
(use default)
Enabled

التحقق من الصحة

بمجرد اكتمال كافة الخطوات، يقوم البريد الإلكتروني بملء لوحة معلومات SET.

يعرض أمر واجهة سطر الأوامر (CLI) الخاص ب SEG > tophosts عدادات قائمة الانتظار لعمليات التسليم النشطة.

```
(Machine esa1.myesa.com)> tophosts

Status as of:                  Fri Feb 16 19:55:34 2024 CST
Hosts marked with '*' were down as of the last delivery attempt.

                               Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host             Recip.    Out     Recip.    Bounced    Bounced

5   the.tdc.queue                   1      0    104,163          0          0
```

استكشاف الأخطاء وإصلاحها

سلوك اتصال TDC:

- يتم فتح 3 إتصالات كحد أدنى عند وجود إدخالات في قائمة الانتظار الوجهة
- يتم إنشاء إتصالات إضافية بشكل ديناميكي باستخدام نفس المنطق لقوائم انتظار وجهة البريد الإلكتروني العادية.
- يتم إغلاق الاتصالات المفتوحة بمجرد أن تصبح قائمة الانتظار فارغة أو ال توجد إدخالات كافية في قائمة انتظار الوجهة.
- يتم إجراء عمليات إعادة المحاولة حسب القيمة الموجودة في الجدول.
- تتم إزالة الرسائل من قائمة الانتظار بعد استنفاد عمليات إعادة المحاولة أو إذا كانت الرسالة في قائمة الانتظار لفترة طويلة (120 ثانية)

آلية إعادة محاولة موصل الدفاع بالتهديد

حالة خطأ	تم إعادة المحاولة	عدد عمليات إعادة المحاولة
أخطاء SMTP 5xx (باستثناء 503/552)	ال	غير متوفر
أخطاء SMTP 4xx (بما في ذلك 503/552)	نعم	1
أخطاء TLS	ال	غير متوفر
الشبكة العامة \ أخطاء الاتصال، أخطاء DNS، وما إلى ذلك.	نعم	1

نموذج سجلات بريد TDC استنادا إلى نتائج التسليم

تحتوي إدخالات السجل المتعلقة ب TDC على القيمة TDC: السابقة لنص السجل.

تقدم العينة تسليم عادي ل TDC.

```
Fri Feb 16 21:19:22 2024 Info: TDC: MID 14501404 with Message-ID '<O7afv777xxreILg2OQ@gostrt-sstp-0>' e
Fri Feb 16 21:19:23 2024 Info: TDC: New SMTP DCID 4566150 interface 10.13.0.99 address 10.10.55.171 por
Fri Feb 16 21:19:23 2024 Info: DCID 4566150 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SH
Fri Feb 16 21:19:23 2024 Info: TDC: Delivery start DCID 4566150 MID 14501404
Fri Feb 16 21:19:24 2024 Info: TDC: MID 14501404 successfully delivered for scanning with Cisco Secure
Fri Feb 16 21:19:24 2024 Info: Message finished MID 14501404 done
```

تقدم العينة خطأ تسليم بسبب الرسالة غير القابلة للتسليم بعد انتهاء مهلة 120 ثانية

```
Wed Nov 29 09:03:05 2023 Info: TDC: Connection Error: DCID 36 domain: the.tdc.queue IP: 10.10.0.3 port:
```

تقدم العينة خطأ تسليم بسبب خطأ TLS.

```
Fri Feb 14 04:10:14 2024 Info: TDC: MID 1450012 delivery failed to Cisco Secure Email Threat Defense:TL
```

تقدم هذه العينة عنوان دفتر يومية SETD غير صالح مما يؤدي إلى ارتداد ثابت.

```
Wed Nov 29 09:07:16 2023 Info: TDC: MID 171 with Message-ID '<20231129090720.24911.11947@vm21bsd0050.cs
dress test@esa.example.com
Wed Nov 29 09:07:16 2023 Info: DNS Error esa.example.com MX - NXDomain
Wed Nov 29 09:07:16 2023 Info: TDC: Hard bounced - 5.1.2 - Bad destination host ('000', 'DNS Hard Error
Wed Nov 29 09:07:16 2023 Info:
TDC: MID 171 delivery failed to Cisco Secure Email Threat Defense: Hard Bounced.
Wed Nov 29 09:07:16 2023 Info: Bounced: DCID 0 MID 171 to RID 0 - Bounced by destination server with re
(MX) :
```

يعرض تعقب الرسائل بمساطة سطرا واحدا يشير إلى التسليم الناجح للرسالة إلى SETD.

تقدم هذه العينة خطأ تسليم بسبب خطأ TLS.

16 فبراير، 2024 م 21:19:24 (GMT -06:00)	TDC: تم تسليم الرسالة 14501404 بنجاح للمسح الضوئي باستخدام برنامج الدفاع الآمن ضد تهديدات البريد الإلكتروني من Cisco.

معلومات ذات صلة

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

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).