Cisco Success Network (CSN) sur Cisco Email Security

Table des matières

Introduction

Ce document fournit des informations sur la fonctionnalité Cisco Success Network qui serait disponible dans le cadre de la version AsyncOS 13.5.1 pour l'appliance de sécurité de la messagerie Cisco (ESA). Cisco Success Network (CSN) est un service cloud activé par l'utilisateur. Lorsque CSN est activé, une connexion sécurisée est établie entre l'ESA et le cloud Cisco (à l'aide de la connexion CTR), pour diffuser des informations d'état de fonctionnalité. La transmission en continu des données CSN permet de sélectionner les données intéressantes dans l'ESA et de les transmettre sous un format structuré aux stations de gestion distantes.

Avantages

- Informer le client des fonctionnalités inutilisées disponibles qui peuvent améliorer l'efficacité du produit.
- Informer le client des services d'assistance technique et de surveillance supplémentaires qui pourraient être disponibles pour le produit.
- Pour aider Cisco à améliorer le produit.

Informations collectées

Voici la liste des informations de fonctionnalité collectées dans le cadre de cette fonctionnalité une fois configurée sur le périphérique ESA :

- Modèle de périphérique (x90, x95, 000v, 100v, 300v, 600v)

- Numéro de série du périphérique (UDI)
- UserAccountID (numéro d'ID VLAN ou SLPIID)
- Version du logiciel
- Date d'installation
- slVAN (Nom du compte virtuel dans les licences Smart)
- Mode de déploiement
- Antispam IronPort
- Désinscription sécurisée de Graymail
- Sophos
- McAfee
- Réputation des fichiers
- Analyse de fichiers
- Prévention des pertes de données
- Flux de menaces externes
- Analyse D'Images Ironport
- Filtres contre les attaques
- Paramètres de chiffrement du courrier électronique Cisco IronPort (chiffrement des enveloppes)
- Cryptage PXE
- Réputation de domaine
- Filtrage des URL
- Bloquer la personnalisation des pages
- Suivi des messages
- Quarantaines des stratégies, des virus et des attaques
- Quarantaine du spam

Conditions préalables

Exigences

Pour configurer cette fonctionnalité, voici quelques-unes des conditions requises qui doivent être remplies :

- Compte CTR (Cisco Threat Response)

Configuration liée au pare-feu

La configuration du pare-feu nécessaire pour que CSN fonctionne dépend actuellement de la communication CTR. Pour plus d'informations, reportez-vous à ce document : Intégration d'ESA avec CTR

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ESA (Email Security Appliance) AsyncOS version 13.5.1.x et ultérieure.

Configurer

Vous pouvez configurer cette fonctionnalité à l'aide de l'interface utilisateur ESA ou de l'interface de ligne de commande. Les détails de ces deux étapes sont présentés ci-dessous.

Dépendances CSN et CTR

La fonctionnalité CSN dépend de la connectivité de la fonctionnalité CTR pour son bon fonctionnement et ce tableau fournit plus d'informations sur la relation entre ces deux processus.

Réponse aux menaces	CSN	Connecteur SSE	Processus CSN
Désactivé	Désactivé	En Bas	Désactivé
Désactivé (désinscription)	Activée	En Bas	En Bas
Désactivé (enregistré)	Activée	Haut	Haut
Activée	Désactivé manuellement	Haut	En Bas
Activée	Activée	Haut	Haut

Configuration CSN à l'aide de l'interface utilisateur

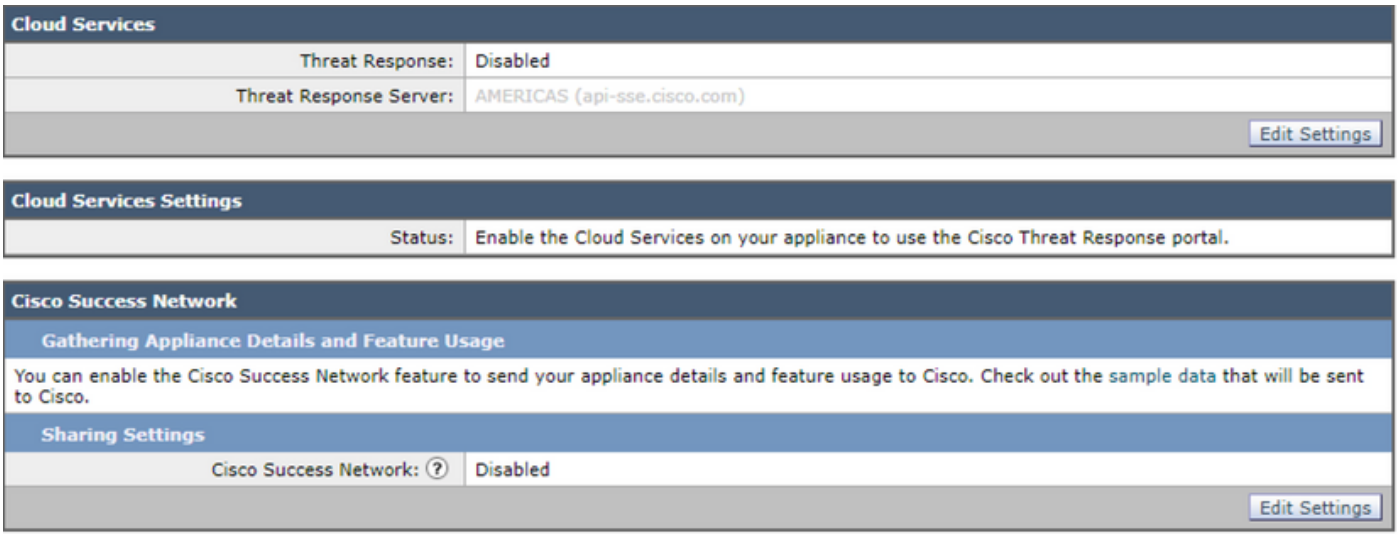
1) Connectez-vous à l'interface utilisateur ESA.

2) Accédez à Network **>>** Cloud Service Settings (je suppose que CTR a été désactivé avant de commencer la mise à niveau vers 13.5.1.x). Avant la mise à niveau, si CTR était activé, CSN sera également activé par défaut. Si CTR a été désactivé, CSN sera également désactivé.

 Remarque : nous supposerons que CTR a été désactivé avant la mise à niveau car CTR dans un déploiement centralisé est censé être désactivé car il est activé uniquement sur le SMA pour l'envoi des informations de rapport à CTR.

---

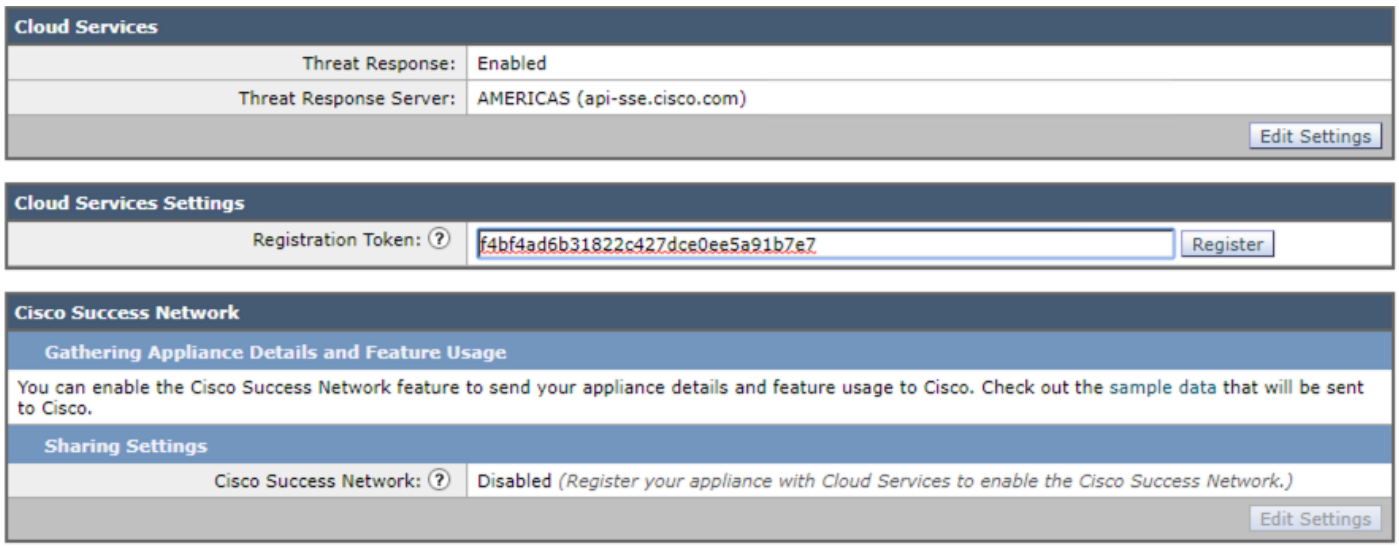
3) Voici ce que vous observeriez par défaut sur le périphérique ESA : -



4) Nous allons maintenant enregistrer cet ESA en activant d'abord les services CTR sur l'ESA et en « soumettant » les modifications.

5) Ce statut apparaît sur la page CTR « Le service cloud Cisco est occupé. Revenez à cette page après un certain temps pour vérifier l'état de l'appliance." Validez les modifications apportées au périphérique.

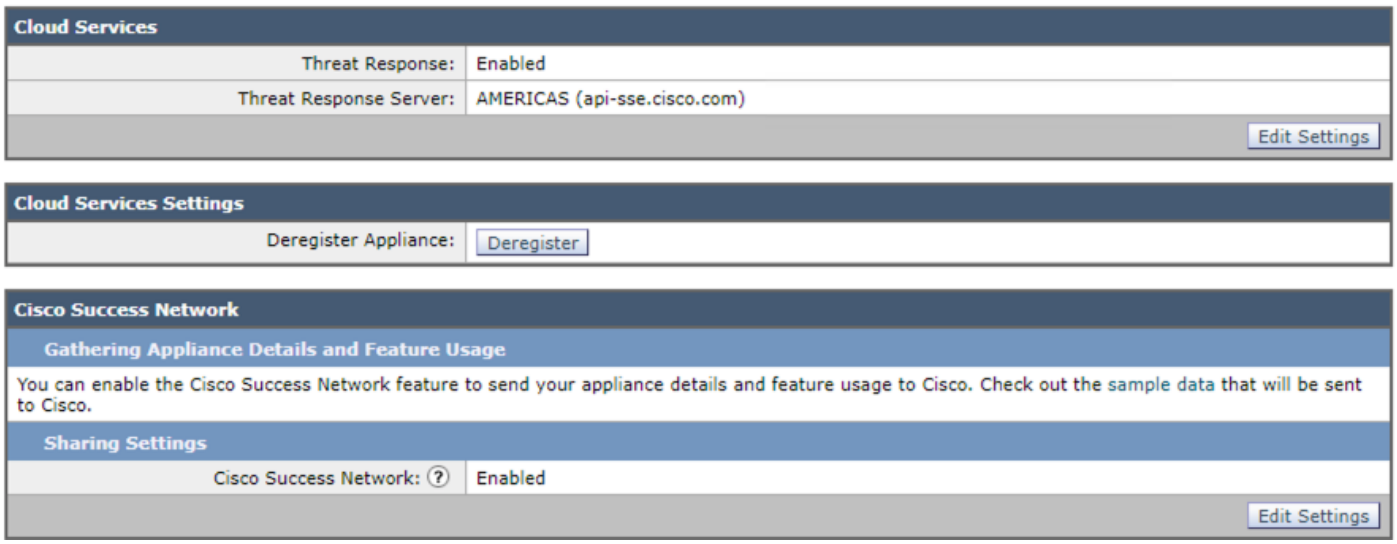
6) Ensuite, vous allez de l'avant et vous obtenez le jeton CTR et enregistrez le périphérique sur CTR :



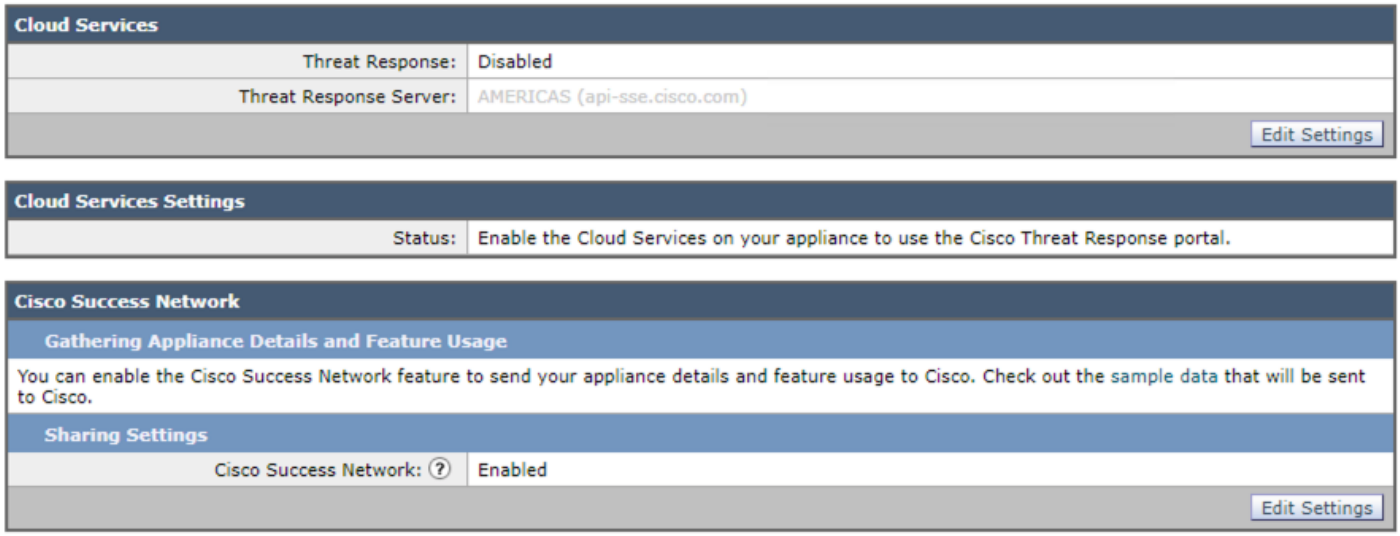
7) Vous devriez voir cet état une fois l'enregistrement réussi :

Réussite : une demande d'enregistrement de votre appliance auprès du portail Cisco Threat Response est lancée. Revenez à cette page après un certain temps pour vérifier l'état de l'appliance.

8) Une fois la page actualisée, les champs CTR Registered et CSN Enabled s'affichent :



9) Comme nous l'avons vu, CTR doit être désactivé dans ce scénario, car cet ESA est centralisé et vous verriez toujours CSN activé comme prévu. Dans le cas où cet ESA n'est pas géré par SMA (non centralisé), vous pouvez maintenir le CTR activé.



Il doit s'agir de l'état final de la configuration. Cette étape doit être suivie pour chaque ESA car ce paramètre est de niveau machine.

Configuration CSN à l'aide de la CLI

<#root>

```
(Machine esa )>
```

csnconfig

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

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.
```

Les modifications doivent être validées dans le cadre de cette activation à l'aide de l'interface de ligne de commande.

Dépannage

Pour dépanner cette fonctionnalité, un journal PUB (/data/pub/csn_logs) est disponible et contient les informations relatives à cette fonctionnalité. L'exemple ci-dessous est le journal au moment où l'enregistrement a été effectué sur le périphérique :

<#root>

(Machine ESA) (SERVICE)> tail

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

11. csn_logs

```
            CSN Logs                            Manual Download     None
12. ctr_logs            CTR Logs                            Manual Download     None
13. dlp                 DLP Logs                            Manual Download     None
14. eaas                Advanced Phishing Protection Logs   Manual Download     None
15. encryption          Encryption Logs                     Manual Download     None
16. error_logs          IronPort Text Mail Logs             Manual Download     None
17. euq_logs            Spam Quarantine Logs                Manual Download     None
18. euqgui_logs         Spam Quarantine GUI Logs            Manual Download     None
19. ftpd_logs           FTP Server Logs                     Manual Download     None
20. gmarchive           Graymail Archive                    Manual Download     None
21. graymail            Graymail Engine Logs                Manual Download     None
22. gui_logs            HTTP Logs                           Manual Download     None
23. ipr_client          IP Reputation Logs                  Manual Download     None
24. mail_logs           IronPort Text Mail Logs             Manual Download     None
25. remediation         Remediation Logs                    Manual Download     None
26. reportd_logs        Reporting Logs                      Manual Download     None
27. reportqueryd_logs   Reporting Query Logs                Manual Download     None
28. s3_client           S3 Client Logs                      Manual Download     None
29. scanning            Scanning Logs                       Manual Download     None
30. sdr_client          Sender Domain Reputation Logs       Manual Download     None
```

```
31. service_logs        Service Logs                    Manual Download     None
32. smartlicense        Smartlicense Logs               Manual Download     None
33. sntpd_logs          NTP logs                        Manual Download     None
34. status              Status Logs                     Manual Download     None
35. system_logs         System Logs                     Manual Download     None
36. threatfeeds         Threat Feeds Logs               Manual Download     None
37. trackerd_logs       Tracking Logs                   Manual Download     None
38. unified-2           Consolidated Event Logs         Manual Download     None
39. updater_logs        Updater Logs                    Manual Download     None
40. upgrade_logs        Upgrade Logs                    Manual Download     None
41. url_rep_client      URL Reputation Logs             Manual Download     None
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.