Cisco Success Network (CSN) op Cisco e-mail security

Inhoud

Inleiding

Dit document bevat de informatie over de optie Cisco Success Network die beschikbaar zou zijn als onderdeel van de release van AsyncOS 13.5.1 voor de Cisco e-mail security applicatie (ESA). Cisco Success Network (CSN) is een door de gebruiker ondersteunde cloudservice. Wanneer CSN is ingeschakeld, wordt een beveiligde verbinding tot stand gebracht tussen de ESA en de Cisco cloud (met behulp van de CTR-verbinding) om de statusinformatie van de functies te stroomen. Streamende CSN-gegevens bieden een mechanisme om de relevante gegevens van de ESA te selecteren en in een gestructureerd formaat naar de afstandsbeheerstations te verzenden.

Voordelen

- Informatie aan de klant over beschikbare ongebruikte functies die de werkzaamheid van het product kunnen verbeteren.
- De klant informeren over aanvullende technische ondersteuningsdiensten en controles die voor het product beschikbaar kunnen zijn.
- Om Cisco te helpen het product te verbeteren.

Verzamelde informatie

Dit is de lijst met functieinformatie die als deel van deze functie wordt verzameld zodra deze op het ESA-apparaat is geconfigureerd:

- Apparaatmodel (x90, x95, 000v, 100v, 300v, 600v)
- Apparaatserienummer (UDI)

- UserAccountID (VLN-id of SLPID)
- Softwareversie
- Datum installatie
- slVAN (Virtual Account Name in Smart Licensing)
- Invoermodus
- IJzeren poort tegen spam
- Graymail Safe-abonnement
- Sfos
- McAfee
- Bestandsreputatie
- Bestandsanalyse
- Gegevensverliespreventie
- Externe bedreigingen
- Afbeeldingsanalyse onjuist
- Uitbraakfilters
- Cisco IronPort-encryptie-instellingen (contentversleuteling)
- PXE-encryptie
- Domain Reputation
- URL-filtering
- Aanpassen van blokpagina
- Berichtentracering
- Quarantines voor beleid, virussen en uitbraken
- Spam Quarantine

Voorwaarden

Vereisten

Voor de configuratie van deze functie dient aan een aantal vereisten te worden voldaan:

- CTR-account (Cisco Threat Response)

Configuratie van firewalls

De firewallconfiguratie die nodig is om CSN functioneel te maken is momenteel afhankelijk van de CTR-communicatie en raadpleeg dit document voor meer informatie: Integratie van ESA met CTR

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- E-mail security applicatie (ESA) AsyncOS, versie 13.5.1.x en hoger.

Configureren

U kunt deze functie configureren met zowel de ESA UI als de CLI. Nadere details over beide stappen worden hieronder gegeven.

Vereisten CSN en CTR

De eigenschap CSN is afhankelijk van de connectiviteit van de eigenschap CTR voor zijn succesvolle werking en deze tabel biedt meer informatie over het verband tussen deze twee processen.

Threat Response	CSN	SSE-connector	CSN-proces
Uitgeschakeld	Uitgeschakeld	Omlaag	Uitgeschakeld
Uitgeschakeld (uit-register)	Ingeschakeld	Omlaag	Omlaag
Uitgeschakeld (geregistreerd)	Ingeschakeld	Omhoog	Omhoog
Ingeschakeld	Handmatig uitgeschakeld	Omhoog	Omlaag
Ingeschakeld	Ingeschakeld	Omhoog	Omhoog

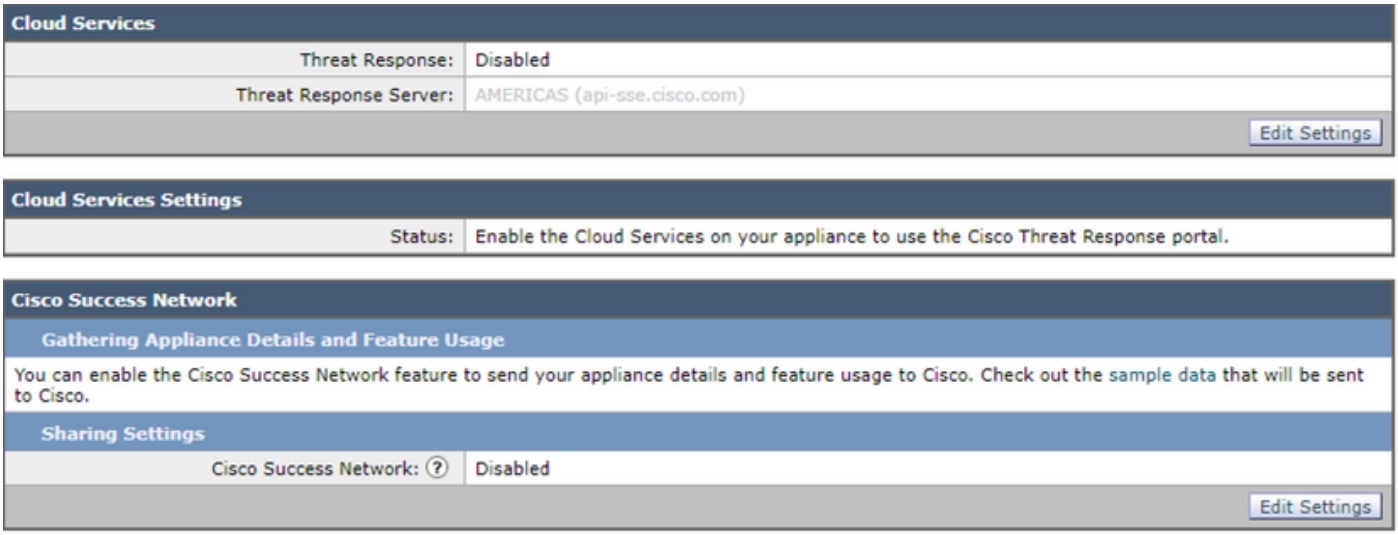
CSN-configuratie met behulp van UI

1) Meld u aan in het ESR UI.

2) Bladeren naar **netwerk >> Cloud Service-instellingen** (ik ga ervan uit dat CTR is uitgeschakeld voordat we zijn gestart met de upgrade naar 13.5.1.x). Voor de upgrade, als CTR was geactiveerd, zal CSN ook standaard ingeschakeld zijn. Als CTR werd uitgeschakeld, wordt CSN ook uitgeschakeld.

> Opmerking: We gaan ervan uit dat CTR voor de upgrade uitgeschakeld was, omdat CTR in een gecentraliseerde implementatie zou moeten worden uitgeschakeld, aangezien deze alleen op de SMA is ingeschakeld voor het doorgeven van de meldingsinformatie aan CTR.

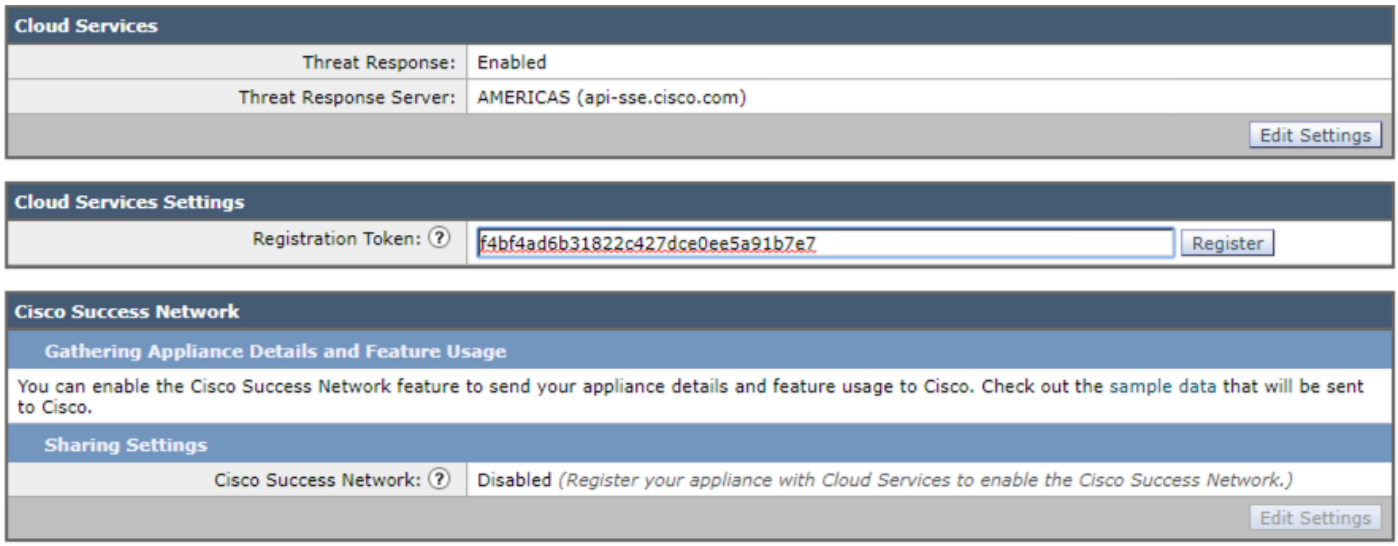
3) Dit ziet u als standaard op het ESR-apparaat: -



4) We zullen dit ESA nu registreren door eerst de CTR-diensten op het ESA in staat te stellen en de wijzigingen voor te leggen.

5) Deze status wordt op de CTR-pagina weergegeven "De Cisco Cloud Service is bezig. Navigeer na enige tijd naar deze pagina om de status van het apparaat te controleren." Voer de wijzigingen in het apparaat in.

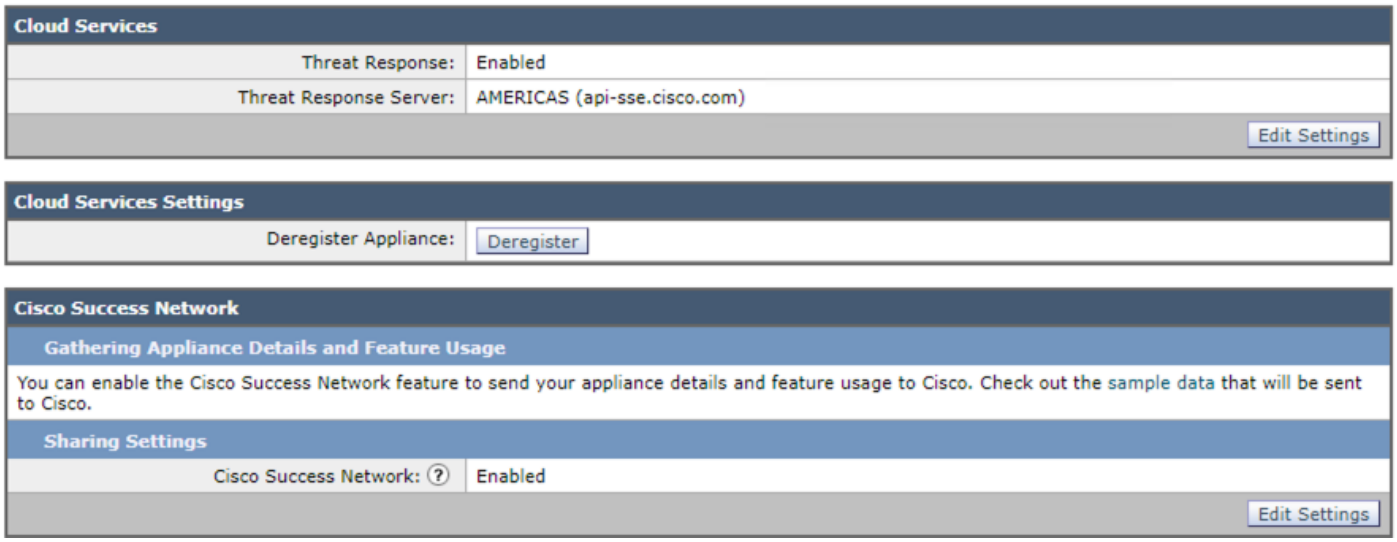
6) U gaat dan verder en krijgt de CTR Token en registreert het apparaat bij CTR:



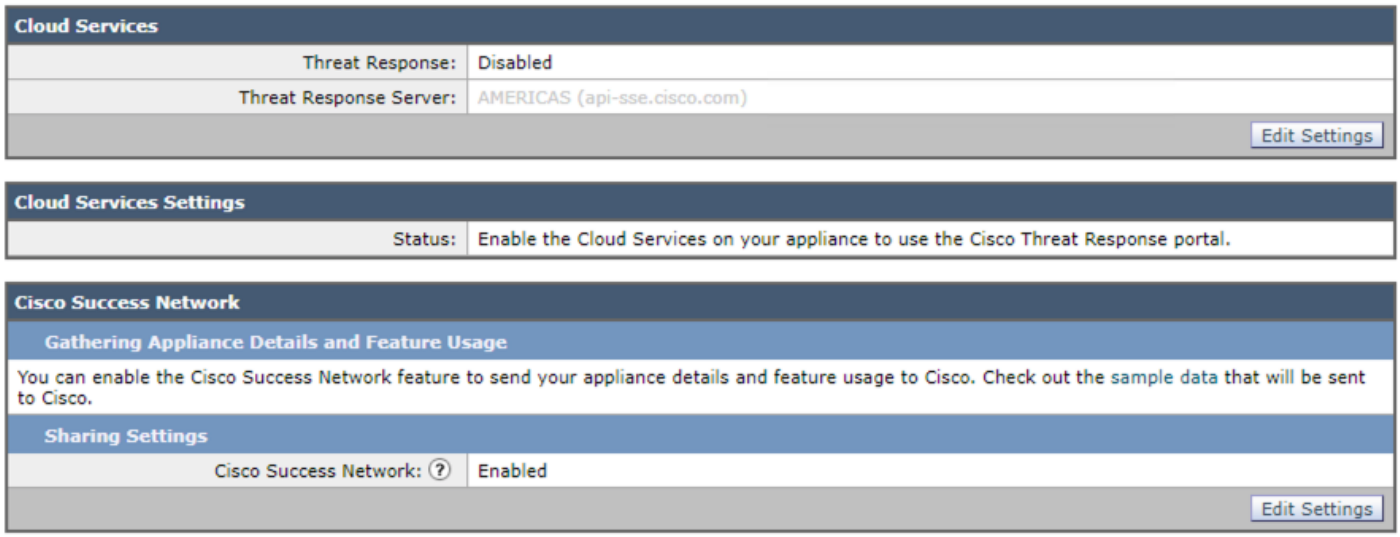
7) U dient deze status te zien zodra de registratie is voltooid:

Succesvol — Een verzoek om uw apparaat te registreren met het Cisco Threat Response-portaal wordt gestart. Navigeer na enige tijd naar deze pagina om de status van het apparaat te controleren.

8) Nadat u de pagina hebt opgefrist, ziet u de CTR geregistreerd en CSN ingeschakeld:



9) Zoals besproken moet CTR in dit scenario worden uitgeschakeld, aangezien deze ESA is gecentraliseerd en u nog steeds CSN zou zien ingeschakeld zoals verwacht. Indien dit ESA niet door SMA (Niet-Gecentraliseerd) wordt beheerd, kunt u de CTR ingeschakeld houden.



Dit moet de laatste configuratie zijn. **Deze stap moet voor elke ESA worden gevolgd aangezien deze instelling op niveau van de machine staat.**

CSN-configuratie met behulp van 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.
```

Wijzigingen zouden moeten worden doorgevoerd als onderdeel van het mogelijk maken van het gebruik van de CLI.

Problemen oplossen

Voor het oplossen van deze optie is er een PUB (**/data/pub/csn_logs**) Log beschikbaar dat de informatie op deze functie heeft. De onderstaande steekproef is het logboek op het tijdstip waarop de registratie op het hulpmiddel werd voltooid:

```
(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**