شبكة نجاح Cisco (CSN) على أمان البريد الإلكتروني من Cisco

المحتويات

المقدمة

قدم هذا المستند المعلومات المتعلقة بميزة شبكة نجاح Cisco التي ستكون متاحة كجزء من إصدار AsyncOS 13.5.1 لجهاز أمان البريد الإلكتروني من Cisco (ESA). شبكة نجاح Cisco (CSN) هي خدمة سحابة ممكنة من قبل المستخدم. عند تمكين CSN، يتم إنشاء اتصال آمن بين ESA وسحابة Cisco (باستخدام اتصال CTR)، لتدفق معلومات حالة الميزة. يوفر دفق بيانات CSN آلية لاختيار البيانات ذات الأهمية من ESA وإرسالها بتنسيق مهيكل إلى محطات الإدارة عن بعد.

الفوائد

- لإعلام العميل بالميزات غير المستخدمة المتاحة التي يمكنها تحسين فعالية المنتج.
- إبلاغ العميل بشأن خدمات الدعم الفني الإضافية والمراقبة التي قد تتوفر للمنتج.
- لمساعدة Cisco في تحسين المنتج.

المعلومات التي تم جمعها

هذا قائمة معلومات الميزة التي يتم تجميعها كجزء من هذه الميزة بمجرد تكوينها على جهاز ESA:

- طراز الجهاز (600v، 300v، 100v، 000v، x95، x90)
- الرقم التسلسلي للجهاز (UDI)
- UserAccountID (رقم معرف VLN أو SLPIID)
- إصدار البرامج
- تاريخ التثبيت
- SLvan (اسم الحساب الظاهري في الترخيص الذكي)
- وضع النشر
- برنامج IronPort Anti-spam

- إلغاء الاشتراك في خدمة Graymail Safe
- سوفوس
- مكافي
- سمعة الملف
- تحليل الملفات
- منع فقدان البيانات
- موجز ويب التهديد الخارجي
- تحليل صورة IronPort
- عوامل تصفية التفشي
- إعدادات تشفير البريد الإلكتروني Cisco IronPort (تشفير المغلفات)
- تشفير PXE
- سمعة المجال
- تصفية URL
- حظر تخصيص الصفحة
- تعقب الرسائل
- السياسة العامة والفيروسات والحجر الصحي من الفاشية
- عزل البريد العشوائي

المتطلبات الأساسية

المتطلبات

لتكوين هذه الميزة، وهذه بعض المتطلبات التي يجب استيفاؤها:

- حساب CTR (الاستجابة للتهديدات من Cisco)

التكوين المرتبط بجدار الحماية

يعتمد تكوين جدار الحماية اللازم لتشغيل CSN حاليا على اتصال CTR، يرجى الرجوع إلى هذا المستند للحصول على مزيد من المعلومات: دمج ESA مع CTR

المكونات المستخدمة

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

- جهاز أمان البريد الإلكتروني (AsyncOS (ESA الإصدار x.13.5.1 والإصدارات الأحدث.

التكوين

أنت يستطيع شكلت هذا سمة يستعمل على حد سواء ال ESA UI أو ال CLI. وترد أدناه تفاصيل عن كلا الخطوتين.

تبعيات CSN و CTR

تعتمد ميزة CSN على اتصال ميزة CTR لتشغيلها بنجاح ويوفر هذا الجدول المزيد من المعلومات حول العلاقة بين هاتين العمليتين.

الإستجابة CSN	موصل	عملية CSN

للتهديدات		SSE	
معطل	معطل	لأسفل	معطل
معطل (إلغاء التسجيل)	ممكن	لأسفل	لأسفل
معطل (مسجل)	ممكن	لأعلى	لأعلى
ممكن	معطل يدويا	لأعلى	لأسفل
ممكن	ممكن	لأعلى	لأعلى

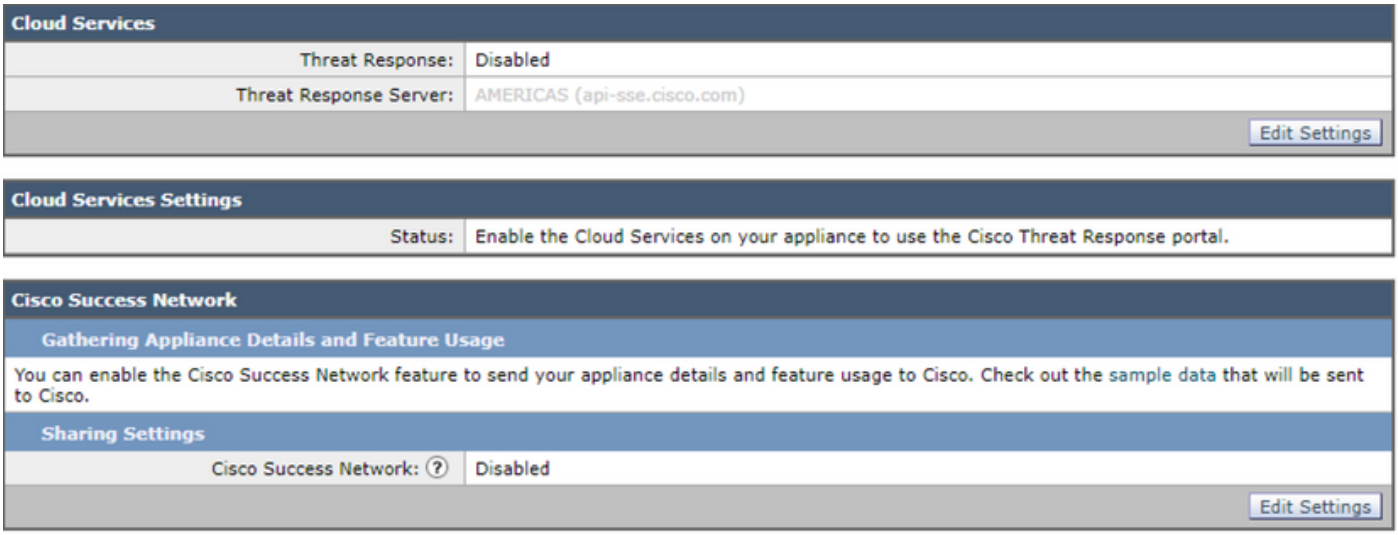
تكوين CSN باستخدام واجهة المستخدم

1) الدخول إلى واجهة مستخدم ESA.

2) استعرض للوصول إلى **الشبكة>إعدادات خدمة السحابة** (سأفترض أنه تم تعطيل CTR قبل بدء الترقية إلى x.13.5.1). قبل الترقية، إذا تم تمكين CTR، فسيتم تمكين CSN أيضا بشكل افتراضي. إذا تم تعطيل CTR، فسيتم تعطيل CSN أيضا.

ملاحظة: سنفرض أن CTR قد تم تعطيله قبل الترقية لأن من المفترض أن يكون CTR في النشر المركزي معطلا لأنه تم تمكينه فقط في SMA لإرسال معلومات التقارير إلى CTR.

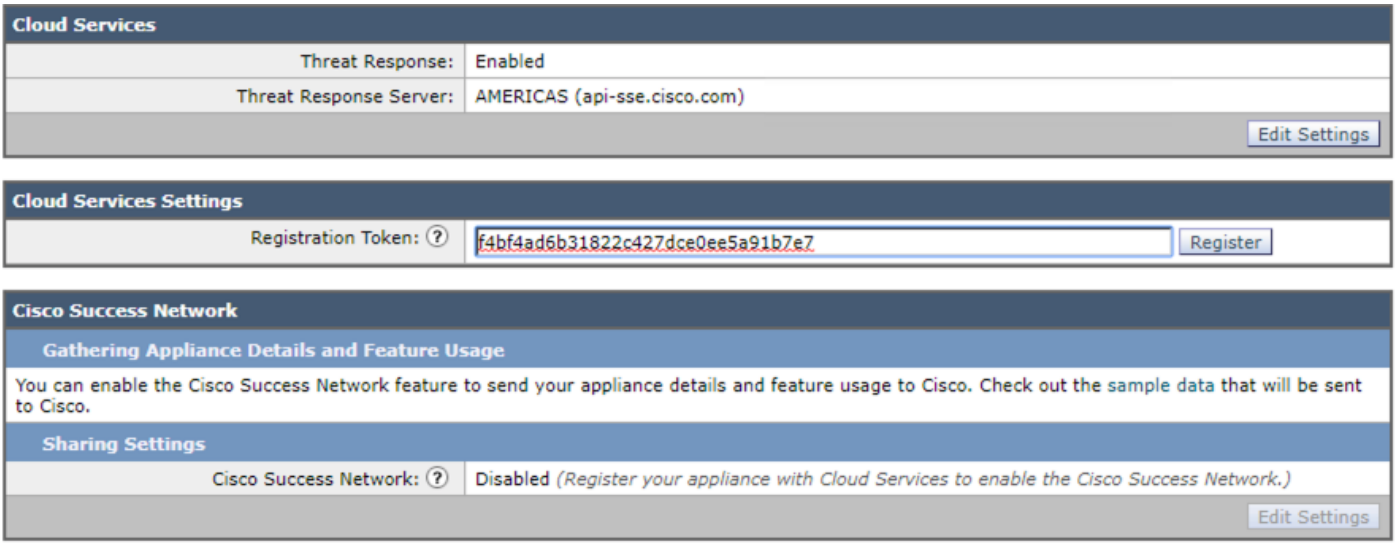
3) هذا ما تلاحظه كافتراضي على جهاز ESA: -



4) سنقوم الآن بتسجيل الإيسا هذه عن طريق تمكين خدمات مركز مراقبة تكنولوجيا المعلومات (CTR) أولا على الإيسا و"إرسال" التغييرات.

5) ستظهر هذه الحالة على صفحة CTR "خدمة سحابة Cisco مشغولة. انتقل إلى هذه الصفحة بعد مرور بعض الوقت للتحقق من حالة الجهاز. قم بتنفيذ التغييرات على الجهاز.

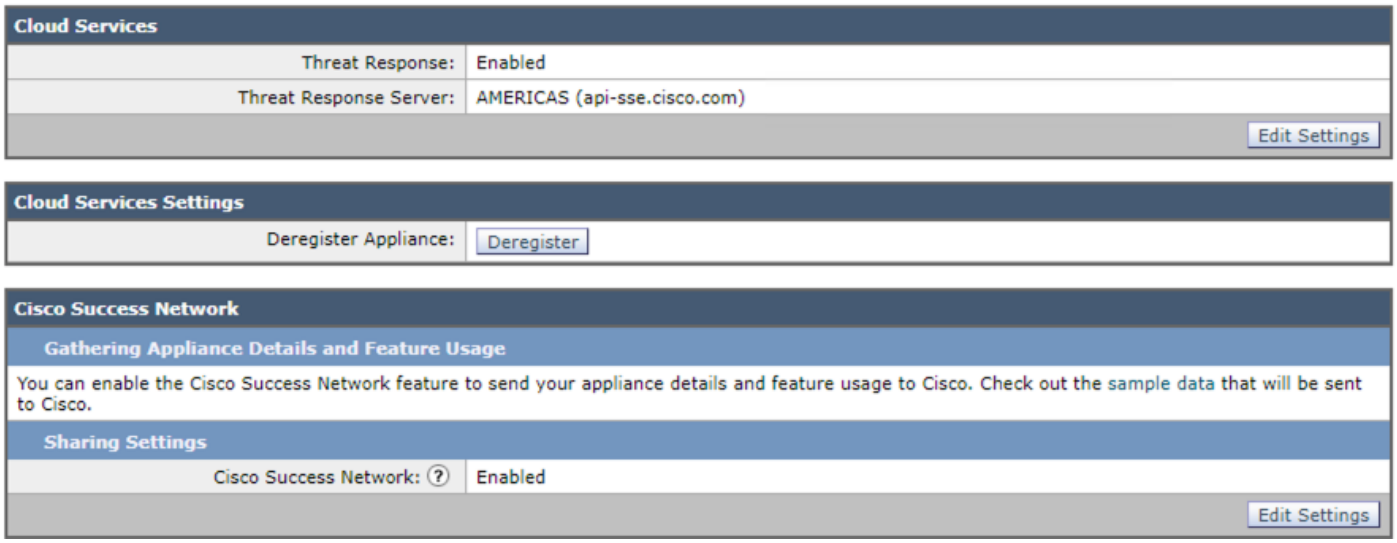
6) بعد ذلك يمكنك التقدم والحصول على الرمز المميز CTR وتسجيل الجهاز في CTR:



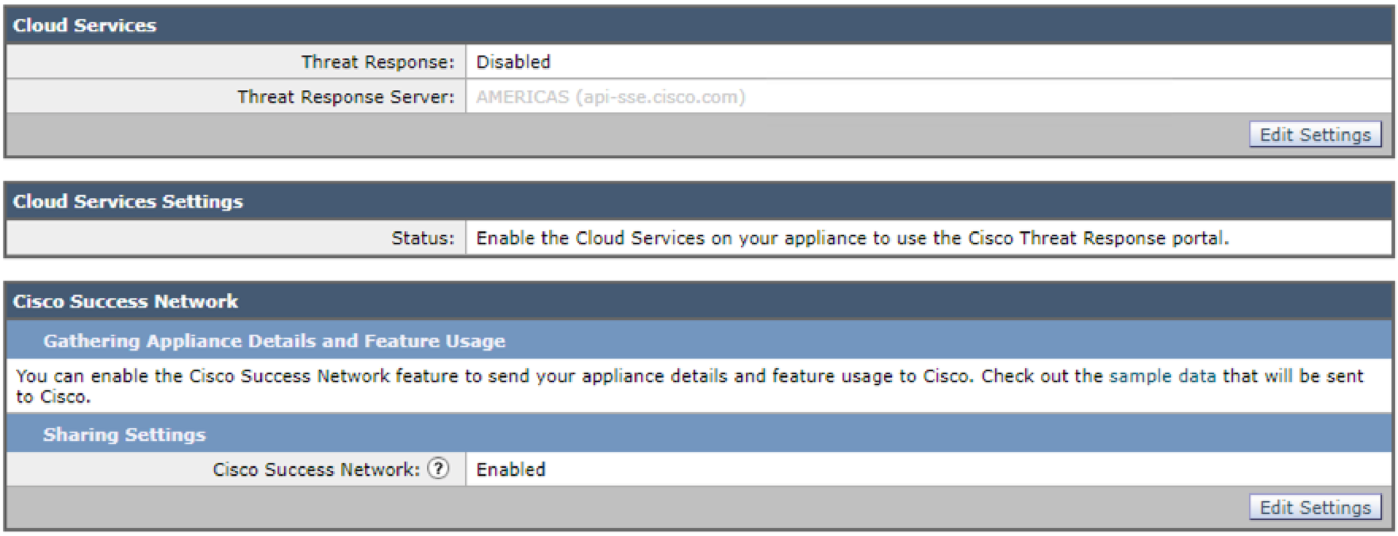
7) يجب أن ترى هذه الحالة بمجرد نجاح التسجيل:

النجاح — تم بدء طلب لتسجيل الجهاز الخاص بك مع بوابة الاستجابة للتهديدات من Cisco. انتقل مرة أخرى إلى هذه الصفحة بعد مرور بعض الوقت للتحقق من حالة الجهاز.

8) بمجرد تحديث الصفحة، سترى CTR مسجلا و CSN ممكنا:



9) وكما تمت مناقشته، يجب تعطيل CTR في هذا السيناريو حيث إن ESA هذه هي المركزية وستظل ترى CSN ممكنة كما هو متوقع. في حالة عدم إدارة ESA هذه بواسطة SMA (غير مركزي)، يمكنك الحفاظ على تمكين CTR.



يجب أن تكون هذه هي الحالة الأخيرة للتكوين. **يجب اتباع هذه الخطوة لكل ESA لأن هذا الإعداد هو "مستوى الجهاز".**

تكوين CSN باستخدام CLI

```
Machine esa )> csnconfig)

You can enable the Cisco Success Network feature to send your appliance details and feature
.usage to Cisco

:Choose the operation you want to perform
.ENABLE - To enable the Cisco Success Network feature on your appliance -
enable <[]

.The Cisco Success Network feature is currently enabled on your appliance
```

يلزم الالتزام بالتغييرات كجزء من تمكين هذا باستخدام واجهة سطر الأوامر.

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء هذه الميزة وإصلاحها، يوجد سجل **/data/pub/csn_log**) PUB) متوفر يحتوي على المعلومات الخاصة بهذه الميزة. النموذج التالي هو السجل في الوقت الذي تم فيه إكمال التسجيل على الجهاز:

```
Machine ESA) (SERVICE)> tail)

:Currently configured logs
    Log Name              Log Type                          Retrieval            Interval
    ---------------------------------------------------------------------------------
    API                   API Logs                          Manual Download      None .1
    amp                   AMP Engine Logs                   Manual Download      None .2
    amparchive            AMP Archive                       Manual Download      None .3
    antispam              Anti-Spam Logs                    Manual Download      None .4
    antivirus             Anti-Virus Logs                   Manual Download      None .5
    asarchive             Anti-Spam Archive                 Manual Download      None .6
    authentication        Authentication Logs               Manual Download      None .7
    avarchive             Anti-Virus Archive                Manual Download      None .8
    bounces               Bounce Logs                       Manual Download      None .9
    cli_logs              CLI Audit Logs                    Manual Download      None .10
    csn_logs              CSN Logs                          Manual Download      None .11
```

```
ctr_logs            CTR Logs                            Manual Download     None .12
dlp                 DLP Logs                            Manual Download     None .13
eaas                Advanced Phishing Protection Logs   Manual Download     None .14
encryption          Encryption Logs                     Manual Download     None .15
error_logs          IronPort Text Mail Logs             Manual Download     None .16
euq_logs            Spam Quarantine Logs                Manual Download     None .17
euqgui_logs         Spam Quarantine GUI Logs            Manual Download     None .18
ftpd_logs           FTP Server Logs                     Manual Download     None .19
gmarchive           Graymail Archive                    Manual Download     None .20
graymail            Graymail Engine Logs                Manual Download     None .21
gui_logs            HTTP Logs                           Manual Download     None .22
ipr_client          IP Reputation Logs                  Manual Download     None .23
mail_logs           IronPort Text Mail Logs             Manual Download     None .24
remediation         Remediation Logs                    Manual Download     None .25
reportd_logs        Reporting Logs                      Manual Download     None .26
reportqueryd_logs   Reporting Query Logs                Manual Download     None .27
s3_client           S3 Client Logs                      Manual Download     None .28
scanning            Scanning Logs                       Manual Download     None .29
sdr_client          Sender Domain Reputation Logs       Manual Download     None .30
service_logs        Service Logs                        Manual Download     None .31
smartlicense        Smartlicense Logs                   Manual Download     None .32
sntpd_logs          NTP logs                            Manual Download     None .33
status              Status Logs                         Manual Download     None .34
system_logs         System Logs                         Manual Download     None .35
threatfeeds         Threat Feeds Logs                   Manual Download     None .36
trackerd_logs       Tracking Logs                       Manual Download     None .37
unified-2           Consolidated Event Logs             Manual Download     None .38
updater_logs        Updater Logs                        Manual Download     None .39
upgrade_logs        Upgrade Logs                        Manual Download     None .40
url_rep_client      URL Reputation Logs                 Manual Download     None .41
                                        .Enter the number of the log you wish to tail
                                                                            11 <[]

                                                        .Press Ctrl-C to stop
                                        Sun Apr 26 18:16:13 2020 Info: Begin Logfile
Sun Apr 26 18:16:13 2020 Info: Version: 13.5.1-177 SN: 564D2E7007BA223114B8-786BB6AB7179
                        Sun Apr 26 18:16:13 2020 Info: Time offset from UTC: -18000 seconds
                                    .Sun Apr 26 18:16:13 2020 Info: System is coming up
                            Sun Apr 26 18:16:13 2020 Info: DAEMON: Watchdog thread started
                        Sun Apr 26 18:16:16 2020 Info: The appliance is uploading CSN data
                Sun Apr 26 18:16:16 2020 Info: The appliance has successfully uploaded CSN data
```

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).