Cisco Success Network (CSN) su Cisco Email Security

Sommario

Introduzione

Questo documento contiene le informazioni sulla funzionalità Cisco Success Network che sarebbe stata disponibile con la versione AsyncOS 13.5.1 per Cisco Email Security Appliance (ESA). Cisco Success Network (CSN) è un servizio cloud abilitato per l'utente. Quando il CSN è abilitato, viene stabilita una connessione protetta tra l'ESA e il cloud Cisco (tramite la connessione CTR), per trasmettere le informazioni sullo stato delle funzionalità. I dati CSN di streaming forniscono un meccanismo per selezionare i dati di interesse dall'ESA e trasmetterli in formato strutturato alle stazioni di gestione remote.

Vantaggi

- Informare il cliente sulle caratteristiche inutilizzate disponibili che possono migliorare l'efficacia del prodotto.
- Per informare il cliente in merito ai servizi di supporto tecnico e di monitoraggio aggiuntivi disponibili per il prodotto.
- Per aiutare Cisco a migliorare il prodotto.

Informazioni raccolte

Di seguito è riportato l'elenco delle informazioni sulle funzionalità raccolte come parte di questa funzionalità una volta configurate sul dispositivo ESA:

- Modello dispositivo (x90, x95, 000v, 100v, 300v, 600v)
- UDI (Device Serial Number)
- UserAccountID (numero ID VLAN o SLPIID)

- Versione del software
- Data installazione
- slVLAN (Nome account virtuale in Smart Licensing)
- Modalità di distribuzione
- IronPort Anti-Spam
- Greymail Safe Annulla sottoscrizione
- Sophos
- McAfee
- Reputazione dei file
- Analisi file
- Prevenzione della perdita dei dati
- Feed minacce esterne
- Analisi immagini Ironport
- Filtri epidemie
- Impostazioni di Cisco IronPort Email Encryption (crittografia envelope)
- Crittografia PXE
- Reputazione del dominio
- Filtro URL
- Personalizzazione pagina blocco
- Verifica messaggi
- Quarantene per virus ed epidemie
- Quarantena posta indesiderata

Prerequisiti

Requisiti

Per configurare questa funzione, è necessario soddisfare alcuni dei seguenti requisiti:

- Account CTR (Cisco Threat Response)

Configurazione correlata al firewall

La configurazione del firewall necessaria per ottenere la funzionalità CSN dipende attualmente dalla comunicazione CTR. Per ulteriori informazioni, fare riferimento a questo documento: Integrating ESA with CTR

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Email Security Appliance (ESA) AsyncOS versione 13.5.1.x e successive.

Configurazione

Èpossibile configurare questa funzione utilizzando sia l'interfaccia utente ESA che la CLI. Di

seguito sono riportati i dettagli di entrambi i passaggi.

Dipendenze CSN e CTR

La funzionalità CSN dipende dalla connettività della funzionalità CTR per la riuscita dell'operazione e questa tabella fornisce ulteriori informazioni sulla relazione tra questi due processi.

Risposta alle minacce	CSN	Connettore SSE	Processo CSN
Disattivato	Disattivato	Giù	Disattivato
Disabilitato (annullamento registrazione)	Attivato	Giù	Giù
Disabilitato (registrato)	Attivato	Su	Su
Attivato	Disattivato manualmente	Su	Giù
Attivato	Attivato	Su	Su

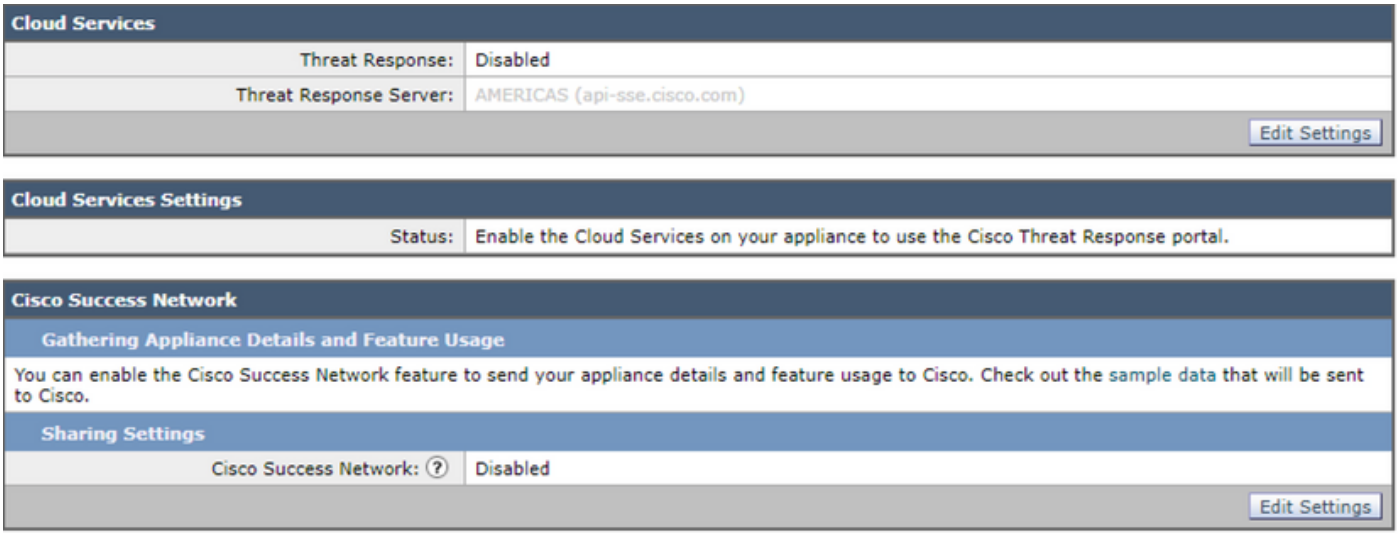
Configurazione CSN tramite interfaccia utente

1) Accedere all'interfaccia utente ESA.

2) Selezionare **Network >> Cloud Service Settings** (Presumo che CTR sia stato disabilitato prima di iniziare l'aggiornamento alla versione 13.5.1.x). Prima dell'aggiornamento, se CTR è stato abilitato, anche CSN verrà abilitato per impostazione predefinita. Se CTR è stato disabilitato, anche CSN verrà disabilitato.

> **Nota:** Si presume che il CTR sia stato disabilitato prima dell'aggiornamento, in quanto il CTR in una distribuzione centralizzata dovrebbe essere disabilitato poiché è abilitato solo sull'SMA per l'invio di informazioni di report al CTR.

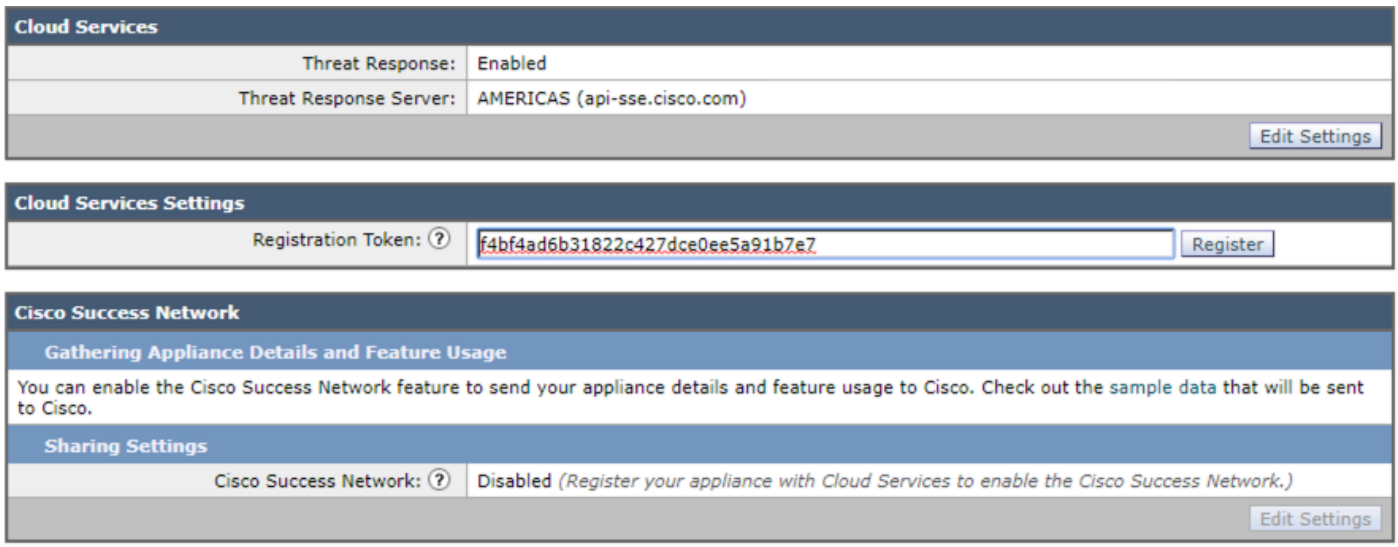
3) Questo è ciò che si osserverebbe come valore predefinito sul dispositivo ESA: -



4) Registreremo questa ESA abilitando prima i servizi CTR sull'ESA e "presentando" le modifiche.

5) Mostrerebbe questo stato sulla pagina CTR "The Cisco Cloud Service is occupato. In seguito, tornare a questa pagina per controllare lo stato dell'accessorio." Eseguire il commit delle modifiche nel dispositivo.

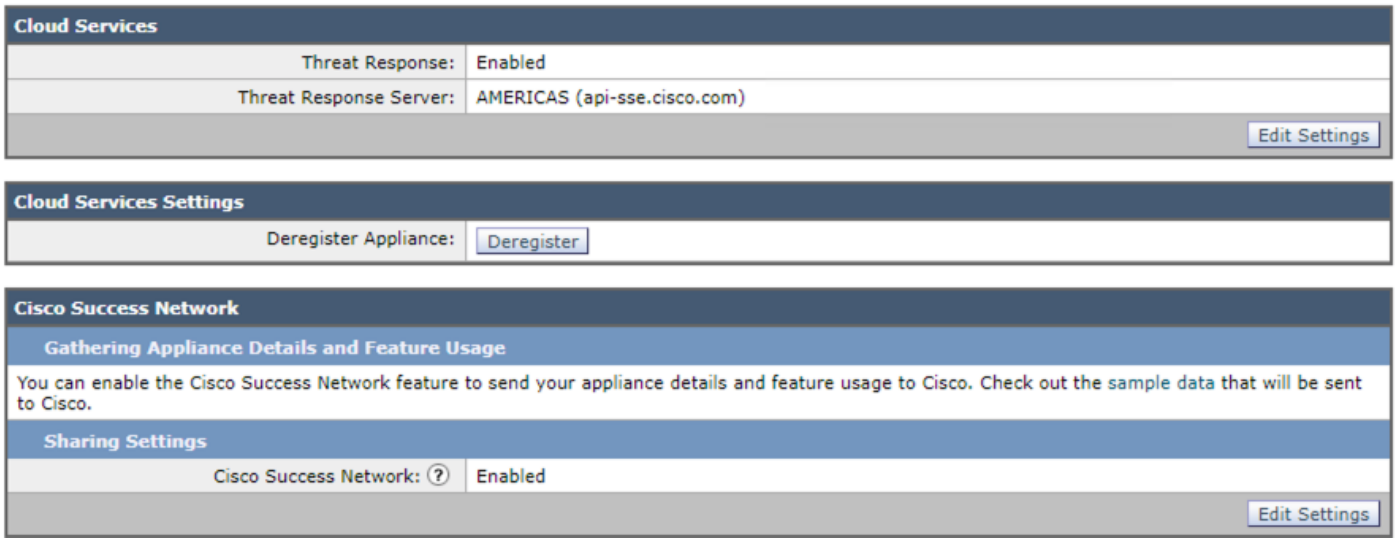
6) In questo modo è possibile ottenere il token CTR e registrare il dispositivo su CTR:



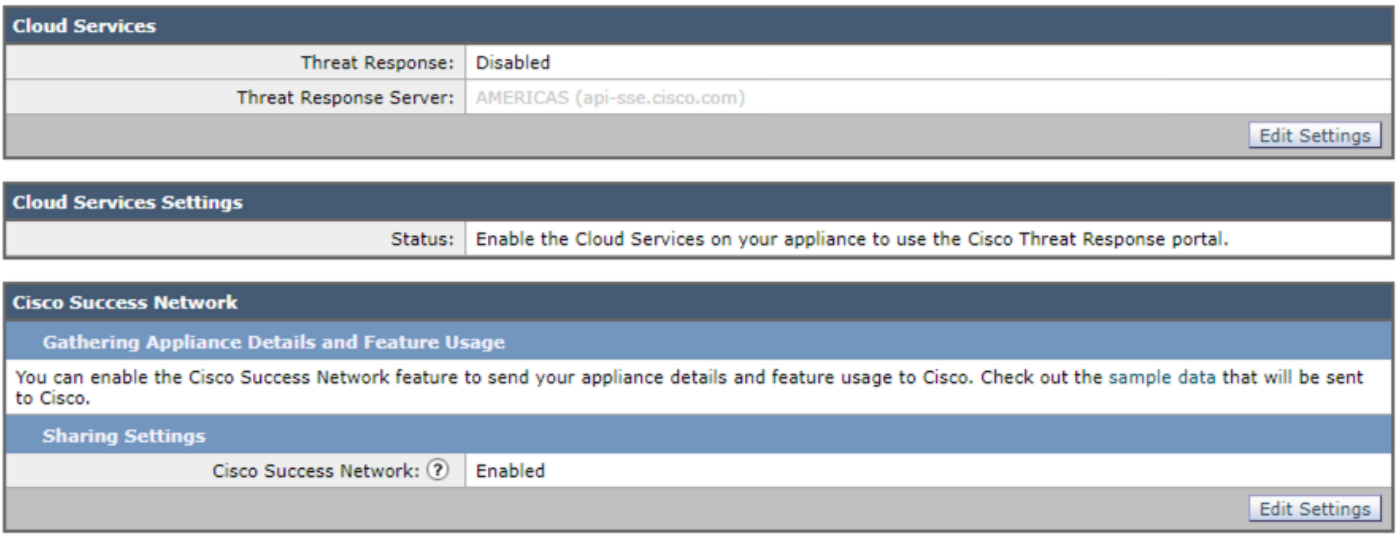
7) Questo stato dovrebbe essere visualizzato una volta completata la registrazione:

Riuscita: viene inviata una richiesta di registrazione dell'appliance sul portale Cisco Threat Response. Tornare a questa pagina in seguito per verificare lo stato dell'accessorio.

8) Una volta aggiornata la pagina, vedrai il CTR registrato e il CSN abilitato:



9) Come accennato, in questo scenario il CTR deve essere disabilitato poiché questa ESA è centralizzata e si vedrebbe ancora il CSN abilitato come previsto. Nel caso in cui l'ESA non sia gestita da SMA (non centralizzato), è possibile mantenere attivato il CTR.



Deve essere lo stato finale della configurazione. **Questo passaggio deve essere seguito per ciascuna UEE poiché questa impostazione è a livello di macchina.**

Configurazione CSN tramite 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.
```

Le modifiche devono essere eseguite come parte dell'abilitazione di questo uso della CLI.

Risoluzione dei problemi

Per risolvere il problema, è disponibile un registro PUB (**/data/pub/csn_logs**) contenente le informazioni su questa funzionalità. L'esempio seguente è il registro al momento in cui è stata completata la registrazione sul dispositivo:

```
(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
```